Linux Virtual Delivery Agent 2210

Contents

Linux Virtual Delivery Agent 2210

December 16, 2022

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

Le Linux VDA permet d'accéder à des applications et des bureaux Linux virtuels, en tout lieu et depuis n'importe quel appareil sur lequel l'application Citrix Workspace est installée.

Vous pouvez fournir des applications et des bureaux virtuels en fonction des distributions Linux prises en charge. Installez le logiciel VDA sur vos machines virtuelles Linux, configurez le Delivery Controller, puis utilisez Citrix Studio pour mettre les bureaux et applications à la disposition des utilisateurs.

Nouveautés

December 16, 2022

Nouveautés dans la version 2210

La version 2210 du Linux VDA comprend les nouvelles fonctionnalités et améliorations suivantes :

Accélération matérielle GPU améliorée pour HDX 3D Pro

Nous avons amélioré l'efficacité du transfert de données entre le GPU et la mémoire du système Linux. Nous avons également réduit la latence lors du rendu graphique 3D et de l'encodage matériel. Ces améliorations optimisent l'utilisation des ressources matérielles et améliorent considérablement les performances des images par seconde (FPS). Pour plus d'informations, consultez la section Encodage matériel H.264.

Limites de taille pour les transferts de données via le presse-papiers

Vous pouvez spécifier la taille maximale (en Ko) des données du presse-papiers que les utilisateurs peuvent transférer entre un client et une session virtuelle Linux au cours d'une seule opération de copier-coller. Pour ce faire, utilisez les paramètres de stratégie suivants :

- Limiter le client du Presse-papiers à la taille de transfert de la session
- Limiter la session du Presse-papiers à la taille de transfert du client

Pour plus d'informations sur les paramètres de stratégie, consultez la section Redirection du Presse-papiers client des paramètres de stratégie ICA.

Pour plus d'informations sur les paramètres de stratégie pris en charge par le Linux VDA, consultez la liste des stratégies prises en charge.

Prise en charge de nouveaux systèmes Linux pour le streaming de machines cibles

Nous avons étendu le streaming Linux aux distributions suivantes :

- RHEL 8.6
- Rocky Linux 8.6
- Ubuntu 22.04

Pour de plus amples informations, veuillez consulter Streaming de machines cibles Linux dans la documentation de Citrix Provisioning.

Amélioration des scripts Shell

Nous avons amélioré les scripts shell pour les rendre faciles à maintenir et avons déplacé les modèles de configuration suivants de `/etc/xdl/mcs/` vers `/etc/xdl/ad_join/` :

- winbind_krb5.conf.tmpl
- winbind_smb.conf.tmpl
- sssd.conf.tmpl
- sssd_krb5.conf.tmpl
- sssd_smb.conf.tmpl
- centrify_krb5.conf.tmpl
- centrify_smb.conf.tmpl

Easy Install utilise également les modèles de configuration correspondant aux méthodes spécifiques pour rejoindre des domaines.

Nouveautés dans les versions précédentes

Pour connaître les nouvelles fonctionnalités incluses dans les versions qui ont été mises à disposition après la version 1912 LTSR jusqu'à la version 2209 CR, consultez l'article Historique des nouveautés.

Problèmes résolus

December 16, 2022

Cette version résout plusieurs problèmes afin d'améliorer la stabilité et les performances générales.

Problèmes connus

July 13, 2023

Les problèmes suivants ont été identifiés dans cette version :

- Les VDA Linux peuvent se désinscrire lorsque vous redémarrez le Cloud Connector ou le Delivery Controller. [CVADHELP-21256]
- Le type de cryptage **RC4_HMAC_MD5** étant autorisé pour Kerberos, le Linux VDA peut ne pas s'enregistrer auprès du Controller et le message d'erreur suivant s'affiche :

  Error: Failure unspecified at GSS-API level (Mechanism level: Encryption type RC4 with HMAC is not supported/enabled)

  Pour contourner ce problème, désactivez **RC4_HMAC_MD5** de manière globale dans votre domaine Active Directory (*ou de façon plus spécifique sur une unité d'organisation*) ou autorisez les types de chiffrement faibles sur le Linux VDA. Ensuite, effacez les tickets Kerberos mis en cache sur le Controller et le Citrix Cloud Connector à l'aide de la commande **klist -li 0x3e4 purge** et redémarrez le Linux VDA.

  Pour désactiver **RC4_HMAC_MD5** de manière globale dans votre domaine Active Directory, procédez comme suit :

  1. Ouvrez la Console de gestion des stratégies de groupe.
  2. Localisez le domaine cible, puis sélectionnez la **stratégie de domaine par défaut**.
  3. Cliquez avec le bouton droit sur **Stratégie de domaine par défaut** et sélectionnez **Modifier**. L'éditeur de gestion des stratégies de groupe s'ouvre.
  4. Sélectionnez **Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité**.
  5. Double-cliquez sur **Sécurité réseau : Configurer les types de chiffrement autorisés pour Kerberos**.
  6. Décochez les cases **DES_CBC_CRC**, **DES_CBC_MD5** et **RC4_HMAC_MD5** et sélectionnez **AES128_HMAC_SHA1**, **AES256_HMAC_SHA1** et **Futurs types de chiffrement**.

  Pour autoriser les types de chiffrement faibles sur le Linux VDA, procédez comme suit :

> **Remarque**
>
> :
>
> Les types de chiffrement faibles rendent votre déploiement vulnérable aux attaques.

1. Ouvrez le fichier /etc/krb5.conf sur le Linux VDA.
2. Ajoutez le paramètre suivant dans la section **[libdefaults]** :

   ```
   allow_weak_crypto= TRUE
   ```

- Le Linux VDA ne prend pas en charge SecureICA pour le chiffrement. L'activation de SecureICA sur le Linux VDA provoque l'échec du lancement de la session.
- Dans une session de bureau GNOME, les tentatives de modification de la disposition du clavier peuvent échouer. [CVADHELP-15639]
- Les applications publiées non transparentes peuvent se fermer peu de temps après leur lancement. Le problème se produit après une mise à niveau de Mutter vers une version supérieure à mutter-3.28.3-4. Pour contourner le problème, utilisez mutter-3.28.3-4 ou une version antérieure. [LNXVDA-6967]
- Une fenêtre inattendue apparaît lors du téléchargement de fichier. La fenêtre n'affecte pas la fonctionnalité de téléchargement de fichier et disparaît automatiquement après un certain temps. [LNXVDA-5646]
- Les paramètres par défaut de PulseAudio provoquent la fermeture du programme du serveur audio après 20 secondes d'inactivité. Lorsque PulseAudio se termine, le son ne fonctionne pas. Pour contourner ce problème, définissez exit-idle-time=-1 dans le fichier /etc/pulse/daemon.conf. [LNXVDA-5464]
- Les sessions ne peuvent pas être lancées dans l'application Citrix Workspace pour Linux lorsque le chiffrement SSL est activé et que la fiabilité de session est désactivée. [RFLNX-1557]
- Graphiques Ubuntu : dans HDX 3D Pro, un cadre noir peut apparaître autour des applications après le redimensionnement de Desktop Viewer, ou dans certains cas, l'arrière-plan peut s'afficher en noir.
- Il est possible que les imprimantes créées par la redirection d'impression de Linux VDA ne puissent pas être supprimées après la fermeture d'une session.
- Les fichiers CDM sont absents lorsqu'un répertoire contient de nombreux fichiers et sous-répertoires. Ce problème peut se produire si le client a trop de fichiers ou de répertoires.
- Dans cette version, seul le codage UTF-8 est pris en charge pour les langues autres que l'anglais.
- L'état du verrouillage des majuscules de l'application Citrix Workspace pour Android peut être inversé lors de l'itinérance de session. L'état de CAPS VERR peut être perdu lors de l'itinérance

d'une connexion existante à l'application Citrix Workspace pour Android. Pour résoudre le problème, utilisez la touche MAJ sur le clavier étendu pour basculer entre les majuscules et les minuscules.

- Les raccourcis ALT ne fonctionnent pas toujours lors d'une connexion à un Linux VDA à l'aide de l'application Citrix Workspace pour Mac. L'application Citrix Workspace pour Mac envoie AltGr pour les touches Options/Alt droite et gauche par défaut. Vous pouvez modifier ce comportement dans les paramètres de l'application Citrix Workspace, mais les résultats varient selon les applications .
- L'enregistrement échoue lorsque le Linux VDA est à nouveau associé au domaine. Cette nouvelle association génère un nouvel ensemble de clés Kerberos. Le broker peut utiliser un ticket de service VDA mis en cache obsolète basé sur le jeu de clés Kerberos précédent. Lorsque le VDA tente de se connecter au broker, le broker peut ne pas être en mesure d'établir un contexte de sécurité pour le VDA. Le symptôme courant est l'échec de l'enregistrement du VDA.

  Ce problème se résout de lui-même lorsque le ticket de service VDA expire, puis est renouvelé. Cependant, les tickets de service ayant en général une durée de vie assez longue, ce processus peut prendre beaucoup de temps.

  Pour résoudre le problème, effacez le cache de ticket du Broker. Redémarrez le broker ou exécutez la commande suivante en tant qu'administrateur sur le broker à partir d'une invite de commande :

  ```
  klist -li 0x3e4 purge
  <!--NeedCopy-->
  ```

  Cette commande supprime tous les tickets de service du cache LSA détenu par le service réseau principal sous lequel le service de broker Citrix s'exécute. Elle supprime également les tickets de service pour d'autres VDA et, potentiellement, d'autres services. Cela ne pose pas de problème : ces tickets de service peuvent être de nouveau acquis depuis le serveur KDC le cas échéant.
- Audio Plug-n-Play n'est pas pris en charge. Vous pouvez connecter un périphérique de capture audio à la machine cliente avant de commencer à enregistrer l'audio dans la session ICA. Si un périphérique de capture est connecté après que l'application d'enregistrement audio a démarré, l'application peut cesser de répondre et vous devez la redémarrer. Un problème similaire peut se produire si un périphérique de capture est déconnecté pendant l'enregistrement.
- L'application Citrix Workspace pour Windows peut rencontrer une distorsion audio lors de l'enregistrement audio.

Avis de tiers

December 16, 2022

Linux Virtual Delivery Agent version 2210 (PDF)

Cette version de Linux VDA peut inclure des logiciels tiers distribués sous licence selon les conditions définies dans le document.

Fin de prise en charge

December 21, 2022

Les annonces de cet article visent à vous avertir à l'avance des plates-formes, des produits Citrix et des fonctionnalités qui vont disparaître pour que vous puissiez prendre les décisions appropriées. Citrix surveille l'utilisation des clients et leurs commentaires pour déterminer quand les retirer. Les annonces peuvent être modifiées dans les versions ultérieures et peuvent ne pas contenir chaque fonctionnalité amenée à disparaître.
Pour obtenir des informations sur la prise en charge du cycle de vie d'un produit, consultez l'article Politique de prise en charge du cycle de vie d'un produit.

Fins de prise en charge et retraits

Le tableau suivant indique les plates-formes, les produits Citrix et les fonctionnalités qui sont obsolètes ou ont été retirés.Les éléments **obsolètes** ne sont pas retirés immédiatement. Citrix continue de les prendre en charge dans cette version, mais ils seront retirés dans une future version.
Les éléments retirés sont retirés, ou ne sont plus pris en charge, dans VDA Linux.

Élément	Abandon annoncé dans	Supprimé dans
Prise en charge de SUSE 15.3	2210	2301
Prise en charge de Debian 10.9	2206	2210
Prise en charge de SUSE 15.2	2206	2209
Prise en charge de RHEL 8.2	2206	2209
Prise en charge de RHEL 8.1, RHEL 8.3	2203	2206

Élément	Abandon annoncé dans	Supprimé dans
Prise en charge de RHEL 7.8, CentOS 7.8	2203	2204
Prise en charge de CentOS 8.x	2110	2201
Prise en charge de SUSE 12.5	2109	2204
Prise en charge de Ubuntu 16.04	2109	2203
Prise en charge de RHEL 7.7, CentOS 7.7	2006	2009
Prise en charge de SUSE 12.3	2006	2006
Prise en charge de RHEL 6.10, CentOS 6.10	2003	2003
Prise en charge de RHEL 6.9, CentOS 6.9	1909	1909
Prise en charge de RHEL 7.5, CentOS 7.5	1903	1903
Prise en charge de RHEL 7.4, CentOS 7.4	1811	1811
Prise en charge de RHEL 6.8, CentOS 6.8	1811	1811
Prise en charge de RHEL 7.3, CentOS 7.3	7.18	7.18
Prise en charge de RHEL 6.6, CentOS 6.6	7.16	7.16
SUSE 11.4	7.16	7.16

Configuration système requise

December 16, 2022

La version actuelle du Linux VDA est alignée sur Citrix Virtual Apps and Desktops. Elle est également rétrocompatible avec les versions antérieures de Citrix Virtual Apps and Desktops qui n'ont pas encore atteint la fin de leur cycle de vie. Pour de plus amples informations sur le cycle de vie des produits Citrix et savoir quand Citrix arrête la prise en charge de versions spécifiques des produits, consultez le tableau du cycle de vie des produits Citrix.

Le processus de configuration des agents Linux VDA diffère légèrement de celui des VDA Windows. Toutefois, toute batterie de Delivery Controller est capable de négocier les connexions aux bureaux Windows et Linux.

La configuration système requise des composants non couverts dans ce document (telles que l'application Citrix Workspace) est décrite dans leur documentation respective.

Pour plus d'informations sur l'utilisation d'une version Current Release (CR) dans un environnement Long Term Service Release (LTSR) et d'autres questions fréquemment posées, consultez cet article du centre de connaissances.

Distributions Linux

Linux VDA prend en charge les distributions Linux suivantes :

> **Important :**
>
> Lorsque la prise en charge du fournisseur de votre système d'exploitation expire, la capacité de résolution des problèmes par Citrix peut être limitée.
> Pour les plates-formes obsolètes ou supprimées, consultez la section Fin de prise en charge.

- Amazon Linux
  - Amazon Linux 2
- CentOS Linux
  - CentOS 7.9
- Linux Debian
  - Debian 11.3
- Red Hat Enterprise Linux
  - Workstation 8.6
  - Workstation 8.4
  - Workstation 7.9
  - Server 8.6
  - Server 8.4
  - Server 7.9
- Rocky Linux 8.6
- SUSE Linux Enterprise :
  - Server 15 Service Pack 3
- Ubuntu Linux

- Ubuntu Desktop 22.04
- Serveur Ubuntu 22.04
- Ubuntu Desktop 20.04
- Ubuntu Server 20.04
- Ubuntu Desktop 18.04
- Ubuntu Server 18.04
- Ubuntu Live Server 18.04

> **Remarque :**
>
> Le projet CentOS va passer à CentOS Stream. CentOS Linux 8, en tant que reconstruction RHEL 8, se terminera à la fin de 2021. CentOS Stream continuera après cette date en tant que branche en amont (développement) de Red Hat Enterprise Linux. Pour de plus amples informations, consultez https://www.redhat.com/en/blog/centos-stream-building-innovative-future-enterprise-linux.

Pour une matrice des distributions Linux et des versions Xorg que cette version du Linux VDA prend en charge, consultez le tableau suivant. Pour plus d'informations, consultez la page XorgModuleABIVersions.

Distribution Linux	Version Xorg	Bureau pris en charge
Amazon Linux 2	1.20	MATE, GNOME, GNOME Classic
Debian 11.3	1.20	MATE, GNOME, GNOME Classic, KDE
RHEL 8.6, RHEL 8.4	1.20	MATE, GNOME, GNOME Classic
RHEL 7.9, CentOS 7.9	1.20	MATE, GNOME, GNOME Classic, KDE
Rocky Linux 8.6	1.20	MATE, GNOME, GNOME Classic, KDE
SUSE 15.3	1.20	MATE, GNOME, GNOME Classic
Ubuntu 22.04	1.21	MATE, GNOME, GNOME Classic, KDE
Ubuntu 20.04	1.20	MATE, GNOME, GNOME Classic, KDE
Ubuntu 18.04	1.19	MATE, GNOME, GNOME Classic, KDE

> **Conseil :**
>
> N'utilisez pas `HWE kernel` ou `HWE Xorg` sur Ubuntu.

> Au moins un bureau doit être installé. Vous pouvez spécifier via le script ctxinstall.sh ou ctxsetup.sh l'environnement de bureau GNOME ou MATE à utiliser dans les sessions.
> Le format de votre nom d'utilisateur doit être conforme aux règles de syntaxe de `systemd` de votre gestionnaire d'affichage actuel. Pour plus d'informations sur la syntaxe du nom d'utilisateur de `systemd`, consultez Syntaxe des noms d'utilisateur/de groupe.

Environnements de virtualisation et plates-formes hôte pris en charge

- Serveurs bare metal
- Amazon Web Services (AWS)
- Citrix Hypervisor
- Google Cloud Platform (GCP)
- KVM
- Microsoft Azure
- Microsoft Hyper-V
- VMware vSphere Hypervisor
- Nutanix AHV

> **Remarque :**
>
> Dans tous les cas, l'architecture de processeur prise en charge est x86-64.
>
> De Citrix Virtual Apps and Desktops 7 2003 à 2112, l'hébergement de Linux VDA sur Microsoft Azure, AWS et GCP était pris en charge uniquement pour Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). À compter de la version 2203, vous pouvez héberger le Linux VDA sur ces clouds publics pour Citrix DaaS et Citrix Virtual Apps and Desktops. Pour ajouter ces connexions hôtes de cloud public à votre déploiement Citrix Virtual Apps and Desktops, vous avez besoin d'une **licence de droits hybrides**. Pour plus d'informations sur la **licence de droits hybrides**, consultez Transition et échange (TTU) avec droits hybrides.

Packages d'intégration d'Active Directory

Linux VDA prend en charge les produits et packages d'intégration d'Active Directory suivants :

	Winbind	SSSD	Centrify	PBIS	Quest
Amazon Linux 2	Oui	Oui	Oui	Oui	Non
Debian 11.3	Oui	Oui	Oui	Oui	Non
RHEL 8.6, RHEL 8.4	Oui	Oui	Oui	Oui	Non

	Winbind	SSSD	Centrify	PBIS	Quest
RHEL 7.9, CentOS 7.9	Oui	Oui	Oui	Oui	Oui (Quest v4.1 et versions ultérieures)
Rocky Linux 8.6	Oui	Oui	Non	Non	Non
SUSE 15.3	Oui	Oui	Oui	Oui	Non
Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04	Oui	Oui	Oui	Oui	Oui (Quest v4.1 et versions ultérieures)

HDX 3D Pro

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.

Hyperviseurs

Pour le Linux VDA, HDX 3D Pro est compatible avec les hyperviseurs suivants :

- Citrix Hypervisor
- VMware vSphere Hypervisor
- Nutanix AHV
- Microsoft Azure
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

> **Remarque :**
>
> Les hyperviseurs sont compatibles avec certaines distributions Linux.
> Pour utiliser HDX 3D Pro pour Amazon Linux 2, nous vous recommandons d'installer le pilote NVIDIA 470.

Processeurs graphiques

Pour savoir quelles cartes GPU NVIDIA sont prises en charge par votre distribution Linux, consultez la matrice NVIDIA product support matrix et consultez les colonnes **Hypervisor or Bare-Metal OS**, **Software Product Deployment**, **Hardware Supported** et **Guest OS Support**.

Assurez-vous d'installer le dernier pilote vGPU pour votre carte GPU. Actuellement, Linux VDA prend en charge jusqu'à vGPU 13. Pour plus d'informations, accédez à la page NVIDIA Virtual GPU Software Supported GPUs.

Présentation de l'installation

December 16, 2022

Cette section vous guide tout au long des procédures suivantes :

- Installation rapide à l'aide d'Easy Install (recommandé pour les nouvelles installations)
- Installation manuelle basée sur différentes distributions Linux
- Utiliser MCS pour créer des machines virtuelles Linux
- Créer des Linux VDA joints et non joints à un domaine dans Citrix DaaS Standard pour Azure (anciennement Citrix Virtual Apps and Desktops Standard pour Azure)
- Utiliser Citrix Provisioning pour créer des machines virtuelles Linux
- Configurer des Delivery Controller pour XenDesktop 7.6 et versions antérieures

Installation rapide à l'aide d'Easy Install (Recommandé)

December 16, 2022

> **Important :**
>
> - Pour les nouvelles installations, nous vous recommandons de consulter cet article pour effectuer une installation rapide. Cet article explique comment installer et configurer Linux VDA à l'aide d'Easy Install. Easy Install permet de gagner du temps et économiser de la main d'œuvre. et il est plus fiable que l'installation manuelle. Elle vous permet de configurer un environnement d'exécution Linux VDA en installant les packages nécessaires et en personnalisant automatiquement les fichiers de configuration.
> - Pour créer des VDA n'appartenant pas à un domaine, vous devez utiliser Machine Creation Services (MCS). Pour plus d'informations, consultez la section Utiliser Machine Creation

> Services (MCS) pour créer des machines virtuelles Linux.
>
> - Pour en savoir plus sur les fonctionnalités disponibles pour les VDA n'appartenant pas à un domaine, consultez la section VDA n'appartenant pas à un domaine.

Étape 1 : préparer les informations de configuration et la machine Linux

Collectez les informations de configuration suivantes qui sont requises pour une installation simple :

- Nom d'hôte : nom d'hôte de la machine sur laquelle le Linux VDA doit être installé
- Adresse IP du serveur de nom de domaine
- Adresse IP ou nom de chaîne du serveur NTP
- Nom de domaine : nom NetBIOS du domaine
- Nom de zone : nom de la zone Kerberos
- Nom de domaine complet (FQDN) du domaine

> **Important :**
>
> - Pour installer le Linux VDA, vérifiez que les référentiels sont ajoutés correctement sur la machine Linux.
> - Pour lancer une session, vérifiez que les environnements de bureau et du système X Windows sont installés.

Considérations

- Le nom du groupe de travail est le nom de domaine par défaut. Pour personnaliser le groupe de travail dans votre environnement, procédez comme suit :

  a. Créez le fichier /tmp/ctxinstall.conf sur la machine Linux VDA.
  b. Ajoutez la ligne « workgroup=\<votre groupe de travail\> » au fichier et enregistrez vos modifications.

- Centrify ne prend pas en charge la configuration DNS IPv6 pures. Au moins un serveur DNS utilisant IPv4 est requis dans /etc/resolv.conf pour que `adclient` puisse trouver les services AD correctement.

  Journal :

```
ADSITE    : Check that this machine's subnet is in a site known by
    AD    : Failed
          : This machine's subnet is not known by AD.
          : We guess you should be in the site Site1.
<!--NeedCopy-->
```

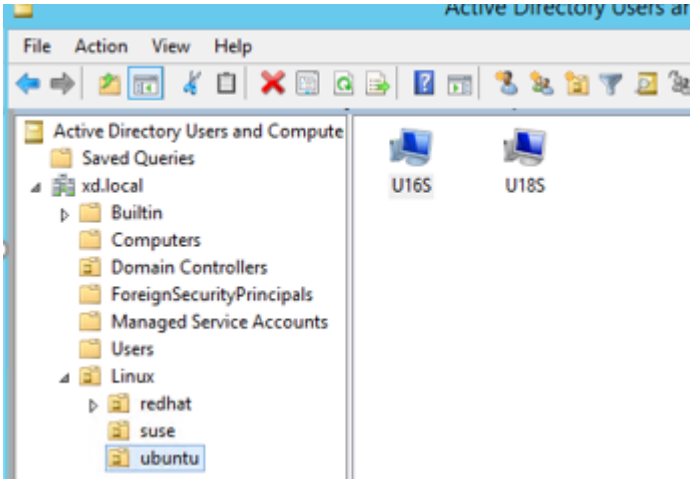

Ce problème est unique à Centrify et à sa configuration. Pour résoudre ce problème, procédez comme suit :

a. Ouvrez **Outils d'administration** sur le contrôleur de domaine.
b. Sélectionnez **Sites et services Active Directory**.
c. Ajoutez une adresse de sous-réseau appropriée pour **Sous-réseaux**.

- Pour joindre votre VDA à une unité d'organisation spécifique, procédez comme suit :

  1. Assurez-vous que l'unité d'organisation spécifique existe sur le contrôleur de domaine.

     Pour obtenir un exemple d'unité d'organisation, consultez la capture d'écran suivante.

  2. Créez le fichier /tmp/ctxinstall.conf sur le VDA.
  3. Ajoutez la ligne ou=<your ou> au fichier /tmp/ctxinstall.conf.

     Les valeurs de l'unité d'organisation varient en fonction des différentes méthodes AD. Voir le tableau suivant.

OS	Winbind	SSSD	Centrify	PBIS
Amazon Linux 2	`ou="Linux/amazon"`	`ou="Linux/amazon"`	`ou="XD.LOCAL/Linux/amazon"`	`ou="Linux/amazon"`
Debian	`ou="Linux/debian"`	`ou="Linux/debian"`	`ou="XD.LOCAL/Linux/debian"`	`ou="Linux/debian"`
RHEL 8, Rocky Linux 8	`ou="OU=redhat,OU=Linux"`	`ou="OU=redhat,OU=Linux"`	`ou="XD.LOCAL/Linux/redhat"`	`ou="Linux/redhat"`

OS	Winbind	SSSD	Centrify	PBIS
RHEL 7	`ou="Linux/redhat"`	`ou="Linux/redhat"`	`ou="XD.LOCAL/Linux/redhat"`	`ou="Linux/redhat"`
SUSE	`ou="Linux/suse"`	`ou="Linux/suse"`	`ou="XD.LOCAL/Linux/suse"`	`ou="Linux/suse"`
Ubuntu	`ou="Linux/ubuntu"`	`ou="Linux/ubuntu"`	`ou="XD.LOCAL/Linux/ubuntu"`	`ou="Linux/ubuntu"`

- Easy Install prend en charge IPv6 pur à partir de la version 7.16 de Linux VDA. Les conditions préalables et limitations suivantes s'appliquent :
  - Vous devez configurer votre référentiel Linux pour vous assurer que votre machine peut télécharger les packages requis dans des environnements IPv6 purs.
  - Centrify n'est pas pris en charge dans les réseaux IPv6 purs.

  > **Remarque :**
  >
  > Si votre réseau est un réseau IPv6 pur et que toutes vos entrées sont au format IPv6 correct, le VDA s'enregistre auprès du Delivery Controller via IPv6. Si votre réseau dispose d'une configuration hybride IPv4 et IPv6, le type de la première adresse IP du DNS détermine si IPv4 ou IPv6 est utilisé pour l'enregistrement.

- Si vous choisissez Centrify comme méthode pour rejoindre un domaine, le script ctxinstall.sh exige le package Centrify. Il existe deux façons pour ctxinstall.sh d'obtenir le package Centrify :
  - Easy Install permet de télécharger le package Centrify depuis Internet automatiquement. Les adresses URL pour chaque distribution sont les suivantes :

    RHEL : wget http://edge.centrify.com/products/centrify-suite/2016-update-1/installers/centrify-suite-2016.1-rhel4-x86_64.tgz?_ga=1.178323680.558673738.1478847956

    CentOS : wget http://edge.centrify.com/products/centrify-suite/2016-update-1/installers/centrify-suite-2016.1-rhel4-x86_64.tgz?_ga=1.186648044.558673738.1478847956

    SUSE : wget http://edge.centrify.com/products/centrify-suite/2016-update-1/installers/centrify-suite-2016.1-suse10-x86_64.tgz?_ga=1.10831088.558673738.1478847956

    Ubuntu/Debian : wget https://downloads.centrify.com/products/infrastructure-services/19.9/centrify-infrastructure-services-19.9-deb8-x86_64.tgz?_ga=2.151462329.1042350071.1592881996-604509155.1572850145

- Récupérez le package Centrify à partir d'un répertoire local. Procédez comme suit pour spécifier le répertoire du package Centrify :

  a. Créez le fichier /tmp/ctxinstall.conf sur le serveur Linux VDA, s'il n'existe pas.
  b. Ajoutez la ligne « centrifypkgpath=\<nom du chemin d'accès\> » au fichier.

  Par exemple :

```
cat /tmp/ctxinstall.conf
set "centrifypkgpath=/home/mydir"
ls  -ls  /home/mydir
    9548 -r-xr-xr-x. 1 root root  9776688 May 13  2016
       adcheck-rhel4-x86_64
    4140 -r--r--r--. 1 root root  4236714 Apr 21  2016
   centrifyda-3.3.1-rhel4-x86_64.rpm
    33492 -r--r--r--. 1 root root 34292673 May 13  2016
   centrifydc-5.3.1-rhel4-x86_64.rpm
    4 -rw-rw-r--. 1 root root     1168 Dec  1  2015
   centrifydc-install.cfg
    756 -r--r--r--. 1 root root   770991 May 13  2016
   centrifydc-ldapproxy-5.3.1-rhel4-x86_64.rpm
    268 -r--r--r--. 1 root root   271296 May 13  2016
   centrifydc-nis-5.3.1-rhel4-x86_64.rpm
    1888 -r--r--r--. 1 root root  1930084 Apr 12  2016
   centrifydc-openssh-7.2p2-5.3.1-rhel4-x86_64.rpm
    124 -rw-rw-r--. 1 root root   124543 Apr 19  2016
   centrify-suite.cfg
    0 lrwxrwxrwx. 1 root root       10 Jul  9  2012 install-
   express.sh -> install.sh
    332 -r-xr-xr--. 1 root root   338292 Apr 10  2016 install
   .sh
    12 -r--r--r--. 1 root root    11166 Apr  9  2015 release-
   notes-agent-rhel4-x86_64.txt
    4 -r--r--r--. 1 root root     3732 Aug 24  2015 release-
   notes-da-rhel4-x86_64.txt
    4 -r--r--r--. 1 root root     2749 Apr  7  2015 release-
   notes-nis-rhel4-x86_64.txt
    12 -r--r--r--. 1 root root     9133 Mar 21  2016 release-
   notes-openssh-rhel4-x86_64.txt
<!--NeedCopy-->
```

- Si vous choisissez PBIS comme méthode pour rejoindre un domaine, le script ctxinstall.sh exige le package PBIS. Le script ctxinstall.sh peut obtenir le package PBIS de deux façons :

  - Easy Install permet de télécharger le package PBIS depuis Internet automatiquement. Par exemple, les adresses URL pour chaque distribution sont les suivantes :

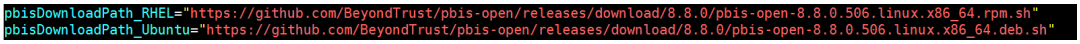
    Amazon Linux 2, CentOS 7, RHEL 8, RHEL 7, SUSE 15.3 : `wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh`

    Debian, Ubuntu : `wget https://github.com/BeyondTrust/pbis-open/`


```
releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.
sh
```

- Le script peut également récupérer une version spécifique du package PBIS à partir d'Internet. Pour ce faire, modifiez les lignes « pbisDownloadRelease » et « pbisDownloadExpectedSHA256 » dans le fichier /opt/Citrix/VDA/sbin/ctxinstall.sh.

  Pour obtenir un exemple, consultez la capture d'écran suivante :



Étape 2 : préparer l'hyperviseur

Certaines modifications sont requises pour l'exécution du Linux VDA en tant que machine virtuelle sur un hyperviseur pris en charge. Apportez les modifications suivantes en fonction de la plateforme d'hyperviseur utilisée. Aucune modification n'est requise si vous utilisez la machine Linux sur un matériel bare metal.

Corriger la synchronisation de l'heure sur Citrix Hypervisor

Si la fonctionnalité de synchronisation de l'heure de Citrix Hypervisor est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée avec NTP et Citrix Hypervisor. En effet, les deux systèmes essaient de gérer l'horloge système. Pour éviter que l'horloge ne soit plus synchronisée avec d'autres serveurs, assurez-vous l'horloge du système de chaque invité Linux est synchronisée avec NTP. Cela nécessite la désactivation de la synchronisation de l'heure de l'hôte. Aucune modification n'est requise en mode HVM.

Si vous utilisez un noyau Linux paravirtualisé avec le composant Citrix VM Tools installé, vous pouvez vérifier si la fonctionnalité de synchronisation de l'heure de Citrix Hypervisor est présente et activée à partir de la VM Linux :

```
su -

cat /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Cette commande renvoie 0 ou 1 :

- 0 - La fonctionnalité de synchronisation de l'heure est activée, et doit être désactivée.
- 1 - La fonctionnalité de synchronisation de l'heure est désactivée, et aucune action n'est requise.

Si le fichier /proc/sys/xen/independent_wallclock n'existe pas, les étapes suivantes ne sont pas nécessaires.

Si la fonctionnalité de synchronisation est activée, désactivez-la en entrant 1 dans le fichier :

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Pour rendre cette modification permanente et persistante après le redémarrage, modifiez le fichier **/etc/sysctl.conf** et ajoutez la ligne :

```
xen.independent_wallclock = 1
```

Pour vérifier ces modifications, redémarrez le système :

```
su -

cat /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Cette commande renvoie la valeur 1.

Corriger la synchronisation de l'heure sur Microsoft Hyper-V

Les VM Linux sur lesquelles Hyper-V Integration Services est installé peuvent tirer parti de la fonctionnalité de synchronisation de l'heure Hyper-V pour utiliser l'heure du système d'exploitation hôte. Pour vous assurer que l'horloge du système est toujours précise, cette fonctionnalité doit être activée avec les services NTP.

Depuis le système d'exploitation de gestion :

1. Ouvrez la console du gestionnaire Hyper-V.
2. Pour les paramètres d'une machine virtuelle Linux, sélectionnez **Integration Services**.
3. Assurez-vous que **Time synchronization** est sélectionné.

> **Remarque :**
>
> Cette approche diffère de VMware et Citrix Hypervisor, pour lesquels la synchronisation de l'heure est désactivée pour éviter tout conflit avec NTP. La synchronisation de l'heure Hyper-V peut co-exister avec la synchronisation de l'heure NTP.

Corriger la synchronisation de l'heure sur ESX et ESXi

Si la fonctionnalité de synchronisation de l'heure de VMware est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée avec l'hyperviseur et NTP. En effet, les deux systèmes essaient de synchroniser l'horloge système. Pour éviter que l'horloge ne soit plus synchronisée avec d'autres serveurs, assurez-vous l'horloge du système de chaque invité Linux est synchronisée avec NTP. Cela nécessite la désactivation de la synchronisation de l'heure de l'hôte.

Si vous exécutez un noyau Linux paravirtualisé sur lequel VMware Tools est installé :

1. Ouvrez vSphere Client.
2. Modifiez les paramètres pour la VM Linux.
3. Dans la boîte de dialogue **Virtual Machine Properties** (Propriétés de la machine virtuelle), ouvrez l'onglet **Options**.
4. Sélectionnez **VMware Tools**.
5. Dans la zone **Advanced** (Avancé), désélectionnez **Synchronize guest time with host** (Synchroniser l'heure de l'invité avec l'hôte).

Étape 3 : installer .NET Runtime 6.0 en tant que condition préalable

Avant d'installer Linux VDA, installez .NET Runtime 6.0 conformément aux instructions de l'article https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

Après avoir installé .NET Runtime 6.0, exécutez la commande **which dotnet** pour trouver votre chemin d'exécution.

En fonction de la sortie de la commande, définissez le chemin binaire de .NET Runtime. Par exemple, si la sortie de la commande est /aa/bb/dotnet, utilisez /aa/bb comme chemin binaire .NET.

Étape 4 : télécharger le package Linux VDA

1. Accédez à la page de téléchargement de Citrix Virtual Apps and Desktops.
2. Développez la version appropriée de Citrix Virtual Apps and Desktops.
3. Cliquez sur **Composants** pour télécharger le package Linux VDA qui correspond à votre distribution Linux et la clé publique GPG que vous pouvez utiliser pour vérifier l'intégrité du package Linux VDA.

   Pour vérifier l'intégrité du package Linux VDA à l'aide de la clé publique :

   - Pour un package RPM, importez la clé publique dans la base de données RPM et exécutez les commandes suivantes :

     ```
     rpmkeys --import <path to the public key>
     rpm --checksig --verbose <path to the Linux VDA package>
     <!--NeedCopy-->
     ```

   - Pour un package DEB, importez la clé publique dans la base de données DEB et exécutez les commandes suivantes :

     ```
     sudo apt-get install dpkg-sig
     gpg --import <path to the public key>
     dpkg-sig --verify <path to the Linux VDA package>
     <!--NeedCopy-->
     ```


Étape 5 : installer le package VDA Linux

Exécutez les commandes suivantes pour configurer l'environnement du Linux VDA.

Pour les distributions RHEL, CentOS et Rocky Linux :

```
sudo yum  -y localinstall   <PATH>/<Linux VDA RPM>
<!--NeedCopy-->
```

> **Remarque :**
>
> Pour RHEL et CentOS, vous devez installer le référentiel EPEL avant de pouvoir installer le Linux VDA. Pour plus d'informations sur l'installation d'EPEL, consultez les instructions sur https://docs.fedoraproject.org/en-US/epel/.

Pour les distributions Ubuntu/Debian :

```
sudo dpkg -i <PATH>/<Linux VDA deb>
sudo apt-get install -f
<!--NeedCopy-->
```

> **Remarque :**
>
> Pour installer les dépendances nécessaires pour une distribution Debian 11.3, ajoutez la ligne `deb http://deb.debian.org/debian/ bullseye main` au fichier /etc/apt/sources.list.

Pour les distributions SUSE :

```
zypper -i install <PATH>/<Linux VDA RPM>
<!--NeedCopy-->
```

Étape 6 : installer les pilotes NVIDIA GRID

Pour activer HDX 3D Pro, vous devez installer les pilotes NVIDIA GRID sur votre hyperviseur et sur les machines VDA.

Pour installer et configurer le gestionnaire de GPU virtuel NVIDIA GRID (pilote hôte) sur les hyperviseurs spécifiques, consultez les guides suivants :

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

Pour installer et configurer les pilotes de VM invitée NVIDIA GRID, effectuez les opérations générales suivantes :

1. Assurez-vous que la VM invitée est arrêtée.
2. Dans le panneau de configuration de l'hyperviseur, attribuez un GPU à la VM.
3. Démarrez la VM.
4. Installez le pilote de VM invitée sur la VM.

Étape 7 : définir l'environnement d'exécution afin de terminer l'installation

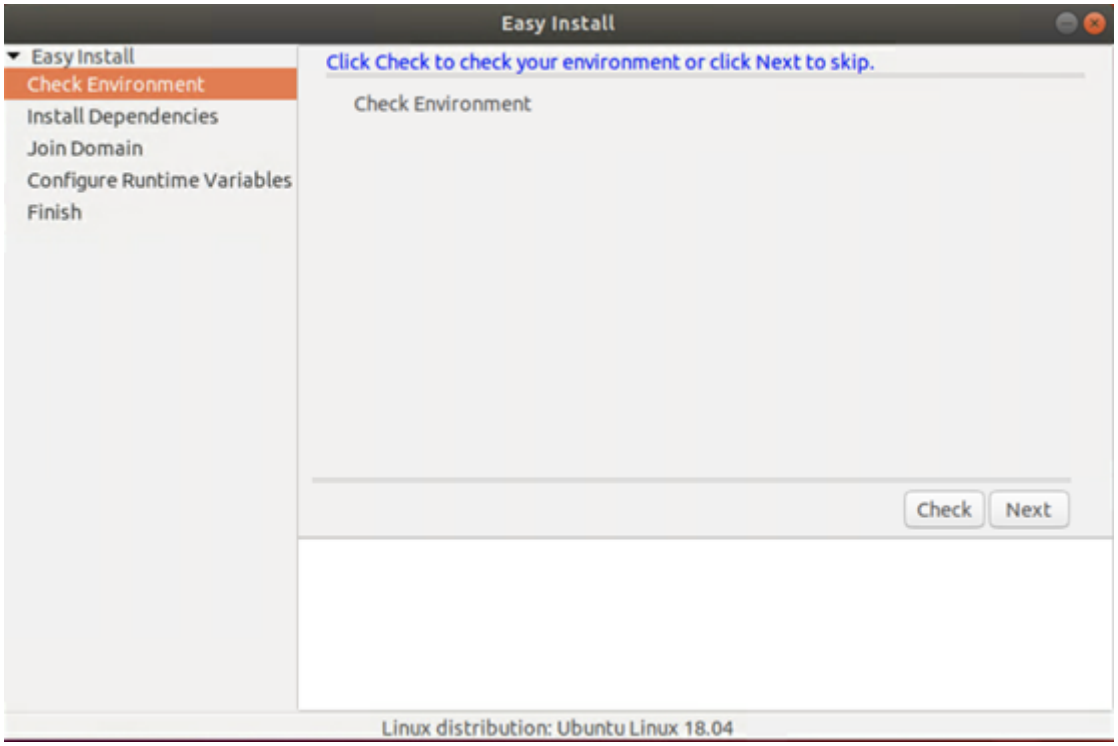
Après l'installation du package Linux VDA, configurez l'environnement d'exécution à l'aide du script ctxinstall.sh. Vous pouvez exécuter le script en mode interactif ou silencieux.

> **Remarque :**
>
> Avant de configurer l'environnement d'exécution, assurez-vous que les paramètres régionaux `en_US.UTF-8` sont installés dans votre système d'exploitation. Si les paramètres régionaux ne sont pas disponibles dans votre système d'exploitation, exécutez la commande `sudo locale-gen en_US.UTF-8`. Pour Debian, modifiez le fichier `/etc/locale.gen` en supprimant les marques de commentaire de la ligne `# en_US.UTF-8 UTF-8`, puis exécutez la commande `sudo locale-gen`.

Mode interactif :

Il existe deux manières d'utiliser Easy Install en mode interactif :

- Exécutez la commande `sudo /opt/Citrix/VDA/sbin/ctxinstall.sh` et saisissez le paramètre approprié à chaque invite de l'interface de ligne de commande.
- Exécutez la commande `/opt/Citrix/VDA/bin/easyinstall` dans l'environnement de bureau de votre VDA, puis suivez les instructions de l'interface utilisateur graphique Easy Install.



L'interface Easy Install vous guide à travers les opérations suivantes :

- Vérifier l'environnement du système
- Installer les dépendances
- Joindre le VDA à un domaine spécifié
- Configurer l'environnement d'exécution

Mode silencieux :

Pour utiliser Easy Install en mode silencieux, définissez les variables d'environnement suivantes avant d'exécuter ctxinstall.sh.

- **CTX_EASYINSTALL_HOSTNAME=host-name** : indique le nom d'hôte du serveur Linux VDA.
- **CTX_EASYINSTALL_DNS=ip-address-of-dns** : adresse IP du DNS.
- **CTX_EASYINSTALL_NTPS=address-of-ntps** : adresse IP ou nom de chaîne du serveur NTP.
- **CTX_EASYINSTALL_DOMAIN=domain-name** : nom NetBIOS du domaine.
- **CTX_EASYINSTALL_REALM=realm-name** : nom de la zone Kerberos.
- **CTX_EASYINSTALL_FQDN=ad-fqdn-name**
- **CTX_EASYINSTALL_ADINTEGRATIONWAY=winbind | sssd | centrify | pbis** : indique la méthode d'intégration d'Active Directory.
- **CTX_EASYINSTALL_USERNAME=domain-user-name** : indique le nom de l'utilisateur du domaine, utilisé pour rejoindre le domaine.
- **CTX_EASYINSTALL_PASSWORD=password** : spécifie le mot de passe de l'utilisateur du domaine, utilisé pour rejoindre le domaine.

Le script ctxsetup.sh utilise les variables suivantes :

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N** : le Linux VDA prend en charge la spécification d'un nom de Delivery Controller à l'aide d'un enregistrement DNS CNAME.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** : le Linux VDA requiert une liste séparée par des espaces de noms de domaines complets de Delivery Controller. Cette dernière sera utilisée pour l'enregistrement auprès d'un Delivery Controller. Au moins un nom de domaine complet (FQDN) ou CNAME doit être spécifié.
- **CTX_XDL_VDA_PORT=port-number** : le Linux VDA communique avec les Delivery Controller via un port TCP/IP.
- **CTX_XDL_REGISTER_SERVICE=Y | N** : les services Linux Virtual Desktop sont lancés après le démarrage de la machine.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** : les services Linux VDA requièrent que les connexions réseau entrantes soient autorisées via le pare-feu du système. Vous pouvez ouvrir automatiquement les ports requis (par défaut, les ports 80 et 1494) dans le pare-feu du système pour Linux Virtual Desktop.
- **CTX_XDL_HDX_3D_PRO=Y | N** : Linux VDA prend en charge HDX 3D Pro, un ensemble de technologies d'accélération GPU conçues pour optimiser la virtualisation des applications riches en graphiques. Si HDX 3D Pro est sélectionné, le Virtual Delivery Agent doit être configuré pour le mode Bureaux VDI (session unique), c'est-à-dire, CTX_XDL_VDI_MODE=Y.
- **CTX_XDL_VDI_MODE=Y | N** : indique si la machine est configurée comme modèle de mise à disposition de bureaux dédiés (VDI) ou comme modèle de mise à disposition de bureaux partagés hébergés. Pour les environnements HDX 3D Pro, définissez cette valeur sur Y.
- **CTX_XDL_SITE_NAME=dns-name** : le Linux VDA découvre les serveurs LDAP à l'aide de DNS. Pour limiter les résultats de recherche DNS à un site local, spécifiez un nom de site DNS. Si cela n'est pas nécessaire, définissez la valeur sur **<none>**.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** : le Linux VDA envoie une requête vers le DNS pour découvrir les serveurs LDAP. Si DNS ne peut pas fournir d'enregistrements de service LDAP, vous pouvez entrer une liste séparée par des espaces de noms de domaines complets LDAP avec ports LDAP. Par exemple, ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268. Si vous spécifiez le numéro de port LDAP 389, le Linux VDA interroge chaque serveur LDAP du domaine spécifié en mode d'interrogation. S'il existe un nombre x de stratégies et y de serveurs LDAP, le Linux VDA effectue le total de X multiplié par Y requêtes. Si le temps d'interrogation dépasse le seuil, les ouvertures de session peuvent échouer. Pour activer les requêtes LDAP plus rapides, activez le **catalogue global** sur un contrôleur de domaine et définissez le numéro de port LDAP correspondant sur 3268. Cette variable est définie sur **<none>** par défaut.

- **CTX_XDL_SEARCH_BASE=search-base-set** : le Linux VDA envoie une requête à LDAP via une base de recherche définie sur la racine du domaine Active Directory (par exemple, D, DC=mycompany,DC=com). Pour améliorer les performances de recherche, vous pouvez spécifier une base de recherche (par exemple, OU=VDI,DC=mycompany,DC=com). Si cela n'est pas nécessaire, définissez la valeur sur **<none>**.
- **CTX_XDL_FAS_LIST='list-fas-servers'** : les serveurs du service d'authentification fédérée (FAS) sont configurés via la stratégie de groupe AD. Le Linux VDA ne prend pas en charge la stratégie de groupe AD mais vous pouvez fournir une liste de serveurs FAS séparés par des points-virgules. La séquence doit être la même que celle configurée dans la stratégie de groupe AD. Si une adresse de serveur est supprimée, remplissez son espace vide avec la chaîne de texte **<none>** et ne modifiez pas l'ordre des adresses de serveur. Pour communiquer correctement avec les serveurs FAS, assurez-vous d'ajouter un numéro de port conforme à celui spécifié sur les serveurs FAS, par exemple CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'.
- **CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime** : chemin d'accès à l'installation de .NET Runtime 6.0 pour la prise en charge du nouveau Broker Agent Service (`ctxvda`). Le chemin par défaut est /usr/bin.
- **CTX_XDL_DESKTOP_ENVIRONMENT=gnome/gnome-classic/mate** : spécifie l'environnement de bureau GNOME, GNOME Classic ou MATE à utiliser dans les sessions. Si vous ne spécifiez pas la variable, le bureau actuellement installé sur le VDA est utilisé. Toutefois, si le bureau actuellement installé est MATE, vous devez définir la valeur de la variable sur **mate**.

  Vous pouvez également modifier l'environnement de bureau d'un utilisateur de session cible en procédant comme suit :

  1. Créez un fichier `.xsession` ou `.Xclients` sous le répertoire **$HOME/<username>** sur le VDA. Si vous utilisez Amazon Linux 2, créez un fichier `.Xclients`. Si vous utilisez d'autres distributions, créez un fichier `.xsession`.
  2. Modifiez le fichier `.xsession` ou `.Xclients` pour spécifier un environnement de bureau basé sur les distributions.

     - **Pour le bureau MATE**

     ```
     MSESSION="$(type -p mate-session)"
     if [ -n "$MSESSION" ]; then
       exec mate-session
     fi
     ```

     - **Pour le bureau GNOME Classic**

     ```
     GSESSION="$(type -p gnome-session)"
     if [ -n "$GSESSION" ]; then
     export GNOME_SHELL_SESSION_MODE=classic
     ```



```
4   exec gnome-session --session=gnome-classic
5   fi
```

- **Pour le bureau GNOME**

```
1   GSESSION="$(type -p gnome-session)"
2   if [ -n "$GSESSION" ]; then
3   exec gnome-session
4   fi
```

3. Partagez l'autorisation de fichier 700 avec l'utilisateur de la session cible.

À partir de la version 2209, les utilisateurs de session peuvent personnaliser leurs environnements de bureau. Pour activer cette fonctionnalité, vous devez installer au préalable des environnements de bureau commutables sur le VDA. Pour plus d'informations, consultez Environnements de bureau personnalisés par utilisateurs de session.

- **CTX_XDL_START_SERVICE=Y | N** : indique si les services Linux VDA sont démarrés lorsque la configuration est terminée.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** : port socket permettant d'écouter Citrix Scout. Le port par défaut est 7503.
- **CTX_XDL_TELEMETRY_PORT** : port de communication avec Citrix Scout. Le port par défaut est 7502.

Si aucun paramètre n'est défini, l'installation retourne en mode interactif et l'utilisateur est invité à intervenir. Lorsque tous les paramètres sont déjà définis via les variables d'environnement, le script ctxinstall.sh invite toujours l'utilisateur à entrer le chemin d'installation de .NET Runtime 6.0.

En mode silencieux, vous devez exécuter les commandes suivantes pour définir des variables d'environnement, puis exécuter le script ctxinstall.sht.

```
1  export CTX_EASYINSTALL_HOSTNAME=host-name
2
3  export CTX_EASYINSTALL_DNS=ip-address-of-dns
4
5  export CTX_EASYINSTALL_NTPS=address-of-ntps
6
7  export CTX_EASYINSTALL_DOMAIN=domain-name
8
9  export CTX_EASYINSTALL_REALM=realm-name
10
11 export CTX_EASYINSTALL_FQDN=ad-fqdn-name
12
13 export CTX_EASYINSTALL_ADINTEGRATIONWAY=winbind | sssd | centrify |
      pbis
14
15 export CTX_EASYINSTALL_USERNAME=domain-user-name
16
17 export CTX_EASYINSTALL_PASSWORD=password
```



```
18
19 export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N
20
21 export CTX_XDL_DDC_LIST='list-ddc-fqdns'
22
23 export CTX_XDL_VDA_PORT=port-number
24
25 export CTX_XDL_REGISTER_SERVICE=Y | N
26
27 export CTX_XDL_ADD_FIREWALL_RULES=Y | N
28
29 export CTX_XDL_HDX_3D_PRO=Y | N
30
31 export CTX_XDL_VDI_MODE=Y | N
32
33 export CTX_XDL_SITE_NAME=dns-site-name | '<none>'
34
35 export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'
36
37 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
38
39 export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'
40
41 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
42
43 export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<
      none>'
44
45 export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number
46
47 export CTX_XDL_TELEMETRY_PORT=port-number
48
49 export CTX_XDL_START_SERVICE=Y | N
50
51 sudo -E /opt/Citrix/VDA/sbin/ctxinstall.sh
52 <!--NeedCopy-->
```

Lors de l'exécution de la commande sudo, entrez l'option -E pour transmettre les variables d'environnement au nouveau shell créé. Nous vous recommandons de créer un fichier de script shell à partir des commandes précédentes avec **#!/bin/bash** en tant que première ligne.

Vous pouvez également spécifier tous les paramètres avec une seule commande :

```
1  sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
2
3  CTX_XDL_DDC_LIST='list-ddc-fqdns' \
4
5  CTX_XDL_VDA_PORT=port-number \
6
7  CTX_XDL_REGISTER_SERVICE=Y|N \
8
9  CTX_XDL_ADD_FIREWALL_RULES=Y|N \
10
```



```
CTX_XDL_AD_INTEGRATION=1|2|3|4 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

Étape 8 : exécuter XDPing

Exécutez `sudo /opt/Citrix/VDA/bin/xdping` pour vérifier les problèmes de configuration courants avec un environnement VDA Linux. Pour de plus amples informations, consultez la section XDPing.

Étape 9 : exécuter le Linux VDA

Démarrer Linux VDA :

Pour démarrer les services Linux VDA :

```
sudo /sbin/service ctxhdx start

sudo /sbin/service ctxvda start
<!--NeedCopy-->
```

Arrêter Linux VDA :

Pour arrêter les services Linux VDA :

```
sudo /sbin/service ctxvda stop
```



```
2
3 sudo /sbin/service ctxhdx stop
4 <!--NeedCopy-->
```

> **Remarque :**
>
> Avant d'arrêter les services `ctxvda` et `ctxhdx`, exécutez la commande `service ctxmonitorservice stop` pour arrêter le démon du service de surveillance. Sinon, le démon du service de surveillance redémarre les services que vous avez arrêtés.

Redémarrer Linux VDA :

Pour redémarrer les services Linux VDA :

```
1 sudo /sbin/service ctxvda stop
2
3 sudo /sbin/service ctxhdx restart
4
5 sudo /sbin/service ctxvda start
6 <!--NeedCopy-->
```

Vérifier l'état de Linux VDA :

Pour vérifier l'état de fonctionnement des services de Linux VDA :

```
1 sudo /sbin/service ctxvda status
2
3 sudo /sbin/service ctxhdx status
4 <!--NeedCopy-->
```

Étape 10 : créer des catalogues de machines dans Citrix Virtual Apps ou Citrix Virtual Desktops

Le processus de création de catalogues de machines et d'ajout de machines Linux VDA est similaire à l'approche traditionnelle avec les VDA Windows. Pour obtenir une description plus détaillée de la méthode à utiliser pour effectuer ces tâches, consultez les sections Créer des catalogues de machines et Gérer des catalogues de machines.

Pour la création de catalogues de machines contenant des machines Linux VDA, il existe quelques restrictions qui différencient ce processus de la création de catalogues de machines pour VDA Windows :

- Pour le système d'exploitation, sélectionnez :
  - l'option **OS à sessions multiples** pour un modèle de mise à disposition de bureaux partagés hébergés ;
  - l'option **OS mono-session** pour un modèle de mise à disposition de bureaux dédiés VDI.

- Ne combinez pas de machines Linux VDA et Windows dans le même catalogue de machines.

> **Remarque :**
>
> Les versions antérieures de Citrix Studio ne prenaient pas en charge la notion de « système d'exploitation Linux. » Toutefois, la sélection de l'option **OS de serveur Windows** ou **OS de serveur** implique un modèle de mise à disposition équivalent de bureaux partagés hébergés. La sélection de l'option **OS de bureau Windows** ou **OS de bureau** implique un modèle de mise à disposition d'un utilisateur unique par machine.
>
> **Conseil :**
>
> Si une supprimez une machine puis que vous la rejoignez au domaine Active Directory, vous devez supprimer et rajouter la machine au catalogue de machines.

Étape 11 : créer des groupes de mise à disposition dans Citrix Virtual Apps ou Citrix Virtual Desktops

Le processus de création d'un groupe de mise à disposition et d'ajout de catalogues de machines contenant des machines Linux VDA est presque identique aux machines VDA Windows. Pour obtenir une description plus détaillée de la méthode à utiliser pour effectuer ces tâches, consultez la section Créer des groupes de mise à disposition.

Lors de la création de groupes de mise à disposition qui contiennent des catalogues de machines Linux VDA, les restrictions suivantes s'appliquent :

- Assurez-vous que les utilisateurs et les groupes AD que vous sélectionnez ont été correctement configurés pour l'ouverture de session sur les machines Linux VDA.
- N'autorisez pas l'ouverture de session d'utilisateurs non authentifiés (anonymes).
- Ne combinez pas le groupe de mise à disposition avec des catalogues de machines contenant des machines Windows.

> **Important :**
>
> La publication d'applications est prise en charge avec la version 1.4 de Linux VDA et les versions supérieures. Toutefois, le Linux VDA ne prend pas en charge la mise à disposition de bureaux et d'applications sur la même machine.

Pour plus d'informations sur la création de catalogues de machines et de groupes de mise à disposition, consultez Citrix Virtual Apps and Desktops 7 2206.

Résolution des problèmes

Utilisez les informations de cette section pour résoudre les problèmes qui peuvent résulter de l'utilisation de la fonctionnalité Easy Install.

Impossible de joindre un domaine en utilisant SSSD

Une erreur peut se produire lorsque vous essayez de rejoindre un domaine, ce qui peut entraîner une sortie du type suivant (vérifiez les journaux pour l'impression d'écran) :

```
Step 6: join Domain!Enter ctxadmin's password:Failed to join domain:
 failed to lookup DC info for domain 'CITRIXLAB.LOCAL'over rpc: The
network name cannot be found
```

/var/log/xdl/vda.log :

```
2016-11-04 02:11:52.317 [INFO ] - The Citrix Desktop Service
    successfully obtained the following list of 1 delivery controller(s)
     with which to register: 'CTXDDC.citrixlab.local (10.158.139.214)'.
2016-11-04 02:11:52.362 [ERROR] - RegistrationManager.
    AttemptRegistrationWithSingleDdc: Failed to register with http://
    CTXDDC.citrixlab.local:80/Citrix/CdsController/IRegistrar. Error:
    General security error (An error occurred in trying to obtain a TGT:
     Client not found in Kerberos database (6))
2016-11-04 02:11:52.362 [ERROR] - The Citrix Desktop Service cannot
    connect to the delivery controller 'http://CTXDDC.citrixlab.local
    :80/Citrix/CdsController/IRegistrar' (IP Address '10.158.139.214')
Check the following:- The system clock is in sync between this machine
    and the delivery controller.
-  The Active Directory provider (e.g. winbind daemon) service is
    running and correctly configured.
-  Kerberos is correctly configured on this machine.
If the problem persists, please refer to Citrix Knowledge Base article
    CTX117248 for further information.
Error Details:
Exception 'General security error (An error occurred in trying to
    obtain a TGT: Client not found in Kerberos database (6))' of type '
    class javax.xml.ws.soap.SOAPFaultException'.
2016-11-04 02:11:52.362 [INFO ] - RegistrationManager.
    AttemptRegistrationWithSingleDdc: The current time for this VDA is
    Fri Nov 04 02:11:52 EDT 2016.
Ensure that the system clock is in sync between this machine and the
    delivery controller.
Verify the NTP daemon is running on this machine and is correctly
    configured.
2016-11-04 02:11:52.364 [ERROR] - Could not register with any
    controllers. Waiting to try again in 120000 ms. Multi-forest - false
2016-11-04 02:11:52.365 [INFO ] - The Citrix Desktop Service failed to
    register with any controllers in the last 470 minutes.
<!--NeedCopy-->
```


/var/log/messages :

```
Nov 4 02:15:27 RH-WS-68 [sssd[ldap_child[14867]]]: Failed to initialize
 credentials using keytab [MEMORY:/etc/krb5.keytab]: Client 'RH-WS-68
$@CITRIXLAB.LOCAL'not found in Kerberos database. Unable to create
 GSSAPI-encrypted LDAP connection.Nov 4 02:15:27 RH-WS-68 [sssd[
ldap_child[14867]]]: Client 'RH-WS-68$@CITRIXLAB.LOCAL'not found
in Kerberos database
```

Pour résoudre ce problème :

1. Exécutez la commande `rm -f /etc/krb5.keytab`.
2. Exécutez la commande `net ads leave $REALM -U $domain-administrator`.
3. Supprimez le catalogue de machines et le groupe de mise à disposition sur le Delivery Controller.
4. Exécutez /opt/Citrix/VDA/sbin/ctxinstall.sh.
5. Créez le catalogue de machines et le groupe de mise à disposition sur le Delivery Controller.

Affichage d'un écran gris dans les sessions de bureau Ubuntu

Ce problème se produit lorsque vous lancez une session qui est ensuite bloquée dans un bureau vide. En outre, la console de la machine affiche également un écran gris lorsque vous vous connectez en utilisant un compte d'utilisateur local.

Pour résoudre ce problème :

1. Exécutez la commande `sudo apt-get update`.
2. Exécutez la commande `sudo apt-get install unity lightdm`.
3. Ajoutez la ligne suivante à `/etc/lightdm/lightdm.conf`:
   `greeter-show-manual-login=true`

Échec du lancement des sessions de bureau Ubuntu en raison d'un répertoire de base manquant

/var/log/xdl/hdx.log:

```
2016-11-02 13:21:19.015 <P22492:S1> citrix-ctxlogin: StartUserSession:
   failed to change to directory(/home/CITRIXLAB/ctxadmin) errno(2)

2016-11-02 13:21:19.017 <P22227> citrix-ctxhdx: logSessionEvent:
   Session started for user ctxadmin.

2016-11-02 13:21:19.023 <P22492:S1> citrix-ctxlogin: ChildPipeCallback:
    Login Process died: normal.

```

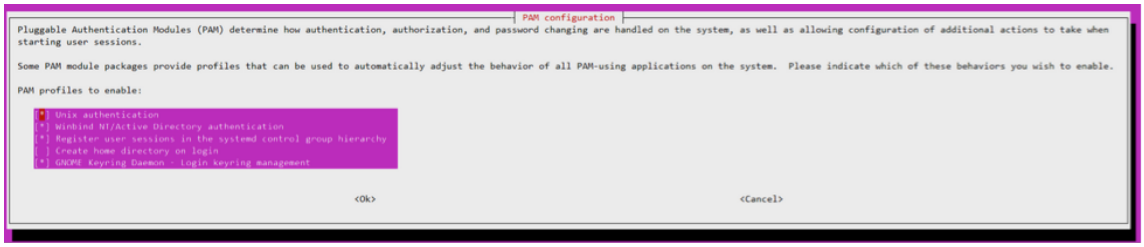


```
2016-11-02 13:21:59.217 <P22449:S1> citrix-ctxgfx: main: Exiting
    normally.
<!--NeedCopy-->
```

> **Conseil :**
>
> La cause de ce problème réside dans le fait que le répertoire de base n'est pas créé pour l'administrateur de domaine.

Pour résoudre ce problème :

1. À partir d'une ligne de commande, saisissez **pam-auth-update**.
2. Dans la boîte de dialogue qui s'affiche, vérifiez que **Create home directory login** est sélectionné.



Échec du démarrage de la session ou fermeture rapide de la session avec une erreur dbus

/var/log/messages (pour RHEL ou CentOS) :

```
Oct 27 04:17:16 CentOS7 citrix-ctxhdx[8978]: Session started for user
    CITRIXLAB\ctxadmin.

Oct 27 04:17:18 CentOS7 kernel: traps: gnome-session[19146] trap int3
    ip:7f89b3bde8d3 sp:7fff8c3409d0 error:0

Oct 27 04:17:18 CentOS7 gnome-session[19146]: ERROR: Failed to connect
    to system bus: Exhausted all available authentication mechanisms (
    tried: EXTERNAL, DBUS_COOKIE_SHA1, ANONYMOUS) (available: EXTERNAL,
    DBUS_COOKIE_SHA1, ANONYMOUS)#012aborting...

Oct 27 04:17:18 CentOS7 gnome-session: gnome-session[19146]: ERROR:
    Failed to connect to system bus: Exhausted all available
    authentication mechanisms (tried: EXTERNAL, DBUS_COOKIE_SHA1,
    ANONYMOUS) (available: EXTERNAL, DBUS_COOKIE_SHA1, ANONYMOUS)

Oct 27 04:17:18 CentOS7 gnome-session: aborting...

Oct 27 04:17:18 CentOS7 citrix-ctxgfx[18981]: Exiting normally.

Oct 27 04:17:18 CentOS7 citrix-ctxhdx[8978]: Session stopped for user
    CITRIXLAB\ctxadmin.
<!--NeedCopy-->
```


Ou, pour les distributions Ubuntu, utilisez le journal /var/log/syslog :

```
Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] pid.c:
    Stale PID file, overwriting.

Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] bluez5-
    util.c: Failed to get D-Bus connection: Did not receive a reply.
    Possible causes include: the remote application did not send a reply
    , the message bus security policy blocked the reply, the reply
    timeout expired, or the network connection was broken.

Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] hashmap
    .c: Assertion 'h' failed at pulsecore/hashmap.c:116, function
    pa_hashmap_free(). Aborting.

Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: [pulseaudio] core-
    util.c: Failed to connect to system bus: Did not receive a reply.
    Possible causes include: the remote application did not send a reply
    , the message bus security policy blocked the reply, the reply
    timeout expired, or the network connection was broken.

Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: message repeated 10
    times: [ [pulseaudio] core-util.c: Failed to connect to system bus:
    Did not receive a reply. Possible causes include: the remote
    application did not send a reply, the message bus security policy
    blocked the reply, the reply timeout expired, or the network
    connection was broken.]

Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: [pulseaudio] pid.c:
    Daemon already running.Nov  3 11:03:58 user01-HVM-domU citrix-ctxgfx
    [24693]: Exiting normally
<!--NeedCopy-->
```

Certains des groupes ou des modules ne prennent effet qu'après un redémarrage. Si les messages d'erreur **dbus** s'affichent dans le journal, nous vous recommandons de redémarrer le système et de réessayer.

SELinux empêche SSHD d'accéder au répertoire de base

L'utilisateur peut lancer une session, mais ne peut pas se connecter.

/var/log/ctxinstall.log :

```
Jan 25 23:30:31 yz-rhel72-1 setroubleshoot[3945]: SELinux is preventing
     /usr/sbin/sshd from setattr access on the directory /root. For
    complete SELinux messages. run sealert -l 32f52c1f-8ff9-4566-a698
    -963a79f16b81

Jan 25 23:30:31 yz-rhel72-1 python[3945]: SELinux is preventing /usr/
    sbin/sshd from setattr access on the directory /root.

```



```
*****  Plugin catchall_boolean (89.3 confidence) suggests
    ******************

If you want to allow polyinstantiation to enabled

   Then you must tell SELinux about this by enabling the '
    polyinstantiation_enabled' boolean.

You can read 'None' man page for more details.

    Do

       setsebool -P polyinstantiation_enabled 1

*****  Plugin catchall (11.6 confidence) suggests
    *************************

If you believe that sshd should be allowed setattr access on the root
    directory by default.

Then you should report this as a bug.

You can generate a local policy module to allow this access.

      Do

       allow this access for now by executing:

       # grep sshd /var/log/audit/audit.log | audit2allow -M mypol

# semodule -i mypol.pp
<!--NeedCopy-->
```

Pour résoudre ce problème :

1. Désactivez SELinux en apportant la modification suivante à /etc/selinux/config.

   SELINUX=disabled

2. Redémarrez le VDA.

Installer manuellement Linux Virtual Delivery Agent pour Amazon Linux 2, CentOS, RHEL et Rocky Linux

September 25, 2023

> **Important :**
>
> Pour les nouvelles installations, nous vous recommandons d'utiliser Easy Install pour effectuer une installation rapide. Easy Install permet de gagner du temps et d'économiser de la main d'œuvre. Cette installation est également plus fiable que l'installation manuelle décrite dans cet article.

Étape 1 : préparer votre distribution Linux pour l'installation du VDA

Étape 1a : vérifier la configuration réseau

Assurez-vous que le réseau est connecté et correctement configuré. Par exemple, vous devez configurer le serveur DNS sur le Linux VDA.

Étape 1b : définir le nom d'hôte

Pour vous assurer que le nom d'hôte de la machine est indiqué correctement, modifiez le fichier **/etc/hostname** afin que celui-ci contienne uniquement le nom d'hôte de la machine.

```
hostname
```

Étape 1c : attribuer une adresse de bouclage au nom d'hôte

Pour vous assurer que le nom de domaine DNS et le nom de domaine complet (FQDN) de la machine sont indiqués correctement, modifiez la ligne suivante du fichier `/etc/hosts` afin que celle-ci inclue le nom de domaine complet et le nom d'hôte dans les deux premières entrées :

```
127.0.0.1 hostname-fqdn hostname localhost localhost.localdomain
localhost4 localhost4.localdomain4
```

Par exemple :

```
127.0.0.1 vda01.example.com vda01 localhost localhost.localdomain
localhost4 localhost4.localdomain4
```

Supprimez toute autre référence à **hostname-fqdn** ou **hostname** des autres entrées du fichier.

> **Remarque :**
>
> Le Linux VDA ne prend actuellement pas en charge la troncation de noms NetBIOS. Le nom d'hôte ne doit pas comporter plus de 15 caractères.
>
> **Conseil :**
>
> Utilisez uniquement les caractères a–z, A–Z, 0–9 et tiret (-). Évitez les caractères de souligne-

> ment (_), les espaces et autres symboles. Ne démarrez pas un nom d'hôte par un chiffre et ne le terminez pas par un tiret. Cette règle s'applique également aux noms d'hôte Delivery Controller.

Étape 1d : vérifier le nom d'hôte

Vérifiez que le nom d'hôte est correctement configuré :

```
hostname
<!--NeedCopy-->
```

Cette commande renvoie uniquement le nom d'hôte de la machine et non son nom de domaine complet (FQDN).

Vérifiez que le nom de domaine complet est correctement configuré :

```
hostname -f
<!--NeedCopy-->
```

Cette commande renvoie le nom de domaine complet de la machine.

Étape 1e : vérifier la résolution de nom et l'accessibilité du service

Vérifiez que vous pouvez résoudre le nom de domaine complet et effectuer un sondage ping sur le contrôleur de domaine et le Delivery Controller :

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

ping delivery-controller-fqdn
<!--NeedCopy-->
```

Si vous ne pouvez pas résoudre le nom de domaine complet ou effectuer un sondage ping sur l'une de ces machines, reprenez les étapes avant de continuer.

Étape 1f : configurer la synchronisation de l'horloge

Il est très important de maintenir la synchronisation de l'horloge entre les VDA, les Delivery Controller et les contrôleurs de domaine. L'hébergement du Linux VDA en tant que machine virtuelle peut entraîner des problèmes de décalage d'horloge. Pour cette raison, il est recommandé de synchroniser l'heure avec un service de temps à distance.

Un environnement par défaut RHEL 8 ou RHEL 7 utilise le démon Chrony (`chronyd`) pour la synchronisation de l'horloge.

Configurer le service Chrony En tant qu'utilisateur racine, modifiez **/etc/chrony.conf** et ajoutez une entrée de serveur pour chaque serveur de temps distant :

```
server peer1-fqdn-or-ip-address iburst

server peer2-fqdn-or-ip-address iburst
<!--NeedCopy-->
```

Dans un déploiement type, synchronisez l'heure depuis les contrôleurs de domaine locaux et non pas directement depuis des serveurs de pool NTP publics. Ajoutez une entrée de serveur pour chaque contrôleur de domaine Active Directory du domaine.

Supprimez toute autre entrée de serveur répertoriée, y compris les entrées d'adresse IP de bouclage, localhost et ***.pool.ntp.org** de serveur public.

Enregistrez les modifications et redémarrez le démon Chrony :

```
sudo /sbin/service chronyd restart
<!--NeedCopy-->
```

Étape 1g : installer OpenJDK 11

Le Linux VDA nécessite la présence d'OpenJDK 11.

- Si vous utilisez CentOS, RHEL ou Rocky Linux, OpenJDK 11 est automatiquement installé en tant que dépendance lorsque vous installez le Linux VDA.
- Si vous utilisez Amazon Linux 2, exécutez la commande suivante pour activer et installer OpenJDK 11 :

  ```
  amazon-linux-extras install java-openjdk11
  <!--NeedCopy-->
  ```

Vérifiez que la version est correcte :

```
sudo yum info java-11-openjdk
<!--NeedCopy-->
```

Le OpenJDK préconditionné peut être une version antérieure. Mise à jour vers OpenJDK 11 :

```
sudo yum -y update java-11-openjdk
<!--NeedCopy-->
```

Étape 1h : installer PostgreSQL

Le Linux VDA requiert PostgreSQL. Les commandes suivantes installent PostgreSQL à partir du package Linux VDA (PostgreSQL 9 pour Amazon Linux 2, RHEL 7 et CentOS 7, et PostgreSQL 10 pour RHEL

8 et Rocky Linux 8).

```
sudo yum -y install postgresql-server

sudo yum -y install postgresql-jdbc
<!--NeedCopy-->
```

L'étape de post-installation suivante est requise pour initialiser la base de données et s'assurer que le service est lancé au démarrage de la machine. Cette opération crée les fichiers de base de données sous **/var/lib/pgsql/data**.

```
sudo postgresql-setup initdb
<!--NeedCopy-->
```

Étape 1i : démarrer PostgreSQL

Une fois la machine démarrée, démarrez le service immédiatement :

```
sudo systemctl enable postgresql

sudo systemctl start postgresql
<!--NeedCopy-->
```

Vérifiez la version de PostgreSQL avec :

```
psql --version
<!--NeedCopy-->
```

(RHEL 7 uniquement) Vérifiez que le répertoire de données est défini à l'aide de l'utilitaire de ligne de commande **psql** :

```
sudo -u postgres psql -c 'show data_directory'
<!--NeedCopy-->
```

Étape 2 : préparer l'hyperviseur

Certaines modifications sont requises pour l'exécution du Linux VDA en tant que machine virtuelle sur un hyperviseur pris en charge. Apportez les modifications suivantes en fonction de la plateforme d'hyperviseur utilisée. Aucune modification n'est requise si vous utilisez la machine Linux sur un matériel bare metal.

Corriger la synchronisation de l'heure sur Citrix Hypervisor

Si la fonctionnalité de synchronisation de l'heure de Citrix Hypervisor est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée avec NTP et Citrix Hypervisor. En effet, les deux

systèmes essaient de gérer l'horloge système. Pour éviter que l'horloge ne soit plus synchronisée avec d'autres serveurs, assurez-vous l'horloge du système de chaque invité Linux est synchronisée avec NTP. Cela nécessite la désactivation de la synchronisation de l'heure de l'hôte. Aucune modification n'est requise en mode HVM.

Si vous utilisez un noyau Linux paravirtualisé avec le composant Citrix VM Tools installé, vous pouvez vérifier si la fonctionnalité de synchronisation de l'heure de Citrix Hypervisor est présente et activée à partir de la VM Linux :

```
su -

cat /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Cette commande renvoie 0 ou 1 :

- 0 - La fonctionnalité de synchronisation de l'heure est activée, et doit être désactivée.
- 1 - La fonctionnalité de synchronisation de l'heure est désactivée, et aucune action n'est requise.

Si le fichier /proc/sys/xen/independent_wallclock n'existe pas, les étapes suivantes ne sont pas nécessaires.

Si la fonctionnalité de synchronisation est activée, désactivez-la en entrant 1 dans le fichier :

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Pour rendre cette modification permanente et persistante après le redémarrage, modifiez le fichier **/etc/sysctl.conf** et ajoutez la ligne :

```
xen.independent_wallclock = 1
```

Pour vérifier ces modifications, redémarrez le système :

```
su -

cat /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Cette commande renvoie la valeur 1.

Corriger la synchronisation de l'heure sur Microsoft Hyper-V

Les VM Linux sur lesquelles Hyper-V Integration Services est installé peuvent tirer parti de la fonctionnalité de synchronisation de l'heure Hyper-V pour utiliser l'heure du système d'exploitation hôte. Pour vous assurer que l'horloge du système est toujours précise, cette fonctionnalité doit être activée avec les services NTP.

Depuis le système d'exploitation de gestion :

1. Ouvrez la console du gestionnaire Hyper-V.
2. Pour les paramètres d'une machine virtuelle Linux, sélectionnez **Integration Services**.
3. Assurez-vous que **Time synchronization** est sélectionné.

> **Remarque :**
>
> Cette approche diffère de VMware et Citrix Hypervisor, pour lesquels la synchronisation de l'heure est désactivée pour éviter tout conflit avec NTP. La synchronisation de l'heure Hyper-V peut co-exister avec la synchronisation de l'heure NTP.

Corriger la synchronisation de l'heure sur ESX et ESXi

Si la fonctionnalité de synchronisation de l'heure de VMware est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée avec l'hyperviseur et NTP. En effet, les deux systèmes essaient de synchroniser l'horloge système. Pour éviter que l'horloge ne soit plus synchronisée avec d'autres serveurs, assurez-vous l'horloge du système de chaque invité Linux est synchronisée avec NTP. Cela nécessite la désactivation de la synchronisation de l'heure de l'hôte.

Si vous exécutez un noyau Linux paravirtualisé sur lequel VMware Tools est installé :

1. Ouvrez vSphere Client.
2. Modifiez les paramètres pour la VM Linux.
3. Dans la boîte de dialogue **Virtual Machine Properties** (Propriétés de la machine virtuelle), ouvrez l'onglet **Options**.
4. Sélectionnez **VMware Tools**.
5. Dans la zone **Advanced** (Avancé), désélectionnez **Synchronize guest time with host** (Synchroniser l'heure de l'invité avec l'hôte).

Étape 3 : ajouter la machine virtuelle (VM) Linux au domaine Windows

Le Linux VDA prend en charge plusieurs méthodes pour ajouter des machines Linux au domaine Active Directory (AD) :

- Samba Winbind
- Quest Authentication Services
- Centrify DirectControl
- SSSD
- PBIS

Suivez les instructions en fonction de la méthode choisie.

> **Remarque :**
>
> Les lancements de session peuvent échouer lorsque le même nom d'utilisateur est utilisé pour le compte local dans le Linux VDA et le compte dans AD.

Samba Winbind

Installez ou mettez à jour les packages requis :

Pour RHEL 8 et Rocky Linux 8 :

```
sudo yum -y install samba-winbind samba-winbind-clients krb5-
    workstation oddjob-mkhomedir realmd authselect
<!--NeedCopy-->
```

Pour Amazon Linux 2, CentOS 7 et RHEL 7 :

```
sudo yum -y install samba-winbind samba-winbind-clients krb5-
    workstation authconfig oddjob-mkhomedir
<!--NeedCopy-->
```

Activer le démon Winbind pour qu'il soit lancé au démarrage de la machine Le démon Winbind doit être configuré pour être lancé au démarrage de la machine :

```
sudo /sbin/chkconfig winbind on
<!--NeedCopy-->
```

Configurer l'authentification Winbind Configurez la machine pour l'authentification Kerberos à l'aide de Winbind :

1. Exécutez la commande suivante :.

   Pour RHEL 8 et Rocky Linux 8 :

   ```
   sudo authselect select winbind with-mkhomedir --force
   <!--NeedCopy-->
   ```

   Pour Amazon Linux 2, CentOS 7 et RHEL 7 :

   ```
   sudo authconfig --disablecache --disablesssd --disablesssdauth --
       enablewinbind --enablewinbindauth --disablewinbindoffline --
       smbsecurity=ads --smbworkgroup=domain --smbrealm=REALM --
       krb5realm=REALM --krb5kdc=fqdn-of-domain-controller --
       winbindtemplateshell=/bin/bash --enablemkhomedir --updateall
   <!--NeedCopy-->
   ```


Où **REALM** est le nom du domaine Kerberos en majuscules et **domain** est le nom NetBIOS du domaine.

Si des recherches DNS sur le nom de domaine et de serveur KDC sont requises, ajoutez les options suivantes à la commande précédente :

```
--enablekrb5kdcdns --enablekrb5realmdns
```

Ignorez les erreurs renvoyées par la commande `authconfig` sur l'échec du démarrage du service `winbind`. Ces erreurs se produisent lorsque `authconfig` essaie de démarrer le service `winbind` sans que la machine ait rejoint le domaine.

2. Ouvrez **/etc/samba/smb.conf** et ajoutez les entrées suivantes dans la section [Global], mais après la section générée par l'outil `authconfig` :

```
kerberos method = secrets and keytab
winbind refresh tickets = true
winbind offline logon = no
```

3. (RHEL 8 et Rocky Linux 8 uniquement) Ouvrez **/etc/krb5.conf** et ajoutez des entrées sous les sections `[libdefaults]`, `[realms]` et `[domain_realm]` :

   Dans la section `[libdefaults]` :

```
default_ccache_name = FILE:/tmp/krb5cc_%{ uid }
default_realm = REALM
dns_lookup_kdc = true
```

   Dans la section `[realms]` :

```
REALM = {
kdc = fqdn-of-domain-controller
}
```

   Dans la section `[domain_realm]` :

```
realm = REALM
.realm = REALM
```

Linux VDA exige l'authentification et l'enregistrement du fichier keytab système /etc/krb5.keytab auprès du Delivery Controller. Le paramètre kerberos method précédent force Winbind à créer le fichier keytab système lorsque la machine rejoint le domaine.

Rejoindre un domaine Windows Votre contrôleur de domaine doit être accessible et vous devez disposer d'un compte utilisateur Active Directory avec les autorisations nécessaires pour ajouter des ordinateurs au domaine :

Pour RHEL 8 et Rocky Linux 8 :


```
sudo realm join -U user --client-software=winbind REALM
<!--NeedCopy-->
```

Pour Amazon Linux 2 et RHEL 7 :

```
sudo net ads join REALM -U user
<!--NeedCopy-->
```

REALM est le nom de domaine Kerberos en majuscules, et **user** est un utilisateur de domaine disposant des autorisations nécessaires pour ajouter les ordinateurs au domaine.

Configurer PAM pour Winbind Par défaut, la configuration du module Winbind PAM (pam_winbind) n'active pas la mise en cache de ticket Kerberos ni la création du répertoire de base. Ouvrez **/etc/security/pam_winbind.conf** et ajoutez ou modifiez les entrées suivantes dans la section [Global] :

```
krb5_auth = yes
krb5_ccache_type = FILE
mkhomedir = yes
```

Assurez-vous que les points-virgules de début de chaque paramètre sont supprimés. Ces modifications requièrent un redémarrage du démon Winbind :

```
sudo /sbin/service winbind restart
<!--NeedCopy-->
```

> **Conseil :**
>
> Le démon `winbind` ne reste en cours d'exécution que si la machine est associée à un domaine.

Ouvrez **/etc/krb5.conf** et modifiez le paramètre suivant dans la section [libdefaults], remplacez le type KEYRING par le type FILE :

```
default_ccache_name = FILE:/tmp/krb5cc_%{ uid }
```

Vérifier l'appartenance à un domaine Le Delivery Controller requiert que toutes les machines VDA (VDA Windows et Linux) aient un objet ordinateur dans **Active Directory**.

Exécutez la commande **net ads** de **Samba** pour vérifier que la machine est associée à un domaine :

```
sudo net ads testjoin
<!--NeedCopy-->
```

Exécutez la commande suivante pour vérifier les informations d'objet de domaine et d'ordinateur supplémentaires :

```
sudo net ads info
<!--NeedCopy-->
```


Vérifier la configuration de Kerberos Pour vous assurer que Kerberos est correctement configuré pour être utilisé avec le Linux VDA, vérifiez que le fichier keytab système a été créé et contient des clés valides :

```
sudo klist -ke
<!--NeedCopy-->
```

Cette commande affiche la liste des clés disponibles pour les différentes combinaisons de noms principaux et de suites de chiffrement. Exécutez la commande `kinit` Kerberos pour authentifier la machine auprès du contrôleur de domaine à l'aide de ces clés :

```
sudo kinit -k MACHINE$@REALM
<!--NeedCopy-->
```

Les noms de machine et de domaine doivent être spécifiés en majuscules. Le signe dollar ($) doit être placé dans une séquence d'échappement avec une barre oblique inverse (\) pour empêcher le remplacement shell. Dans certains environnements, le nom de domaine DNS est différent du nom de domaine Kerberos. Assurez-vous que le nom de domaine est utilisé. Si cette commande réussit, aucun résultat n'est affiché.

Vérifiez que le ticket TGT pour le compte de machine a été mis en cache à l'aide de :

```
sudo klist
<!--NeedCopy-->
```

Examinez les détails du compte de machine à l'aide de :

```
sudo net ads status
<!--NeedCopy-->
```

Vérifier l'authentification utilisateur Utilisez l'outil **wbinfo** pour vérifier que les utilisateurs de domaine peuvent s'authentifier auprès du domaine :

```
wbinfo --krb5auth=domain\username%password
<!--NeedCopy-->
```

Le domaine spécifié ici est le nom de domaine Active Directory, et non le nom de domaine Kerberos. Pour le shell bash, la barre oblique inverse (\) doit être placée dans une séquence d'échappement avec une autre barre oblique inverse. Cette commande renvoie un message indiquant la réussite ou l'échec.

Pour vérifier que le module PAM Winbind est correctement configuré, ouvrez une session sur le Linux VDA à l'aide d'un compte d'utilisateur de domaine qui n'a jamais été utilisé.

```
ssh localhost -l domain\username
id -u
<!--NeedCopy-->
```


Vérifiez que les tickets dans le cache d'identification de Kerberos sont valides et n'ont pas expiré :

```
klist
<!--NeedCopy-->
```

Quittez la session.

```
exit
<!--NeedCopy-->
```

Le même test peut être réalisé en ouvrant une session directement sur la console KDE ou Gnome. Passez à l'étape 6 : installer le Linux VDA après vérification de la jonction du domaine.

Quest Authentication Services

Configurer Quest sur le contrôleur de domaine Cette procédure suppose que vous avez installé et configuré le logiciel Quest sur les contrôleurs de domaine Active Directory et disposez des droits Administrateur pour créer des objets ordinateur dans Active Directory.

Autoriser les utilisateurs de domaine à ouvrir une session sur des machines Linux VDA Pour autoriser les utilisateurs de domaine à établir des sessions HDX sur une machine Linux VDA :

1. Dans la console de gestion Utilisateurs et ordinateurs Active Directory, ouvrez les propriétés de l'utilisateur Active Directory pour ce compte d'utilisateur.
2. Sélectionnez l'onglet **Unix Account**.
3. Sélectionnez **Unix-enabled**.
4. Définissez **Primary GID Number** sur l'ID d'un groupe d'utilisateurs de domaine.

> **Remarque :**
>
> Ces instructions sont les mêmes que pour la configuration d'utilisateurs de domaine pour l'ouverture de session à l'aide de la console, RDP, SSH ou tout autre protocole de communication à distance.

Configurer Quest sur un Linux VDA

Solution à l'application forcée de la stratégie SELinux L'environnement RHEL par défaut applique entièrement SELinux. Cette mise en œuvre interfère avec les mécanismes IPC de socket de domaine Unix utilisés par Quest et empêche les utilisateurs de domaine d'ouvrir une session.

Le moyen pratique de remédier à ce problème consiste à désactiver SELinux. En tant qu'utilisateur racine, modifiez **/etc/selinux/config** en modifiant le paramètre **SELinux** :

```
SELINUX=permissive
```


Cette modification nécessite le redémarrage de la machine :

```
reboot
<!--NeedCopy-->
```

> **Important :**
>
> Utilisez ce paramètre avec précaution. La réactivation de l'application forcée de la stratégie SELinux après sa désactivation peut entraîner un verrouillage complet, même pour l'utilisateur racine et d'autres utilisateurs locaux.

Configurer le démon VAS Le renouvellement automatique des tickets Kerberos doit être activé et déconnecté. L'authentification (ouverture de session en mode déconnecté) doit être désactivée.

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-
    interval 32400

sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-
    auth false
<!--NeedCopy-->
```

Cette commande définit l'intervalle de renouvellement sur 9 heures (32 400 secondes), ce qui représente une heure de moins que la valeur par défaut de 10 heures pour la durée de vie d'un ticket. Définissez ce paramètre sur une valeur inférieure sur les systèmes avec une durée de vie de ticket plus courte.

Configuration de PAM et de NSS Pour permettre l'ouverture de session d'utilisateur de domaine via HDX et d'autres services tels que su, ssh et RDP, exécutez les commandes suivantes pour configurer manuellement PAM et NSS :

```
sudo /opt/quest/bin/vastool configure pam

sudo /opt/quest/bin/vastool configure nss
<!--NeedCopy-->
```

Rejoindre un domaine Windows Associez la machine Linux au domaine Active Directory à l'aide de la commande Quest **vastool** :

```
sudo /opt/quest/bin/vastool -u user join domain-name
<!--NeedCopy-->
```

L'utilisateur est un utilisateur de domaine disposant des autorisations nécessaires pour associer des ordinateurs au domaine Active Directory. Le paramètre **domain-name** est le nom DNS du domaine ; par exemple, exemple.com.

Vérifier l'appartenance à un domaine Le Delivery Controller requiert que toutes les machines VDA (VDA Windows et Linux) aient un objet ordinateur dans `Active Directory`. Pour vérifier qu'une machine Linux associée à Quest se trouve sur le domaine :

```
sudo /opt/quest/bin/vastool info domain
<!--NeedCopy-->
```

Si la machine est associée à un domaine, cette commande renvoie le nom de domaine. Si la machine n'est pas associée à un domaine, l'erreur suivante apparaît :

```
ERROR: No domain could be found.
ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm
default_realm not configured in vas.conf. Computer may not be joined
to domain
```

Vérifier l'authentification utilisateur Pour vérifier que Quest peut authentifier les utilisateurs de domaine via PAM, ouvrez une session sur le Linux VDA à l'aide d'un compte d'utilisateur de domaine qui n'a jamais été utilisé.

```
ssh localhost -l domain\username
id -u
<!--NeedCopy-->
```

Vérifiez qu'un fichier cache d'identification Kerberos correspondant a été créé pour le UID renvoyé par la commande **id -u** :

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Vérifiez que les tickets dans le cache d'identification de Kerberos sont valides et n'ont pas expiré :

```
/opt/quest/bin/vastool klist
<!--NeedCopy-->
```

Quittez la session.

```
exit
<!--NeedCopy-->
```

Le même test peut être réalisé en ouvrant une session directement sur la console KDE ou Gnome. Passez à l'étape 6 : installer le Linux VDA après vérification de la jonction du domaine.

Centrify DirectControl

Rejoindre un domaine Windows Une fois Centrify DirectControl Agent installé, associez la machine Linux au domaine Active Directory à l'aide de la commande Centrify `adjoin` :


```
su -
adjoin -w -V -u user domain-name
<!--NeedCopy-->
```

Le paramètre user est un utilisateur de domaine Active Directory disposant des autorisations nécessaires pour associer des ordinateurs au domaine Active Directory. Le paramètre **domain-name** est le nom du domaine auquel associer la machine Linux.

Vérifier l'appartenance à un domaine Le Delivery Controller requiert que toutes les machines VDA (VDA Windows et Linux) aient un objet ordinateur dans Active Directory. Pour vérifier qu'une machine Linux associée à Centrify se trouve sur le domaine :

```
su -
adinfo
<!--NeedCopy-->
```

Vérifiez que la valeur Joined to domain est valide et que CentrifyDC mode renvoie connected. Si le mode reste bloqué à l'état de démarrage, le client Centrify rencontre des problèmes de connexion au serveur ou d'authentification.

Des informations plus complètes sur le système et les diagnostics sont disponibles à l'aide de :

```
adinfo --sysinfo all
adinfo -diag
<!--NeedCopy-->
```

Testez la connectivité avec les différents services Active Directory et Kerberos.

```
adinfo --test
<!--NeedCopy-->
```

Passez à l'étape 6 : installer le Linux VDA après vérification de la jonction du domaine.

SSSD

Si vous utilisez SSSD, suivez les instructions de cette section. Cette section comprend des instructions permettant de connecter une machine Linux VDA à un domaine Windows et des indications sur la configuration de l'authentification Kerberos.

Pour configurer SSSD sur RHEL et CentOS, procédez comme suit :

1. Rejoindre le domaine et créer un fichier keytab hôte
2. Configurer SSSD
3. Activer SSSD
4. Vérifier la configuration de Kerberos
5. Vérifier l'authentification utilisateur

Rejoindre le domaine et créer un fichier keytab hôte SSSD ne fournit pas de fonctions de client Active Directory pour rejoindre le domaine et gérer le fichier keytab système. Vous pouvez utiliser **adcli**, **realmd**ou **Samba** à la place.

Cette section décrit l'approche **Samba** pour Amazon Linux 2 et RHEL 7, et l'approche `adcli` pour RHEL 8. Pour **realmd**, reportez-vous à la documentation RHEL ou CentOS. Ces étapes doivent être suivies avant la configuration de SSSD.

- **Samba (Amazon Linux 2 et RHEL 7) :**

  Installez ou mettez à jour les packages requis :

  ```
  1  sudo yum -y install krb5-workstation authconfig oddjob-mkhomedir
        samba-common-tools
  2  <!--NeedCopy-->
  ```

  Sur le client Linux avec des fichiers correctement configurés :

  - /etc/krb5.conf
  - /etc/samba/smb.conf :

  Configurez la machine pour l'authentification Kerberos et **Samba** :

  ```
  1  sudo authconfig --smbsecurity=ads --smbworkgroup=domain --
        smbrealm=REALM --krb5realm=REALM --krb5kdc=fqdn-of-domain-
        controller --update
  2  <!--NeedCopy-->
  ```

  Où **REALM** est le nom du domaine Kerberos en majuscules et **domain** est le nom NetBIOS court du domaine Active Directory.

  > **Remarque :**
  >
  > Les paramètres de cet article sont destinés au modèle à domaine et à forêt uniques. Configurez Kerberos en fonction de votre infrastructure AD.

  Si des recherches DNS sur le nom de domaine et de serveur KDC sont requises, ajoutez les options suivantes à la commande précédente :

  ```
  --enablekrb5kdcdns --enablekrb5realmdns
  ```

  Ouvrez **/etc/samba/smb.conf** et ajoutez les entrées suivantes dans la section **[Global]**, mais après la section générée par l'outil **authconfig** :

  ```
  kerberos method = secrets and keytab
  winbind offline logon = no
  ```

  Rejoignez le domaine Windows. Assurez-vous que votre contrôleur de domaine est accessible et que vous disposez d'un compte utilisateur Active Directory avec les autorisations nécessaires pour ajouter des ordinateurs au domaine.


```
sudo net ads join REALM -U user
<!--NeedCopy-->
```

REALM est le nom de domaine Kerberos en majuscules, et **user** est un utilisateur de domaine disposant des autorisations nécessaires pour ajouter les ordinateurs au domaine.

- **Adcli (RHEL 8 et Rocky Linux 8) :**

  Installez ou mettez à jour les packages requis :

```
sudo yum -y install samba-common samba-common-tools krb5-
   workstation authconfig oddjob-mkhomedir realmd oddjob
   authselect
<!--NeedCopy-->
```

  Configurez la machine pour l'authentification Kerberos et **Samba** :

```
sudo authselect select sssd with-mkhomedir --force
<!--NeedCopy-->
```

  Ouvrez **/etc/krb5.conf** et ajoutez les entrées sous les sections [realms] et [domain_realm].

  Dans la section [realms] :

```
REALM = {
kdc = fqdn-of-domain-controller
}
```

  Dans la section [domain_realm] :

```
realm = REALM
.realm = REALM
```

  Rejoignez le domaine Windows. Assurez-vous que votre contrôleur de domaine est accessible et que vous disposez d'un compte utilisateur Active Directory avec les autorisations nécessaires pour ajouter des ordinateurs au domaine.

```
sudo realm join REALM -U user
<!--NeedCopy-->
```

  REALM est le nom de domaine Kerberos en majuscules, et **user** est un utilisateur de domaine disposant des autorisations nécessaires pour ajouter les ordinateurs au domaine.

Configurer SSSD La configuration de SSSD comprend les étapes suivantes :

- Installez le package **sssd-ad** sur le Linux VDA en exécutant la commande `sudo yum -y install sssd`.
- Apportez des modifications de configuration à plusieurs fichiers (par exemple, sssd.conf).
- Démarrez le service **sssd**.

Exemple de configuration **sssd.conf** pour RHEL 7 (des options supplémentaires peuvent être ajoutées si nécessaire) :

```
[sssd]
config_file_version = 2
domains = ad.example.com
services = nss, pam

[domain/ad.example.com]
# Uncomment if you need offline logins
# cache_credentials = true

id_provider = ad
auth_provider = ad
access_provider = ad
ldap_id_mapping = true
ldap_schema = ad

# Should be specified as the lower-case version of the long version of the Active Directory domain.
ad_domain = ad.example.com

# Kerberos settings
krb5_ccachedir = /tmp
krb5_ccname_template = FILE:%d/krb5cc_%U

# Uncomment if service discovery is not working
# ad_server = server.ad.example.com

# Comment out if the users have the shell and home dir set on the AD side
default_shell = /bin/bash
fallback_homedir = /home/%d/%u

# Uncomment and adjust if the default principal SHORTNAME$@REALM is not available
# ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
```

Remplacez **ad.example.com**, **server.ad.example.com** par les valeurs correspondantes. Pour plus de détails, reportez-vous à la page sssd-ad(5) - Linux man.

(RHEL 8 uniquement)
Ouvrez **/etc/sssd/sssd.conf** et ajoutez les entrées suivantes dans la section domain/ad.example.com :

```
ad_gpo_access_control = permissive
full_name_format = %2$s\\%1$s
fallback_homedir = /home/%d/%u
# Kerberos settings
krb5_ccachedir = /tmp
krb5_ccname_template = FILE:%d/krb5cc_%U
```

Définissez les autorisations et les propriétaires de fichier sur sssd.conf :

```
chown root:root /etc/sssd/sssd.conf
chmod 0600 /etc/sssd/sssd.conf
restorecon /etc/sssd/sssd.conf
```


Activer SSSD **Pour RHEL 8 et Rocky Linux 8 :**

Exécutez les commandes suivantes pour activer SSSD :

```
sudo systemctl restart sssd
sudo systemctl enable sssd.service
sudo chkconfig sssd on
<!--NeedCopy-->
```

Pour Amazon Linux 2, CentOS 7 et RHEL 7 :

Utilisez **authconfig** pour activer SSSD. Installez **oddjob-mkhomedir** pour vous assurer que la création du répertoire de base est compatible avec SELinux :

```
authconfig --enablesssd --enablesssdauth --enablemkhomedir --update

sudo service sssd start

sudo chkconfig sssd on
<!--NeedCopy-->
```

Vérifier la configuration de Kerberos Vérifiez que le fichier **keytab** système a été créé et qu'il contient des clés valides :

```
sudo klist -ke
<!--NeedCopy-->
```

Cette commande affiche la liste des clés disponibles pour les différentes combinaisons de noms principaux et de suites de chiffrement. Exécutez la commande **kinit** Kerberos pour authentifier la machine auprès du contrôleur de domaine à l'aide de ces clés :

```
sudo kinit  – k MACHINE$@REALM
<!--NeedCopy-->
```

Les noms de machine et de domaine doivent être spécifiés en majuscules. Le signe dollar (**$**) doit être placé dans une séquence d'échappement avec une barre oblique inverse (****) pour empêcher le remplacement shell. Dans certains environnements, le nom de domaine DNS est différent du nom de domaine Kerberos. Assurez-vous que le nom de domaine est utilisé. Si cette commande réussit, aucun résultat n'est affiché.

Vérifiez que le ticket TGT pour le compte de machine a été mis en cache à l'aide de :

```
sudo klist
<!--NeedCopy-->
```

Vérifier l'authentification utilisateur Utilisez la commande **getent** pour vérifier que le format d'ouverture de session est pris en charge et que NSS fonctionne :


```
sudo getent passwd DOMAIN\username
<!--NeedCopy-->
```

Le paramètre **DOMAIN** indique la version courte du nom de domaine. Si un autre format d'ouverture de session est nécessaire, vérifiez en utilisant d'abord la commande **getent**.

Les formats d'ouverture de session pris en charge sont :

- Nom d'ouverture de session de niveau inférieur : `DOMAIN\username`
- Nom d'utilisateur principal (UPN) : `username@domain.com`
- Format du suffixe NetBIOS : `username@DOMAIN`

Pour vérifier que le module PAM SSSD est correctement configuré, ouvrez une session sur le Linux VDA à l'aide d'un compte d'utilisateur de domaine qui n'a jamais été utilisé.

```
sudo ssh localhost  – l DOMAIN\username

id -u
<!--NeedCopy-->
```

Vérifiez qu'un fichier cache d'identification Kerberos correspondant a été créé pour le **UID** renvoyé par la commande :

```
ls /tmp/krb5cc_{
 uid }

<!--NeedCopy-->
```

Vérifiez que les tickets dans le cache d'identification Kerberos de l'utilisateur sont valides et n'ont pas expiré.

```
klist
<!--NeedCopy-->
```

Passez à l'étape 6 : installer le Linux VDA après vérification de la jonction du domaine.

PBIS

Télécharger le package PBIS requis

```
wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/
   pbis-open-9.1.0.551.linux.x86_64.rpm.sh
<!--NeedCopy-->
```

Rendre le script d'installation PBIS exécutable

```
chmod +x pbis-open-9.1.0.551.linux.x86_64.rpm.sh
<!--NeedCopy-->
```


Exécuter le script d'installation PBIS

```
sh pbis-open-9.1.0.551.linux.x86_64.rpm.sh
<!--NeedCopy-->
```

Rejoindre un domaine Windows Votre contrôleur de domaine doit être accessible et vous devez disposer d'un compte utilisateur Active Directory avec les autorisations nécessaires pour ajouter des ordinateurs au domaine :

```
/opt/pbis/bin/domainjoin-cli join domain-name user
<!--NeedCopy-->
```

L'**utilisateur** est un utilisateur de domaine disposant des autorisations nécessaires pour ajouter des ordinateurs au domaine Active Directory. Le paramètre **domain-name** est le nom DNS du domaine ; par exemple, exemple.com.

Remarque : pour définir Bash en tant que shell par défaut, exécutez la commande **/opt/pbis/bin/-config LoginShellTemplate/bin/bash**.

Vérifier l'appartenance à un domaine Le Delivery Controller requiert que toutes les machines VDA (VDA Windows et Linux) aient un objet ordinateur dans Active Directory. Pour vérifier qu'une machine Linux associée à PBIS se trouve sur le domaine :

```
/opt/pbis/bin/domainjoin-cli query
<!--NeedCopy-->
```

Si la machine est associée à un domaine, cette commande renvoie les informations sur le domaine AD et l'unité d'organisation auxquels la machine est actuellement associée. Sinon, seul le nom d'hôte apparaît.

Vérifier l'authentification utilisateur Pour vérifier que PBIS peut authentifier les utilisateurs de domaine via PAM, ouvrez une session sur le Linux VDA à l'aide d'un compte d'utilisateur de domaine qui n'a jamais été utilisé.

```
ssh localhost -l domain\user

id -u
<!--NeedCopy-->
```

Vérifiez qu'un fichier cache d'identification Kerberos correspondant a été créé pour le UID renvoyé par la commande **id -u** :

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Quittez la session.


```
exit
<!--NeedCopy-->
```

Passez à l'étape 6 : installer le Linux VDA après vérification de la jonction du domaine.

Étape 4 : installer .NET Runtime 6.0 en tant que condition préalable

Avant d'installer Linux VDA, installez .NET Runtime 6.0 conformément aux instructions de l'article https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

Après avoir installé .NET Runtime 6.0, exécutez la commande **which dotnet** pour trouver votre chemin d'exécution.

En fonction de la sortie de la commande, définissez le chemin binaire de .NET Runtime. Par exemple, si la sortie de la commande est /aa/bb/dotnet, utilisez /aa/bb comme chemin binaire .NET.

Étape 5 : télécharger le package Linux VDA

1. Accédez à la page de téléchargement de Citrix Virtual Apps and Desktops.
2. Développez la version appropriée de Citrix Virtual Apps and Desktops.
3. Cliquez sur **Composants** pour télécharger le package Linux VDA qui correspond à votre distribution Linux et la clé publique GPG que vous pouvez utiliser pour vérifier l'intégrité du package Linux VDA.

   Pour vérifier l'intégrité du package Linux VDA, importez la clé publique dans la base de données RPM et exécutez les commandes suivantes :

   ```
   ```
   rpmkeys --import <path to the public key>
   rpm --checksig --verbose <path to the Linux VDA package>
   <!--NeedCopy--> ```
   ```

### Étape 6 : installer le Linux VDA

Vous pouvez effectuer une nouvelle installation ou effectuer une mise à niveau d'une installation existante à partir des deux versions précédentes et d'une version LTSR.

#### Pour effectuer une nouvelle installation

1. (Facultatif) Désinstaller l'ancienne version

 
   ```

Si vous avez installé une version antérieure autre que les deux précédentes et une version LTSR, désinstallez-la avant d'installer la nouvelle version.

a) Arrêtez les services Linux VDA :

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
<!--NeedCopy-->
```

> **Remarque :**
>
> Avant d'arrêter les services `ctxvda` et `ctxhdx`, exécutez la commande **service ctx-monitorservice stop** pour arrêter le démon du service de surveillance. Sinon, le démon du service de surveillance redémarre les services que vous avez arrêtés.

b) Désinstallez le package :

```
sudo rpm -e XenDesktopVDA
<!--NeedCopy-->
```

> **Remarque :**
>
> Pour exécuter une commande, le chemin d'accès complet est nécessaire ; vous pouvez ajouter **/opt/Citrix/VDA/sbin** et **/opt/Citrix/VDA/bin** au chemin du système.

2. Télécharger le package Linux VDA

   Accédez à la page de téléchargement de Citrix Virtual Apps and Desktops. Développez la version appropriée de Citrix Virtual Apps and Desktops et cliquez sur **Composants** pour télécharger le package Linux VDA correspondant à votre distribution Linux.

3. Installer le Linux VDA

   > **Remarque :**
   >
   > Pour RHEL et CentOS, vous devez installer le référentiel EPEL avant de pouvoir installer le Linux VDA. Pour plus d'informations sur l'installation d'EPEL, consultez les instructions sur https://docs.fedoraproject.org/en-US/epel/.

   - Installez le logiciel Linux VDA à l'aide de `Yum` :

     Pour Amazon Linux 2 :

     ```
     sudo yum install -y XenDesktopVDA-<version>.amzn2.x86_64.rpm
     <!--NeedCopy-->
     ```

     Pour RHEL 8 et Rocky Linux 8 :


```
sudo yum install -y XenDesktopVDA-<version>.el8_x.x86_64.rpm
<!--NeedCopy-->
```

Pour CentOS 7 et RHEL 7 :

```
sudo yum install -y XenDesktopVDA-<version>.el7_x.x86_64.rpm
<!--NeedCopy-->
```

- Installez le logiciel Linux VDA à l'aide du gestionnaire de package RPM. Avant de procéder, vous devez résoudre les dépendances suivantes :

Pour Amazon Linux 2 :

```
sudo rpm -i XenDesktopVDA-<version>.amzn2.x86_64.rpm
<!--NeedCopy-->
```

Pour RHEL 8 et Rocky Linux 8 :

```
sudo rpm -i XenDesktopVDA-<version>.el8_x.x86_64.rpm
<!--NeedCopy-->
```

Pour CentOS 7 et RHEL 7 :

```
sudo rpm -i XenDesktopVDA-<version>.el7_x.x86_64.rpm
<!--NeedCopy-->
```

Liste des dépendances RPM pour RHEL 8 et Rocky Linux 8 :

```
postgresql-server >= 10.5

postgresql-jdbc >= 42.2.3

java-11-openjdk >= 11

icoutils >= 0.32

firewalld >= 0.6.3

policycoreutils-python >= 2.8.9

policycoreutils-python-utils >= 2.8

python3-policycoreutils >= 2.8

dbus >= 1.12.8

dbus-common >= 1.12.8

dbus-daemon >= 1.12.8

dbus-tools >= 1.12.8

```



```
dbus-x11 >= 1.12.8

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.4

libXpm >= 3.5.12

libXrandr >= 1.5.1

libXtst >= 1.2.3

pam >= 1.3.1

util-linux >= 2.32.1

util-linux-user >= 2.32.1

xorg-x11-utils >= 7.5

bash >= 4.3

findutils >= 4.6

gawk >= 4.2

sed >= 4.5

cups >= 1.6.0

foomatic-filters >= 4.0.9

cups-filters >= 1.20.0

ghostscript >= 9.25

libxml2 >= 2.9

libmspack >= 0.7

krb5-workstation >= 1.13

ibus >= 1.5

nss-tools >= 3.44.0

gperftools-libs >= 2.4

cyrus-sasl-gssapi >= 2.1

python3 >= 3.6~

qt5-qtbase >= 5.5~
```



```
78
79  qt5-qtbase-gui >= 5.5~
80
81  qrencode-libs >= 3.4.4
82
83  imlib2 >= 1.4.9
84  <!--NeedCopy-->
```

Liste des dépendances RPM pour CentOS 7 et RHEL 7 :

```
1   postgresql-server >= 9.2
2
3   postgresql-jdbc >= 9.2
4
5   java-11-openjdk >= 11
6
7   ImageMagick >= 6.7.8.9
8
9   firewalld >= 0.3.9
10
11  policycoreutils-python >= 2.0.83
12
13  dbus >= 1.6.12
14
15  dbus-x11 >= 1.6.12
16
17  xorg-x11-server-utils >= 7.7
18
19  xorg-x11-xinit >= 1.3.2
20
21  xorg-x11-server-Xorg >= 1.20.4
22
23  libXpm >= 3.5.10
24
25  libXrandr >= 1.4.1
26
27  libXtst >= 1.2.2
28
29  pam >= 1.1.8
30
31  util-linux >= 2.23.2
32
33  bash >= 4.2
34
35  findutils >= 4.5
36
37  gawk >= 4.0
38
39  sed >= 4.2
40
41  cups >= 1.6.0
42
43  foomatic-filters >= 4.0.9
```



```
libxml2 >= 2.9

libmspack >= 0.5

ibus >= 1.5

cyrus-sasl-gssapi >= 2.1

python3 >= 3.6~

gperftools-libs >= 2.4

nss-tools >= 3.44.0

qt5-qtbase >= 5.5~

qt5-qtbase >= 5.5~

imlib2 >= 1.4.5
<!--NeedCopy-->
```

Liste des dépendances RPM pour Amazon Linux 2 :

```
postgresql-server >= 9.2

postgresql-jdbc >= 9.2

java-11-openjdk >= 11

ImageMagick >= 6.7.8.9

firewalld >= 0.3.9

policycoreutils-python >= 2.0.83

dbus >= 1.6.12

dbus-x11 >= 1.6.12

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.2

xorg-x11-server-Xorg >= 1.20.4

libXpm >= 3.5.10

libXrandr >= 1.4.1

libXtst >= 1.2.2

pam >= 1.1.8
```



```
30
31  util-linux >= 2.23.2
32
33  bash >= 4.2
34
35  findutils >= 4.5
36
37  gawk >= 4.0
38
39  sed >= 4.2
40
41  cups >= 1.6.0
42
43  foomatic-filters >= 4.0.9
44
45  libxml2 >= 2.9
46
47  libmspack >= 0.5
48
49  ibus >= 1.5
50
51  cyrus-sasl-gssapi >= 2.1
52
53  gperftools-libs >= 2.4
54
55  nss-tools >= 3.44.0
56
57  qt5-qtbase >= 5.5~
58
59  qrencode-libs >= 3.4.1
60
61  imlib2 >= 1.4.5
62  <!--NeedCopy-->
```

> **Remarque :**
>
> Pour une matrice des distributions Linux et des versions Xorg que cette version du VDA Linux prend en charge, consultez la section Configuration système requise.
>
> Après avoir installé le Linux VDA sur RHEL 7.x, exécutez la commande `sudo yum install -y python-websockify x11vnc`. Le but est d'installer `python-websockify` et `x11vnc` manuellement pour utiliser la fonctionnalité d'observation de session. Pour plus d'informations, consultez la section Observer des sessions.

Pour effectuer une mise à niveau d'une installation existante

Vous pouvez effectuer une mise à niveau d'une installation existante à partir des deux versions précédentes et d'une version LTSR.

Remarque :

La mise à niveau d'une installation existante remplace les fichiers de configuration sous /etc/xdl. Avant de procéder à une mise à niveau, assurez-vous de sauvegarder les fichiers.

- Pour effectuer une mise à niveau de votre logiciel à l'aide de `Yum` :

  Pour Amazon Linux 2 :

  ```
  sudo yum install -y XenDesktopVDA-<version>.amzn2.x86_64.rpm
  <!--NeedCopy-->
  ```

  Pour RHEL 8 et Rocky Linux 8 :

  ```
  sudo yum install -y XenDesktopVDA-<version>.el8_x.x86_64.rpm
  <!--NeedCopy-->
  ```

  Pour CentOS 7 et RHEL 7 :

  ```
  sudo yum install -y XenDesktopVDA-<version>.el7_x.x86_64.rpm
  <!--NeedCopy-->
  ```

- Pour effectuer une mise à niveau de votre logiciel à l'aide du gestionnaire de package RPM :

  Pour Amazon Linux 2 :

  ```
  sudo rpm -U XenDesktopVDA-<version>.amzn2.x86_64.rpm
  <!--NeedCopy-->
  ```

  Pour RHEL 8 :

  ```
  sudo rpm -U XenDesktopVDA-<version>.el8_x.x86_64.rpm
  <!--NeedCopy-->
  ```

  Pour CentOS 7 et RHEL 7 :

  ```
  sudo rpm -U XenDesktopVDA-<version>.el7_x.x86_64.rpm
  <!--NeedCopy-->
  ```

Remarque :

Si vous utilisez RHEL 7, assurez-vous de suivre les étapes suivantes après avoir exécuté les commandes de mise à niveau précédentes :

1. Exécutez `/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent"-t "REG_SZ"-v "DotNetRuntimePath"-d "/opt/rh/rh-dotnet31/root/usr/bin/"--force` pour définir le bon chemin d'exécution .NET.
2. Redémarrez le service `ctxvda`.

> **Important :**
>
> Redémarrez la machine Linux VDA après la mise à niveau du logiciel.

Étape 7 : installer les pilotes NVIDIA GRID

Pour activer HDX 3D Pro, vous devez installer les pilotes NVIDIA GRID sur votre hyperviseur et sur les machines VDA.

> **Remarque :**
>
> Pour utiliser HDX 3D Pro pour Amazon Linux 2, nous vous recommandons d'installer le pilote NVIDIA 470. Pour plus d'informations, consultez la section Configuration système requise.

Pour installer et configurer le gestionnaire de GPU virtuel NVIDIA GRID (pilote hôte) sur les hyperviseurs spécifiques, consultez les guides suivants :

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

Pour installer et configurer les pilotes de VM invitée NVIDIA GRID, effectuez les opérations suivantes :

1. Assurez-vous que la VM invitée est arrêtée.
2. Dans XenCenter, attribuez un GPU à la VM.
3. Démarrez la VM.
4. Préparez la VM pour le pilote NVIDIA GRID :

```
yum install gcc

yum install "kernel-devel-$(uname -r)"

systemctl set-default multi-user.target
<!--NeedCopy-->
```

5. Suivez les étapes décrites dans le document Red Hat Enterprise Linux pour installer les pilotes NVIDIA GRID.

> **Remarque :**
>
> Pendant l'installation du pilote GPU, sélectionnez la valeur par défaut (no) pour chaque question.
>
> **Important :**

> Une fois la fonctionnalité GPU pass-through activée, la VM Linux n'est plus accessible via XenCenter. Utilisez SSH pour vous connecter.

```
nvidia-smi
```

```
+-----------------------------------------------------+
| NVIDIA-SMI 352.70     Driver Version: 352.70        |
|-------------------------------+----------------------+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|===============================+======================+======================|
|   0  Tesla M60           Off  | 0000:00:05.0     Off |                  Off |
| N/A   20C    P0    37W / 150W |     19MiB /  8191MiB |      0%      Default |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                       GPU Memory |
|  GPU       PID  Type  Process name                               Usage      |
|=============================================================================|
|  No running processes found                                                 |
+-----------------------------------------------------------------------------+
```

Définissez la configuration correcte pour la carte :

`etc/X11/ctx-nvidia.sh`

Pour bénéficier des résolutions élevées et des capacités multi-écrans, vous avez besoin d'une licence NVIDIA valide. Pour appliquer la licence, suivez les instructions de la documentation du produit, « GRID Licensing Guide.pdf - DU-07757-001 Septembre 2015 ».

Étape 8 : configurer le Linux VDA

Après l'installation du package, vous devez configurer le Linux VDA en exécutant le script ctxsetup.sh. Avant d'apporter des modifications, le script vérifie l'environnement et s'assure que toutes les dépendances sont installées. Si nécessaire, vous pouvez exécuter le script à tout moment pour modifier les paramètres.

Vous pouvez exécuter le script manuellement avec invite, ou automatiquement avec réponses préconfigurées. Consultez l'aide sur le script avant de continuer :

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
<!--NeedCopy-->
```

Configuration avec invites

Exécutez une configuration manuelle avec questions :


```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

Configuration automatique

Pour une installation automatique, fournissez les options requises par le script d'installation avec des variables d'environnement. Si toutes les variables requises sont présentes, le script n'invite pas à entrer des informations.

Les variables d'environnement prises en charge sont les suivantes :

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N** : le Linux VDA prend en charge la spécification d'un nom de Delivery Controller à l'aide d'un enregistrement DNS CNAME. La valeur est définie par défaut sur N.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** : le Linux VDA requiert une liste séparée par des espaces de noms de domaines complets de Delivery Controller. Cette dernière sera utilisée pour l'enregistrement auprès d'un Delivery Controller. Au moins un alias de nom de domaine complet (FQDN) ou CNAME doit être spécifié.
- **CTX_XDL_VDA_PORT = port-number** : le Linux VDA communique avec les Delivery Controller à l'aide d'un port (80 par défaut) TCP/IP.
- **CTX_XDL_REGISTER_SERVICE = Y | N** : les services Linux VDA sont lancés après le démarrage de la machine. La valeur est définie sur Y par défaut.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** : les services Linux VDA requièrent que les connexions réseau entrantes soient autorisées via le pare-feu du système. Vous pouvez ouvrir automatiquement les ports requis (ports 80 et 1494 par défaut) dans le pare-feu du système pour Linux Virtual Desktop. Valeur définie sur Y par défaut.
- **CTX_XDL_AD_INTEGRATION = 1 | 2 | 3 | 4 |5** : le Linux VDA requiert que les paramètres de configuration Kerberos s'authentifient auprès des Delivery Controller. La configuration de Kerberos est déterminée depuis l'outil d'intégration d'Active Directory installé et configuré sur le système. Spécifiez la méthode d'intégration d'Active Directory prise en charge à utiliser :
  - 1 –Samba Winbind
  - 2 –Quest Authentication Services
  - 3 –Centrify DirectControl
  - 4 –SSSD
  - 5 –PBIS
- **CTX_XDL_HDX_3D_PRO=Y | N** : Linux VDA prend en charge HDX 3D Pro, un ensemble de technologies d'accélération GPU conçues pour optimiser la virtualisation des applications riches en

graphiques. Si HDX 3D Pro est sélectionné, le Virtual Delivery Agent doit être configuré pour le mode Bureaux VDI (session unique), c'est-à-dire, CTX_XDL_VDI_MODE=Y.

- **CTX_XDL_VDI_MODE=Y | N** : indique si la machine est configurée comme modèle de mise à disposition de bureaux dédiés (VDI) ou comme modèle de mise à disposition de bureaux partagés hébergés. Pour les environnements HDX 3D Pro, définissez cette variable sur Y. Elle est définie par défaut sur N.
- **CTX_XDL_SITE_NAME=dns-name** : le Linux VDA découvre les serveurs LDAP à l'aide de DNS. Pour limiter les résultats de recherche DNS à un site local, spécifiez un nom de site DNS. Cette variable est définie sur **<none>** par défaut.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** : le Linux VDA envoie une requête vers le DNS pour découvrir les serveurs LDAP. Si DNS ne peut pas fournir d'enregistrements de service LDAP, vous pouvez entrer une liste séparée par des espaces de noms de domaines complets LDAP avec ports LDAP. Par exemple, ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268. Si vous spécifiez le numéro de port LDAP 389, le Linux VDA interroge chaque serveur LDAP du domaine spécifié en mode d'interrogation. S'il existe un nombre x de stratégies et y de serveurs LDAP, le Linux VDA effectue le total de X multiplié par Y requêtes. Si le temps d'interrogation dépasse le seuil, les ouvertures de session peuvent échouer. Pour activer les requêtes LDAP plus rapides, activez le **catalogue global** sur un contrôleur de domaine et définissez le numéro de port LDAP correspondant sur 3268. Cette variable est définie sur **<none>** par défaut.
- **CTX_XDL_SEARCH_BASE=search-base-set** : le Linux VDA envoie une requête à LDAP via une base de recherche définie sur la racine du domaine Active Directory (par exemple, D, DC=mycompany,DC=com). Pour améliorer les performances de recherche, vous pouvez spécifier une base de recherche (par exemple, OU=VDI,DC=mycompany,DC=com). Cette variable est définie sur **<none>** par défaut.
- **CTX_XDL_FAS_LIST='list-fas-servers'** : les serveurs du service d'authentification fédérée (FAS) sont configurés via la stratégie de groupe AD. Le Linux VDA ne prend pas en charge la stratégie de groupe AD mais vous pouvez fournir une liste de serveurs FAS séparés par des points-virgules. La séquence doit être la même que celle configurée dans la stratégie de groupe AD. Si une adresse de serveur est supprimée, remplissez son espace vide avec la chaîne de texte **<none>** et ne modifiez pas l'ordre des adresses de serveur. Pour communiquer correctement avec les serveurs FAS, assurez-vous d'ajouter un numéro de port conforme à celui spécifié sur les serveurs FAS, par exemple CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'.
- **CTX_XDL_DOTNET_ runtime_path=Path-to-install-dotnet-runtime** : chemin d'accès à l'installation de .NET Runtime 6.0 pour la prise en charge du nouveau Broker Agent Service (`ctxvda`). Le chemin par défaut est /usr/bin.

- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate** : spécifie l'environnement de bureau GNOME, GNOME Classic ou MATE à utiliser dans les sessions. Si vous ne spécifiez pas la variable, le bureau actuellement installé sur le VDA est utilisé. Toutefois, si le bureau actuellement installé est MATE, vous devez définir la valeur de la variable sur **mate**.

  Vous pouvez également modifier l'environnement de bureau d'un utilisateur de session cible en procédant comme suit :

  1. Créez un fichier `.xsession` ou `.Xclients` sous le répertoire **$HOME/<username>** sur le VDA. Si vous utilisez Amazon Linux 2, créez un fichier `.Xclients`. Si vous utilisez d'autres distributions, créez un fichier `.xsession`.
  2. Modifiez le fichier `.xsession` ou `.Xclients` pour spécifier un environnement de bureau.
     - **Pour le bureau MATE**

     ```
     MSESSION="$(type -p mate-session)"
     if [ -n "$MSESSION" ]; then
       exec mate-session
     fi
     ```

     - **Pour le bureau GNOME Classic**

     ```
     GSESSION="$(type -p gnome-session)"
     if [ -n "$GSESSION" ]; then
     export GNOME_SHELL_SESSION_MODE=classic
     exec gnome-session --session=gnome-classic
     fi
     ```

     - **Pour le bureau GNOME**

     ```
     GSESSION="$(type -p gnome-session)"
     if [ -n "$GSESSION" ]; then
     exec gnome-session
     fi
     ```

  3. Partagez l'autorisation de fichier 700 avec l'utilisateur de la session cible.

  À partir de la version 2209, les utilisateurs de session peuvent personnaliser leurs environnements de bureau. Pour activer cette fonctionnalité, vous devez installer au préalable des environnements de bureau commutables sur le VDA. Pour plus d'informations, consultez Environnements de bureau personnalisés par utilisateurs de session.

- **CTX_XDL_START_SERVICE = Y | N** : indique si les services Linux VDA sont lancés lorsque la configuration de Linux VDA est terminée. Valeur définie sur Y par défaut.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** : port socket permettant d'écouter Citrix Scout. Le port par défaut est 7503.

- **CTX_XDL_TELEMETRY_PORT** : port de communication avec Citrix Scout. Le port par défaut est 7502.

Définissez la variable d'environnement et exécutez le script de configuration :

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3|4|5

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-site-name | '<none>'

export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'

export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'

export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<
    none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

Lors de l'exécution de la commande sudo, entrez l'option **-E** pour transmettre les variables d'environnement au nouveau shell créé. Nous vous recommandons de créer un fichier de script shell à partir des commandes précédentes avec **#!/bin/bash** en tant que première ligne.

Vous pouvez également spécifier tous les paramètres avec une seule commande :

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST='list-ddc-fqdns' \

```



```
CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4|5 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

Supprimer les modifications de configuration

Dans certains scénarios, il peut être nécessaire de supprimer les modifications de configuration effectuées par le script **ctxsetup.sh** sans désinstaller le package Linux VDA.

Consultez l'aide sur ce script avant de continuer :

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
<!--NeedCopy-->
```

Pour supprimer les modifications de configuration :

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
<!--NeedCopy-->
```


> **Important :**
>
> Ce script supprime toutes les données de configuration de la base de données et empêche Linux VDA de fonctionner.

Journaux de configuration

Les scripts **ctxsetup.sh** et **ctxcleanup.sh** affichent les erreurs dans la console, avec des informations supplémentaires consignées dans le fichier journal de configuration **/tmp/xdl.configure.log**.

Redémarrez les services de Linux VDA pour que les modifications prennent effet.

Étape 9 : exécuter XDPing

Exécutez `sudo /opt/Citrix/VDA/bin/xdping` pour vérifier les problèmes de configuration courants avec un environnement VDA Linux. Pour de plus amples informations, consultez la section XDPing.

Étape 10 : exécuter le Linux VDA

Une fois que vous avez configuré Linux VDA à l'aide du script **ctxsetup.sh**, utilisez les commandes suivantes pour contrôler Linux VDA.

Démarrer Linux VDA :

Pour démarrer les services Linux VDA :

```
sudo /sbin/service ctxhdx start

sudo /sbin/service ctxvda start
<!--NeedCopy-->
```

Arrêter Linux VDA :

Pour arrêter les services Linux VDA :

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
<!--NeedCopy-->
```

> **Remarque :**
>
> Avant d'arrêter les services `ctxvda` et `ctxhdx`, exécutez la commande `service`

> `ctxmonitorservice stop` pour arrêter le démon du service de surveillance. Sinon, le démon du service de surveillance redémarre les services que vous avez arrêtés.

Redémarrer Linux VDA :

Pour redémarrer les services Linux VDA :

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx restart

sudo /sbin/service ctxvda start
<!--NeedCopy-->
```

Vérifier l'état de Linux VDA :

Pour vérifier l'état de fonctionnement des services de Linux VDA :

```
sudo /sbin/service ctxvda status

sudo /sbin/service ctxhdx status
<!--NeedCopy-->
```

Étape 11 : créer le catalogue de machines dans Citrix Virtual Apps ou Citrix Virtual Desktops

Le processus de création de catalogues de machines et d'ajout de machines Linux VDA est similaire à l'approche traditionnelle avec les VDA Windows. Pour obtenir une description plus détaillée de la méthode à utiliser pour effectuer ces tâches, consultez les sections Créer des catalogues de machines et Gérer des catalogues de machines.

Pour la création de catalogues de machines contenant des machines Linux VDA, il existe quelques restrictions qui différencient ce processus de la création de catalogues de machines pour VDA Windows :

- Pour le système d'exploitation, sélectionnez :
  - l'option **OS à sessions multiples** pour un modèle de mise à disposition de bureaux partagés hébergés ;
  - l'option **OS mono-session** pour un modèle de mise à disposition de bureaux dédiés VDI.
- Ne combinez pas de machines Linux VDA et Windows dans le même catalogue de machines.

> **Remarque :**
>
> Les versions antérieures de Citrix Studio ne prenaient pas en charge la notion de « système d'exploitation Linux. » Toutefois, la sélection de l'option **OS de serveur Windows** ou **OS de serveur**

> implique un modèle de mise à disposition équivalent de bureaux partagés hébergés. La sélection de l'option **OS de bureau Windows** ou **OS de bureau** implique un modèle de mise à disposition d'un utilisateur unique par machine.
>
> **Conseil :**
>
> Lorsque vous rejoignez une machine supprimée dans le domaine Active Directory, supprimez-la et ajoutez-la à nouveau à son catalogue de machines.

Étape 12 : créer le groupe de mise à disposition dans Citrix Virtual Apps ou Citrix Virtual Desktops

Le processus de création d'un groupe de mise à disposition et d'ajout de catalogues de machines contenant des machines Linux VDA est presque identique aux machines VDA Windows. Pour obtenir une description plus détaillée de la méthode à utiliser pour effectuer ces tâches, consultez la section Créer des groupes de mise à disposition.

Lors de la création de groupes de mise à disposition qui contiennent des catalogues de machines Linux VDA, les restrictions suivantes s'appliquent :

- Assurez-vous que les utilisateurs et les groupes AD que vous sélectionnez ont été correctement configurés pour l'ouverture de session sur les machines Linux VDA.
- N'autorisez pas l'ouverture de session d'utilisateurs non authentifiés (anonymes).
- Ne combinez pas le groupe de mise à disposition avec des catalogues de machines contenant des machines Windows.

> **Important :**
>
> La publication d'applications est prise en charge avec la version 1.4 de Linux VDA et les versions supérieures. Toutefois, le Linux VDA ne prend pas en charge la mise à disposition de bureaux et d'applications sur la même machine.

Pour plus d'informations sur la création de catalogues de machines et de groupes de mise à disposition, consultez Citrix Virtual Apps and Desktops 7 2209.

Installer manuellement Linux Virtual Delivery Agent pour SUSE

February 9, 2024

> **Important :**
>
> Pour les nouvelles installations, nous vous recommandons d'utiliser Easy Install pour effectuer une installation rapide. Easy Install permet de gagner du temps et d'économiser de la main d'œuvre. Cette installation est également plus fiable que l'installation manuelle décrite dans cet article.

Étape 1 : préparer l'installation

Étape 1 a : démarrer l'outil YaST

L'outil SUSE Linux Enterprise YaST est utilisé pour configurer tous les aspects du système d'exploitation.

Pour démarrer l'outil YaST basé sur texte :

```
su -

yast
<!--NeedCopy-->
```

Pour démarrer l'outil YaST basé sur l'interface utilisateur :

```
su -

yast2 &
<!--NeedCopy-->
```

Étape 1b : configurer le réseau

Les sections suivantes fournissent des informations sur la configuration des paramètres et services réseau utilisés par le Linux VDA. La configuration du réseau est effectuée par le biais de l'outil YaST, et non via d'autres méthodes, telles que le Gestionnaire de réseau. Ces instructions sont basées sur l'utilisation de l'outil YaST avec interface utilisateur. L'outil YaST basé sur texte peut être utilisé mais propose une autre méthode de navigation qui n'est pas abordée ici.

Configurer le nom d'hôte et le DNS (Domain Name System)

1. Démarrez l'outil YaST basé sur l'interface utilisateur.
2. Sélectionnez **System** (Système), puis **Network Settings** (Paramètres réseau).
3. Ouvrez l'onglet **Hostname/DNS** (Nom d'hôte/DNS).
4. Sélectionnez l'option **no** pour **Set hostname via DHCP** (Définir le nom d'hôte via DHCP).

5. Sélectionnez l'option **Use Custom Policy** (Utiliser une stratégie personnalisée) pour **Modify DNS Configuration** (Modifier la configuration DNS).
6. Modifiez les options suivantes pour refléter votre configuration réseau :
   - **Static Hostname** (Nom d'hôte statique) : ajoutez le nom d'hôte DNS de la machine.
   - **Name Server** (Nom du serveur) : entrez l'adresse IP du serveur DNS. Il s'agit généralement de l'adresse IP du contrôleur de domaine AD.
   - **Domain Search List** (Liste de recherche de domaine) : ajoutez le nom de domaine DNS.
7. Modifiez la ligne suivante du fichier `/etc/hosts` pour inclure le nom de domaine complet et le nom d'hôte en tant que deux premières entrées :

   ```
   127.0.0.1 <FQDN of the VDA> <hostname of the VDA> localhost
   ```

> **Remarque :**
>
> Le Linux VDA ne prend actuellement pas en charge la troncation de noms NetBIOS. Par conséquent, le nom d'hôte ne doit pas comporter plus de 15 caractères.
>
> **Conseil :**
>
> Utilisez uniquement les caractères a–z, A–Z, 0–9 et tiret (-). Évitez les caractères de soulignement (_), les espaces et autres symboles. Ne démarrez pas un nom d'hôte par un chiffre et ne le terminez pas par un tiret. Cette règle s'applique également aux noms d'hôte Delivery Controller.

Vérifier le nom d'hôte Vérifiez que le nom d'hôte est correctement configuré :

```
hostname
<!--NeedCopy-->
```

Cette commande renvoie uniquement le nom d'hôte de la machine et non son nom de domaine complet (FQDN).

Vérifiez que le nom de domaine complet est correctement configuré :

```
hostname -f
<!--NeedCopy-->
```

Cette commande renvoie le nom de domaine complet de la machine.

Vérifier la résolution de nom et l'accessibilité du service Vérifiez que vous pouvez résoudre le nom de domaine complet et effectuer un sondage ping sur le contrôleur de domaine et le Delivery Controller :

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn
```



```
4
5 nslookup delivery-controller-fqdn
6
7 ping delivery-controller-fqdn
8 <!--NeedCopy-->
```

Si vous ne pouvez pas résoudre le nom de domaine complet ou effectuer un sondage ping sur l'une de ces machines, reprenez les étapes avant de continuer.

Étape 1c : configurer le service NTP

Il est très important de maintenir la synchronisation de l'horloge entre les VDA, les Delivery Controller et les contrôleurs de domaine. L'hébergement du Linux VDA en tant que machine virtuelle peut entraîner des problèmes de décalage d'horloge. Pour cette raison, il est recommandé de synchroniser l'heure avec un service NTP à distance. Il peut être nécessaire d'apporter des modifications aux paramètres NTP par défaut.

Pour SUSE 15.3 :

1. Démarrez l'outil YaST basé sur l'interface utilisateur.
2. Sélectionnez **Network Services** (Services réseau), puis **NTP Configuration** (Configuration NTP).
3. Dans la section **Start NTP Daemon** (Lancer le démon NTP), sélectionnez **Now and on Boot** (Maintenant et au démarrage).
4. Sélectionnez **Dynamic** (Dynamique) pour **Configuration Source** (Source de configuration).
5. Ajoutez des serveurs NTP si nécessaire. Le service NTP est généralement hébergé sur le contrôleur de domaine Active Directory.
6. Supprimez ou commentez la ligne suivante dans /etc/chrony.conf, si elle existe.

   `include /etc/chrony.d/*.conf`

   Après avoir modifié chrony.conf, redémarrez le service `chronyd`.

   ```
   1 sudo systemctl restart chronyd.service
   2 <!--NeedCopy-->
   ```

Étape 1d : installer les packages dépendants de Linux VDA

Le logiciel Linux VDA pour SUSE Linux Enterprise fonctionne avec les packages suivants :

- Postgresql13-server 13 ou version ultérieure
- OpenJDK 11

- Open Motif Runtime Environment 2.3.1 ou version ultérieure
- Cups 1.6.0 ou version ultérieure
- ImageMagick 6.8 ou version ultérieure

Ajouter des référentiels Vous pouvez obtenir la plupart des packages requis à partir des référentiels officiels, à l'exception d'ImageMagick. Pour obtenir les packages ImageMagick, activez le référentiel `sle-module-desktop-applications` à l'aide de YaST ou de la commande suivante :

```
SUSEConnect -p sle-module-desktop-applications/<version number>/
x86_64
```

Installer le client Kerberos Installez le client Kerberos pour l'authentification mutuelle entre le Linux VDA et les Delivery Controller :

```
1 sudo zypper install krb5-client
2 <!--NeedCopy-->
```

La configuration du client Kerberos dépend de l'approche d'intégration d'Active Directory utilisée. Consultez la description ci-dessous.

Installer OpenJDK 11 Le Linux VDA nécessite la présence d'OpenJDK 11.

Pour installer OpenJDK 11, exécutez la commande suivante :

```
1 sudo zypper install java-11-openjdk
2 <!--NeedCopy-->
```

Installer PostgreSQL Pour installer `Postgresql`, exécutez les commandes suivantes :

```
1 sudo zypper install postgresql-server
2
3 sudo zypper install postgresql-jdbc
4 <!--NeedCopy-->
```

Les étapes de post-installation sont requises pour initialiser le service de base de données et s'assurer que PostgreSQL est lancé au démarrage de la machine.

```
1 sudo systemctl enable postgresql
2
3 sudo systemctl restart postgresql
4 <!--NeedCopy-->
```

Les fichiers de base de données se trouvent dans /var/lib/pgsql/data.

Étape 2 : préparer une VM Linux pour l'hyperviseur

Certaines modifications sont requises pour l'exécution du Linux VDA en tant que machine virtuelle sur un hyperviseur pris en charge. Apportez les modifications suivantes en fonction de la plateforme d'hyperviseur utilisée. Aucune modification n'est requise si vous utilisez la machine Linux sur un matériel bare metal.

Corriger la synchronisation de l'heure sur Citrix Hypervisor

Si la fonctionnalité de synchronisation de l'heure de Citrix Hypervisor est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée avec NTP et Citrix Hypervisor. En effet, les deux systèmes essaient de gérer l'horloge système. Pour éviter que l'horloge ne soit plus synchronisée avec d'autres serveurs, synchronisez l'horloge du système de chaque invité Linux avec NTP. Cela nécessite la désactivation de la synchronisation de l'heure de l'hôte. Aucune modification n'est requise en mode HVM.

Si vous utilisez un noyau Linux paravirtualisé avec le composant Citrix VM Tools installé, vous pouvez vérifier si la fonctionnalité de synchronisation de l'heure de Citrix Hypervisor est présente et activée à partir de la VM Linux :

```
su -

cat /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Cette commande renvoie 0 ou 1 :

- 0 - La fonctionnalité de synchronisation de l'heure est activée, et doit être désactivée.
- 1 - La fonctionnalité de synchronisation de l'heure est désactivée, et aucune action n'est requise.

Si le fichier **/proc/sys/xen/independent_wallclock** n'existe pas, les étapes suivantes ne sont pas nécessaires.

Si la fonctionnalité de synchronisation est activée, désactivez-la en entrant **1** dans le fichier :

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Pour rendre cette modification permanente et persistante après le redémarrage, modifiez le fichier **/etc/sysctl.conf** et ajoutez la ligne :

```
xen.independent_wallclock = 1
```

Pour vérifier ces modifications, redémarrez le système :


```
reboot
<!--NeedCopy-->
```

Après le redémarrage, vérifiez que le paramètre est correct :

```
su -

cat /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Cette commande renvoie la valeur 1.

Corriger la synchronisation de l'heure sur Microsoft Hyper-V

Les VM Linux sur lesquelles Hyper-V Integration Services est installé peuvent appliquer la fonctionnalité de synchronisation de l'heure Hyper-V pour utiliser l'heure du système d'exploitation hôte. Pour vous assurer que l'horloge du système est toujours précise, activez cette fonctionnalité avec les services NTP.

Depuis le système d'exploitation de gestion :

1. Ouvrez la console du gestionnaire Hyper-V.
2. Pour les paramètres d'une machine virtuelle Linux, sélectionnez **Integration Services**.
3. Assurez-vous que **Time synchronization** est sélectionné.

> **Remarque :**
>
> Cette approche diffère de VMware et Citrix Hypervisor, pour lesquels la synchronisation de l'heure est désactivée pour éviter tout conflit avec NTP. La synchronisation de l'heure Hyper-V peut co-exister avec la synchronisation de l'heure NTP.

Corriger la synchronisation de l'heure sur ESX et ESXi

Si la fonctionnalité de synchronisation de l'heure de VMware est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée avec l'hyperviseur et NTP. En effet, les deux systèmes essaient de synchroniser l'horloge système. Pour éviter que l'horloge ne soit plus synchronisée avec d'autres serveurs, synchronisez l'horloge du système de chaque invité Linux avec NTP. Cela nécessite la désactivation de la synchronisation de l'heure de l'hôte.

Si vous exécutez un noyau Linux paravirtualisé sur lequel VMware Tools est installé :

1. Ouvrez vSphere Client.
2. Modifiez les paramètres pour la VM Linux.

3. Dans la boîte de dialogue **Virtual Machine Properties** (Propriétés de la machine virtuelle), ouvrez l'onglet **Options**.
4. Sélectionnez **VMware Tools**.
5. Dans la zone **Advanced** (Avancé), désélectionnez **Synchronize guest time with host** (Synchroniser l'heure de l'invité avec l'hôte).

Étape 3 : ajouter la machine virtuelle (VM) Linux au domaine Windows

Le Linux VDA prend en charge plusieurs méthodes pour ajouter des machines Linux au domaine Active Directory (AD) :

- Samba Winbind
- Quest Authentication Service
- Centrify DirectControl
- SSSD
- PBIS

Suivez les instructions en fonction de la méthode choisie.

> **Remarque :**
>
> Les lancements de session peuvent échouer lorsque le même nom d'utilisateur est utilisé pour le compte local dans le Linux VDA et le compte dans AD.

Samba Winbind

Rejoindre un domaine Windows Votre contrôleur de domaine doit être accessible et vous devez disposer d'un compte utilisateur Active Directory avec les autorisations nécessaires pour ajouter des machines au domaine :

1. Lancez YaST, sélectionnez **Network Services** (Services réseau), puis **Windows Domain Membership** (Appartenance au domaine Windows).
2. Apportez les modifications suivantes :
    - Définissez le **domaine (Domain) ou le groupe de travail (Workgroup)** sur le nom de votre domaine Active Directory ou l'adresse IP du contrôleur de domaine. Assurez-vous que le nom du domaine est entré en majuscules.
    - Sélectionnez **Use SMB information for Linux Authentication** (Utiliser les informations SMB pour l'authentification Linux).
        - Sélectionnez **Create Home Directory on Login** (Créer un répertoire de base à la connexion).
        - Sélectionnez **Single Sign-on for SSH** (Authentification unique pour SSH).

- Assurez-vous que **Offline Authentification** (Authentification en mode déconnecté) n'est pas sélectionné. Cette option n'est pas compatible avec le Linux VDA.

3. Cliquez sur **OK**. Si vous êtes invité(e) à installer des packages, cliquez sur **Install**.
4. Si un contrôleur de domaine est trouvé, vous êtes invité à joindre le domaine. Cliquez sur **Oui**.
5. Lorsque vous y êtes invité(e), saisissez les informations d'identification d'un utilisateur de domaine avec les autorisations nécessaires pour ajouter des machines au domaine, et cliquez sur **OK**.
6. Redémarrez vos services manuellement ou redémarrez la machine. Nous vous recommandons de redémarrer la machine :

```
su -
reboot
<!--NeedCopy-->
```

Vérifier l'appartenance à un domaine Le Delivery Controller requiert que toutes les machines VDA (VDA Windows et Linux) aient un objet ordinateur dans Active Directory.

Exécutez la commande **net ads** de **Samba** pour vérifier que la machine est associée à un domaine :

```
sudo net ads testjoin
<!--NeedCopy-->
```

Exécutez la commande suivante pour vérifier les informations d'objet de domaine et d'ordinateur supplémentaires :

```
sudo net ads info
<!--NeedCopy-->
```

Vérifier la configuration de Kerberos Vérifiez que le fichier keytab système a été créé et qu'il contient des clés valides.

```
sudo klist -ke
<!--NeedCopy-->
```

Cette commande affiche la liste des clés disponibles pour les différentes combinaisons de noms principaux et de suites de chiffrement. Exécutez la commande `kinit` Kerberos pour authentifier la machine auprès du contrôleur de domaine à l'aide de ces clés :

```
sudo kinit -k MACHINE$@REALM
<!--NeedCopy-->
```

Les noms de machine et de domaine doivent être spécifiés en majuscules. Le signe dollar ($) doit être placé dans une séquence d'échappement avec une barre oblique inverse (\) pour empêcher le

remplacement shell. Dans certains environnements, le nom de domaine DNS est différent du nom de domaine Kerberos. Assurez-vous que le nom de domaine est utilisé. Si cette commande réussit, aucun résultat n'est affiché.

Vérifiez que le ticket TGT pour le compte de machine a été mis en cache à l'aide de :

```
sudo klist
<!--NeedCopy-->
```

Examinez les détails du compte de machine à l'aide de :

```
sudo net ads status
<!--NeedCopy-->
```

Vérifier l'authentification utilisateur Utilisez l'outil **wbinfo** pour vérifier que les utilisateurs de domaine peuvent s'authentifier auprès du domaine :

```
wbinfo --krb5auth=domain\username%password
<!--NeedCopy-->
```

Le domaine spécifié ici est le nom de domaine Active Directory, et non le nom de domaine Kerberos. Pour le shell bash, la barre oblique inverse (\) doit être placée dans une séquence d'échappement avec une autre barre oblique inverse. Cette commande renvoie un message indiquant la réussite ou l'échec.

Vérifiez que le module Winbind PAM est correctement configuré. Pour ce faire, connectez-vous au Linux VDA à l'aide d'un compte d'utilisateur de domaine qui n'a jamais été utilisé auparavant.

```
ssh localhost -l domain\username
id -u
<!--NeedCopy-->
```

Vérifiez qu'un fichier cache d'identification Kerberos correspondant a été créé pour le UID renvoyé par la commande **id -u** :

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Vérifiez que les tickets dans le cache d'identification Kerberos de l'utilisateur sont valides et n'ont pas expiré :

```
klist
<!--NeedCopy-->
```

Quittez la session.

```
exit
<!--NeedCopy-->
```


Le même test peut être réalisé en ouvrant une session directement sur la console KDE ou Gnome. Passez à l'étape 6 : installer le Linux VDA après vérification de la jonction du domaine.

Service d'authentification Quest

Configurer Quest sur le contrôleur de domaine Cette procédure suppose que vous avez installé et configuré le logiciel Quest sur les contrôleurs de domaine et disposez des droits Administrateur pour créer des objets ordinateur dans `Active Directory`.

Autoriser les utilisateurs de domaine à ouvrir une session sur des machines Linux VDA Pour autoriser les utilisateurs de domaine à établir des sessions HDX sur une machine Linux VDA :

1. Dans la console de gestion Utilisateurs et ordinateurs Active Directory, ouvrez les propriétés de l'utilisateur Active Directory pour ce compte d'utilisateur.
2. Sélectionnez l'onglet **Unix Account**.
3. Sélectionnez **Unix-enabled**.
4. Définissez **Primary GID Number** sur l'ID d'un groupe d'utilisateurs de domaine.

> **Remarque :**
>
> Ces instructions sont les mêmes que pour la configuration d'utilisateurs de domaine pour l'ouverture de session à l'aide de la console, RDP, SSH ou tout autre protocole de communication à distance.

Configurer Quest sur un Linux VDA

Configurer le démon VAS Le renouvellement automatique des tickets Kerberos doit être activé et déconnecté. L'authentification (ouverture de session en mode déconnecté) doit être désactivée :

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-
    interval 32400

sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-
    auth false
<!--NeedCopy-->
```

Cette commande définit l'intervalle de renouvellement sur 9 heures (32 400 secondes), ce qui représente une heure de moins que la valeur par défaut de 10 heures pour la durée de vie d'un ticket. Définissez ce paramètre sur une valeur inférieure sur les systèmes avec une durée de vie de ticket plus courte.

Configuration de PAM et de NSS Pour permettre les ouvertures de session d'utilisateur de domaine via HDX et d'autres services tels que su, ssh et RDP, configure manuellement PAM et NSS :

```
sudo /opt/quest/bin/vastool configure pam

sudo /opt/quest/bin/vastool configure nss
<!--NeedCopy-->
```

Rejoindre un domaine Windows Joignez la machine Linux au domaine Active Directory à l'aide de la commande Quest `vastool` :

```
sudo /opt/quest/bin/vastool -u user join domain-name
<!--NeedCopy-->
```

L'**utilisateur** est un utilisateur de domaine disposant des autorisations nécessaires pour joindre des machines au domaine Active Directory. Le paramètre **domain-name** est le nom DNS du domaine ; par exemple, exemple.com.

Vérifier l'appartenance à un domaine Le Delivery Controller requiert que toutes les machines VDA (VDA Windows et Linux) aient un objet ordinateur dans `Active Directory`. Pour vérifier qu'une machine Linux associée à Quest se trouve sur le domaine :

```
sudo /opt/quest/bin/vastool info domain
<!--NeedCopy-->
```

Si la machine est associée à un domaine, cette commande renvoie le nom de domaine. Si la machine n'est pas associée à un domaine, l'erreur suivante apparaît :

```
ERROR: No domain could be found.
ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm
default_realm not configured in vas.conf. Computer may not be joined
to domain
```

Vérifier l'authentification utilisateur Vérifiez que Quest peut authentifier les utilisateurs du domaine via PAM. Pour ce faire, connectez-vous au Linux VDA à l'aide d'un compte d'utilisateur de domaine qui n'a jamais été utilisé auparavant.

```
ssh localhost -l domain\username
id -u
<!--NeedCopy-->
```

Vérifiez qu'un fichier cache d'identification Kerberos correspondant a été créé pour le UID renvoyé par la commande **id -u** :


```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Vérifiez que les tickets dans le cache d'identification de Kerberos sont valides et n'ont pas expiré :

```
/opt/quest/bin/vastool klist
<!--NeedCopy-->
```

Quittez la session.

```
exit
<!--NeedCopy-->
```

Le même test peut être réalisé en ouvrant une session directement sur la console KDE ou Gnome. Passez à l'étape 6 : installer le Linux VDA après vérification de la jonction du domaine.

Centrify DirectControl

Rejoindre un domaine Windows Une fois Centrify DirectControl Agent installé, associez la machine Linux au domaine Active Directory à l'aide de la commande Centrify **adjoin** :

```
sudo adjoin -w -V -u user domain-name
<!--NeedCopy-->
```

L'**utilisateur** est un utilisateur de domaine disposant des autorisations nécessaires pour joindre des machines au domaine Active Directory. Le paramètre **domain-name** est le nom du domaine auquel associer la machine Linux.

Vérifier l'appartenance à un domaine Le Delivery Controller requiert que toutes les machines VDA (VDA Windows et Linux) aient un objet ordinateur dans Active Directory. Pour vérifier qu'une machine Linux associée à Centrify se trouve sur le domaine :

```
sudo adinfo
<!--NeedCopy-->
```

Vérifiez que la valeur **Joined to domain** est valide et que **CentrifyDC mode** renvoie **connected**. Si le mode reste bloqué à l'état de démarrage, le client Centrify rencontre des problèmes de connexion au serveur ou d'authentification.

Des informations plus complètes sur le système et les diagnostics sont disponibles à l'aide de :

```
adinfo --sysinfo all

adinfo  – diag
<!--NeedCopy-->
```

Testez la connectivité avec les différents services Active Directory et Kerberos.


```
adinfo --test
<!--NeedCopy-->
```

Passez à l'étape 6 : installer le Linux VDA après vérification de la jonction du domaine.

SSSD

Si vous utilisez SSSD sur SUSE, suivez les instructions de cette section. Cette section comprend des instructions permettant de connecter une machine Linux VDA à un domaine Windows et des indications sur la configuration de l'authentification Kerberos.

Pour configurer SSSD sur SUSE, procédez comme suit :

1. Rejoindre le domaine et créer un fichier keytab hôte
2. Configurer PAM pour SSSD
3. Configurer SSSD
4. Activer SSSD
5. Vérifier l'appartenance à un domaine
6. Vérifier la configuration de Kerberos
7. Vérifier l'authentification utilisateur

Rejoindre le domaine et créer un fichier keytab hôte SSSD ne fournit pas de fonctions de client Active Directory pour rejoindre le domaine et gérer le fichier keytab système. Vous pouvez utiliser l'approche **Samba** à la place. Procédez comme suit avant de configurer SSSD.

1. Arrêtez et désactivez le démon NSCD (Name Service Cache Daemon).

   ```
   sudo systemctl stop nscd
   sudo systemctl disable nscd
   <!--NeedCopy-->
   ```

2. Vérifiez le nom d'hôte et la synchronisation de l'horloge Chrony.

   ```
   hostname
   hostname -f
   chronyc traking
   <!--NeedCopy-->
   ```

3. Installez ou mettez à jour les packages requis :

   ```
   sudo zypper install samba-client sssd-ad
   <!--NeedCopy-->
   ```

4. Modifiez le fichier `/etc/krb5.conf` en tant qu'utilisateur racine pour permettre à l'utilitaire **kinit** de communiquer avec le domaine cible. Ajoutez les entrées suivantes sous les sections **[libdefaults]**, **[realms]** et **[domain_realm]** :

> **Remarque :**
>
> Configurez Kerberos en fonction de votre infrastructure AD. Les paramètres suivants sont destinés au modèle à domaine et à forêt uniques.

```
[libdefaults]

    dns_canonicalize_hostname = false

    rdns = false

    default_realm = REALM

    forwardable = true

[realms]

    REALM = {


        kdc = fqdn-of-domain-controller

        default_domain = realm

        admin_server = fqdn-of-domain-controller
     }

[domain_realm]

    .realm = REALM
<!--NeedCopy-->
```

L'élément **realm** est le nom du domaine Kerberos, tel que exemple.com. L'élément **REALM** est le nom du domaine Kerberos en majuscules, tel que EXAMPLE.COM.

5. Modifiez le fichier `/etc/samba/smb.conf` en tant qu'utilisateur racine pour permettre à l'utilitaire **net** de communiquer avec le domaine cible. Ajoutez les entrées suivantes sous la section **[global]** :

```
[global]
    workgroup = domain

    client signing = yes

    client use spnego = yes

    kerberos method = secrets and keytab

    realm = REALM

    security = ADS
<!--NeedCopy-->
```


L'élément **domain** est le nom NetBIOS court d'un domaine Active Directory, tel que EXAMPLE.

6. Modifiez les entrées **passwd** et **group** dans le fichier `/etc/nsswitch.conf` pour référencer SSSD lors de la résolution d'utilisateurs et de groupes.

```
passwd: compat sss

group: compat sss
<!--NeedCopy-->
```

7. Utilisez le client Kerberos configuré pour vous authentifier auprès du domaine cible en tant qu'administrateur.

```
kinit administrator
<!--NeedCopy-->
```

8. Utilisez l'utilitaire **net** pour joindre le système au domaine et générer un fichier keytab système.

```
net ads join osname="SUSE Linux Enterprise Server" osVersion=15 -U
    administrator
<!--NeedCopy-->
```

Configurer PAM pour SSSD Avant de configurer PAM pour SSSD, installez ou mettez à jour les packages requis :

```
sudo zypper install sssd sssd-ad
<!--NeedCopy-->
```

Configurez le module PAM pour l'authentification utilisateur via SSSD et créez des répertoires de base pour les ouvertures de session utilisateur.

```
sudo pam-config --add  --sss
sudo pam-config --add --mkhomedir
<!--NeedCopy-->
```

Configurer SSSD

1. Modifiez `/etc/sssd/sssd.conf` en tant qu'utilisateur racine pour permettre au démon SSSD de communiquer avec le domaine cible. Exemple de configuration `sssd.conf` (des options supplémentaires peuvent être ajoutées si nécessaire) :

```
[sssd]
    config_file_version = 2
    services = nss,pam
    domains = domain-dns-name

```



```
[domain/domain-dns-name]
    id_provider = ad
    auth_provider = ad
    access_provider = ad
    ad_domain = domain-dns-name
    ad_server = fqdn-of-domain-controller
    ldap_id_mapping = true
    ldap_schema = ad

# Kerberos settings
    krb5_ccachedir = /tmp
    krb5_ccname_template = FILE:%d/krb5cc_%U

# Comment out if the users have the shell and home dir set on the AD side

    fallback_homedir = /home/%d/%u
    default_shell = /bin/bash

# Uncomment and adjust if the default principal SHORTNAME$@REALM is not available

# ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM

    ad_gpo_access_control = permissive

<!--NeedCopy-->
```

L'élément **domain-dns-name** est le nom de domaine DNS, tel que example.com.

> **Remarque :**
>
> **ldap_id_mapping** est défini sur true de façon à ce que SSSD se charge de mapper les SID Windows avec les UID Unix. Sinon, Active Directory doit être en mesure de fournir des extensions POSIX. L'élément **ad_gpo_access_control** est défini sur **permissive** pour éviter une erreur d'ouverture de session non valide pour les sessions Linux. Consultez les pages du manuel pour `sssd.conf` et `sssd-ad`.

2. Définissez les autorisations et les propriétaires de fichier sur `sssd.conf` :

```
sudo chmod 0600 /etc/sssd/sssd.conf
<!--NeedCopy-->
```

Activer SSSD Exécutez les commandes suivantes pour activer et démarrer le démon SSSD au démarrage du système :

```
sudo systemctl enable sssd
sudo systemctl start sssd
<!--NeedCopy-->
```


Vérifier l'appartenance à un domaine

1. Exécutez la commande `net ads` de **Samba** pour vérifier que la machine est associée à un domaine :

```
sudo net ads testjoin
<!--NeedCopy-->
```

2. Exécutez la commande suivante pour vérifier les informations d'objet de domaine et d'ordinateur supplémentaires :

```
sudo net ads info
<!--NeedCopy-->
```

Vérifier la configuration de Kerberos Vérifiez que le fichier keytab système a été créé et qu'il contient des clés valides.

```
sudo klist -ke
<!--NeedCopy-->
```

Cette commande affiche la liste des clés disponibles pour les différentes combinaisons de noms principaux et de suites de chiffrement.

Exécutez la commande **kinit** Kerberos pour authentifier la machine auprès du contrôleur de domaine à l'aide de ces clés :

```
sudo kinit –k MACHINE$@REALM
<!--NeedCopy-->
```

Les noms de machine et de domaine doivent être spécifiés en majuscules. Le signe dollar (**$**) doit être placé dans une séquence d'échappement avec une barre oblique inverse (****) pour empêcher le remplacement shell. Dans certains environnements, le nom de domaine DNS est différent du nom de domaine Kerberos. Assurez-vous que le nom de domaine est utilisé. Si cette commande réussit, aucun résultat n'est affiché.

Vérifiez que le ticket TGT pour le compte de machine a été mis en cache à l'aide de :

```
sudo klist
<!--NeedCopy-->
```

Vérifier l'authentification utilisateur SSSD ne fournit pas d'outil de ligne de commande pour tester l'authentification directement avec le démon. Cela peut uniquement être effectué via PAM.

Pour vérifier que le module PAM SSSD est correctement configuré, ouvrez une session sur le Linux VDA à l'aide d'un compte d'utilisateur de domaine qui n'a jamais été utilisé.

```
ssh localhost -l domain\username
```



```
2
3 id -u
4
5 klist
6
7 exit
8 <!--NeedCopy-->
```

Vérifiez que les tickets Kerberos renvoyés par la commande `klist` sont corrects pour cet utilisateur et qu'ils n'ont pas expiré.

En tant qu'utilisateur racine, vérifiez qu'un fichier cache de ticket correspondant a été créé pour l'UID renvoyé par la commande `id -u` précédente :

```
1 ls /tmp/krb5cc_uid
2 <!--NeedCopy-->
```

Le même test peut être réalisé en ouvrant une session directement sur la console KDE ou Gnome. Passez à l'étape 6 : installer le Linux VDA après vérification de la jonction du domaine.

PBIS

Télécharger le package PBIS requis Par exemple :

```
1 wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/
     pbis-open-9.1.0.551.linux.x86_64.rpm.sh
2 <!--NeedCopy-->
```

Rendre le script d'installation PBIS exécutable Par exemple :

```
1 chmod +x pbis-open-9.1.0.551.linux.x86_64.rpm.sh
2 <!--NeedCopy-->
```

Exécuter le script d'installation PBIS Par exemple :

```
1 sh pbis-open-9.1.0.551.linux.x86_64.rpm.sh
2 <!--NeedCopy-->
```

Rejoindre un domaine Windows Votre contrôleur de domaine doit être accessible et vous devez disposer d'un compte utilisateur Active Directory avec les autorisations nécessaires pour ajouter des machines au domaine :

```
1 /opt/pbis/bin/domainjoin-cli join domain-name user
2 <!--NeedCopy-->
```


L'**utilisateur** est un utilisateur de domaine disposant des autorisations nécessaires pour ajouter des machines au domaine Active Directory. Le paramètre **domain-name** est le nom DNS du domaine ; par exemple, exemple.com.

Remarque : pour définir Bash en tant que shell par défaut, exécutez la commande **/opt/pbis/bin/-config LoginShellTemplate/bin/bash**.

Vérifier l'appartenance à un domaine Le Delivery Controller requiert que toutes les machines VDA (VDA Windows et Linux) aient un objet ordinateur dans `Active Directory`. Pour vérifier qu'une machine Linux associée à PBIS se trouve sur le domaine :

```
/opt/pbis/bin/domainjoin-cli query
<!--NeedCopy-->
```

Si la machine est associée à un domaine, cette commande renvoie les informations sur le domaine AD et l'unité d'organisation auxquels la machine est actuellement associée. Sinon, seul le nom d'hôte apparaît.

Vérifier l'authentification utilisateur Vérifiez que PBIS peut authentifier les utilisateurs du domaine via PAM. Pour ce faire, connectez-vous au Linux VDA à l'aide d'un compte d'utilisateur de domaine qui n'a jamais été utilisé auparavant.

```
ssh localhost -l domain\user

id -u
<!--NeedCopy-->
```

Vérifiez qu'un fichier cache d'identification Kerberos correspondant a été créé pour le UID renvoyé par la commande **id -u** :

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Quittez la session.

```
exit
<!--NeedCopy-->
```

Passez à l'étape 6 : installer le Linux VDA après vérification de la jonction du domaine.

Étape 4 : installer .NET Runtime 6.0 en tant que condition préalable

Avant d'installer Linux VDA, installez .NET Runtime 6.0 conformément aux instructions de l'article https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

Après avoir installé .NET Runtime 6.0, exécutez la commande **which dotnet** pour trouver votre chemin d'exécution.

En fonction de la sortie de la commande, définissez le chemin binaire de .NET Runtime. Par exemple, si la sortie de la commande est /aa/bb/dotnet, utilisez /aa/bb comme chemin binaire .NET.

Étape 5 : télécharger le package Linux VDA

1. Accédez à la page de téléchargement de Citrix Virtual Apps and Desktops.
2. Développez la version appropriée de Citrix Virtual Apps and Desktops.
3. Cliquez sur **Composants** pour télécharger le package Linux VDA qui correspond à votre distribution Linux et la clé publique GPG que vous pouvez utiliser pour vérifier l'intégrité du package Linux VDA.

   Pour vérifier l'intégrité du package Linux VDA à l'aide de la clé publique, importez la clé publique dans la base de données RPM et exécutez les commandes suivantes :

   ```
   rpmkeys --import <path to the public key>
   rpm --checksig --verbose <path to the Linux VDA package>
   <!--NeedCopy-->
   ```

Étape 6 : installer le Linux VDA

Étape 6a : désinstaller l'ancienne version

Si vous avez installé une version antérieure autre que les deux précédentes et une version LTSR, désinstallez-la avant d'installer la nouvelle version.

1. Arrêtez les services Linux VDA :

   ```
   sudo /sbin/service ctxvda stop

   sudo /sbin/service ctxhdx stop
   <!--NeedCopy-->
   ```

   > **Remarque :**
   >
   > Avant d'arrêter les services `ctxvda` et `ctxhdx`, exécutez la commande `service ctxmonitorservice stop` pour arrêter le démon du service de surveillance. Sinon, le démon du service de surveillance redémarre les services que vous avez arrêtés.

2. Désinstallez le package :

   ```
   sudo rpm -e XenDesktopVDA
   <!--NeedCopy-->
   ```


> **Important :**
>
> La mise à niveau à partir des deux dernières versions est prise en charge.
>
> **Remarque :**
>
> Vous pouvez trouver les composants installés sous **/opt/Citrix/VDA/**.
>
> Pour exécuter une commande, le chemin d'accès complet est nécessaire ; vous pouvez ajouter **/opt/Citrix/VDA/sbin** et **/opt/Citrix/VDA/bin** au chemin du système.

Étape 6b : installer le Linux VDA

Installer le logiciel Linux VDA à l'aide de Zypper :

```
sudo zypper install XenDesktopVDA-<version>.sle15_x.x86_64.rpm
<!--NeedCopy-->
```

Installez le logiciel Linux VDA à l'aide du gestionnaire de package RPM :

```
sudo rpm -i XenDesktopVDA-<version>.sle15_x.x86_64.rpm
<!--NeedCopy-->
```

Étape 6c : mettre à niveau le Linux VDA (facultatif)

Vous pouvez effectuer une mise à niveau d'une installation existante à partir des deux versions précédentes et d'une version LTSR.

> **Remarque :**
>
> La mise à niveau d'une installation existante remplace les fichiers de configuration sous /etc/xdl. Avant de procéder à une mise à niveau, assurez-vous de sauvegarder les fichiers.

```
sudo rpm -U XenDesktopVDA-<version>.sle15_x.x86_64.rpm
<!--NeedCopy-->
```

Liste des dépendances RPM pour SUSE 15 :

```
postgresql >= 13

postgresql-server >= 13

postgresql-jdbc >= 9.4

java-11-openjdk >= 11

ImageMagick >= 7.0

```



```
dbus-1 >= 1.12.2

dbus-1-x11 >= 1.12.2

xorg-x11 >= 7.6_1

libXpm4 >= 3.5.12

libXrandr2 >= 1.5.1

libXtst6 >= 1.2.3

pam >= 1.3.0

bash >= 4.4

findutils >= 4.6

gawk >= 4.2

sed >= 4.4

cups >= 2.2

cups-filters >= 1.25

libxml2-2 >= 2.9

libmspack0 >= 0.6

ibus >= 1.5

libtcmalloc4 >= 2.5

libcap-progs >= 2.26

mozilla-nss-tools >= 3.53.1

libpython3_6m1_0 >= 3.6~

libQt5Widgets5 >= 5.12

libqrencode4 >= 4.0.0

libImlib2-1 >= 1.4.10
<!--NeedCopy-->
```

> **Important :**
>
> Redémarrez la machine Linux VDA après la mise à niveau.

Étape 7 : installer les pilotes NVIDIA GRID

Pour activer HDX 3D Pro, vous devez installer les pilotes NVIDIA GRID sur votre hyperviseur et sur les machines VDA.

Pour installer et configurer le gestionnaire de GPU virtuel NVIDIA GRID (pilote hôte) sur les hyperviseurs spécifiques, consultez les guides suivants :

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

Pour installer et configurer les pilotes de VM invitée NVIDIA GRID, effectuez les opérations générales suivantes :

1. Assurez-vous que la VM invitée est arrêtée.
2. Dans le panneau de configuration de l'hyperviseur, attribuez un GPU à la VM.
3. Démarrez la VM.
4. Installez le pilote de VM invitée sur la VM.

Étape 8 : configurer le Linux VDA

Après l'installation du package, vous devez configurer le Linux VDA en exécutant le script `ctxsetup.sh`. Avant d'apporter des modifications, le script vérifie l'environnement et s'assure que toutes les dépendances sont installées. Si nécessaire, vous pouvez exécuter le script à tout moment pour modifier les paramètres.

Vous pouvez exécuter le script manuellement avec invite, ou automatiquement avec réponses préconfigurées. Consultez l'aide sur le script avant de continuer :

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh –help
<!--NeedCopy-->
```

Configuration avec invites

Exécutez une configuration manuelle avec questions :

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

Configuration automatique

Pour une installation automatique, fournissez les options requises par le script d'installation avec des variables d'environnement. Si toutes les variables requises sont présentes, le script n'invite pas

à entrer des informations.

Les variables d'environnement prises en charge sont les suivantes :

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N** : le Linux VDA prend en charge la spécification d'un nom de Delivery Controller à l'aide d'un enregistrement DNS CNAME. La valeur est définie par défaut sur N.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** : le Linux VDA requiert une liste séparée par des espaces de noms de domaines complets de Delivery Controller. Cette dernière sera utilisée pour l'enregistrement auprès d'un Delivery Controller. Au moins un alias de nom de domaine complet (FQDN) ou CNAME doit être spécifié.
- **CTX_XDL_VDA_PORT = port-number** : le Linux VDA communique avec les Delivery Controller à l'aide d'un port (80 par défaut) TCP/IP.
- **CTX_XDL_REGISTER_SERVICE = Y | N** : les services Linux VDA sont lancés après le démarrage de la machine. La valeur est définie sur Y par défaut.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** : les services Linux VDA requièrent que les connexions réseau entrantes soient autorisées via le pare-feu du système. Vous pouvez ouvrir automatiquement les ports requis (ports 80 et 1494 par défaut) dans le pare-feu du système pour Linux VDA. Valeur définie sur Y par défaut.
- **CTX_XDL_AD_INTEGRATION = 1 | 2 | 3 | 4** : le Linux VDA requiert que les paramètres de configuration Kerberos s'authentifient auprès des Delivery Controller. La configuration de Kerberos est déterminée depuis l'outil d'intégration d'Active Directory installé et configuré sur le système. Spécifiez la méthode d'intégration d'Active Directory prise en charge à utiliser :
  - 1 –Samba Winbind
  - 2 –Service d'authentification Quest
  - 3 –Centrify DirectControl
  - 4 –SSSD
- **CTX_XDL_HDX_3D_PRO=Y | N** : Linux VDA prend en charge HDX 3D Pro, un ensemble de technologies d'accélération GPU conçues pour optimiser la virtualisation des applications riches en graphiques. Si HDX 3D Pro est sélectionné, le Virtual Delivery Agent doit être configuré pour le mode Bureaux VDI (session unique), c'est-à-dire, CTX_XDL_VDI_MODE=Y.
- **CTX_XDL_VDI_MODE=Y | N** : indique si la machine est configurée comme modèle de mise à disposition de bureaux dédiés (VDI) ou comme modèle de mise à disposition de bureaux partagés hébergés. Pour les environnements HDX 3D Pro, définissez cette variable sur Y. Elle est définie par défaut sur N.
- **CTX_XDL_SITE_NAME=dns-name** : le Linux VDA découvre les serveurs LDAP à l'aide de DNS. Pour limiter les résultats de recherche DNS à un site local, spécifiez un nom de site DNS. Cette variable est définie sur **<none>** par défaut.

- **CTX_XDL_LDAP_LIST='list-ldap-servers'** : le Linux VDA envoie une requête vers le DNS pour découvrir les serveurs LDAP. Si DNS ne peut pas fournir d'enregistrements de service LDAP, vous pouvez entrer une liste séparée par des espaces de noms de domaines complets LDAP avec ports LDAP. Par exemple, ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268. Si vous spécifiez le numéro de port LDAP 389, le Linux VDA interroge chaque serveur LDAP du domaine spécifié en mode d'interrogation. S'il existe un nombre x de stratégies et y de serveurs LDAP, le Linux VDA effectue le total de X multiplié par Y requêtes. Si le temps d'interrogation dépasse le seuil, les ouvertures de session peuvent échouer. Pour activer les requêtes LDAP plus rapides, activez le **catalogue global** sur un contrôleur de domaine et définissez le numéro de port LDAP correspondant sur 3268. Cette variable est définie sur **<none>** par défaut.
- **CTX_XDL_SEARCH_BASE=search-base-set** : le Linux VDA envoie une requête à LDAP via une base de recherche définie sur la racine du domaine Active Directory (par exemple, D, DC=mycompany,DC=com). Pour améliorer les performances de recherche, vous pouvez spécifier une base de recherche (par exemple, OU=VDI,DC=mycompany,DC=com). Cette variable est définie sur **<none>** par défaut.
- **CTX_XDL_FAS_LIST='list-fas-servers'** : les serveurs du service d'authentification fédérée (FAS) sont configurés via la stratégie de groupe AD. Le Linux VDA ne prend pas en charge la stratégie de groupe AD mais vous pouvez fournir une liste de serveurs FAS séparés par des points-virgules. La séquence doit être la même que celle configurée dans la stratégie de groupe AD. Si une adresse de serveur est supprimée, remplissez son espace vide avec la chaîne de texte **<none>** et ne modifiez pas l'ordre des adresses de serveur. Pour communiquer correctement avec les serveurs FAS, assurez-vous d'ajouter un numéro de port conforme à celui spécifié sur les serveurs FAS, par exemple CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'.
- **CTX_XDL_DOTNET_ runtime_path=Path-to-install-dotnet-runtime** : chemin d'accès à l' installation de .NET Runtime 6.0 pour la prise en charge du nouveau Broker Agent Service (`ctxvda`). Le chemin par défaut est /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate** : spécifie l'environnement de bureau GNOME, GNOME Classic ou MATE à utiliser dans les sessions. Si vous ne spécifiez pas la variable, le bureau actuellement installé sur le VDA est utilisé. Toutefois, si le bureau actuellement installé est MATE, vous devez définir la valeur de la variable sur **mate**.

  Vous pouvez également modifier l'environnement de bureau d'un utilisateur de session cible en procédant comme suit :

  1. Créez un fichier `.xsession` sous le répertoire **$HOME/<username>** sur le VDA.
  2. Modifiez le fichier `.xsession` pour spécifier un environnement de bureau.
     - **Pour le bureau MATE sur SUSE 15**


```
MSESSION="$(type -p mate-session)"
if [ -n "$MSESSION" ]; then
  exec mate-session
fi
```

- **Pour le bureau GNOME Classic sur SUSE 15**

```
GSESSION="$(type -p gnome-session)"
if [ -n "$GSESSION" ]; then
export GNOME_SHELL_SESSION_MODE=classic
exec gnome-session --session=gnome-classic
fi
```

- **Pour le bureau GNOME sur SUSE 15**

```
GSESSION="$(type -p gnome-session)"
if [ -n "$GSESSION" ]; then
exec gnome-session
fi
```

3. Partagez l'autorisation de fichier 700 avec l'utilisateur de la session cible.

À partir de la version 2209, les utilisateurs de session peuvent personnaliser leurs environnements de bureau. Pour activer cette fonctionnalité, vous devez installer au préalable des environnements de bureau commutables sur le VDA. Pour plus d'informations, consultez Environnements de bureau personnalisés par utilisateurs de session.

- **CTX_XDL_START_SERVICE = Y | N** : indique si les services Linux VDA sont lancés lorsque la configuration de Linux VDA est terminée. Valeur définie sur Y par défaut.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** : port socket permettant d'écouter Citrix Scout. Le port par défaut est 7503.
- **CTX_XDL_TELEMETRY_PORT** : port de communication avec Citrix Scout. Le port par défaut est 7502.

Définissez la variable d'environnement et exécutez le script de configuration :

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3|4

export CTX_XDL_HDX_3D_PRO=Y|N
```



```
14
15 export CTX_XDL_VDI_MODE=Y|N
16
17 export CTX_XDL_SITE_NAME=dns-site-name | '<none>'
18
19 export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'
20
21 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
22
23 export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'
24
25 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
26
27 export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<
      none>'
28
29 export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number
30
31 export CTX_XDL_TELEMETRY_PORT=port-number
32
33 export CTX_XDL_START_SERVICE=Y|N
34
35 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
36 <!--NeedCopy-->
```

Lors de l'exécution de la commande sudo, entrez l'option **-E** pour transmettre les variables d'environnement au nouveau shell créé. Nous vous recommandons de créer un fichier de script shell à partir des commandes précédentes avec **#!/bin/bash** en tant que première ligne.

Vous pouvez également spécifier tous les paramètres avec une seule commande :

```
1  sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
2
3  CTX_XDL_DDC_LIST='list-ddc-fqdns' \
4
5  CTX_XDL_VDA_PORT=port-number \
6
7  CTX_XDL_REGISTER_SERVICE=Y|N \
8
9  CTX_XDL_ADD_FIREWALL_RULES=Y|N \
10
11 CTX_XDL_AD_INTEGRATION=1|2|3|4 \
12
13 CTX_XDL_HDX_3D_PRO=Y|N \
14
15 CTX_XDL_VDI_MODE=Y|N \
16
17 CTX_XDL_SITE_NAME=dns-name \
18
19 CTX_XDL_LDAP_LIST='list-ldap-servers' \
20
21 CTX_XDL_SEARCH_BASE=search-base-set \
22
```



```
CTX_XDL_FAS_LIST='list-fas-servers' \

CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

Supprimer les modifications de configuration

Dans certains scénarios, il peut être nécessaire de supprimer les modifications de configuration effectuées par le script **ctxsetup.sh** sans désinstaller le package Linux VDA.

Consultez l'aide sur ce script avant de continuer :

```
sudo /usr/local/sbin/ctxcleanup.sh --help
<!--NeedCopy-->
```

Pour supprimer les modifications de configuration :

```
sudo /usr/local/sbin/ctxcleanup.sh
<!--NeedCopy-->
```

> **Important :**
>
> Ce script supprime toutes les données de configuration de la base de données et empêche Linux VDA de fonctionner.

Journaux de configuration

Les scripts **ctxsetup.sh** et **ctxcleanup.sh** affichent les erreurs dans la console, avec des informations supplémentaires consignées dans un fichier journal de configuration :

`/tmp/xdl.configure.log`

Redémarrez les services de Linux VDA pour que les modifications prennent effet.

Étape 9 : exécuter XDPing

Exécutez `sudo /opt/Citrix/VDA/bin/xdping` pour vérifier les problèmes de configuration courants avec un environnement VDA Linux. Pour de plus amples informations, consultez la section

XDPing.

Étape 10 : exécuter le Linux VDA

Une fois que vous avez configuré Linux VDA à l'aide du script **ctxsetup.sh**, utilisez les commandes suivantes pour contrôler Linux VDA.

Démarrer Linux VDA :

Pour démarrer les services Linux VDA :

```
sudo /sbin/service ctxhdx start

sudo /sbin/service ctxvda start
<!--NeedCopy-->
```

Arrêter Linux VDA :

Pour arrêter les services Linux VDA :

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
<!--NeedCopy-->
```

> **Remarque :**
>
> Avant d'arrêter les services `ctxvda` et `ctxhdx`, exécutez la commande `service ctxmonitorservice stop` pour arrêter le démon du service de surveillance. Sinon, le démon du service de surveillance redémarre les services que vous avez arrêtés.

Redémarrer Linux VDA :

Pour redémarrer les services Linux VDA :

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx restart

sudo /sbin/service ctxvda start
<!--NeedCopy-->
```

Vérifier l'état de Linux VDA :

Pour vérifier l'état de fonctionnement des services de Linux VDA :

```
sudo /sbin/service ctxvda status

sudo /sbin/service ctxhdx status
<!--NeedCopy-->
```


Étape 11 : créer le catalogue de machines dans Citrix Virtual Apps ou Citrix Virtual Desktops

Le processus de création de catalogues de machines et d'ajout de machines Linux VDA est similaire à l'approche traditionnelle avec les VDA Windows. Pour obtenir une description plus détaillée de la méthode à utiliser pour effectuer ces tâches, consultez les sections Créer des catalogues de machines et Gérer des catalogues de machines.

Pour la création de catalogues de machines contenant des machines Linux VDA, il existe quelques restrictions qui différencient ce processus de la création de catalogues de machines pour VDA Windows :

- Pour le système d'exploitation, sélectionnez :
  - l'option **OS à sessions multiples** pour un modèle de mise à disposition de bureaux partagés hébergés ;
  - l'option **OS mono-session** pour un modèle de mise à disposition de bureaux dédiés VDI.
- Ne combinez pas de machines Linux VDA et Windows dans le même catalogue de machines.

> **Remarque :**
>
> Les versions antérieures de Citrix Studio ne prenaient pas en charge la notion de « système d'exploitation Linux. » Toutefois, la sélection de l'option **OS de serveur Windows** ou **OS de serveur** implique un modèle de mise à disposition équivalent de bureaux partagés hébergés. La sélection de l'option **OS de bureau Windows** ou **OS de bureau** implique un modèle de mise à disposition d'un utilisateur unique par machine.
>
> **Conseil :**
>
> Si une supprimez une machine puis que vous la rejoignez au domaine Active Directory, vous devez supprimer et rajouter la machine au catalogue de machines.

Étape 12 : créer le groupe de mise à disposition dans Citrix Virtual Apps ou Citrix Virtual Desktops

Le processus de création d'un groupe de mise à disposition et d'ajout de catalogues de machines contenant des machines Linux VDA est presque identique aux machines VDA Windows. Pour obtenir une description plus détaillée de la méthode à utiliser pour effectuer ces tâches, consultez la section Créer des groupes de mise à disposition.

Lors de la création de groupes de mise à disposition qui contiennent des catalogues de machines Linux VDA, les restrictions suivantes s'appliquent :

- Assurez-vous que les utilisateurs et les groupes AD que vous sélectionnez ont été correctement configurés pour l'ouverture de session sur les machines Linux VDA.
- N'autorisez pas l'ouverture de session d'utilisateurs non authentifiés (anonymes).
- Ne combinez pas le groupe de mise à disposition avec des catalogues de machines contenant des machines Windows.

> **Important :**
>
> La publication d'applications est prise en charge avec la version 1.4 de Linux VDA et les versions supérieures. Toutefois, le Linux VDA ne prend pas en charge la mise à disposition de bureaux et d'applications sur la même machine.

Pour plus d'informations sur la création de catalogues de machines et de groupes de mise à disposition, consultez Citrix Virtual Apps and Desktops 7 2206.

Installer manuellement Linux Virtual Delivery Agent pour Ubuntu

December 16, 2022

> **Important :**
>
> Pour les nouvelles installations, nous vous recommandons d'utiliser Easy Install pour effectuer une installation rapide. Easy Install permet de gagner du temps et d'économiser de la main d'œuvre. Cette installation est également plus fiable que l'installation manuelle décrite dans cet article.

Étape 1 : préparer Ubuntu pour l'installation du VDA

Étape 1a : vérifier la configuration réseau

Assurez-vous que le réseau est connecté et correctement configuré. Par exemple, vous devez configurer le serveur DNS sur le Linux VDA.

Si vous utilisez un serveur Ubuntu 18.04 Live Server, effectuez la modification suivante dans le fichier de configuration **/etc/cloud/cloud.cfg** avant de définir le nom d'hôte :

```
preserve_hostname: true
```

Étape 1b : définir le nom d'hôte

Pour vous assurer que le nom d'hôte de la machine est indiqué correctement, modifiez le fichier **/etc/hostname** afin que celui-ci contienne uniquement le nom d'hôte de la machine.


```
hostname
```

Étape 1c : attribuer une adresse de bouclage au nom d'hôte

Assurez-vous que le nom de domaine DNS et le nom de domaine complet (FQDN) de la machine sont signalés correctement. Pour ce faire, modifiez la ligne suivante du fichier **/etc/hosts** pour inclure le nom de domaine complet et le nom d'hôte en tant que deux premières entrées :

```
127.0.0.1 hostname-fqdn hostname localhost
```

Par exemple :

```
127.0.0.1 vda01.example.com vda01 localhost
```

Supprimez toute autre référence à `hostname-fqdn` ou `hostname` des autres entrées du fichier.

> **Remarque :**
>
> Le Linux VDA ne prend actuellement pas en charge la troncation de noms NetBIOS. Par conséquent, le nom d'hôte ne doit pas comporter plus de 15 caractères.
>
> **Conseil :**
>
> Utilisez uniquement les caractères a–z, A–Z, 0–9 et tiret (-). Évitez les caractères de soulignement (_), les espaces et autres symboles. Ne démarrez pas un nom d'hôte par un chiffre et ne le terminez pas par un tiret. Cette règle s'applique également aux noms d'hôte Delivery Controller.

Étape 1d : vérifier le nom d'hôte

Vérifiez que le nom d'hôte est correctement configuré :

```
1 hostname
2 <!--NeedCopy-->
```

Cette commande renvoie uniquement le nom d'hôte de la machine et non son nom de domaine complet.

Vérifiez que le nom de domaine complet est correctement configuré :

```
1 hostname -f
2 <!--NeedCopy-->
```

Cette commande renvoie le nom de domaine complet de la machine.

Étape 1e : désactiver DNS multidiffusion

Les paramètres par défaut activent DNS multidiffusion (**mDNS**), ce qui peut entraîner des résultats incohérents de résolution de nom.

Pour désactiver **mDNS**, modifiez **/etc/nsswitch.conf** et dans la ligne suivante remplacez :

```
hosts: files mdns_minimal [NOTFOUND=return] dns
```

par :

```
hosts: files dns
```

Étape 1f : vérifier la résolution de nom et l'accessibilité du service

Vérifiez que vous pouvez résoudre le nom de domaine complet et effectuer un sondage ping sur le contrôleur de domaine et le Delivery Controller :

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

ping delivery-controller-fqdn
<!--NeedCopy-->
```

Si vous ne pouvez pas résoudre le nom de domaine complet ou effectuer un sondage ping sur l'une de ces machines, reprenez les étapes avant de continuer.

Étape 1g : configurer la synchronisation de l'horloge (chrony)

Il est très important de maintenir la synchronisation de l'horloge entre les VDA, les Delivery Controller et les contrôleurs de domaine. L'hébergement du Linux VDA en tant que machine virtuelle peut entraîner des problèmes de décalage d'horloge. Pour cette raison, il est recommandé de synchroniser l'heure avec un service de temps à distance.

Installez chrony :

```
apt-get install chrony
<!--NeedCopy-->
```

En tant qu'utilisateur racine, modifiez **/etc/chrony/chrony.conf** et ajoutez une entrée de serveur pour chaque serveur de temps distant :

```
server peer1-fqdn-or-ip-address iburst
server peer2-fqdn-or-ip-address iburst
```

Dans un déploiement type, synchronisez l'heure depuis les contrôleurs de domaine locaux et non pas directement depuis des serveurs de pool NTP publics. Ajoutez une entrée de serveur pour chaque contrôleur de domaine Active Directory du domaine.

Supprimez toute autre entrée **server** ou **pool** répertoriée, y compris les entrées d'adresse IP de bouclage, localhost et ***.pool.ntp.org** de serveur public.

Enregistrez les modifications et redémarrez le démon Chrony :

```
sudo systemctl restart chrony
<!--NeedCopy-->
```

Étape 1h : installer OpenJDK 11

Le Linux VDA nécessite la présence d'OpenJDK 11.

Sur Ubuntu 20.04 et Ubuntu 18.04, installez OpenJDK 11 en utilisant :

```
sudo apt-get install -y openjdk-11-jdk
<!--NeedCopy-->
```

Étape 1i : installer PostgreSQL

Le Linux VDA requiert PostgreSQL version 9.x sur Ubuntu :

```
sudo apt-get install -y postgresql

sudo apt-get install -y libpostgresql-jdbc-java
<!--NeedCopy-->
```

Étape 1j : installer Motif

```
sudo apt-get install -y libxm4
<!--NeedCopy-->
```

Étape 1k : installer les autres packages

Pour Ubuntu 22.04 :

```
sudo apt-get install -y libsasl2-2
sudo apt-get install -y libsasl2-modules-gssapi-mit
sudo apt-get install -y libldap-2.5-0
sudo apt-get install -y krb5-user
sudo apt-get install -y libgtk2.0-0
<!--NeedCopy-->
```

Pour Ubuntu 20.04 et Ubuntu 18.04 :


```
sudo apt-get install -y libsasl2-2
sudo apt-get install -y libsasl2-modules-gssapi-mit
sudo apt-get install -y libldap-2.4-2
sudo apt-get install -y krb5-user
sudo apt-get install -y libgtk2.0-0
<!--NeedCopy-->
```

Étape 2 : préparer l'hyperviseur

Certaines modifications sont requises pour l'exécution du Linux VDA en tant que machine virtuelle sur un hyperviseur pris en charge. Apportez les modifications suivantes en fonction de la plateforme d'hyperviseur utilisée. Aucune modification n'est requise si vous utilisez la machine Linux sur un matériel bare metal.

Corriger la synchronisation de l'heure sur Citrix Hypervisor

Si la fonctionnalité de synchronisation de l'heure de Citrix Hypervisor est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée avec NTP et Citrix Hypervisor. En effet, les deux systèmes essaient de gérer l'horloge système. Pour éviter que l'horloge ne soit plus synchronisée avec d'autres serveurs, assurez-vous l'horloge du système de chaque invité Linux est synchronisée avec NTP. Cela nécessite la désactivation de la synchronisation de l'heure de l'hôte. Aucune modification n'est requise en mode HVM.

Si vous utilisez un noyau Linux paravirtualisé avec le composant Citrix VM Tools installé, vous pouvez vérifier si la fonctionnalité de synchronisation de l'heure de Citrix Hypervisor est présente et activée à partir de la VM Linux :

```
su -

cat /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Cette commande renvoie 0 ou 1 :

- 0 - La fonctionnalité de synchronisation de l'heure est activée, et doit être désactivée.
- 1 - La fonctionnalité de synchronisation de l'heure est désactivée, et aucune action n'est requise.

Si le fichier /proc/sys/xen/independent_wallclock n'existe pas, les étapes suivantes ne sont pas nécessaires.

Si la fonctionnalité de synchronisation est activée, désactivez-la en entrant 1 dans le fichier :

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```


Pour rendre cette modification permanente et persistante après le redémarrage, modifiez le fichier **/etc/sysctl.conf** et ajoutez la ligne :

```
xen.independent_wallclock = 1
```

Pour vérifier ces modifications, redémarrez le système :

```
su -

cat /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Cette commande renvoie la valeur 1.

Corriger la synchronisation de l'heure sur Microsoft Hyper-V

Les VM Linux sur lesquelles Hyper-V Integration Services est installé peuvent utiliser la fonctionnalité de synchronisation de l'heure Hyper-V pour utiliser l'heure du système d'exploitation hôte. Pour vous assurer que l'horloge du système est toujours précise, activez cette fonctionnalité avec les services NTP.

Depuis le système d'exploitation de gestion :

1. Ouvrez la console du gestionnaire Hyper-V.
2. Pour les paramètres d'une machine virtuelle Linux, sélectionnez **Integration Services**.
3. Assurez-vous que **Time synchronization** est sélectionné.

> **Remarque :**
>
> cette approche diffère de VMware et Citrix Hypervisor, pour lesquels la synchronisation de l'heure est désactivée pour éviter tout conflit avec NTP. La synchronisation de l'heure Hyper-V peut co-exister avec la synchronisation de l'heure NTP.

Corriger la synchronisation de l'heure sur ESX et ESXi

Si la fonctionnalité de synchronisation de l'heure de VMware est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée avec l'hyperviseur et NTP. En effet, les deux systèmes essaient de synchroniser l'horloge système. Pour éviter que l'horloge ne soit plus synchronisée avec d'autres serveurs, assurez-vous l'horloge du système de chaque invité Linux est synchronisée avec NTP. Cela nécessite la désactivation de la synchronisation de l'heure de l'hôte.

Si vous exécutez un noyau Linux paravirtualisé sur lequel VMware Tools est installé :

1. Ouvrez vSphere Client.
2. Modifiez les paramètres pour la VM Linux.

3. Dans la boîte de dialogue **Virtual Machine Properties** (Propriétés de la machine virtuelle), ouvrez l'onglet **Options**.
4. Sélectionnez **VMware Tools**.
5. Dans la zone **Advanced** (Avancé), désélectionnez **Synchronize guest time with host** (Synchroniser l'heure de l'invité avec l'hôte).

Étape 3 : ajouter la machine virtuelle (VM) Linux au domaine Windows

Le Linux VDA prend en charge plusieurs méthodes pour ajouter des machines Linux au domaine Active Directory (AD) :

- Samba Winbind
- Quest Authentication Service
- Centrify DirectControl
- SSSD
- PBIS

Suivez les instructions en fonction de la méthode choisie.

> **Remarque :**
>
> Les lancements de session peuvent échouer lorsque le même nom d'utilisateur est utilisé pour le compte local dans le Linux VDA et le compte dans AD.

Samba Winbind

Installer ou mettre à jour les packages requis

```
sudo apt-get install winbind samba libnss-winbind libpam-winbind krb5-config krb5-locales krb5-user
<!--NeedCopy-->
```

Activer le démon Winbind pour qu'il soit lancé au démarrage de la machine Le démon Winbind doit être configuré pour être lancé au démarrage de la machine :

```
sudo systemctl enable winbind
<!--NeedCopy-->
```

> **Remarque :**
>
> Assurez-vous que le script `winbind` se trouve sous `/etc/init.d`.

Configurer Kerberos Ouvrez **/etc/krb5.conf** en tant qu'utilisateur racine et configurez les paramètres suivants :

> **Remarque :**
>
> Configurez Kerberos en fonction de votre infrastructure AD. Les paramètres suivants sont destinés au modèle à domaine et à forêt uniques.

```
[libdefaults]
default_realm = REALM
dns_lookup_kdc = false
[realms]
REALM = {
admin_server = domain-controller-fqdn
kdc = domain-controller-fqdn
}
[domain_realm]
domain-dns-name = REALM
.domain-dns-name = REALM
```

Le paramètre **domain-dns-name** dans ce contexte est le nom de domaine DNS, tel que **example.com**. L'élément **REALM** est le nom du domaine Kerberos en majuscules, tel que **EXAMPLE.COM**.

Configurer l'authentification Winbind Vous devez configurer Winbind manuellement car Ubuntu ne possède pas d'outil tel que **authconfig** dans RHEL et yast2 dans SUSE.

Ouvrez **/etc/samba/smb.conf** et configurez les paramètres suivants :

```
[global]
workgroup = WORKGROUP
security = ADS
realm = REALM
encrypt passwords = yes
idmap config *:range = 16777216-33554431
winbind trusted domains only = no
kerberos method = secrets and keytab
winbind refresh tickets = yes
template shell = /bin/bash
```


WORKGROUP est le premier champ dans **REALM**, et **REALM** est le nom de domaine Kerberos en majuscules.

Configurer nsswitch Ouvrez **/etc/nsswitch.conf** et ajoutez **winbind** aux lignes suivantes :

```
passwd: compat winbind
group: compat winbind
```

Rejoindre un domaine Windows Votre contrôleur de domaine doit être accessible et vous devez disposer d'un compte utilisateur Active Directory avec les autorisations nécessaires pour ajouter des ordinateurs au domaine :

```
1 sudo net ads join REALM -U user
2 <!--NeedCopy-->
```

Où **REALM** est le nom de domaine Kerberos en majuscules, et **user** est un utilisateur de domaine disposant des autorisations nécessaires pour ajouter les ordinateurs au domaine.

Redémarrer winbind

```
1 sudo systemctl restart winbind
2 <!--NeedCopy-->
```

Configurer PAM pour Winbind Exécutez la commande suivante et assurez-vous que les options **Winbind NT/Active Directory authentication** et **Create home directory on login** sont sélectionnées :

```
1 sudo pam-auth-update
2 <!--NeedCopy-->
```

> **Conseil :**
>
> Le démon **winbind** ne reste en cours d'exécution que si la machine est associée à un domaine.

Vérifier l'appartenance à un domaine Le Delivery Controller requiert que toutes les machines VDA, Windows ou Linux, aient un objet ordinateur dans Active Directory.

Exécutez la commande **net ads** de **Samba** pour vérifier que la machine est associée à un domaine :

```
1 sudo net ads testjoin
2 <!--NeedCopy-->
```

Exécutez la commande suivante pour vérifier les informations d'objet de domaine et d'ordinateur supplémentaires :


```
sudo net ads info
<!--NeedCopy-->
```

Vérifier la configuration de Kerberos Pour vérifier que Kerberos est correctement configuré pour être utilisé avec le Linux VDA, vérifiez que le fichier **keytab** système a été créé et contient des clés valides :

```
sudo klist -ke
<!--NeedCopy-->
```

Cette commande affiche la liste des clés disponibles pour les différentes combinaisons de noms principaux et de suites de chiffrement. Exécutez la commande **kinit** Kerberos pour authentifier la machine auprès du contrôleur de domaine à l'aide de ces clés :

```
sudo kinit -k MACHINE$@REALM
<!--NeedCopy-->
```

Les noms de machine et de domaine doivent être spécifiés en majuscules. Le signe dollar ($) doit être placé dans une séquence d'échappement avec une barre oblique inverse (\) pour empêcher le remplacement shell. Dans certains environnements, le nom de domaine DNS est différent du nom de domaine Kerberos. Assurez-vous que le nom de domaine est utilisé. Si cette commande réussit, aucun résultat n'est affiché.

Vérifiez que le ticket TGT pour le compte de machine a été mis en cache à l'aide de :

```
sudo klist
<!--NeedCopy-->
```

Examinez les détails du compte de machine à l'aide de :

```
sudo net ads status
<!--NeedCopy-->
```

Vérifier l'authentification utilisateur Utilisez l'outil **wbinfo** pour vérifier que les utilisateurs de domaine peuvent s'authentifier auprès du domaine :

```
wbinfo --krb5auth=domain\username%password
<!--NeedCopy-->
```

Le domaine spécifié ici est le nom de domaine Active Directory, et non le nom de domaine Kerberos. Pour le shell bash, la barre oblique inverse (\) doit être placée dans une séquence d'échappement avec une autre barre oblique inverse. Cette commande renvoie un message indiquant la réussite ou l'échec.

Pour vérifier que le module PAM Winbind est correctement configuré, ouvrez une session sur le Linux VDA à l'aide d'un compte d'utilisateur de domaine qui n'a jamais été utilisé.

```
ssh localhost -l domain\username

id -u
<!--NeedCopy-->
```

> **Remarque :**
>
> Pour exécuter une commande SSH avec succès, assurez-vous que SSH est activé et fonctionne correctement.

Vérifiez qu'un fichier cache d'identification Kerberos correspondant a été créé pour le UID renvoyé par la commande **id -u** :

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Vérifiez que les tickets dans le cache d'identification Kerberos de l'utilisateur sont valides et n'ont pas expiré :

```
klist
<!--NeedCopy-->
```

Quittez la session.

```
exit
<!--NeedCopy-->
```

Le même test peut être réalisé en ouvrant une session directement sur la console KDE ou Gnome. Passez à l'étape 6 : installer le Linux VDA après vérification de la jonction du domaine.

> **Conseil :**
>
> Si l'authentification utilisateur réussit mais que vous ne pouvez pas afficher votre bureau lors de la connexion avec un compte de domaine, redémarrez la machine et réessayez.

Service d'authentification Quest

Configurer Quest sur le contrôleur de domaine Cette procédure suppose que vous avez installé et configuré le logiciel Quest sur les contrôleurs de domaine Active Directory et disposez des droits Administrateur pour créer des objets ordinateur dans `Active Directory`.

Autoriser les utilisateurs de domaine à ouvrir une session sur des machines Linux VDA Pour autoriser les utilisateurs de domaine à établir des sessions HDX sur une machine Linux VDA :

1. Dans la console de gestion Utilisateurs et ordinateurs Active Directory, ouvrez les propriétés de l'utilisateur Active Directory pour ce compte d'utilisateur.
2. Sélectionnez l'onglet **Unix Account**.
3. Sélectionnez **Unix-enabled**.
4. Définissez **Primary GID Number** sur l'ID d'un groupe d'utilisateurs de domaine.

> **Remarque :**
>
> Ces instructions sont les mêmes que pour la configuration d'utilisateurs de domaine pour l'ouverture de session à l'aide de la console, RDP, SSH ou tout autre protocole de communication à distance.

Configurer Quest sur un Linux VDA

Solution à l'application forcée de la stratégie SELinux L'environnement RHEL par défaut applique entièrement SELinux. Cette mise en œuvre interfère avec les mécanismes IPC de socket de domaine Unix utilisés par Quest et empêche les utilisateurs de domaine d'ouvrir une session.

Le moyen pratique de remédier à ce problème consiste à désactiver SELinux. En tant qu'utilisateur racine, modifiez **/etc/selinux/config** en modifiant le paramètre **SELinux** :

```
SELINUX=disabled
```

Cette modification nécessite le redémarrage de la machine :

```
reboot
<!--NeedCopy-->
```

> **Important :**
>
> Utilisez ce paramètre avec précaution. La réactivation de l'application forcée de la stratégie SELinux après sa désactivation peut entraîner un verrouillage complet, même pour l'utilisateur racine et d'autres utilisateurs locaux.

Configurer le démon VAS Le renouvellement automatique des tickets Kerberos doit être activé et déconnecté. L'authentification (ouverture de session en mode déconnecté) doit être désactivée :

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-
    interval 32400

sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-
    auth false
<!--NeedCopy-->
```

Cette commande définit l'intervalle de renouvellement sur 9 heures (32 400 secondes), ce qui représente une heure de moins que la valeur par défaut de 10 heures pour la durée de vie d'un ticket.

Définissez ce paramètre sur une valeur inférieure sur les systèmes avec une durée de vie de ticket plus courte.

Configuration de PAM et de NSS Pour permettre l'ouverture de session d'utilisateur de domaine via HDX et d'autres services tels que su, ssh et RDP, exécutez les commandes suivantes pour configurer manuellement PAM et NSS :

```
sudo /opt/quest/bin/vastool configure pam

sudo /opt/quest/bin/vastool configure nss
<!--NeedCopy-->
```

Rejoindre un domaine Windows Associez la machine Linux au domaine Active Directory à l'aide de la commande Quest **vastool** :

```
sudo /opt/quest/bin/vastool -u user join domain-name
<!--NeedCopy-->
```

L'utilisateur est un utilisateur de domaine disposant des autorisations nécessaires pour associer des ordinateurs au domaine Active Directory. Le paramètre **domain-name** est le nom DNS du domaine ; par exemple, exemple.com.

Vérifier l'appartenance à un domaine Le Delivery Controller requiert que toutes les machines VDA, Windows ou Linux, aient un objet ordinateur dans Active Directory. Pour vérifier qu'une machine Linux associée à Quest se trouve sur le domaine :

```
sudo /opt/quest/bin/vastool info domain
<!--NeedCopy-->
```

Si la machine est associée à un domaine, cette commande renvoie le nom de domaine. Si la machine n'est pas associée à un domaine, l'erreur suivante apparaît :

```
ERROR: No domain could be found.
ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm
default_realm not configured in vas.conf. Computer may not be joined
to domain
```

Vérifier l'authentification utilisateur Pour vérifier que Quest peut authentifier les utilisateurs de domaine via PAM, ouvrez une session sur le Linux VDA à l'aide d'un compte d'utilisateur de domaine qui n'a jamais été utilisé.

```
ssh localhost -l domain\username

```



```
id -u
<!--NeedCopy-->
```

Vérifiez qu'un fichier cache d'identification Kerberos correspondant a été créé pour le UID renvoyé par la commande **id -u** :

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Vérifiez que les tickets dans le cache d'identification de Kerberos sont valides et n'ont pas expiré :

```
/opt/quest/bin/vastool klist
<!--NeedCopy-->
```

Quittez la session.

```
exit
<!--NeedCopy-->
```

Passez à l'étape 6 : installer le Linux VDA après vérification de la jonction du domaine.

Centrify DirectControl

Rejoindre un domaine Windows Une fois Centrify DirectControl Agent installé, associez la machine Linux au domaine Active Directory à l'aide de la commande Centrify **adjoin** :

```
su -
adjoin -w -V -u user domain-name
<!--NeedCopy-->
```

Le paramètre **user** est un utilisateur de domaine Active Directory disposant des autorisations nécessaires pour joindre des ordinateurs au domaine **Active Directory**. Le paramètre **domain-name** est le nom du domaine auquel associer la machine Linux.

Vérifier l'appartenance à un domaine Le Delivery Controller requiert que toutes les machines VDA, Windows ou Linux, aient un objet ordinateur dans **Active Directory**. Pour vérifier qu'une machine Linux associée à Centrify se trouve sur le domaine :

```
su -

adinfo
<!--NeedCopy-->
```

Vérifiez que la valeur **Joined to domain** est valide et que **CentrifyDC mode** renvoie **connected**. Si le mode reste bloqué à l'état de démarrage, le client Centrify rencontre des problèmes de connexion au serveur ou d'authentification.

Des informations plus complètes sur le système et les diagnostics sont disponibles à l'aide de :


```
adinfo --sysinfo all

adinfo --diag
<!--NeedCopy-->
```

Testez la connectivité avec les différents services Active Directory et Kerberos.

```
adinfo --test
<!--NeedCopy-->
```

Passez à l'étape 6 : installer le Linux VDA après vérification de la jonction du domaine.

SSSD

Configurer Kerberos Exécutez la commande suivante pour installer Kerberos :

```
sudo apt-get install krb5-user
<!--NeedCopy-->
```

Pour configurer Kerberos, ouvrez **/etc/krb5.conf** en tant qu'utilisateur racine et définissez les paramètres :

> **Remarque :**
>
> Configurez Kerberos en fonction de votre infrastructure AD. Les paramètres suivants sont destinés au modèle à domaine et à forêt uniques.

```
[libdefaults]

default_realm = REALM

dns_lookup_kdc = false

[realms]

REALM = {

admin_server = domain-controller-fqdn

kdc = domain-controller-fqdn

}

[domain_realm]

domain-dns-name = REALM

.domain-dns-name = REALM
```

La propriété `domain-dns-name` dans ce contexte est le nom de domaine DNS, tel que example.com. L'élément *REALM* est le nom du domaine Kerberos en majuscules, tel que EXAMPLE.COM.

Joindre le domaine SSSD doit être configuré pour pouvoir utiliser Active Directory en tant que fournisseur d'identité et Kerberos pour l'authentification. Toutefois, SSSD ne fournit pas de fonctions de client Active Directory pour rejoindre le domaine et gérer le fichier keytab du système. Vous pouvez utiliser **adcli**, **realmd**ou **Samba** à la place.

> **Remarque :**
>
> Cette section fournit des informations uniquement pour **adcli** et **Samba**.

- **Si vous utilisez adcli pour rejoindre le domaine, procédez comme suit :**

1. Installez **adcli**.

```
sudo apt-get install adcli
<!--NeedCopy-->
```

2. Rejoignez le domaine avec **adcli**.

   Supprimez l'ancien fichier keytab du système et rejoignez le domaine à l'aide de :

```
su -

rm -rf /etc/krb5.keytab

adcli join domain-dns-name -U user -H hostname-fqdn
<!--NeedCopy-->
```

   user est un utilisateur du domaine autorisé à ajouter des machines au domaine. **hostname-fqdn** est le nom d'hôte au format FQDN de la machine.

   L'option **-H** est requise pour permettre à **adcli** de générer SPN au format host/hostname-fqdn@REALM, ce qui est requis par Linux VDA.

3. Vérifiez l'appartenance à un domaine.

   Pour les machines Ubuntu 22.04 et Ubuntu 20.04, exécutez la commande `adcli testjoin` pour tester si les machines sont jointes au domaine.

   Pour une machine Ubuntu 18.04, exécutez la commande `sudo klist -ket`. La capacité de l'outil **adcli** est limitée. L'outil ne permet pas de tester si une machine est jointe au domaine. Le meilleur moyen consiste à vérifier que le fichier keytab système a été créé. Vérifiez que l'horodatage de chaque clé correspond à l'heure à laquelle la machine a été jointe au domaine.

- **Si vous utilisez Samba pour rejoindre le domaine, procédez comme suit :**

1. Installez le pack.

```
sudo apt-get install samba krb5-user
<!--NeedCopy-->
```


2. Configurer **Samba**.

   Ouvrez **/etc/samba/smb.conf** et configurez les paramètres suivants :

   ```
   [global]
   workgroup = WORKGROUP
   security = ADS
   realm = REALM
   client signing = yes
   client use spnego = yes
   kerberos method = secrets and keytab
   ```

   WORKGROUP est le premier champ dans **REALM**, et **REALM** est le nom de domaine Kerberos en majuscules.

3. Rejoignez le domaine avec **Samba**.

   Votre contrôleur de domaine doit être accessible et vous devez disposer d'un compte Windows avec les autorisations nécessaires pour ajouter des ordinateurs au domaine.

   ```
   sudo net ads join REALM -U user
   <!--NeedCopy-->
   ```

   Où **REALM** est le nom de domaine Kerberos en majuscules, et **user** est un utilisateur de domaine disposant des autorisations nécessaires pour ajouter les ordinateurs au domaine.

Configurer SSSD **Installer ou mettre à jour les packages requis :**

Installez les packages de configuration et SSSD requis s'ils ne sont pas déjà installés :

```
sudo apt-get install sssd
<!--NeedCopy-->
```

Si les packages sont déjà installés, une mise à jour est recommandée :

```
sudo apt-get install --only-upgrade sssd
<!--NeedCopy-->
```

> **Remarque :**
>
> Par défaut, le processus d'installation dans Ubuntu configure automatiquement **nsswitch.conf** et le module de connexion PAM.

Configurer SSSD Des modifications doivent être apportées à la configuration SSSD avant de démarrer le démon SSSD. Pour certaines versions de SSSD, le fichier de configuration **/etc/sssd/sssd.conf**

n'est pas installé par défaut et doit être créé manuellement. En tant qu'utilisateur racine, créez ou ouvrez **/etc/sssd/sssd.conf** et configurez les paramètres suivants :

```
[sssd]

services = nss, pam

config_file_version = 2

domains = domain-dns-name

[domain/domain-dns-name]

id_provider = ad

access_provider = ad

auth_provider = krb5

krb5_realm = REALM

# Set krb5_renewable_lifetime higher if TGT renew lifetime is longer
than 14 days

krb5_renewable_lifetime = 14d

# Set krb5_renew_interval to lower value if TGT ticket lifetime is
shorter than 2 hours

krb5_renew_interval = 1h

krb5_ccachedir = /tmp

krb5_ccname_template = FILE:%d/krb5cc_%U

# This ldap_id_mapping setting is also the default value

ldap_id_mapping = true

override_homedir = /home/%d/%u

default_shell = /bin/bash

ad_gpo_map_remote_interactive = +ctxhdx
```

> **Remarque :**
>
> ldap_id_mapping est défini sur **true** de façon à ce que SSSD se charge de mapper les SID Windows avec les UID Unix. Sinon, Active Directory doit être en mesure de fournir des extensions POSIX. Le service PAM `ctxhdx` est ajouté au paramètre ad_gpo_map_remote_interactive.
>
> Le paramètre **domain-dns-name** dans ce contexte est le nom de domaine DNS, tel que example.com. L'élément **REALM** est le nom du domaine Kerberos en majuscules, tel que EXAMPLE.COM. Il n'est pas nécessaire de configurer le nom de domaine NetBIOS.

> Pour de plus amples informations sur les paramètres de configuration, consultez les pages man pour sssd.conf et `sssd-ad`.

Le démon SSSD nécessite que le fichier de configuration dispose uniquement de l'autorisation d'accès en lecture de propriétaire :

```
sudo chmod 0600 /etc/sssd/sssd.conf
<!--NeedCopy-->
```

Démarrer le démon SSSD Exécutez les commandes suivantes pour démarrer le démon SSSD maintenant et pour permettre le lancement du démon au démarrage de la machine :

```
sudo systemctl start sssd

sudo systemctl enable sssd
<!--NeedCopy-->
```

Configuration de PAM Exécutez la commande suivante et assurez-vous que les options **SSS authentication** et **Create home directory on login** sont sélectionnées :

```
sudo pam-auth-update
<!--NeedCopy-->
```

Vérifier l'appartenance à un domaine Le Delivery Controller requiert que toutes les machines VDA (VDA Windows et Linux) aient un objet ordinateur dans `Active Directory`.

- Si vous utilisez **adcli** pour vérifier l'appartenance à un domaine, exécutez la commande `sudo adcli info domain-dns-name` pour afficher les informations sur le domaine.
- Si vous utilisez **Samba** pour vérifier l'appartenance à un domaine, exécutez la commande `sudo net ads testjoin` pour vérifier que la machine est jointe à un domaine et la commande `sudo net ads info` pour vérifier des informations supplémentaires sur le domaine et l'objet Ordinateur.

Vérifier la configuration de Kerberos Pour vérifier que Kerberos est correctement configuré pour être utilisé avec le Linux VDA, vérifiez que le fichier keytab système a été créé et contient des clés valides :

```
sudo klist -ke
<!--NeedCopy-->
```

Cette commande affiche la liste des clés disponibles pour les différentes combinaisons de noms principaux et de suites de chiffrement. Exécutez la commande `kinit` Kerberos pour authentifier la machine auprès du contrôleur de domaine à l'aide de ces clés :


```
sudo kinit -k MACHINE$@REALM
<!--NeedCopy-->
```

Les noms de machine et de domaine doivent être spécifiés en majuscules. Le signe dollar ($) doit être placé dans une séquence d'échappement avec une barre oblique inverse (\) pour empêcher le remplacement shell. Dans certains environnements, le nom de domaine DNS est différent du nom de domaine Kerberos. Assurez-vous que le nom de domaine est utilisé. Si cette commande réussit, aucun résultat n'est affiché.

Vérifiez que le TGT pour le compte de machine a été mis en cache à l'aide de :

```
sudo klist
<!--NeedCopy-->
```

Vérifier l'authentification utilisateur SSSD ne fournit pas d'outil de ligne de commande pour tester l'authentification directement avec le démon. Cela peut uniquement être effectué via PAM.

Pour vérifier que le module PAM SSSD est correctement configuré, ouvrez une session sur le Linux VDA à l'aide d'un compte d'utilisateur de domaine qui n'a jamais été utilisé.

```
ssh localhost -l domain\username

id -u

klist

exit
<!--NeedCopy-->
```

Vérifiez que les tickets Kerberos renvoyés par la commande **klist** sont corrects pour cet utilisateur et qu'ils n'ont pas expiré.

En tant qu'utilisateur racine, vérifiez qu'un fichier cache de ticket correspondant a été créé pour l'UID renvoyé par la commande **id -u** précédente :

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Le même test peut être réalisé en ouvrant une session directement sur KDE ou Gnome Display Manager. Passez à l'étape 6 : installer le Linux VDA après vérification de la jonction du domaine.

PBIS

Télécharger le package PBIS requis

```
sudo wget https://github.com/BeyondTrust/pbis-open/releases/download
    /9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh
<!--NeedCopy-->
```


Rendre le script d'installation PBIS exécutable

```
sudo chmod +x pbis-open-9.1.0.551.linux.x86_64.deb.sh
<!--NeedCopy-->
```

Exécuter le script d'installation PBIS

```
sudo sh pbis-open-9.1.0.551.linux.x86_64.deb.sh
<!--NeedCopy-->
```

Rejoindre un domaine Windows Votre contrôleur de domaine doit être accessible et vous devez disposer d'un compte utilisateur Active Directory avec les autorisations nécessaires pour ajouter des ordinateurs au domaine :

```
sudo /opt/pbis/bin/domainjoin-cli join domain-name user
<!--NeedCopy-->
```

L'**utilisateur** est un utilisateur de domaine disposant des autorisations nécessaires pour ajouter des ordinateurs au domaine Active Directory. Le paramètre **domain-name** est le nom DNS du domaine ; par exemple, exemple.com.

Remarque : pour définir Bash en tant que shell par défaut, exécutez la commande **sudo /opt/pbis/bin/config LoginShellTemplate/bin/bash**.

Vérifier l'appartenance à un domaine Le Delivery Controller requiert que toutes les machines VDA (VDA Windows et Linux) aient un objet ordinateur dans `Active Directory`. Pour vérifier qu'une machine Linux associée à PBIS se trouve sur le domaine :

```
/opt/pbis/bin/domainjoin-cli query
<!--NeedCopy-->
```

Si la machine est associée à un domaine, cette commande renvoie les informations sur le domaine AD et l'unité d'organisation auxquels la machine est actuellement associée. Sinon, seul le nom d'hôte apparaît.

Vérifier l'authentification utilisateur Pour vérifier que PBIS peut authentifier les utilisateurs de domaine via PAM, ouvrez une session sur le Linux VDA à l'aide d'un compte d'utilisateur de domaine qui n'a jamais été utilisé.

```
sudo ssh localhost -l domain\user

id -u
<!--NeedCopy-->
```

Vérifiez qu'un fichier cache d'identification Kerberos correspondant a été créé pour le UID renvoyé par la commande **id -u** :


```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Quittez la session.

```
exit
<!--NeedCopy-->
```

Passez à l'étape 6 : installer le Linux VDA après vérification de la jonction du domaine.

Étape 4 : installer .NET Runtime 6.0 en tant que condition préalable

Avant d'installer Linux VDA, installez .NET Runtime 6.0 conformément aux instructions de l'article https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

Après avoir installé .NET Runtime 6.0, exécutez la commande **which dotnet** pour trouver votre chemin d'exécution.

En fonction de la sortie de la commande, définissez le chemin binaire de .NET Runtime. Par exemple, si la sortie de la commande est /aa/bb/dotnet, utilisez /aa/bb comme chemin binaire .NET.

Étape 5 : télécharger le package Linux VDA

1. Accédez à la page de téléchargement de Citrix Virtual Apps and Desktops.
2. Développez la version appropriée de Citrix Virtual Apps and Desktops.
3. Cliquez sur **Composants** pour télécharger le package Linux VDA qui correspond à votre distribution Linux et la clé publique GPG que vous pouvez utiliser pour vérifier l'intégrité du package Linux VDA.

   Pour vérifier l'intégrité du package Linux VDA à l'aide de la clé publique, importez la clé publique dans la base de données DEB et exécutez les commandes suivantes :

   ```
   ```
   sudo apt-get install dpkg-sig
   gpg --import <path to the public key>
   dpkg-sig --verify <path to the Linux VDA package>
   <!--NeedCopy--> ```
   ```

### Étape 6 : installer le Linux VDA

#### Étape 6a : installer le Linux VDA

Installez le logiciel Linux VDA à l'aide du gestionnaire de package Debian :

 
   ```

Pour Ubuntu 22.04 :

```
sudo dpkg -i xendesktopvda_<version>.ubuntu22.04_amd64.deb
<!--NeedCopy-->
```

Pour Ubuntu 20.04 :

```
sudo dpkg -i xendesktopvda_<version>.ubuntu20.04_amd64.deb
<!--NeedCopy-->
```

Pour Ubuntu 18.04 :

```
sudo dpkg -i xendesktopvda_<version>.ubuntu18.04_amd64.deb
<!--NeedCopy-->
```

Liste des dépendances Debian pour Ubuntu 22.04 :

```
postgresql >= 14

libpostgresql-jdbc-java >= 42.3

openjdk-11-jdk >= 11

imagemagick >= 8:6.9.11

libgtkmm-3.0-1v5 >= 3.24.5

ufw >= 0.36

ubuntu-desktop >= 1.481

libxrandr2 >= 2:1.5.2

libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8

util-linux >= 2.37

gtk3-nocsd >= 3

bash >= 5.1

findutils >= 4.8.0

sed >= 4.8

cups >= 2.4

libmspack0 >= 0.10

ibus >= 1.5

```



```
libgoogle-perftools4 >= 2.9~

libpython3.10 >= 3.10~

libsasl2-modules-gssapi-mit >= 2.1.~

libnss3-tools >= 2:3.68

libqt5widgets5 >= 5.15~

libqrencode4 >= 4.1.1

libimlib2 >= 1.7.4
<!--NeedCopy-->
```

Liste des dépendances Debian pour Ubuntu 20.04 :

```
postgresql >= 12

libpostgresql-jdbc-java >= 42.2

openjdk-11-jdk >= 11

imagemagick >= 8:6.9.10

libgtkmm-3.0-1v5 >= 3.24.2

ufw >= 0.36

ubuntu-desktop >= 1.450

libxrandr2 >= 2:1.5.2

libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8

util-linux >= 2.34

gtk3-nocsd >= 3

bash >= 5.0

findutils >= 4.7.0

sed >= 4.7

cups >= 2.3

libmspack0 >= 0.10

ibus >= 1.5

```



```
libgoogle-perftools4 >= 2.7~

libpython3.8 >= 3.8~

libsasl2-modules-gssapi-mit >= 2.1.~

libnss3-tools >= 2:3.49

libqt5widgets5 >= 5.7~

libqrencode4 >= 4.0.0

libimlib2 >= 1.6.1
<!--NeedCopy-->
```

Liste des dépendances Debian pour Ubuntu 18.04 :

```
postgresql >= 9.5

libpostgresql-jdbc-java >= 9.2

openjdk-11-jdk >= 11

imagemagick >= 8:6.8.9.9

ufw >= 0.35

libgtkmm-3.0-1v5 >= 3.22.2

ubuntu-desktop >= 1.361

libxrandr2 >= 2:1.5.0

libxtst6 >= 2:1.2.2

libxm4 >= 2.3.4

util-linux >= 2.27.1

gtk3-nocsd >= 3

bash >= 4.3

findutils >= 4.6.0

sed >= 4.2.2

cups >= 2.1

libmspack0 >= 0.6

ibus >= 1.5

```



```
libsasl2-modules-gssapi-mit >= 2.1.~

libgoogle-perftools4 >= 2.4~

libpython3.6 >= 3.6~

libnss3-tools >= 2:3.35

libqt5widgets5 >= 5.7~

libqrencode3 >= 3.4.4

libimlib2 >= 1.4.10
<!--NeedCopy-->
```

> **Remarque :**
>
> pour une matrice des distributions Linux et des versions Xorg que cette version du VDA Linux prend en charge, consultez la section Configuration système requise.

Étape 6b : mettre à niveau le Linux VDA (facultatif)

Vous pouvez effectuer une mise à niveau d'une installation existante à partir des deux versions précédentes et d'une version LTSR.

```
sudo dpkg -i <PATH>/<Linux VDA deb>
<!--NeedCopy-->
```

> **Remarque :**
>
> La mise à niveau d'une installation existante remplace les fichiers de configuration sous /etc/xdl. Avant de procéder à une mise à niveau, assurez-vous de sauvegarder les fichiers.

Étape 7 : installer les pilotes NVIDIA GRID

Pour activer HDX 3D Pro, vous devez installer les pilotes NVIDIA GRID sur votre hyperviseur et sur les machines VDA.

Pour installer et configurer le gestionnaire de GPU virtuel NVIDIA GRID (pilote hôte) sur les hyperviseurs spécifiques, consultez les guides suivants :

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

Pour installer et configurer les pilotes de VM invitée NVIDIA GRID, effectuez les opérations générales suivantes :

1. Assurez-vous que la VM invitée est arrêtée.
2. Dans le panneau de configuration de l'hyperviseur, attribuez un GPU à la VM.
3. Démarrez la VM.
4. Installez le pilote de VM invitée sur la VM.

Étape 8 : configurer le Linux VDA

Après l'installation du package, vous devez configurer le Linux VDA en exécutant le script ctxsetup.sh. Avant d'apporter des modifications, le script vérifie l'environnement et s'assure que toutes les dépendances sont installées. Si nécessaire, vous pouvez exécuter le script à tout moment pour modifier les paramètres.

Vous pouvez exécuter le script manuellement avec invite, ou automatiquement avec réponses préconfigurées. Consultez l'aide sur le script avant de continuer :

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
<!--NeedCopy-->
```

Configuration avec invites

Exécutez une configuration manuelle avec questions :

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

Configuration automatique

Pour une installation automatique, les options requises par le script d'installation peuvent être fournies avec des variables d'environnement. Si toutes les variables requises sont présentes, le script ne demande aucune information à l'utilisateur, ce qui permet de procéder à l'installation à l'aide d'un script.

Les variables d'environnement prises en charge sont les suivantes :

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N** : le Linux VDA prend en charge la spécification d'un nom de Delivery Controller à l'aide d'un enregistrement DNS CNAME. La valeur est définie par défaut sur N.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** : le Linux VDA requiert une liste séparée par des espaces de noms de domaines complets de Delivery Controller. Cette dernière sera utilisée pour l'enregistrement auprès d'un Delivery Controller. Au moins un alias de nom de domaine complet (FQDN) ou CNAME doit être spécifié.

- **CTX_XDL_VDA_PORT = port-number** : le Linux VDA communique avec les Delivery Controller à l'aide d'un port (80 par défaut) TCP/IP.
- **CTX_XDL_REGISTER_SERVICE = Y | N** : les services Linux VDA sont lancés après le démarrage de la machine. Valeur définie sur Y par défaut.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** : les services Linux VDA requièrent que les connexions réseau entrantes soient autorisées via le pare-feu du système. Vous pouvez ouvrir automatiquement les ports requis (ports 80 et 1494 par défaut) dans le pare-feu du système pour Linux VDA. Valeur définie sur Y par défaut.
- **CTX_XDL_AD_INTEGRATION = 1 | 2 | 3 | 4 |5** : le Linux VDA requiert que les paramètres de configuration Kerberos s'authentifient auprès des Delivery Controller. La configuration de Kerberos est déterminée depuis l'outil d'intégration d'Active Directory installé et configuré sur le système. Spécifiez la méthode d'intégration d'Active Directory prise en charge à utiliser :
  - 1 –Samba Winbind
  - 2 –Service d'authentification Quest
  - 3 –Centrify DirectControl
  - 4 –SSSD
  - 5 –PBIS
- **CTX_XDL_HDX_3D_PRO=Y | N** : Linux VDA prend en charge HDX 3D Pro, un ensemble de technologies d'accélération GPU conçues pour optimiser la virtualisation des applications riches en graphiques. Si HDX 3D Pro est sélectionné, le Virtual Delivery Agent doit être configuré pour le mode Bureaux VDI (session unique), c'est-à-dire, CTX_XDL_VDI_MODE=Y.
- **CTX_XDL_VDI_MODE=Y | N** : indique si la machine est configurée comme modèle de mise à disposition de bureaux dédiés (VDI) ou comme modèle de mise à disposition de bureaux partagés hébergés. Pour les environnements HDX 3D Pro, définissez cette variable sur Y. Elle est définie par défaut sur N.
- **CTX_XDL_SITE_NAME=dns-name** : le Linux VDA découvre les serveurs LDAP à l'aide de DNS. Pour limiter les résultats de recherche DNS à un site local, spécifiez un nom de site DNS. Cette variable est définie sur **<none>** par défaut.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** : le Linux VDA envoie une requête vers le DNS pour découvrir les serveurs LDAP. Si DNS ne peut pas fournir d'enregistrements de service LDAP, vous pouvez entrer une liste séparée par des espaces de noms de domaines complets LDAP avec ports LDAP. Par exemple, ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268. Si vous spécifiez le numéro de port LDAP 389, le Linux VDA interroge chaque serveur LDAP du domaine spécifié en mode d'interrogation. S'il existe un nombre x de stratégies et y de serveurs LDAP, le Linux VDA effectue le total de X multiplié par Y requêtes. Si le temps d'interrogation dépasse le seuil, les ouvertures de session peuvent

échouer. Pour activer les requêtes LDAP plus rapides, activez le **catalogue global** sur un contrôleur de domaine et définissez le numéro de port LDAP correspondant sur 3268. Cette variable est définie sur **<none>** par défaut.

- **CTX_XDL_SEARCH_BASE=search-base-set** : le Linux VDA envoie une requête à LDAP via une base de recherche définie sur la racine du domaine Active Directory (par exemple, D, DC=mycompany,DC=com). Toutefois, pour améliorer les performances de recherche, vous pouvez spécifier une base de recherche (par exemple, OU=VDI,DC=mycompany,DC=com). Cette variable est définie sur **<none>** par défaut.
- **CTX_XDL_FAS_LIST='list-fas-servers'** : les serveurs du service d'authentification fédérée (FAS) sont configurés via la stratégie de groupe AD. Le Linux VDA ne prend pas en charge la stratégie de groupe AD mais vous pouvez fournir une liste de serveurs FAS séparés par des points-virgules. La séquence doit être la même que celle configurée dans la stratégie de groupe AD. Si une adresse de serveur est supprimée, remplissez son espace vide avec la chaîne de texte **<none>** et ne modifiez pas l'ordre des adresses de serveur. Pour communiquer correctement avec les serveurs FAS, assurez-vous d'ajouter un numéro de port conforme à celui spécifié sur les serveurs FAS, par exemple CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'.
- **CTX_XDL_DOTNET_ runtime_path=Path-to-install-dotnet-runtime** : chemin d'accès à l'installation de .NET Runtime 6.0 pour la prise en charge du nouveau Broker Agent Service (`ctxvda`). Le chemin par défaut est /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate** : spécifie l'environnement de bureau GNOME, GNOME Classic ou MATE à utiliser dans les sessions. Si vous ne spécifiez pas la variable, le bureau actuellement installé sur le VDA est utilisé. Toutefois, si le bureau actuellement installé est MATE, vous devez définir la valeur de la variable sur **mate**.

  Vous pouvez également modifier l'environnement de bureau d'un utilisateur de session cible en procédant comme suit :

  1. Créez un fichier `.xsession` sous le répertoire **$HOME/<username>** sur le VDA.
  2. Modifiez le fichier `.xsession` pour spécifier un environnement de bureau basé sur les distributions.

     - **Pour le bureau MATE**

     ```
     MSESSION="$(type -p mate-session)"
     if [ -n "$MSESSION" ]; then
       exec mate-session
     fi
     ```

     - **Pour le bureau GNOME Classic**

     ```
     GSESSION="$(type -p gnome-session)"
     ```



```
if [ -n "$GSESSION" ]; then
export GNOME_SHELL_SESSION_MODE=classic
exec gnome-session --session=gnome-classic
fi
```

- **Pour le bureau GNOME**

```
GSESSION="$(type -p gnome-session)"
if [ -n "$GSESSION" ]; then
exec gnome-session
fi
```

3. Partagez l'autorisation de fichier 700 avec l'utilisateur de la session cible.

À partir de la version 2209, les utilisateurs de session peuvent personnaliser leurs environnements de bureau. Pour activer cette fonctionnalité, vous devez installer au préalable des environnements de bureau commutables sur le VDA. Pour plus d'informations, consultez Environnements de bureau personnalisés par utilisateurs de session.

- **CTX_XDL_START_SERVICE = Y | N** : indique si les services Linux VDA sont lancés lorsque la configuration de Linux VDA est terminée. Valeur définie sur Y par défaut.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** : port socket permettant d'écouter Citrix Scout. Le port par défaut est 7503.
- **CTX_XDL_TELEMETRY_PORT** : port de communication avec Citrix Scout. Le port par défaut est 7502.

Définissez la variable d'environnement et exécutez le script de configuration :

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3|4|5

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-site-name | '<none>'

export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'

export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'

```



```
export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<
   none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

Lors de l'exécution de la commande sudo, entrez l'option **-E** pour transmettre les variables d'environnement au nouveau shell créé. Nous vous recommandons de créer un fichier de script shell à partir des commandes précédentes avec **#!/bin/bash** en tant que première ligne.

Vous pouvez également spécifier tous les paramètres avec une seule commande :

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST='list-ddc-fqdns' \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4|5 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \
```



```
32
33 CTX_XDL_START_SERVICE=Y|N \
34
35 /opt/Citrix/VDA/sbin/ctxsetup.sh
36 <!--NeedCopy-->
```

Supprimer les modifications de configuration

Dans certains scénarios, il peut être nécessaire de supprimer les modifications de configuration effectuées par le script **ctxsetup.sh** sans désinstaller le package Linux VDA.

Consultez l'aide sur ce script avant de continuer :

```
1 sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
2 <!--NeedCopy-->
```

Pour supprimer les modifications de configuration :

```
1 sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
2 <!--NeedCopy-->
```

> **Important :**
>
> Ce script supprime toutes les données de configuration de la base de données et empêche Linux VDA de fonctionner.

Journaux de configuration

Les scripts **ctxsetup.sh** et **ctxcleanup.sh** affichent les erreurs dans la console, avec des informations supplémentaires consignées dans le fichier journal de configuration **/tmp/xdl.configure.log**.

Redémarrez les services de Linux VDA pour que les modifications prennent effet.

Désinstaller le logiciel Linux VDA

Pour vérifier que le Linux VDA est installé et pour afficher la version du package installé :

```
1 dpkg -l xendesktopvda
2 <!--NeedCopy-->
```

Pour afficher des informations plus détaillées :

```
1 apt-cache show xendesktopvda
2 <!--NeedCopy-->
```

Pour désinstaller le logiciel Linux VDA :


```
dpkg -r xendesktopvda
<!--NeedCopy-->
```

> **Remarque :**
>
> La désinstallation du logiciel Linux VDA supprime le PostgreSQL associé et d'autres données de configuration. Toutefois, le package PostgreSQL et les autres packages dépendants qui ont été installés avant l'installation du Linux VDA ne sont pas supprimés.
>
> **Conseil :**
>
> Les informations figurant dans cette section ne couvrent pas la suppression de packages dépendants, y compris PostgreSQL.

Étape 9 : exécuter XDPing

Exécutez `sudo /opt/Citrix/VDA/bin/xdping` pour vérifier les problèmes de configuration courants avec un environnement VDA Linux. Pour de plus amples informations, consultez la section XDPing.

Étape 10 : exécuter le Linux VDA

Une fois que vous avez configuré le Linux VDA à l'aide du script **ctxsetup.sh**, utilisez les commandes suivantes pour contrôler le Linux VDA.

Démarrer Linux VDA :

Pour démarrer les services Linux VDA :

```
sudo systemctl start ctxhdx

sudo systemctl start ctxvda
<!--NeedCopy-->
```

Arrêter Linux VDA :

Pour arrêter les services Linux VDA :

```
sudo systemctl stop ctxvda

sudo systemctl stop ctxhdx
<!--NeedCopy-->
```

> **Remarque :**
>
> Avant d'arrêter les services `ctxvda` et `ctxhdx`, exécutez la commande `service`

> `ctxmonitorservice stop` pour arrêter le démon du service de surveillance. Sinon, le démon du service de surveillance redémarre les services que vous avez arrêtés.

Redémarrer Linux VDA :

Pour redémarrer les services Linux VDA :

```
sudo systemctl stop ctxvda

sudo systemctl restart ctxhdx

sudo systemctl restart ctxvda
<!--NeedCopy-->
```

Vérifier l'état de Linux VDA :

Pour vérifier l'état de fonctionnement des services de Linux VDA :

```
sudo systemctl status ctxvda

sudo systemctl status ctxhdx
<!--NeedCopy-->
```

Étape 11 : créer le catalogue de machines dans Citrix Virtual Apps ou Citrix Virtual Desktops

Le processus de création de catalogues de machines et d'ajout de machines Linux VDA est similaire à l'approche traditionnelle avec les VDA Windows. Pour obtenir une description plus détaillée de la méthode à utiliser pour effectuer ces tâches, consultez les sections Créer des catalogues de machines et Gérer des catalogues de machines.

Pour la création de catalogues de machines contenant des machines Linux VDA, il existe quelques restrictions qui différencient ce processus de la création de catalogues de machines pour VDA Windows :

- Pour le système d'exploitation, sélectionnez :
  - l'option **OS à sessions multiples** pour un modèle de mise à disposition de bureaux partagés hébergés ;
  - l'option **OS mono-session** pour un modèle de mise à disposition de bureaux dédiés VDI.
- Ne combinez pas de machines Linux VDA et Windows dans le même catalogue de machines.

> **Remarque :**
>
> Les versions antérieures de Citrix Studio ne prenaient pas en charge la notion de « système d'exploitation Linux. » Toutefois, la sélection de l'option **OS de serveur Windows** ou **OS de serveur**

> implique un modèle de mise à disposition équivalent de bureaux partagés hébergés. La sélection de l'option **OS de bureau Windows** ou **OS de bureau** implique un modèle de mise à disposition d'un utilisateur unique par machine.
>
> **Conseil :**
>
> Si une supprimez une machine puis que vous la rejoignez au domaine Active Directory, vous devez supprimer et rajouter la machine au catalogue de machines.

Étape 12 : créer le groupe de mise à disposition dans Citrix Virtual Apps ou Citrix Virtual Desktops

Le processus de création d'un groupe de mise à disposition et d'ajout de catalogues de machines contenant des machines Linux VDA est presque identique aux machines VDA Windows. Pour obtenir une description plus détaillée de la méthode à utiliser pour effectuer ces tâches, consultez la section Créer des groupes de mise à disposition.

Lors de la création de groupes de mise à disposition qui contiennent des catalogues de machines Linux VDA, les restrictions suivantes s'appliquent :

- Assurez-vous que les utilisateurs et les groupes AD que vous sélectionnez ont été correctement configurés pour l'ouverture de session sur les machines Linux VDA.
- N'autorisez pas l'ouverture de session d'utilisateurs non authentifiés (anonymes).
- Ne combinez pas le groupe de mise à disposition avec des catalogues de machines contenant des machines Windows.

Pour plus d'informations sur la création de catalogues de machines et de groupes de mise à disposition, consultez Citrix Virtual Apps and Desktops 7 2209.

Installer manuellement Linux Virtual Delivery Agent pour Debian

December 16, 2022

> **Important :**
>
> Pour les nouvelles installations, nous vous recommandons d'utiliser Easy Install pour effectuer une installation rapide. Easy Install permet de gagner du temps et d'économiser de la main d'œuvre. Cette installation est également plus fiable que l'installation manuelle décrite dans cet article.

Étape 1 : préparer Debian pour l'installation du VDA

Étape 1a : vérifier la configuration réseau

Assurez-vous que le réseau est connecté et correctement configuré. Par exemple, vous devez configurer le serveur DNS sur le Linux VDA.

Étape 1b : définir le nom d'hôte

Pour vous assurer que le nom d'hôte de la machine est indiqué correctement, modifiez le fichier **/etc/hostname** afin que celui-ci contienne uniquement le nom d'hôte de la machine.

```
hostname
```

Étape 1c : attribuer une adresse de bouclage au nom d'hôte

Assurez-vous que le nom de domaine DNS et le nom de domaine complet (FQDN) de la machine sont signalés correctement. Pour ce faire, modifiez la ligne suivante du fichier **/etc/hosts** pour inclure le nom de domaine complet et le nom d'hôte en tant que deux premières entrées :

```
127.0.0.1 hostname-fqdn hostname localhost
```

Par exemple :

```
127.0.0.1 vda01.example.com vda01 localhost
```

Supprimez toute autre référence à `hostname-fqdn` ou `hostname` des autres entrées du fichier.

> **Remarque :**
>
> Le Linux VDA ne prend actuellement pas en charge la troncation de noms NetBIOS. Le nom d'hôte ne doit pas comporter plus de 15 caractères.
>
> **Conseil :**
>
> Utilisez uniquement les caractères a–z, A–Z, 0–9 et tiret (-). Évitez les caractères de soulignement (_), les espaces et autres symboles. Ne démarrez pas un nom d'hôte par un chiffre et ne le terminez pas par un tiret. Cette règle s'applique également aux noms d'hôte Delivery Controller.

Étape 1d : vérifier le nom d'hôte

Vérifiez que le nom d'hôte est correctement configuré :

```
hostname
<!--NeedCopy-->
```


Cette commande renvoie uniquement le nom d'hôte de la machine et non son nom de domaine complet.

Vérifiez que le nom de domaine complet est correctement configuré :

```
hostname -f
<!--NeedCopy-->
```

Cette commande renvoie le nom de domaine complet de la machine.

Étape 1e : désactiver DNS multidiffusion

Les paramètres par défaut activent DNS multidiffusion (**mDNS**), ce qui peut entraîner des résultats incohérents de résolution de nom.

Pour désactiver **mDNS**, modifiez **/etc/nsswitch.conf** et dans la ligne suivante remplacez :

```
hosts: files mdns_minimal [NOTFOUND=return] dns
```

par :

```
hosts: files dns
```

Étape 1f : vérifier la résolution de nom et l'accessibilité du service

Vérifiez que vous pouvez résoudre le nom de domaine complet et effectuer un sondage ping sur le contrôleur de domaine et le Delivery Controller :

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

ping delivery-controller-fqdn
<!--NeedCopy-->
```

Si vous ne pouvez pas résoudre le nom de domaine complet ou effectuer un sondage ping sur l'une de ces machines, reprenez les étapes avant de continuer.

Étape 1g : configurer la synchronisation de l'horloge (chrony)

Il est très important de maintenir la synchronisation de l'horloge entre les VDA, les Delivery Controller et les contrôleurs de domaine. L'hébergement du Linux VDA en tant que machine virtuelle peut entraîner des problèmes de décalage d'horloge. Pour cette raison, il est recommandé de synchroniser l'heure avec un service de temps à distance.

Installez chrony :

```
apt-get install chrony
<!--NeedCopy-->
```

En tant qu'utilisateur racine, modifiez **/etc/chrony/chrony.conf** et ajoutez une entrée de serveur pour chaque serveur de temps distant :

```
server peer1-fqdn-or-ip-address iburst
server peer2-fqdn-or-ip-address iburst
```

Dans un déploiement type, synchronisez l'heure depuis les contrôleurs de domaine locaux et non pas directement depuis des serveurs de pool NTP publics. Ajoutez une entrée de serveur pour chaque contrôleur de domaine Active Directory du domaine.

Supprimez toute autre entrée **server** ou **pool** répertoriée, y compris les entrées d'adresse IP de bouclage, localhost et ***.pool.ntp.org** de serveur public.

Enregistrez les modifications et redémarrez le démon Chrony :

```
sudo systemctl restart chrony
<!--NeedCopy-->
```

Étape 1h : installer les packages

```
sudo apt-get install -y libsasl2-2

sudo apt-get install -y libgtk2.0-0
<!--NeedCopy-->
```

Étape 1i : ajouter des référentiels pour installer les dépendances nécessaires

Pour Debian 11.3, ajoutez la ligne `deb http://deb.debian.org/debian/ bullseye main` au fichier /etc/apt/sources.list.

Étape 1j : installer PostgreSQL

Le Linux VDA requiert PostgreSQL sur Debian :

```
sudo apt-get install -y postgresql

sudo apt-get install -y libpostgresql-jdbc-java
<!--NeedCopy-->
```


Étape 2 : préparer l'hyperviseur

Certaines modifications sont requises pour l'exécution du Linux VDA en tant que machine virtuelle sur un hyperviseur pris en charge. Apportez les modifications suivantes en fonction de la plateforme d'hyperviseur utilisée. Aucune modification n'est requise si vous utilisez la machine Linux sur un matériel bare metal.

Corriger la synchronisation de l'heure sur Citrix Hypervisor

Si la fonctionnalité de synchronisation de l'heure de Citrix Hypervisor est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée avec NTP et Citrix Hypervisor. En effet, les deux systèmes essaient de gérer l'horloge système. Pour éviter que l'horloge ne soit plus synchronisée avec d'autres serveurs, assurez-vous l'horloge du système de chaque invité Linux est synchronisée avec NTP. Cela nécessite la désactivation de la synchronisation de l'heure de l'hôte. Aucune modification n'est requise en mode HVM.

Si vous utilisez un noyau Linux paravirtualisé avec le composant Citrix VM Tools installé, vous pouvez vérifier si la fonctionnalité de synchronisation de l'heure de Citrix Hypervisor est présente et activée à partir de la VM Linux :

```
su -
cat /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Cette commande renvoie 0 ou 1 :

- 0 - La fonctionnalité de synchronisation de l'heure est activée, et doit être désactivée.
- 1 - La fonctionnalité de synchronisation de l'heure est désactivée, et aucune action n'est requise.

Si le fichier /proc/sys/xen/independent_wallclock n'existe pas, les étapes suivantes ne sont pas nécessaires.

Si la fonctionnalité de synchronisation est activée, désactivez-la en entrant 1 dans le fichier :

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Pour rendre cette modification permanente et persistante après le redémarrage, modifiez le fichier **/etc/sysctl.conf** et ajoutez la ligne :

```
xen.independent_wallclock = 1
```

Pour vérifier ces modifications, redémarrez le système :

```
su -
cat /proc/sys/xen/independent_wallclock
```



```
<!--NeedCopy-->
```

Cette commande renvoie la valeur 1.

Corriger la synchronisation de l'heure sur Microsoft Hyper-V

Les VM Linux sur lesquelles Hyper-V Integration Services est installé peuvent utiliser la fonctionnalité de synchronisation de l'heure Hyper-V pour utiliser l'heure du système d'exploitation hôte. Pour vous assurer que l'horloge du système est toujours précise, activez cette fonctionnalité avec les services NTP.

Depuis le système d'exploitation de gestion :

1. Ouvrez la console du gestionnaire Hyper-V.
2. Pour les paramètres d'une machine virtuelle Linux, sélectionnez **Integration Services**.
3. Assurez-vous que **Time synchronization** est sélectionné.

> **Remarque :**
>
> cette approche diffère de VMware et Citrix Hypervisor, pour lesquels la synchronisation de l'heure est désactivée pour éviter tout conflit avec NTP. La synchronisation de l'heure Hyper-V peut co-exister avec la synchronisation de l'heure NTP.

Corriger la synchronisation de l'heure sur ESX et ESXi

Si la fonctionnalité de synchronisation de l'heure de VMware est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée avec l'hyperviseur et NTP. En effet, les deux systèmes essaient de synchroniser l'horloge système. Pour éviter que l'horloge ne soit plus synchronisée avec d'autres serveurs, assurez-vous l'horloge du système de chaque invité Linux est synchronisée avec NTP. Cela nécessite la désactivation de la synchronisation de l'heure de l'hôte.

Si vous exécutez un noyau Linux paravirtualisé sur lequel VMware Tools est installé :

1. Ouvrez vSphere Client.
2. Modifiez les paramètres pour la VM Linux.
3. Dans la boîte de dialogue **Virtual Machine Properties** (Propriétés de la machine virtuelle), ouvrez l'onglet **Options**.
4. Sélectionnez **VMware Tools**.
5. Dans la zone **Advanced** (Avancé), désélectionnez **Synchronize guest time with host** (Synchroniser l'heure de l'invité avec l'hôte).

Étape 3 : ajouter la machine virtuelle (VM) Linux au domaine Windows

Le Linux VDA prend en charge plusieurs méthodes pour ajouter des machines Linux au domaine Active Directory (AD) :

- Samba Winbind
- Quest Authentication Service
- Centrify DirectControl
- SSSD
- PBIS

Suivez les instructions en fonction de la méthode choisie.

> **Remarque :**
>
> Les lancements de session peuvent échouer lorsque le même nom d'utilisateur est utilisé pour le compte local dans le Linux VDA et le compte dans AD.

Samba Winbind

Installer ou mettre à jour les packages requis

```
sudo apt-get install winbind samba libnss-winbind libpam-winbind krb5-config krb5-locales krb5-user
<!--NeedCopy-->
```

Activer le démon Winbind pour qu'il soit lancé au démarrage de la machine Le démon Winbind doit être configuré pour être lancé au démarrage de la machine :

```
sudo systemctl enable winbind
<!--NeedCopy-->
```

> **Remarque :**
>
> Assurez-vous que le script `winbind` se trouve sous `/etc/init.d`.

Configurer Kerberos Ouvrez **/etc/krb5.conf** en tant qu'utilisateur racine et configurez les paramètres suivants :

> **Remarque :**
>
> Configurez Kerberos en fonction de votre infrastructure AD. Les paramètres suivants sont destinés au modèle à domaine et à forêt uniques.

```
[libdefaults]
default_realm = REALM
```



```
dns_lookup_kdc = false

[realms]

REALM = {

admin_server = domain-controller-fqdn

kdc = domain-controller-fqdn

}

[domain_realm]

domain-dns-name = REALM

.domain-dns-name = REALM
```

Le paramètre **domain-dns-name** dans ce contexte est le nom de domaine DNS, tel que **example.com**. L'élément **REALM** est le nom du domaine Kerberos en majuscules, tel que **EXAMPLE.COM**.

Configurer l'authentification Winbind Ouvrez **/etc/samba/smb.conf** et configurez les paramètres suivants :

```
[global]

workgroup = WORKGROUP

security = ADS

realm = REALM

encrypt passwords = yes

idmap config *:range = 16777216-33554431

winbind trusted domains only = no

kerberos method = secrets and keytab

winbind refresh tickets = yes

template shell = /bin/bash
```

WORKGROUP est le premier champ dans **REALM**, et **REALM** est le nom de domaine Kerberos en majuscules.

Configurer `nsswitch` Ouvrez **/etc/nsswitch.conf** et ajoutez `winbind` aux lignes suivantes :

```
passwd: systemd winbind
group: systemd winbind
```


Rejoindre un domaine Windows Votre contrôleur de domaine doit être accessible et vous devez disposer d'un compte utilisateur Active Directory avec les autorisations nécessaires pour ajouter des ordinateurs au domaine :

```
sudo net ads join REALM -U user
<!--NeedCopy-->
```

Où **REALM** est le nom de domaine Kerberos en majuscules, et **user** est un utilisateur de domaine disposant des autorisations nécessaires pour ajouter les ordinateurs au domaine.

Redémarrer Winbind

```
sudo systemctl restart winbind
<!--NeedCopy-->
```

Configurer PAM pour Winbind Exécutez la commande suivante et assurez-vous que les options **Winbind NT/Active Directory authentication** et **Create home directory on login** sont sélectionnées :

```
sudo pam-auth-update
<!--NeedCopy-->
```

> **Conseil :**
>
> Le démon `winbind` ne reste en cours d'exécution que si la machine est associée à un domaine.

Vérifier l'appartenance à un domaine Le Delivery Controller requiert que toutes les machines VDA, Windows ou Linux, aient un objet ordinateur dans `Active Directory`.

Exécutez la commande **net ads** de **Samba** pour vérifier que la machine est associée à un domaine :

```
sudo net ads testjoin
<!--NeedCopy-->
```

Exécutez la commande suivante pour vérifier les informations d'objet de domaine et d'ordinateur supplémentaires :

```
sudo net ads info
<!--NeedCopy-->
```

Vérifier la configuration de Kerberos Pour vérifier que Kerberos est correctement configuré pour être utilisé avec le Linux VDA, vérifiez que le fichier **keytab** système a été créé et contient des clés valides :

```
sudo klist -ke
<!--NeedCopy-->
```


Cette commande affiche la liste des clés disponibles pour les différentes combinaisons de noms principaux et de suites de chiffrement. Exécutez la commande **kinit** Kerberos pour authentifier la machine auprès du contrôleur de domaine à l'aide de ces clés :

```
sudo kinit -k MACHINE$@REALM
<!--NeedCopy-->
```

Les noms de machine et de domaine doivent être spécifiés en majuscules. Le signe dollar ($) doit être placé dans une séquence d'échappement avec une barre oblique inverse (\) pour empêcher le remplacement shell. Dans certains environnements, le nom de domaine DNS est différent du nom de domaine Kerberos. Assurez-vous que le nom de domaine est utilisé. Si cette commande réussit, aucun résultat n'est affiché.

Vérifiez que le ticket TGT pour le compte de machine a été mis en cache à l'aide de :

```
sudo klist
<!--NeedCopy-->
```

Examinez les détails du compte de machine à l'aide de :

```
sudo net ads status
<!--NeedCopy-->
```

Vérifier l'authentification utilisateur Utilisez l'outil **wbinfo** pour vérifier que les utilisateurs de domaine peuvent s'authentifier auprès du domaine :

```
wbinfo --krb5auth=domain\username%password
<!--NeedCopy-->
```

Le domaine spécifié ici est le nom de domaine Active Directory, et non le nom de domaine Kerberos. Pour le shell bash, la barre oblique inverse (\) doit être placée dans une séquence d'échappement avec une autre barre oblique inverse. Cette commande renvoie un message indiquant la réussite ou l'échec.

Pour vérifier que le module PAM Winbind est correctement configuré, ouvrez une session sur le Linux VDA à l'aide d'un compte d'utilisateur de domaine qui n'a jamais été utilisé.

```
ssh localhost -l domain\username

id -u
<!--NeedCopy-->
```

> **Remarque :**
>
> Pour exécuter une commande SSH avec succès, assurez-vous que SSH est activé et fonctionne correctement.

Vérifiez qu'un fichier cache d'identification Kerberos correspondant a été créé pour le UID renvoyé par la commande **id -u** :

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Vérifiez que les tickets dans le cache d'identification Kerberos de l'utilisateur sont valides et n'ont pas expiré :

```
klist
<!--NeedCopy-->
```

Quittez la session.

```
exit
<!--NeedCopy-->
```

Le même test peut être réalisé en ouvrant une session directement sur la console KDE ou Gnome. Passez à l'étape 6 : installer le Linux VDA après vérification de la jonction du domaine.

> **Conseil :**
>
> Si l'authentification utilisateur réussit mais que vous ne pouvez pas afficher votre bureau lors de la connexion avec un compte de domaine, redémarrez la machine et réessayez.

Service d'authentification Quest

Configurer Quest sur le contrôleur de domaine Cette procédure suppose que vous avez installé et configuré le logiciel Quest sur les contrôleurs de domaine Active Directory et disposez des droits Administrateur pour créer des objets ordinateur dans `Active Directory`.

Autoriser les utilisateurs de domaine à ouvrir une session sur des machines Linux VDA Pour autoriser les utilisateurs de domaine à établir des sessions HDX sur une machine Linux VDA :

1. Dans la console de gestion Utilisateurs et ordinateurs Active Directory, ouvrez les propriétés de l'utilisateur Active Directory pour ce compte d'utilisateur.
2. Sélectionnez l'onglet **Unix Account**.
3. Sélectionnez **Unix-enabled**.
4. Définissez **Primary GID Number** sur l'ID d'un groupe d'utilisateurs de domaine.

> **Remarque :**
>
> Ces instructions sont les mêmes que pour la configuration d'utilisateurs de domaine pour l'ouverture de session à l'aide de la console, RDP, SSH ou tout autre protocole de communication à distance.

Configurer Quest sur un Linux VDA

Solution à l'application forcée de la stratégie SELinux L'environnement RHEL par défaut applique entièrement SELinux. Cette mise en œuvre interfère avec les mécanismes IPC de socket de domaine Unix utilisés par Quest et empêche les utilisateurs de domaine d'ouvrir une session.

Le moyen pratique de remédier à ce problème consiste à désactiver SELinux. En tant qu'utilisateur racine, modifiez **/etc/selinux/config** en modifiant le paramètre **SELinux** :

```
SELINUX=disabled
```

Cette modification nécessite le redémarrage de la machine :

```
reboot
<!--NeedCopy-->
```

> **Important :**
>
> Utilisez ce paramètre avec précaution. La réactivation de l'application forcée de la stratégie SELinux après sa désactivation peut entraîner un verrouillage complet, même pour l'utilisateur racine et d'autres utilisateurs locaux.

Configurer le démon VAS Le renouvellement automatique des tickets Kerberos doit être activé et déconnecté. L'authentification (ouverture de session en mode déconnecté) doit être désactivée :

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-
    interval 32400

sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-
    auth false
<!--NeedCopy-->
```

Cette commande définit l'intervalle de renouvellement sur 9 heures (32 400 secondes), ce qui représente une heure de moins que la valeur par défaut de 10 heures pour la durée de vie d'un ticket. Définissez ce paramètre sur une valeur inférieure sur les systèmes avec une durée de vie de ticket plus courte.

Configuration de PAM et de NSS Pour permettre l'ouverture de session d'utilisateur de domaine via HDX et d'autres services tels que su, ssh et RDP, exécutez les commandes suivantes pour configurer manuellement PAM et NSS :

```
sudo /opt/quest/bin/vastool configure pam
sudo /opt/quest/bin/vastool configure nss
<!--NeedCopy-->
```


Rejoindre un domaine Windows Joignez la machine Linux au domaine Active Directory à l'aide de la commande Quest `vastool` :

```
sudo /opt/quest/bin/vastool -u user join domain-name
<!--NeedCopy-->
```

L'utilisateur est un utilisateur de domaine disposant des autorisations nécessaires pour associer des ordinateurs au domaine Active Directory. Le paramètre `domain-name` est le nom DNS du domaine ; par exemple, exemple.com.

Vérifier l'appartenance à un domaine Le Delivery Controller requiert que toutes les machines VDA, Windows ou Linux, aient un objet ordinateur dans `Active Directory`. Pour vérifier qu'une machine Linux associée à Quest se trouve sur le domaine :

```
sudo /opt/quest/bin/vastool info domain
<!--NeedCopy-->
```

Si la machine est associée à un domaine, cette commande renvoie le nom de domaine. Si la machine n'est pas associée à un domaine, l'erreur suivante apparaît :

```
ERROR: No domain could be found.
ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm
default_realm not configured in vas.conf. Computer may not be joined
to domain
```

Vérifier l'authentification utilisateur Pour vérifier que Quest peut authentifier les utilisateurs de domaine via PAM, ouvrez une session sur le Linux VDA à l'aide d'un compte d'utilisateur de domaine qui n'a jamais été utilisé.

```
ssh localhost -l domain\username

id -u
<!--NeedCopy-->
```

Vérifiez qu'un fichier cache d'identification Kerberos correspondant a été créé pour le UID renvoyé par la commande **id -u** :

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Vérifiez que les tickets dans le cache d'identification de Kerberos sont valides et n'ont pas expiré :

```
/opt/quest/bin/vastool klist
<!--NeedCopy-->
```

Quittez la session.


```
exit
<!--NeedCopy-->
```

Passez à l'étape 6 : installer le Linux VDA après vérification de la jonction du domaine.

Centrify DirectControl

Rejoindre un domaine Windows Une fois Centrify DirectControl Agent installé, associez la machine Linux au domaine Active Directory à l'aide de la commande Centrify `adjoin` :

```
su -
adjoin -w -V -u user domain-name
<!--NeedCopy-->
```

Le paramètre **user** est un utilisateur de domaine Active Directory disposant des autorisations nécessaires pour joindre des ordinateurs au domaine Active Directory. Le paramètre **domain-name** est le nom du domaine auquel associer la machine Linux.

Vérifier l'appartenance à un domaine Le Delivery Controller requiert que toutes les machines VDA, Windows ou Linux, aient un objet ordinateur dans Active Directory. Pour vérifier qu'une machine Linux associée à Centrify se trouve sur le domaine :

```
su -

adinfo
<!--NeedCopy-->
```

Vérifiez que la valeur **Joined to domain** est valide et que **CentrifyDC mode** renvoie **connected**. Si le mode reste bloqué à l'état de démarrage, le client Centrify rencontre des problèmes de connexion au serveur ou d'authentification.

Des informations plus complètes sur le système et les diagnostics sont disponibles à l'aide de :

```
adinfo --sysinfo all

adinfo --diag
<!--NeedCopy-->
```

Testez la connectivité avec les différents services Active Directory et Kerberos.

```
adinfo --test
<!--NeedCopy-->
```

Passez à l'étape 6 : installer le Linux VDA après vérification de la jonction du domaine.

SSSD

Configurer Kerberos Exécutez la commande suivante pour installer Kerberos :

```
sudo apt-get install krb5-user
<!--NeedCopy-->
```

Pour configurer Kerberos, ouvrez **/etc/krb5.conf** en tant qu'utilisateur racine et définissez les paramètres :

> **Remarque :**
>
> Configurez Kerberos en fonction de votre infrastructure AD. Les paramètres suivants sont destinés au modèle à domaine et à forêt uniques.

```
[libdefaults]
default_realm = REALM
dns_lookup_kdc = false
[realms]
REALM = {
admin_server = domain-controller-fqdn
kdc = domain-controller-fqdn
}
[domain_realm]
domain-dns-name = REALM
.domain-dns-name = REALM
```

La propriété `domain-dns-name` dans ce contexte est le nom de domaine DNS, tel que example.com. L'élément *REALM* est le nom du domaine Kerberos en majuscules, tel que EXAMPLE.COM.

Joindre le domaine SSSD doit être configuré pour pouvoir utiliser Active Directory en tant que fournisseur d'identité et Kerberos pour l'authentification. Toutefois, SSSD ne fournit pas de fonctions de client Active Directory pour rejoindre le domaine et gérer le fichier keytab du système. Vous pouvez utiliser **adcli**, **realmd**ou **Samba** à la place.

> **Remarque :**
>
> Cette section fournit des informations uniquement pour **adcli** et **Samba**.

- **Si vous utilisez adcli pour rejoindre le domaine, procédez comme suit :**

1. Installez **adcli**.

```
sudo apt-get install adcli
<!--NeedCopy-->
```

2. Rejoignez le domaine avec **adcli**.

   Supprimez l'ancien fichier keytab du système et rejoignez le domaine à l'aide de :

```
su -

rm -rf /etc/krb5.keytab

adcli join domain-dns-name -U user -H hostname-fqdn
<!--NeedCopy-->
```

   user est un utilisateur du domaine autorisé à ajouter des machines au domaine. **hostname-fqdn** est le nom d'hôte au format FQDN de la machine.

   L'option **-H** est requise pour permettre à **adcli** de générer SPN au format host/hostname-fqdn@REALM, ce qui est requis par Linux VDA.

3. Vérifiez le fichier keytab système.

   Exécutez la commande `sudo klist -ket` pour vous assurer que le fichier keytab système a été créé.

   Vérifiez que l'horodatage de chaque clé correspond à l'heure à laquelle la machine a été jointe au domaine.

- **Si vous utilisez Samba pour rejoindre le domaine, procédez comme suit :**

1. Installez le pack.

```
sudo apt-get install samba krb5-user
<!--NeedCopy-->
```

2. Configurer **Samba**.

   Ouvrez **/etc/samba/smb.conf** et configurez les paramètres suivants :

```
[global]

workgroup = WORKGROUP

security = ADS

realm = REALM

client signing = yes

client use spnego = yes

kerberos method = secrets and keytab
```


WORKGROUP est le premier champ dans **REALM**, et **REALM** est le nom de domaine Kerberos en majuscules.

3. Rejoignez le domaine avec **Samba**.

   Votre contrôleur de domaine doit être accessible et vous devez disposer d'un compte Windows avec les autorisations nécessaires pour ajouter des ordinateurs au domaine.

   ```
   sudo net ads join REALM -U user
   <!--NeedCopy-->
   ```

   Où **REALM** est le nom de domaine Kerberos en majuscules, et **user** est un utilisateur de domaine disposant des autorisations nécessaires pour ajouter les ordinateurs au domaine.

Configurer SSSD **Installer ou mettre à jour les packages requis :**

Installez les packages de configuration et SSSD requis s'ils ne sont pas déjà installés :

```
sudo apt-get install sssd
<!--NeedCopy-->
```

Si les packages sont déjà installés, une mise à jour est recommandée :

```
sudo apt-get install --only-upgrade sssd
<!--NeedCopy-->
```

> **Remarque :**
>
> Par défaut, le processus d'installation dans Ubuntu configure automatiquement **nsswitch.conf** et le module de connexion PAM.

Configurer SSSD Des modifications doivent être apportées à la configuration SSSD avant de démarrer le démon SSSD. Pour certaines versions de SSSD, le fichier de configuration **/etc/sssd/sssd.conf** n'est pas installé par défaut et doit être créé manuellement. En tant qu'utilisateur racine, créez ou ouvrez **/etc/sssd/sssd.conf** et configurez les paramètres suivants :

```
[sssd]
services = nss, pam
config_file_version = 2
domains = domain-dns-name
[domain/domain-dns-name]
id_provider = ad
access_provider = ad
```



```
auth_provider = krb5

krb5_realm =REALM

# Set krb5_renewable_lifetime higher if TGT renew lifetime is longer
than 14 days

krb5_renewable_lifetime = 14d

# Set krb5_renew_interval to lower value if TGT ticket lifetime is
shorter than 2 hours

krb5_renew_interval = 1h

krb5_ccachedir = /tmp

krb5_ccname_template = FILE:%d/krb5cc_%U

# This ldap_id_mapping setting is also the default value

ldap_id_mapping = true

override_homedir = /home/%d/%u

default_shell = /bin/bash

ad_gpo_map_remote_interactive = +ctxhdx
```

> **Remarque :**
>
> ldap_id_mapping est défini sur **true** de façon à ce que SSSD se charge de mapper les SID Windows avec les UID Unix. Sinon, `Active Directory` doit être en mesure de fournir des extensions POSIX. Le service PAM `ctxhdx` est ajouté au paramètre ad_gpo_map_remote_interactive.
>
> Le paramètre **domain-dns-name** dans ce contexte est le nom de domaine DNS, tel que example.com. L'élément **REALM** est le nom du domaine Kerberos en majuscules, tel que EXAMPLE.COM. Il n'est pas nécessaire de configurer le nom de domaine NetBIOS.
>
> Pour de plus amples informations sur les paramètres de configuration, consultez les pages man pour sssd.conf et `sssd-ad`.

Le démon SSSD nécessite que le fichier de configuration dispose uniquement de l'autorisation d'accès en lecture de propriétaire :

```
1 sudo chmod 0600 /etc/sssd/sssd.conf
2 <!--NeedCopy-->
```

Démarrer le démon SSSD Exécutez les commandes suivantes pour démarrer le démon SSSD maintenant et pour permettre le lancement du démon au démarrage de la machine :


```
sudo systemctl start sssd

sudo systemctl enable sssd
<!--NeedCopy-->
```

Configuration de PAM Exécutez la commande suivante et assurez-vous que les options **SSS authentication** et **Create home directory on login** sont sélectionnées :

```
sudo pam-auth-update
<!--NeedCopy-->
```

Vérifier l'appartenance à un domaine Le Delivery Controller requiert que toutes les machines VDA (VDA Windows et Linux) aient un objet ordinateur dans `Active Directory`.

- Si vous utilisez **adcli** pour vérifier l'appartenance à un domaine, exécutez la commande `sudo adcli info domain-dns-name` pour afficher les informations sur le domaine.
- Si vous utilisez **Samba** pour vérifier l'appartenance à un domaine, exécutez la commande `sudo net ads testjoin` pour vérifier que la machine est jointe à un domaine et la commande `sudo net ads info` pour vérifier des informations supplémentaires sur le domaine et l'objet Ordinateur.

Vérifier la configuration de Kerberos Pour vérifier que Kerberos est correctement configuré pour être utilisé avec le Linux VDA, vérifiez que le fichier keytab système a été créé et contient des clés valides :

```
sudo klist -ke
<!--NeedCopy-->
```

Cette commande affiche la liste des clés disponibles pour les différentes combinaisons de noms principaux et de suites de chiffrement. Exécutez la commande `kinit` Kerberos pour authentifier la machine auprès du contrôleur de domaine à l'aide de ces clés :

```
sudo kinit -k MACHINE$@REALM
<!--NeedCopy-->
```

Les noms de machine et de domaine doivent être spécifiés en majuscules. Le signe dollar ($) doit être placé dans une séquence d'échappement avec une barre oblique inverse (\) pour empêcher le remplacement shell. Dans certains environnements, le nom de domaine DNS est différent du nom de domaine Kerberos. Assurez-vous que le nom de domaine est utilisé. Si cette commande réussit, aucun résultat n'est affiché.

Vérifiez que le TGT pour le compte de machine a été mis en cache à l'aide de :


```
sudo klist
<!--NeedCopy-->
```

Vérifier l'authentification utilisateur SSSD ne fournit pas d'outil de ligne de commande pour tester l'authentification directement avec le démon. Cela peut uniquement être effectué via PAM.

Pour vérifier que le module PAM SSSD est correctement configuré, ouvrez une session sur le Linux VDA à l'aide d'un compte d'utilisateur de domaine qui n'a jamais été utilisé.

```
ssh localhost -l domain\username

id -u

klist

exit
<!--NeedCopy-->
```

Vérifiez que les tickets Kerberos renvoyés par la commande **klist** sont corrects pour cet utilisateur et qu'ils n'ont pas expiré.

En tant qu'utilisateur racine, vérifiez qu'un fichier cache de ticket correspondant a été créé pour l'UID renvoyé par la commande **id -u** précédente :

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Le même test peut être réalisé en ouvrant une session directement sur KDE ou Gnome Display Manager. Passez à l'étape 6 : installer le Linux VDA après vérification de la jonction du domaine.

PBIS

Télécharger le package PBIS requis

```
sudo wget https://github.com/BeyondTrust/pbis-open/releases/download
   /9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh
<!--NeedCopy-->
```

Rendre le script d'installation PBIS exécutable

```
sudo chmod +x pbis-open-9.1.0.551.linux.x86_64.deb.sh
<!--NeedCopy-->
```

Exécuter le script d'installation PBIS

```
sudo sh pbis-open-9.1.0.551.linux.x86_64.deb.sh
<!--NeedCopy-->
```


Rejoindre un domaine Windows Votre contrôleur de domaine doit être accessible et vous devez disposer d'un compte utilisateur Active Directory avec les autorisations nécessaires pour ajouter des ordinateurs au domaine :

```
sudo /opt/pbis/bin/domainjoin-cli join domain-name user
<!--NeedCopy-->
```

L'**utilisateur** est un utilisateur de domaine disposant des autorisations nécessaires pour ajouter des ordinateurs au domaine Active Directory. Le paramètre **domain-name** est le nom DNS du domaine ; par exemple, exemple.com.

Remarque : pour définir Bash en tant que shell par défaut, exécutez la commande **sudo /opt/pbis/bin/config LoginShellTemplate/bin/bash**.

Vérifier l'appartenance à un domaine Le Delivery Controller requiert que toutes les machines VDA (VDA Windows et Linux) aient un objet ordinateur dans `Active Directory`. Pour vérifier qu'une machine Linux associée à PBIS se trouve sur le domaine :

```
/opt/pbis/bin/domainjoin-cli query
<!--NeedCopy-->
```

Si la machine est associée à un domaine, cette commande renvoie les informations sur le domaine AD et l'unité d'organisation auxquels la machine est actuellement associée. Sinon, seul le nom d'hôte apparaît.

Vérifier l'authentification utilisateur Pour vérifier que PBIS peut authentifier les utilisateurs de domaine via PAM, ouvrez une session sur le Linux VDA à l'aide d'un compte d'utilisateur de domaine qui n'a jamais été utilisé.

```
sudo ssh localhost -l domain\user

id -u
<!--NeedCopy-->
```

Vérifiez qu'un fichier cache d'identification Kerberos correspondant a été créé pour le UID renvoyé par la commande **id -u** :

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Quittez la session.

```
exit
<!--NeedCopy-->
```

Passez à l'étape 6 : installer le Linux VDA après vérification de la jonction du domaine.

Étape 4 : installer .NET Runtime 6.0 en tant que condition préalable

Avant d'installer Linux VDA, installez .NET Runtime 6.0 conformément aux instructions de l'article https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

Après avoir installé .NET Runtime 6.0, exécutez la commande **which dotnet** pour trouver votre chemin d'exécution.

En fonction de la sortie de la commande, définissez le chemin binaire de .NET Runtime. Par exemple, si la sortie de la commande est /aa/bb/dotnet, utilisez /aa/bb comme chemin binaire .NET.

Étape 5 : télécharger le package Linux VDA

1. Accédez à la page de téléchargement de Citrix Virtual Apps and Desktops.
2. Développez la version appropriée de Citrix Virtual Apps and Desktops.
3. Cliquez sur **Composants** pour télécharger le package Linux VDA qui correspond à votre distribution Linux et la clé publique GPG que vous pouvez utiliser pour vérifier l'intégrité du package Linux VDA.

   Pour vérifier l'intégrité du package Linux VDA, importez la clé publique dans la base de données DEB et exécutez les commandes suivantes :

   ```
   ```
   sudo apt-get install dpkg-sig
   gpg --import <path to the public key>
   dpkg-sig --verify <path to the Linux VDA package>
   <!--NeedCopy--> ```
   ```

### Étape 6 : installer le Linux VDA

#### Étape 6a : installer le Linux VDA

Installez le logiciel Linux VDA à l'aide du gestionnaire de package Debian :

```
sudo dpkg -i xendesktopvda_<version>.debian10_amd64.deb
<!--NeedCopy-->
```

Liste des dépendances pour Debian 11.3 :

```
postgresql >= 13

libpostgresql-jdbc-java >= 42.2

openjdk-11-jdk >= 11

```


```

```
imagemagick >= 8:6.9.10

ufw >= 0.36

desktop-base >= 10.0.2

libxrandr2 >= 2:1.5.1

libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8

util-linux >= 2.33

gtk3-nocsd >= 3

bash >= 5.0

findutils >= 4.6.0

sed >= 4.7

cups >= 2.2

ghostscript >= 9.53~

libmspack0 >= 0.10

ibus >= 1.5

libgoogle-perftools4 >= 2.7~

libpython3.9 >= 3.9~

libsasl2-modules-gssapi-mit >= 2.1.~

libqt5widgets5 >= 5.5~

mutter >= 3.38.6~

libqrencode4 >= 4.0.0

libimlib2 >= 1.5.1
<!--NeedCopy-->
```

> **Remarque :**
>
> pour une matrice des distributions Linux et des versions Xorg que cette version du VDA Linux prend en charge, consultez la section Configuration système requise.

Étape 6b : mettre à niveau le Linux VDA (facultatif)

Vous pouvez effectuer une mise à niveau d'une installation existante à partir des deux versions précédentes et d'une version LTSR.

```
sudo dpkg -i <PATH>/<Linux VDA deb>
<!--NeedCopy-->
```

> **Remarque :**
>
> La mise à niveau d'une installation existante remplace les fichiers de configuration sous /etc/xdl. Avant de procéder à une mise à niveau, assurez-vous de sauvegarder les fichiers.

Étape 7 : installer les pilotes NVIDIA GRID

Pour activer HDX 3D Pro, vous devez installer les pilotes NVIDIA GRID sur votre hyperviseur et sur les machines VDA.

Pour installer et configurer le gestionnaire de GPU virtuel NVIDIA GRID (pilote hôte) sur les hyperviseurs spécifiques, consultez les guides suivants :

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

Pour installer et configurer les pilotes de VM invitée NVIDIA GRID, effectuez les opérations générales suivantes :

1. Assurez-vous que la VM invitée est arrêtée.
2. Dans le panneau de configuration de l'hyperviseur, attribuez un GPU à la VM.
3. Démarrez la VM.
4. Installez le pilote de VM invitée sur la VM.

Étape 8 : configurer le Linux VDA

Après l'installation du package, vous devez configurer le Linux VDA en exécutant le script ctxsetup.sh. Avant d'apporter des modifications, le script vérifie l'environnement et s'assure que toutes les dépendances sont installées. Si nécessaire, vous pouvez exécuter le script à tout moment pour modifier les paramètres.

Vous pouvez exécuter le script manuellement avec invite, ou automatiquement avec réponses préconfigurées. Consultez l'aide sur le script avant de continuer :

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
<!--NeedCopy-->
```


Configuration avec invites

Exécutez une configuration manuelle avec questions :

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

Configuration automatique

Pour une installation automatique, les options requises par le script d'installation peuvent être fournies avec des variables d'environnement. Si toutes les variables requises sont présentes, le script ne demande aucune information à l'utilisateur, ce qui permet de procéder à l'installation à l'aide d'un script.

Les variables d'environnement prises en charge sont les suivantes :

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N** : le Linux VDA prend en charge la spécification d'un nom de Delivery Controller à l'aide d'un enregistrement DNS CNAME. La valeur est définie par défaut sur N.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** : le Linux VDA requiert une liste séparée par des espaces de noms de domaines complets de Delivery Controller. Cette dernière sera utilisée pour l'enregistrement auprès d'un Delivery Controller. Au moins un alias de nom de domaine complet (FQDN) ou CNAME doit être spécifié.
- **CTX_XDL_VDA_PORT = port-number** : le Linux VDA communique avec les Delivery Controller à l'aide d'un port (80 par défaut) TCP/IP.
- **CTX_XDL_REGISTER_SERVICE = Y | N** : les services Linux VDA sont lancés après le démarrage de la machine. Valeur définie sur Y par défaut.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** : les services Linux VDA requièrent que les connexions réseau entrantes soient autorisées via le pare-feu du système. Vous pouvez ouvrir automatiquement les ports requis (ports 80 et 1494 par défaut) dans le pare-feu du système pour Linux VDA. Valeur définie sur Y par défaut.
- **CTX_XDL_AD_INTEGRATION = 1 | 2 | 3 | 4 |5** : le Linux VDA requiert que les paramètres de configuration Kerberos s'authentifient auprès des Delivery Controller. La configuration de Kerberos est déterminée depuis l'outil d'intégration d'Active Directory installé et configuré sur le système. Spécifiez la méthode d'intégration d'Active Directory prise en charge à utiliser :
  - 1 –Samba Winbind
  - 2 –Service d'authentification Quest
  - 3 –Centrify DirectControl
  - 4 –SSSD

  - 5 –PBIS

- **CTX_XDL_HDX_3D_PRO=Y | N** : Linux VDA prend en charge HDX 3D Pro, un ensemble de technologies d'accélération GPU conçues pour optimiser la virtualisation des applications riches en graphiques. Si HDX 3D Pro est sélectionné, le Virtual Delivery Agent doit être configuré pour le mode Bureaux VDI (session unique), c'est-à-dire, CTX_XDL_VDI_MODE=Y.
- **CTX_XDL_VDI_MODE=Y | N** : indique si la machine est configurée comme modèle de mise à disposition de bureaux dédiés (VDI) ou comme modèle de mise à disposition de bureaux partagés hébergés. Pour les environnements HDX 3D Pro, définissez cette variable sur Y. Elle est définie par défaut sur N.
- **CTX_XDL_SITE_NAME=dns-name** : le Linux VDA découvre les serveurs LDAP à l'aide de DNS. Pour limiter les résultats de recherche DNS à un site local, spécifiez un nom de site DNS. Cette variable est définie sur **<none>** par défaut.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** : le Linux VDA envoie une requête vers le DNS pour découvrir les serveurs LDAP. Si DNS ne peut pas fournir d'enregistrements de service LDAP, vous pouvez entrer une liste séparée par des espaces de noms de domaines complets LDAP avec ports LDAP. Par exemple, ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268. Si vous spécifiez le numéro de port LDAP 389, le Linux VDA interroge chaque serveur LDAP du domaine spécifié en mode d'interrogation. S'il existe un nombre x de stratégies et y de serveurs LDAP, le Linux VDA effectue le total de X multiplié par Y requêtes. Si le temps d'interrogation dépasse le seuil, les ouvertures de session peuvent échouer. Pour activer les requêtes LDAP plus rapides, activez le **catalogue global** sur un contrôleur de domaine et définissez le numéro de port LDAP correspondant sur 3268. Cette variable est définie sur **<none>** par défaut.
- **CTX_XDL_SEARCH_BASE=search-base-set** : le Linux VDA envoie une requête à LDAP via une base de recherche définie sur la racine du domaine Active Directory (par exemple, D, DC=mycompany,DC=com). Toutefois, pour améliorer les performances de recherche, vous pouvez spécifier une base de recherche (par exemple, OU=VDI,DC=mycompany,DC=com). Cette variable est définie sur **<none>** par défaut.
- **CTX_XDL_FAS_LIST='list-fas-servers'** : les serveurs du service d'authentification fédérée (FAS) sont configurés via la stratégie de groupe AD. Le Linux VDA ne prend pas en charge la stratégie de groupe AD mais vous pouvez fournir une liste de serveurs FAS séparés par des points-virgules. La séquence doit être la même que celle configurée dans la stratégie de groupe AD. Si une adresse de serveur est supprimée, remplissez son espace vide avec la chaîne de texte **<none>** et ne modifiez pas l'ordre des adresses de serveur. Pour communiquer correctement avec les serveurs FAS, assurez-vous d'ajouter un numéro de port conforme à celui spécifié sur les serveurs FAS, par exemple CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'.

- **CTX_XDL_DOTNET_ runtime_path=Path-to-install-dotnet-runtime** : chemin d'accès à l'installation de .NET Runtime 6.0 pour la prise en charge du nouveau Broker Agent Service (`ctxvda`). Le chemin par défaut est /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate** : spécifie l'environnement de bureau GNOME, GNOME Classic ou MATE à utiliser dans les sessions. Si vous ne spécifiez pas la variable, le bureau actuellement installé sur le VDA est utilisé. Toutefois, si le bureau actuellement installé est MATE, vous devez définir la valeur de la variable sur **mate**.

  Vous pouvez également modifier l'environnement de bureau d'un utilisateur de session cible en procédant comme suit :

  1. Créez un fichier `.xsession` sous le répertoire **$HOME/<username>** sur le VDA.
  2. Modifiez le fichier `.xsession` pour spécifier un environnement de bureau basé sur les distributions.

     - **Pour le bureau MATE**

     ```
     MSESSION="$(type -p mate-session)"
     if [ -n "$MSESSION" ]; then
       exec mate-session
     fi
     ```

     - **Pour le bureau GNOME Classic**

     ```
     GSESSION="$(type -p gnome-session)"
     if [ -n "$GSESSION" ]; then
     export GNOME_SHELL_SESSION_MODE=classic
     exec gnome-session --session=gnome-classic
     fi
     ```

     - **Pour le bureau GNOME**

     ```
     GSESSION="$(type -p gnome-session)"
     if [ -n "$GSESSION" ]; then
     exec gnome-session
     fi
     ```

  3. Partagez l'autorisation de fichier 700 avec l'utilisateur de la session cible.

  À partir de la version 2209, les utilisateurs de session peuvent personnaliser leurs environnements de bureau. Pour activer cette fonctionnalité, vous devez installer au préalable des environnements de bureau commutables sur le VDA. Pour plus d'informations, consultez Environnements de bureau personnalisés par utilisateurs de session.

- **CTX_XDL_START_SERVICE = Y | N** : indique si les services Linux VDA sont lancés lorsque la configuration de Linux VDA est terminée. Valeur définie sur Y par défaut.

- **CTX_XDL_TELEMETRY_SOCKET_PORT** : port socket permettant d'écouter Citrix Scout. Le port par défaut est 7503.
- **CTX_XDL_TELEMETRY_PORT** : port de communication avec Citrix Scout. Le port par défaut est 7502.

Définissez la variable d'environnement et exécutez le script de configuration :

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3|4|5

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-site-name | '<none>'

export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'

export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'

export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<
   none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

Lors de l'exécution de la commande sudo, entrez l'option **-E** pour transmettre les variables d'environnement au nouveau shell créé. Nous vous recommandons de créer un fichier de script shell à partir des commandes précédentes avec **#!/bin/bash** en tant que première ligne.

Vous pouvez également spécifier tous les paramètres avec une seule commande :


```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST='list-ddc-fqdns' \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4|5 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

/opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

Supprimer les modifications de configuration

Dans certains scénarios, il peut être nécessaire de supprimer les modifications de configuration effectuées par le script **ctxsetup.sh** sans désinstaller le package Linux VDA.

Consultez l'aide sur ce script avant de continuer :

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
<!--NeedCopy-->
```

Pour supprimer les modifications de configuration :

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
<!--NeedCopy-->
```


> **Important :**
>
> Ce script supprime toutes les données de configuration de la base de données et empêche Linux VDA de fonctionner.

Journaux de configuration

Les scripts **ctxsetup.sh** et **ctxcleanup.sh** affichent les erreurs dans la console, avec des informations supplémentaires consignées dans le fichier journal de configuration **/tmp/xdl.configure.log**.

Redémarrez les services de Linux VDA pour que les modifications prennent effet.

Désinstaller le logiciel Linux VDA

Pour vérifier que le Linux VDA est installé et pour afficher la version du package installé :

```
1 dpkg -l xendesktopvda
2 <!--NeedCopy-->
```

Pour afficher des informations plus détaillées :

```
1 apt-cache show xendesktopvda
2 <!--NeedCopy-->
```

Pour désinstaller le logiciel Linux VDA :

```
1 dpkg -r xendesktopvda
2 <!--NeedCopy-->
```

> **Remarque :**
>
> La désinstallation du logiciel Linux VDA supprime le PostgreSQL associé et d'autres données de configuration. Toutefois, le package PostgreSQL et les autres packages dépendants qui ont été installés avant l'installation du Linux VDA ne sont pas supprimés.
>
> **Conseil :**
>
> Les informations figurant dans cette section ne couvrent pas la suppression de packages dépendants, y compris PostgreSQL.

Étape 9 : exécuter XDPing

Exécutez `sudo /opt/Citrix/VDA/bin/xdping` pour vérifier les problèmes de configuration courants avec un environnement VDA Linux. Pour de plus amples informations, consultez la section XDPing.

Étape 10 : exécuter le Linux VDA

Une fois que vous avez configuré le Linux VDA à l'aide du script **ctxsetup.sh**, utilisez les commandes suivantes pour contrôler le Linux VDA.

Démarrer Linux VDA :

Pour démarrer les services Linux VDA :

```
sudo systemctl start ctxhdx

sudo systemctl start ctxvda
<!--NeedCopy-->
```

Arrêter Linux VDA :

Pour arrêter les services Linux VDA :

```
sudo systemctl stop ctxvda

sudo systemctl stop ctxhdx
<!--NeedCopy-->
```

> **Remarque :**
>
> Avant d'arrêter les services `ctxvda` et `ctxhdx`, exécutez la commande `service ctxmonitorservice stop` pour arrêter le démon du service de surveillance. Sinon, le démon du service de surveillance redémarre les services que vous avez arrêtés.

Redémarrer Linux VDA :

Pour redémarrer les services Linux VDA :

```
sudo systemctl stop ctxvda

sudo systemctl restart ctxhdx

sudo systemctl restart ctxvda
<!--NeedCopy-->
```

Vérifier l'état de Linux VDA :

Pour vérifier l'état de fonctionnement des services de Linux VDA :

```
sudo systemctl status ctxvda

sudo systemctl status ctxhdx
<!--NeedCopy-->
```


Étape 11 : créer le catalogue de machines dans Citrix Virtual Apps ou Citrix Virtual Desktops

Le processus de création de catalogues de machines et d'ajout de machines Linux VDA est similaire à l'approche traditionnelle avec les VDA Windows. Pour obtenir une description plus détaillée de la méthode à utiliser pour effectuer ces tâches, consultez les sections Créer des catalogues de machines et Gérer des catalogues de machines.

Pour la création de catalogues de machines contenant des machines Linux VDA, il existe quelques restrictions qui différencient ce processus de la création de catalogues de machines pour VDA Windows :

- Pour le système d'exploitation, sélectionnez :
  - l'option **OS à sessions multiples** pour un modèle de mise à disposition de bureaux partagés hébergés ;
  - l'option **OS mono-session** pour un modèle de mise à disposition de bureaux dédiés VDI.
- Ne combinez pas de machines Linux VDA et Windows dans le même catalogue de machines.

> **Remarque :**
>
> Les versions antérieures de Citrix Studio ne prenaient pas en charge la notion de « système d'exploitation Linux. » Toutefois, la sélection de l'option **OS de serveur Windows** ou **OS de serveur** implique un modèle de mise à disposition équivalent de bureaux partagés hébergés. La sélection de l'option **OS de bureau Windows** ou **OS de bureau** implique un modèle de mise à disposition d'un utilisateur unique par machine.
>
> **Conseil :**
>
> Si une supprimez une machine puis que vous la rejoignez au domaine Active Directory, vous devez supprimer et rajouter la machine au catalogue de machines.

Étape 12 : créer le groupe de mise à disposition dans Citrix Virtual Apps ou Citrix Virtual Desktops

Le processus de création d'un groupe de mise à disposition et d'ajout de catalogues de machines contenant des machines Linux VDA est presque identique aux machines VDA Windows. Pour obtenir une description plus détaillée de la méthode à utiliser pour effectuer ces tâches, consultez la section Créer des groupes de mise à disposition.

Lors de la création de groupes de mise à disposition qui contiennent des catalogues de machines Linux VDA, les restrictions suivantes s'appliquent :

- Assurez-vous que les utilisateurs et les groupes AD que vous sélectionnez ont été correctement configurés pour l'ouverture de session sur les machines Linux VDA.
- N'autorisez pas l'ouverture de session d'utilisateurs non authentifiés (anonymes).
- Ne combinez pas le groupe de mise à disposition avec des catalogues de machines contenant des machines Windows.

Pour plus d'informations sur la création de catalogues de machines et de groupes de mise à disposition, consultez Citrix Virtual Apps and Desktops 7 2206.

Créer des Linux VDA dans Citrix DaaS Standard pour Azure

June 16, 2023

Vous pouvez créer des Linux VDA joints et non joints à un domaine dans Citrix DaaS Standard pour Azure (anciennement Citrix Virtual Apps and Desktops Standard pour Azure) pour mettre à disposition des applications et des bureaux virtuels sur n'importe quel appareil à partir de Microsoft Azure. Pour plus d'informations, consultez Citrix DaaS Standard pour Azure.

Distributions Linux prises en charge

Les distributions Linux suivantes prennent en charge cette fonctionnalité :

- RHEL 8.6
- RHEL 8.4
- Rocky Linux 8.6
- Ubuntu 22.04
- Ubuntu 20.04
- Ubuntu 18.04

Étapes

Pour créer des Linux VDA dans Citrix DaaS Standard pour Azure, procédez comme suit :

1. Préparez une image principale dans Azure :

   > **Remarque :**
   >
   > Vous pouvez également utiliser la fonctionnalité Mise à jour automatique de Linux VDA pour planifier des mises à jour logicielles automatiques. Pour ce faire, ajoutez des lignes de commande au fichier etc/xdl/mcs/mcs_local_setting.reg de l'image principale.

> Par exemple, vous pouvez ajouter les lignes de commande suivantes :
>
> ```
> create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_DWORD" -v "fEnabled" -d "0x00000001" –force
>
> create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v "ScheduledTime" -d "Immediately" –force
>
> create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v "Url" -d "<Your-Azure-Container-Url>" –force
>
> create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v "CaCertificate" -d "<Local-Certificate-Path-of-PortalAzureCom>" --force
> <!--NeedCopy-->
> ```

a) Dans Azure, créez une machine virtuelle Linux d'une distribution prise en charge.

b) Installez un environnement de bureau sur la machine virtuelle Linux si nécessaire.

c) Sur la machine virtuelle, installez .NET Runtime 6.0 conformément aux instructions de https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

d) (Pour Ubuntu uniquement) Ajoutez la ligne `source /etc/network/interfaces.d/*` dans le fichier `/etc/network/interfaces`.

e) (Pour Ubuntu uniquement) Pointez `/etc/resolv.conf` sur `/run/systemd/resolve/resolv.conf` au lieu de `/run/systemd/resolve/stub-resolv.conf` :

```
unlink /etc/resolv.conf

ln -s /run/systemd/resolve/resolv.conf /etc/resolv.conf
<!--NeedCopy-->
```

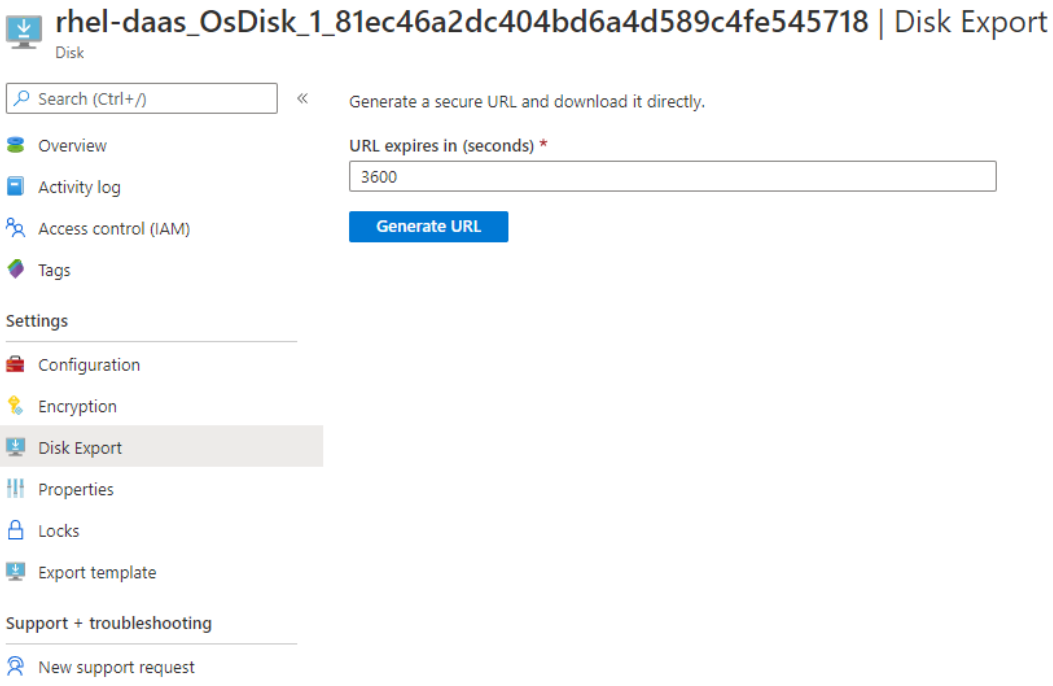
f) Installez le package Linux VDA.

g) Modifiez les variables dans /etc/xdl/mcs/mcs.conf. Le fichier de configuration `mcs.conf` contient des variables pour la configuration de MCS et du Linux VDA.

> **Remarque :**
>
> Laissez la variable dns non spécifiée.
> Si vous sélectionnez le type **Statique** ou **Aléatoire** lors de la création d'un catalogue de machines, définissez `VDI_MODE=Y`.

h) Exécutez `/opt/Citrix/VDA/sbin/deploymcs.sh`.

i) Dans Azure, arrêtez (ou désallouez) la machine virtuelle. Cliquez sur **Exportation de disque** pour générer une URL SAS pour le fichier de disque dur virtuel (VHD) que vous pouvez utiliser comme image principale pour créer d'autres machines virtuelles.



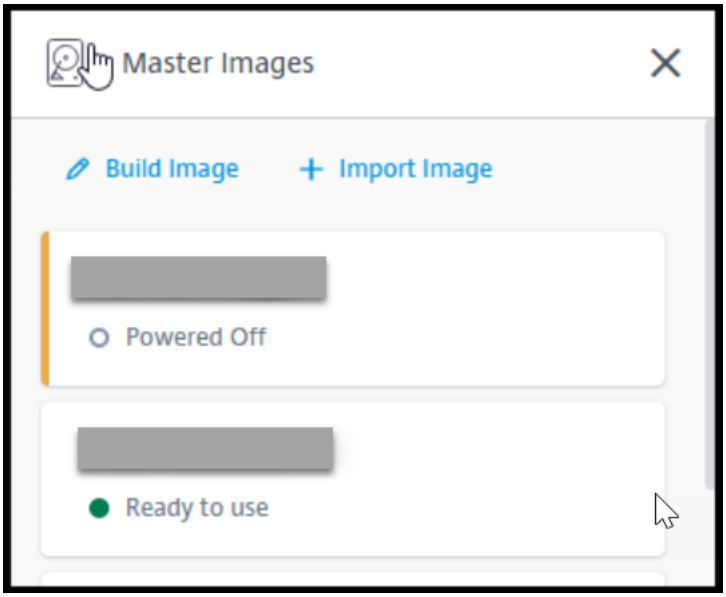
j) (Facultatif) Réglez des paramètres de stratégie de groupe sur l'image principale. Vous pouvez utiliser l'outil `ctxreg` pour définir des paramètres de stratégie de groupe. Par exemple, la commande suivante active la stratégie **Créer automatiquement l'imprimante universelle PDF** pour l'impression PDF.

```
1    /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
        GroupPolicy\Defaults\PrintingPolicies" -t "REG_DWORD" -v
         "AutoCreatePDFPrinter" -d "0x00000001" –force
2    <!--NeedCopy-->
```

2. Importez l'image principale à partir d'Azure.

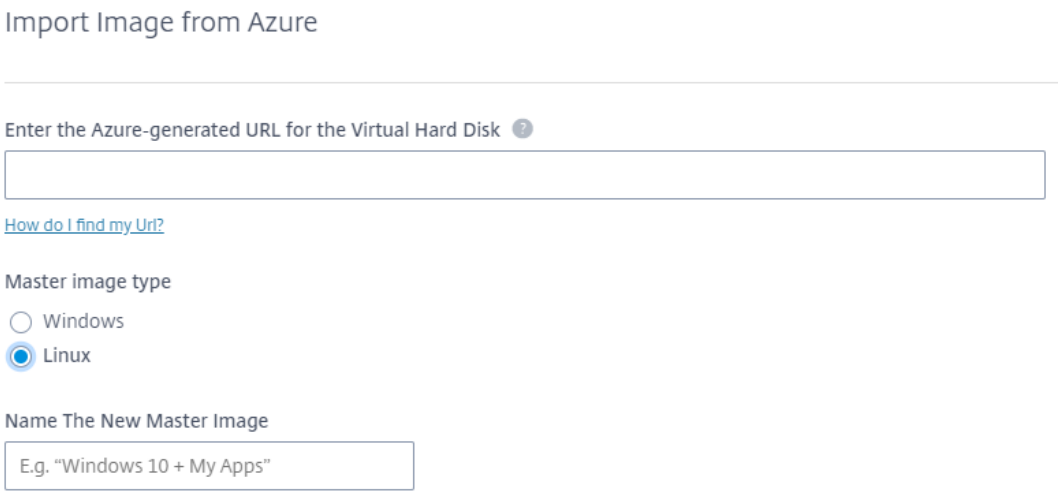
a) Dans le tableau de bord Gérer, développez **Images principales** sur la droite. L'affichage répertorie les images principales fournies par Citrix et les images que vous avez créées et importées.

Conseil : La plupart des activités d'administrateur de ce service sont gérées via les tableaux de bord **Gérer** et **Surveiller**. Après avoir créé votre premier catalogue, le tableau de bord **Gérer** se lance automatiquement après vous être connecté à Citrix Cloud et avoir sélectionné le service **Bureaux gérés**.



b) Cliquez sur **Importer une image**.

c) Entrez l'URL SAS du fichier VHD que vous avez généré dans Azure. Sélectionnez **Linux** en tant que type d'image principale.



d) Suivez les instructions de l'assistant pour procéder à l'importation de l'image principale.

3. Créez un catalogue de machines.

   Accédez au tableau de bord Gérer et cliquez sur **Créer un catalogue**. Lors de la création du catalogue de machines, choisissez l'image principale que vous avez créée précédemment.

   > **Remarque :**
   >
   > La machine virtuelle utilisée en tant qu'image principale n'est pas accessible via SSH ou

> RDP. Pour accéder à la machine virtuelle, utilisez la console série du portail Azure.

Utiliser Machine Creation Services (MCS) pour créer des machines virtuelles Linux

January 11, 2024

Distributions prises en charge

	Winbind	SSSD	Centrify	PBIS
Debian 11.3	Oui	Oui	Non	Oui
RHEL 8.6, RHEL 8.4	Oui	Non	Oui	Oui
Rocky Linux 8.6	Oui	Non	Non	Non
RHEL 7.9, CentOS 7.9	Oui	Oui	Oui	Oui
SUSE 15.3	Oui	Oui	Non	Oui
Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04	Oui	Oui	Non	Oui

Hyperviseurs pris en charge

- AWS
- Citrix Hypervisor
- GCP
- Microsoft Azure
- Nutanix AHV
- VMware vSphere

Des résultats inattendus peuvent se produire si vous essayez de préparer une image principale sur des hyperviseurs autres que ceux qui sont compatibles.

Utiliser MCS pour créer des machines virtuelles Linux

Considérations

- De Citrix Virtual Apps and Desktops 7 2003 à Citrix Virtual Apps and Desktops 7 2112, l'hébergement de Linux VDA sur Microsoft Azure, AWS et GCP était pris en charge uniquement pour Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). À compter de la version 2203, vous pouvez héberger le Linux VDA sur ces clouds publics pour Citrix DaaS et Citrix Virtual Apps and Desktops. Pour ajouter ces connexions hôtes de cloud public à votre déploiement Citrix Virtual Apps and Desktops, vous avez besoin d'une **licence de droits hybrides**. Pour plus d'informations sur la **licence de droits hybrides**, consultez Transition et échange (TTU) avec droits hybrides.
- Les serveurs bare metal ne sont pas pris en charge lorsqu'ils sont utilisés avec MCS pour créer des machines virtuelles.
- Citrix utilise les versions de Centrify suivantes pour la validation initiale des fonctionnalités sur les distributions Linux concernées :

Distribution Linux	Version de Centrify
RHEL	5.8.0
SUSE	5.7.1
Debian, Ubuntu	5.6.1

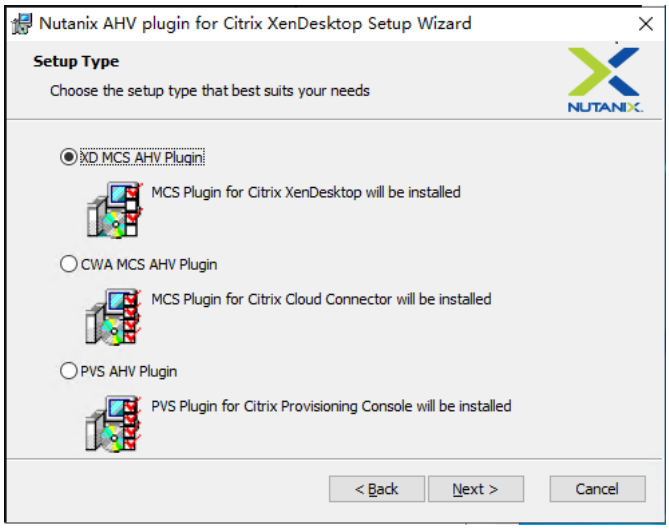
  L'utilisation d'autres versions de Centrify peut provoquer des erreurs. N'utilisez pas Centrify pour joindre un modèle de machine à un domaine.

- Si vous utilisez PBIS ou Centrify pour joindre des machines créées avec MCS à des domaines Windows, effectuez les tâches suivantes :
  - Sur la machine modèle, configurez le chemin de téléchargement du package PBIS ou Centrify dans le fichier `/etc/xdl/mcs/mcs.conf` ou installez directement le package PBIS ou Centrify.
  - Avant d'exécuter `/opt/Citrix/VDA/sbin/deploymcs.sh`, créez une unité d'organisation dotée d'autorisations d'écriture et de réinitialisation de mot de passe sur toutes ses machines subordonnées créées avec MCS.
  - Avant de redémarrer les machines créées avec MCS une fois l'exécution de `/opt/Citrix/VDA/sbin/deploymcs.sh` terminée, exécutez `klist -li 0x3e4 purge` sur votre Delivery Controller ou sur votre Citrix Cloud Connector en fonction de votre déploiement.

(Pour Nutanix uniquement) Étape 1 : installer et enregistrer le plug-in Nutanix AHV

Procurez-vous le package de plug-in Nutanix AHV auprès de Nutanix. Installez et enregistrez le plug-in dans votre environnement Citrix Virtual Apps and Desktops. Pour de plus amples informations, consultez le Guide d'installation du plugin Nutanix Acropolis MCS, disponible sur le portail d'assistance Nutanix.

Étape 1a : installer et enregistrer le plug-in Nutanix AHV pour les Delivery Controller locaux
Après avoir installé Citrix Virtual Apps and Desktops, sélectionnez et installez **XD MCS AHV Plugin** sur vos Delivery Controller.



Étape 1b : installer et enregistrer le plug-in Nutanix AHV pour les Delivery Controller cloud
Sélectionnez et installez **CWA MCS AHV Plugin** sur les Citrix Cloud Connector. Installez le plug-in sur tous les Citrix Cloud Connector enregistrés auprès du client Citrix Cloud. Vous devez enregistrer les Citrix Cloud Connector même lorsqu'ils desservent un emplacement de ressources sans AHV.

Étape 1c : effectuer les étapes suivantes après l'installation du plug-in

- Vérifiez qu'un dossier Nutanix Acropolis a été créé dans `C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0`.
- Exécutez la commande `"C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe"-PluginsRoot "C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"`.
- Redémarrez Citrix Host, Citrix Broker et Citrix Machine Creation Services sur vos Delivery Controller locaux ou redémarrez Citrix RemoteHCLServer Service sur les Citrix Cloud Connector.

> **Conseil :**
>
> Nous vous recommandons d'arrêter, puis de redémarrer Citrix Host, Citrix Broker et Machine Creation Services lorsque vous installez ou mettez à jour le plug-in Nutanix AHV.

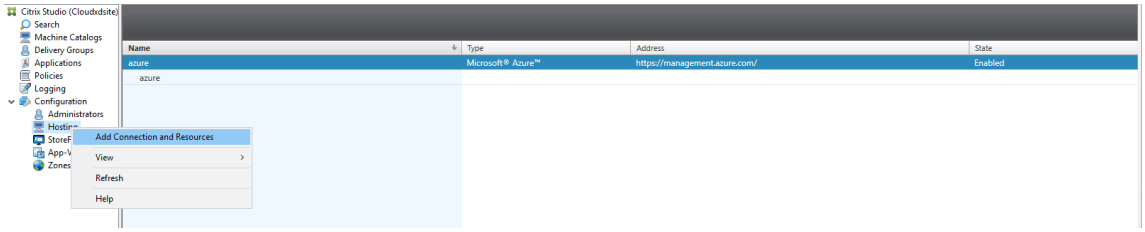
Étape 2 : créer une connexion d'hébergement

Cette section explique comment créer une connexion d'hébergement à Azure, AWS, GCP, Nutanix AHV et VMware vSphere :

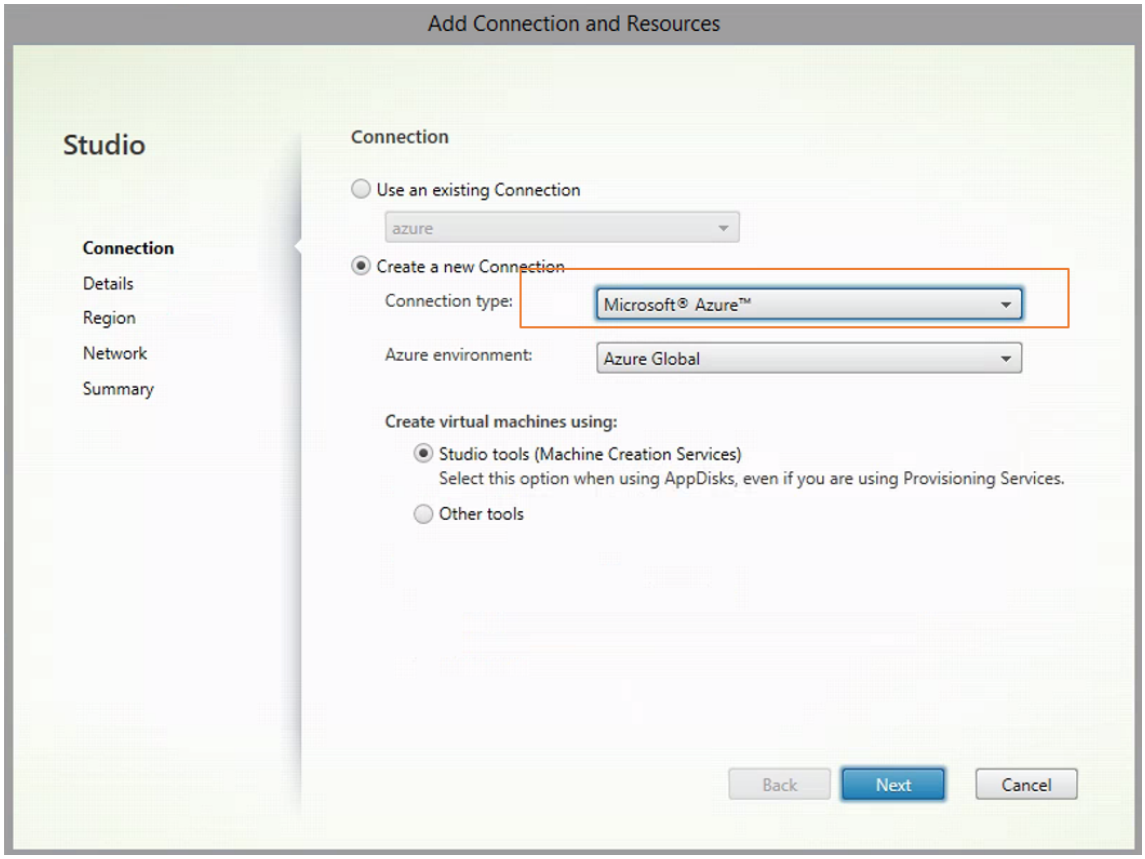
- Créer une connexion d'hébergement à Azure dans Citrix Studio
- Créer une connexion d'hébergement à AWS dans Citrix Studio
- Créer une connexion d'hébergement à GCP dans Citrix Studio
- Créer une connexion d'hébergement à Nutanix dans Citrix Studio
- Créer une connexion d'hébergement vers VMware dans Citrix Studio

Créer une connexion d'hébergement à Azure dans Citrix Studio

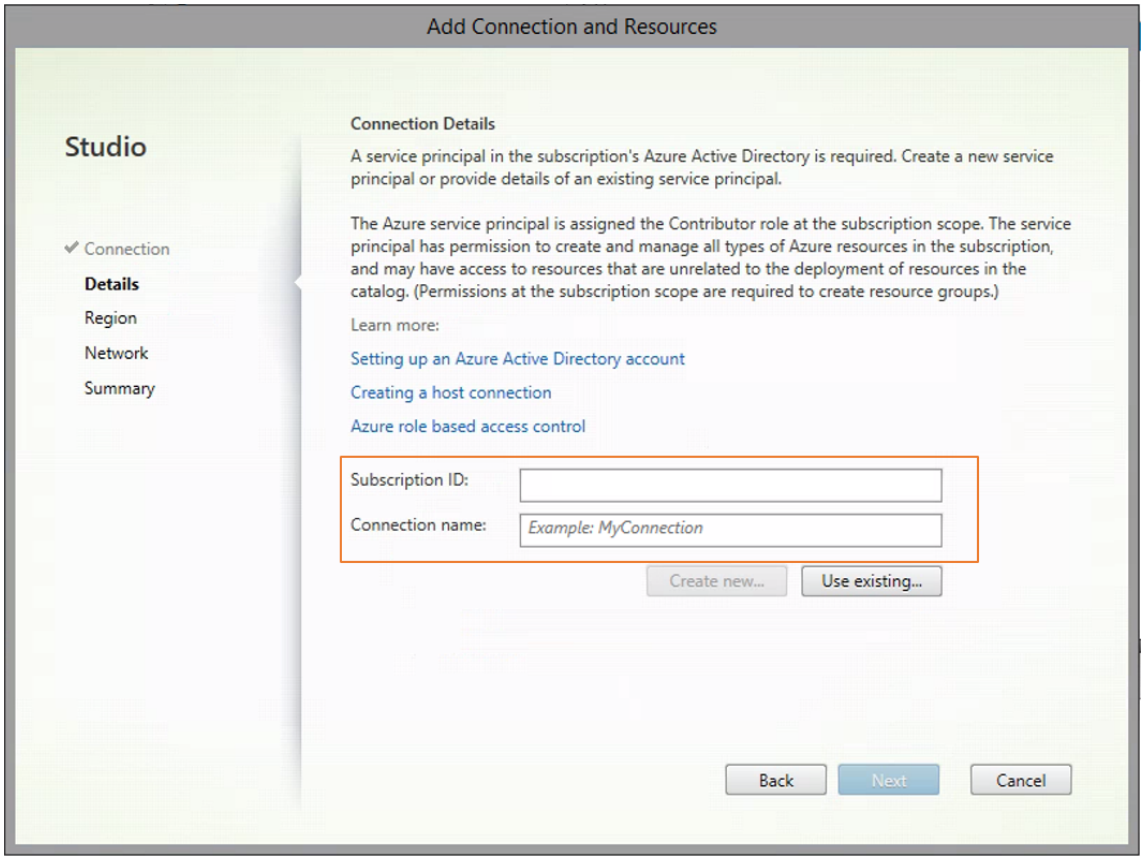
1. Dans Citrix Studio, sur Citrix Cloud, sélectionnez **Configuration > Hébergement > Ajouter une connexion et des ressources** pour créer une connexion à Azure.



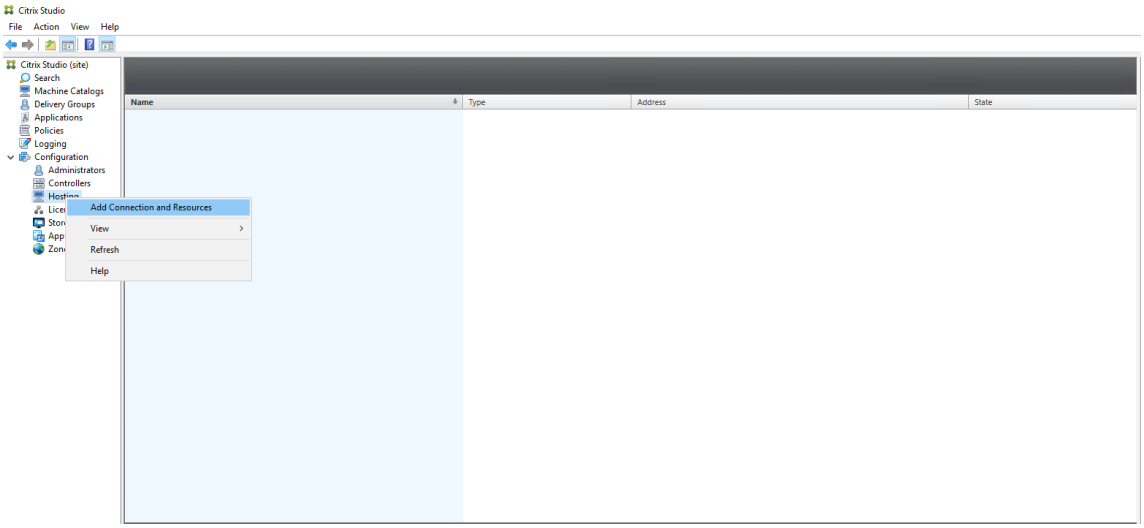
2. Sélectionnez le type de connexion Microsoft Azure.



3. Entrez l'ID d'abonnement de votre compte Azure, ainsi que votre nom de connexion.

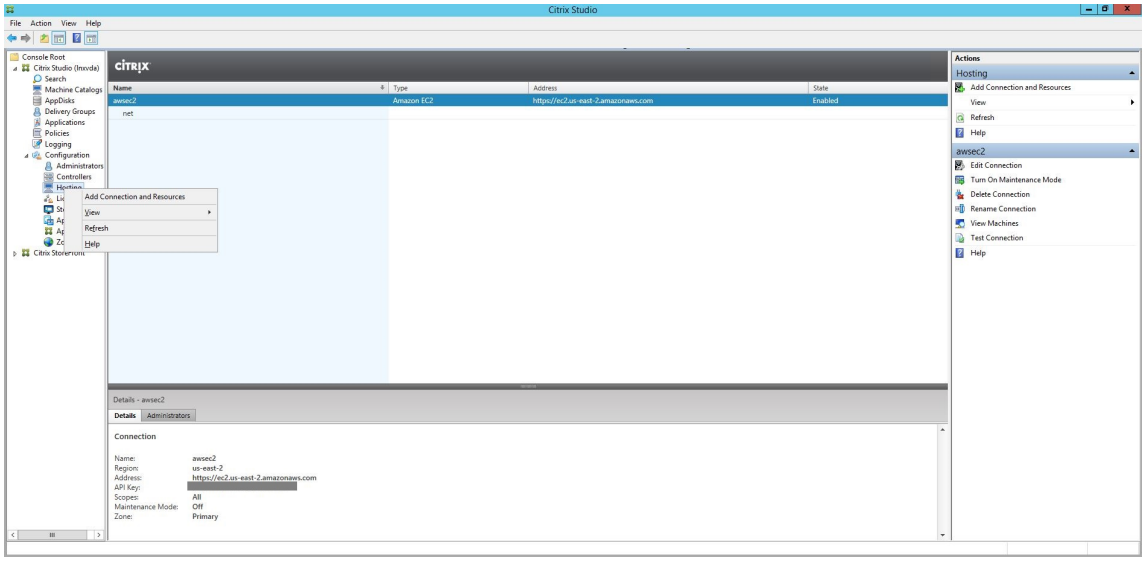


Une nouvelle connexion apparaît dans le panneau d'hébergement.

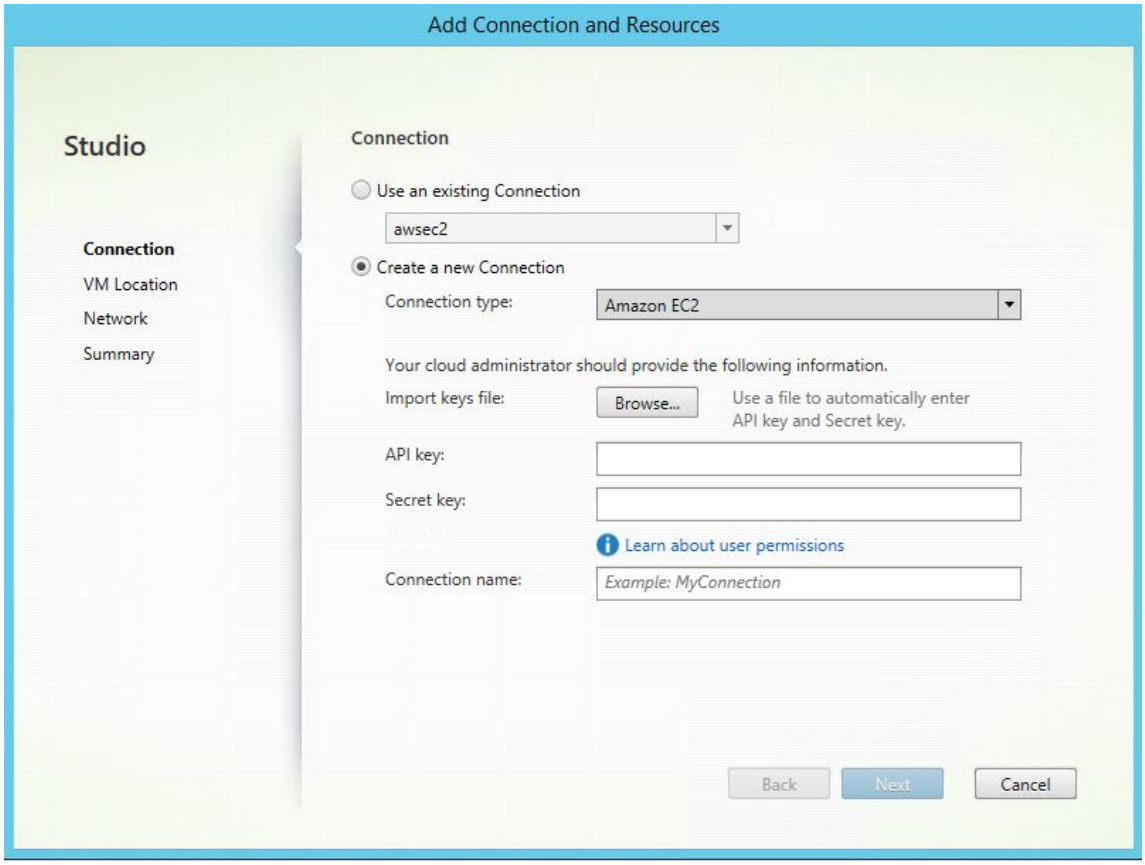


Créer une connexion d'hébergement à AWS dans Citrix Studio

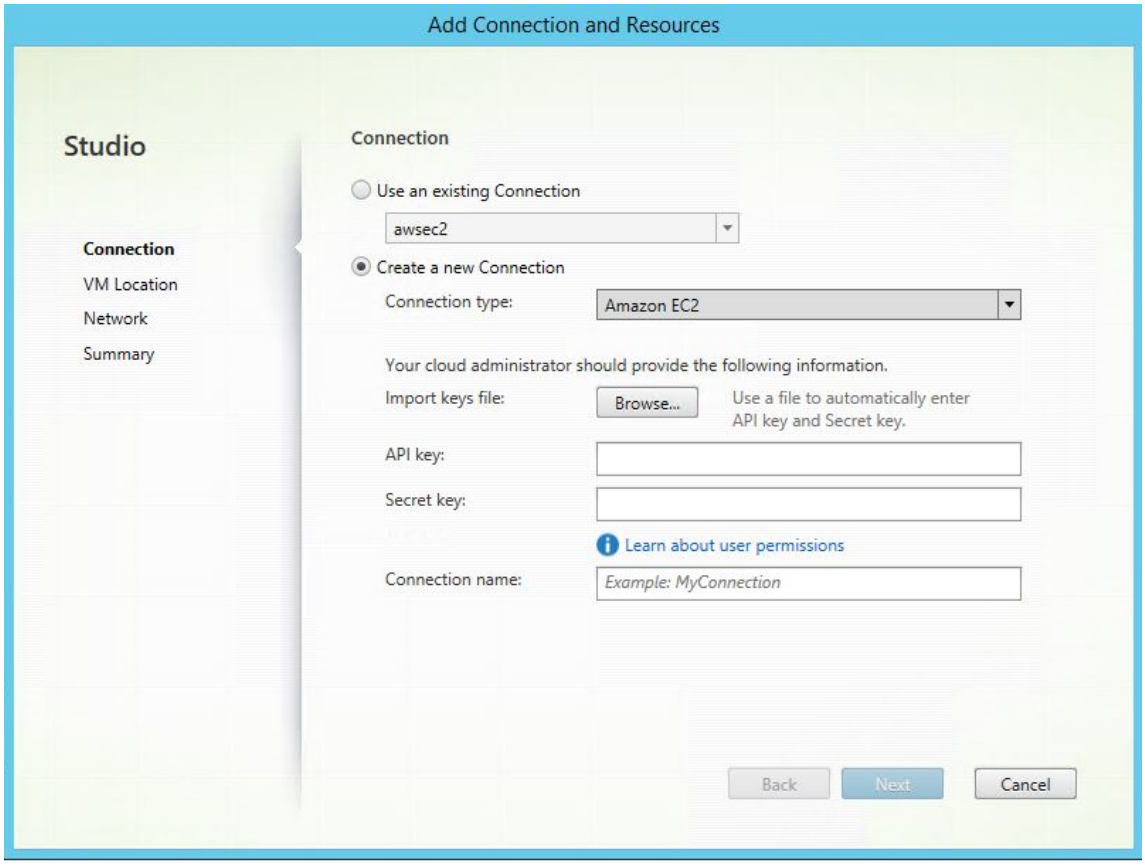
1. Dans Citrix Studio, sur Citrix Cloud, sélectionnez **Configuration** > **Hébergement** > **Ajouter une connexion et des ressources** pour créer une connexion à AWS.



2. Choisissez le type de connexion **Amazon EC2**.



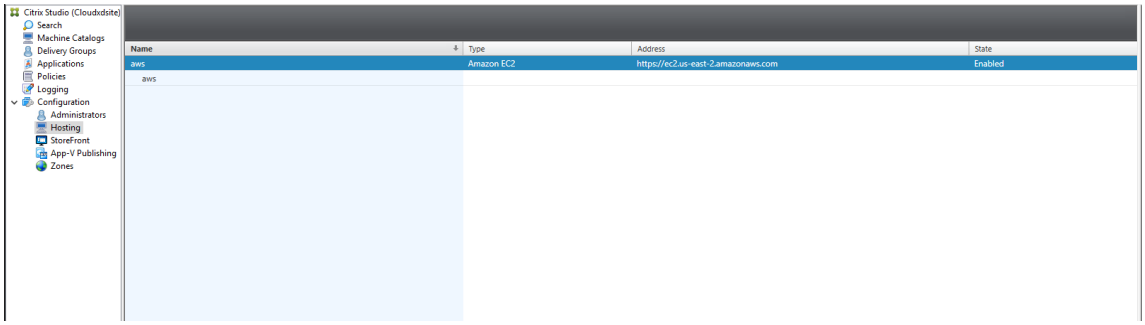
3. Entrez la clé API et la clé secrète de votre compte AWS, puis entrez le nom de votre connexion.



La **clé API** correspond à l'ID de votre clé d'accès et la **clé secrète** à votre clé d'accès secrète. Elles sont considérées comme une paire de clés d'accès. Si vous perdez votre clé d'accès secrète, vous pouvez la supprimer et en créer une autre. Pour créer une clé d'accès, procédez comme suit :

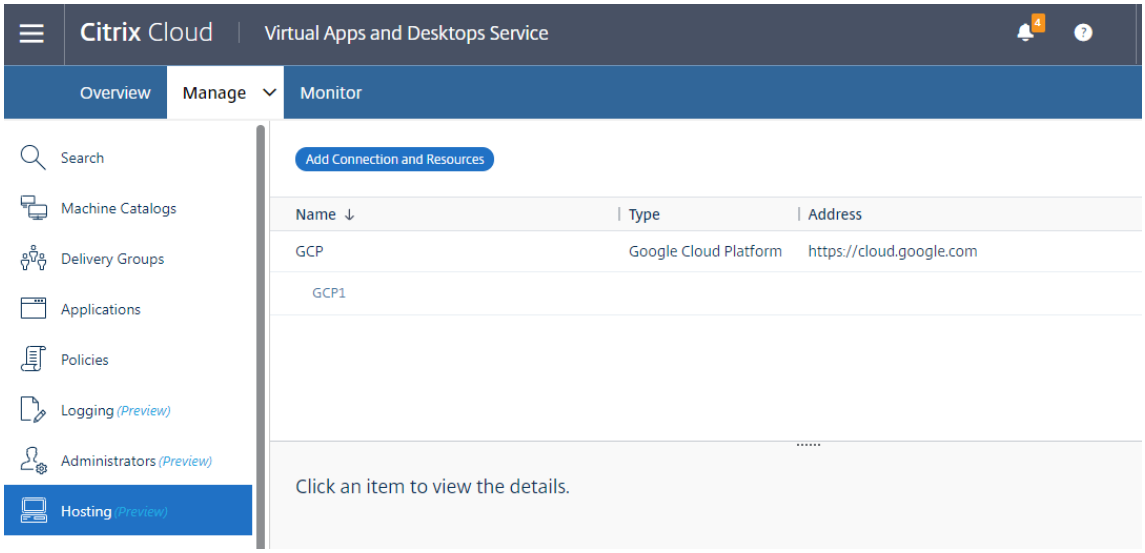
a) Connectez-vous aux services AWS.
b) Accédez à la console Identity and Access Management (IAM).
c) Dans le panneau de navigation de gauche, choisissez **Users**.
d) Sélectionnez l'utilisateur cible et faites défiler vers le bas pour sélectionner l'onglet **Security credentials**.
e) Faites défiler vers le bas et cliquez sur **Create access key**. Une nouvelle fenêtre apparaît.
f) Cliquez sur **Download .csv file** et enregistrez la clé d'accès dans un emplacement sécurisé.

Une nouvelle connexion apparaît dans le panneau d'hébergement.

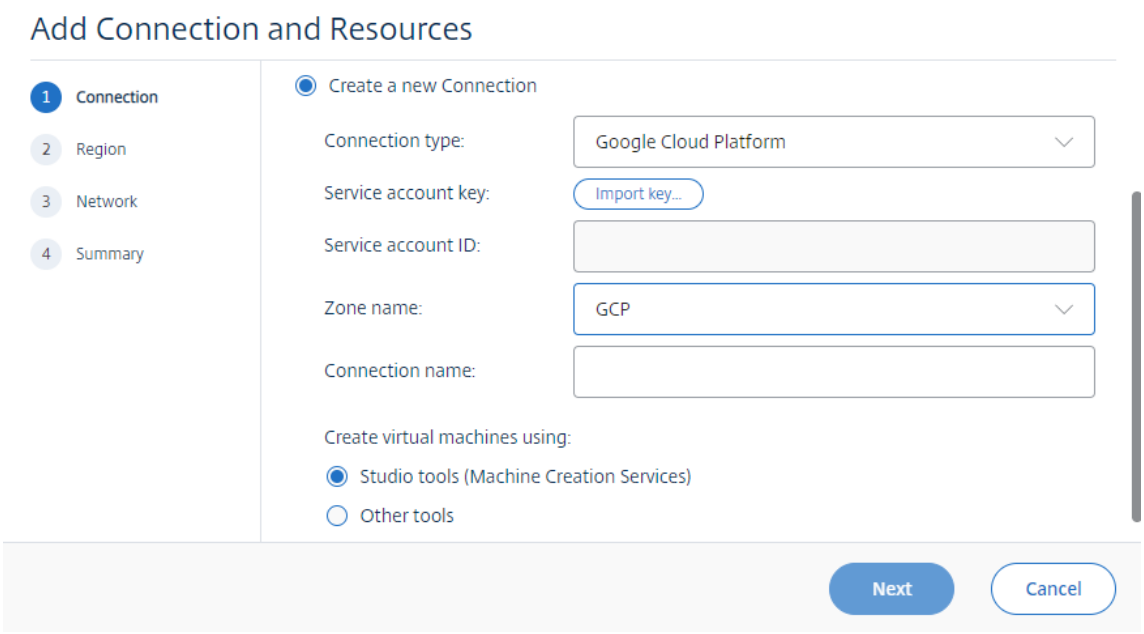


Créer une connexion d'hébergement à GCP dans Citrix Studio Configurez votre environnement GCP en fonction des environnements de virtualisation Google Cloud Platform, puis suivez les étapes ci-dessous pour créer une connexion d'hébergement à GCP.

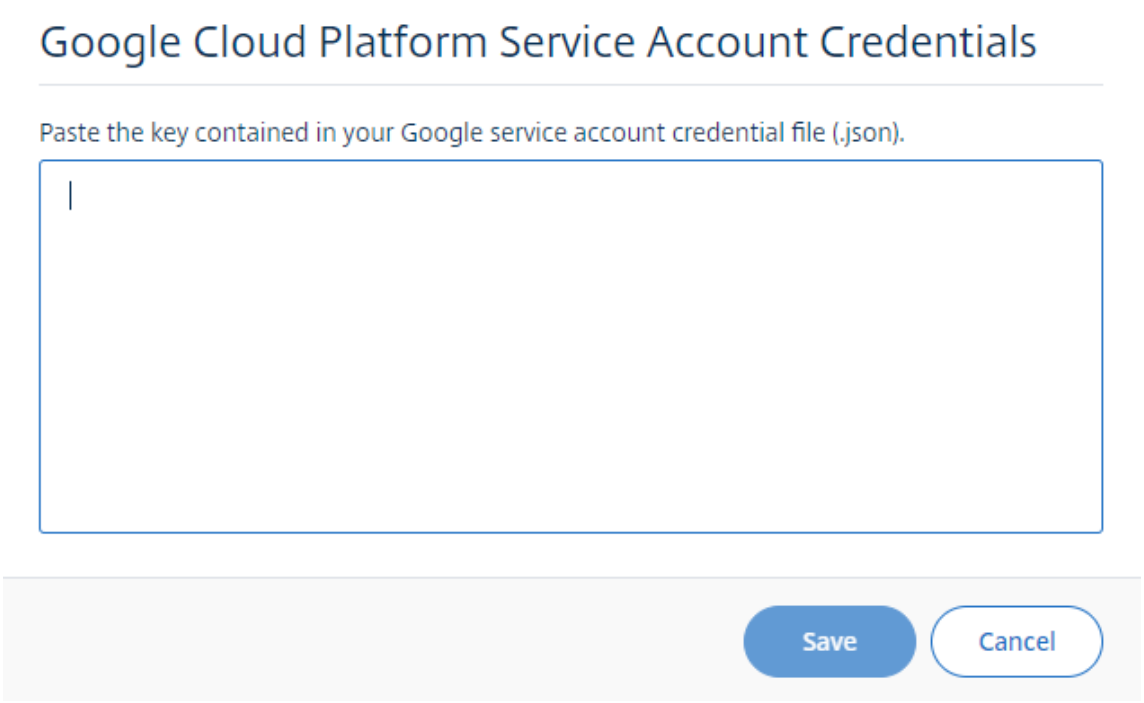
1. Dans Citrix Studio, sur Citrix Cloud, sélectionnez **Configuration** > **Hébergement** > **Ajouter une connexion et des ressources** pour créer une connexion à GCP.



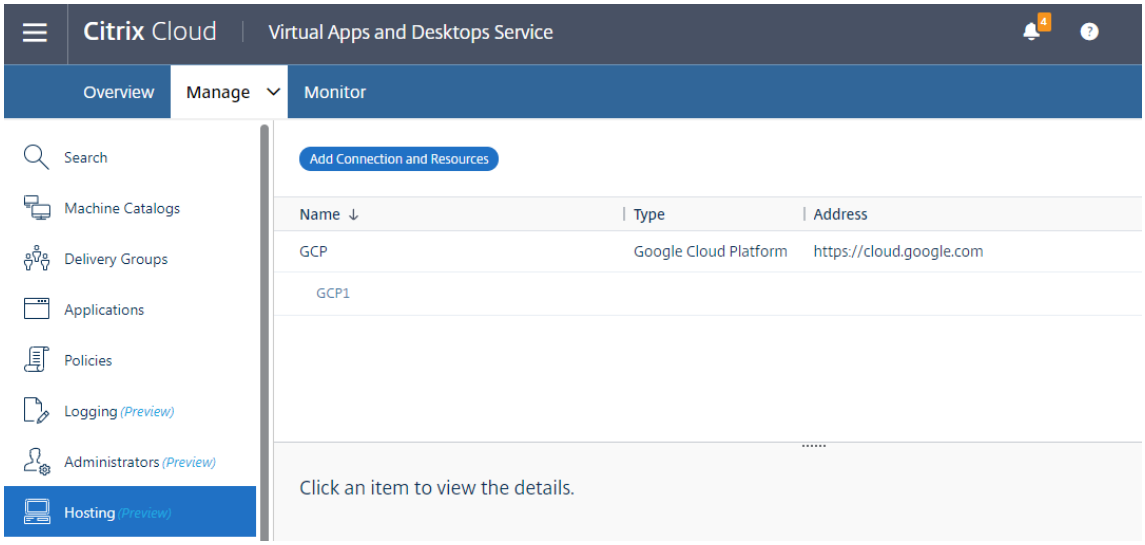
2. Sélectionnez **Google Cloud Platform** comme type de connexion.



3. Importez la clé de compte de service de votre compte GCP et saisissez votre nom de connexion.



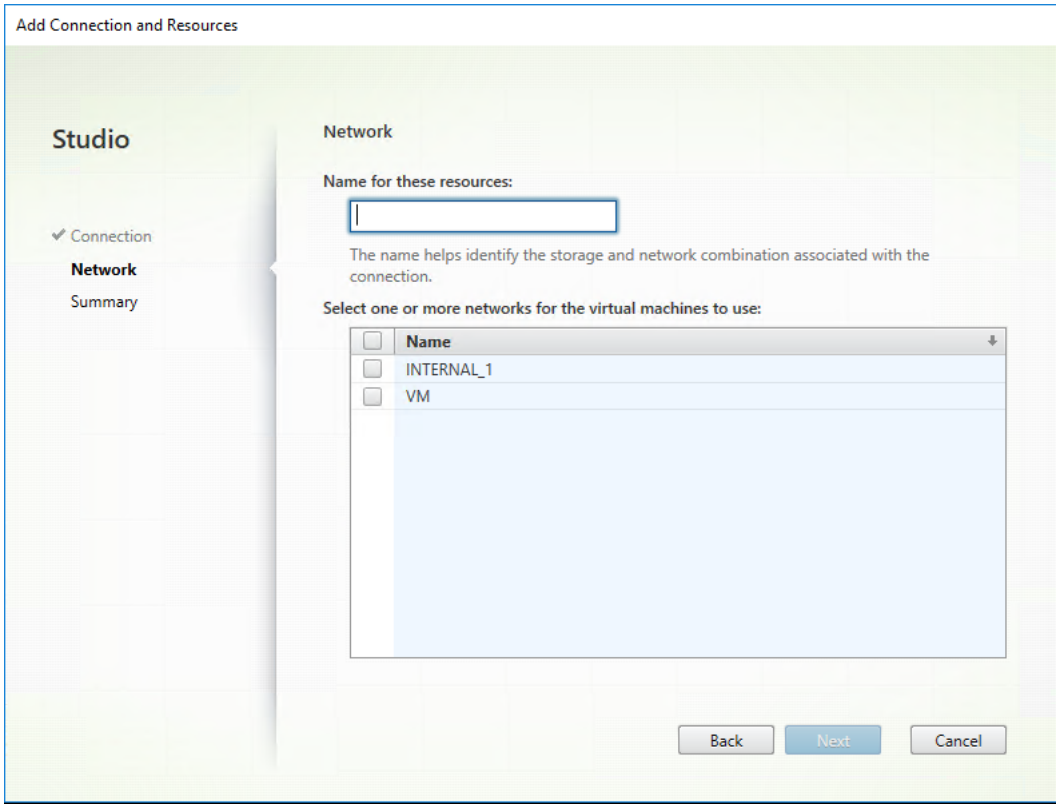
Une nouvelle connexion apparaît dans le panneau d'hébergement.



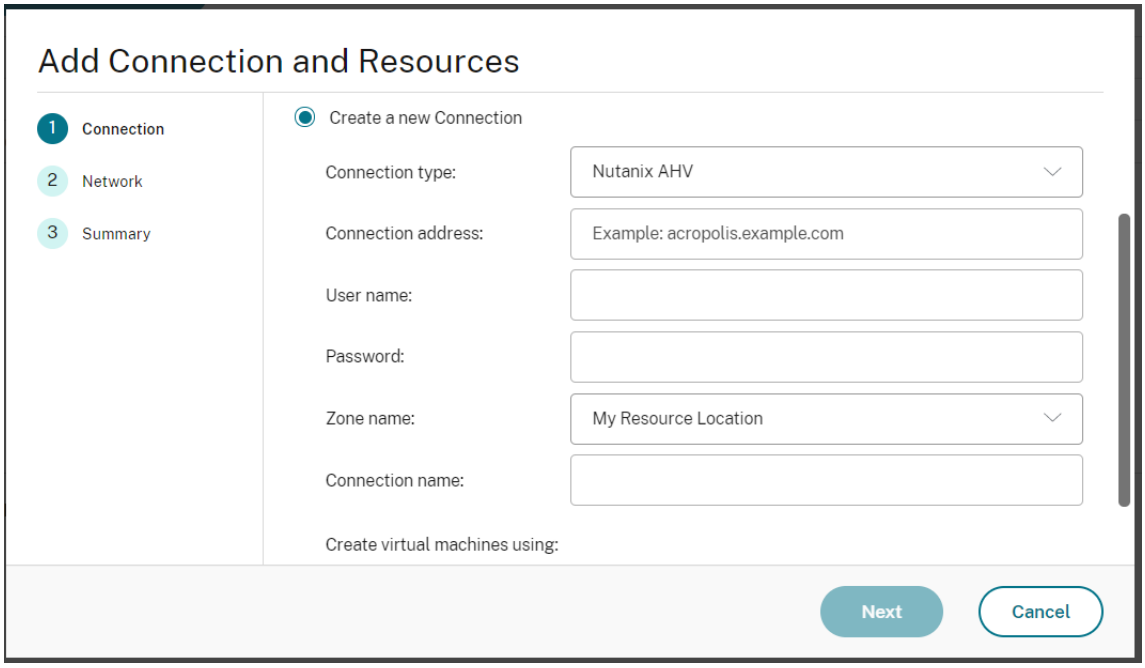
Créer une connexion d'hébergement à Nutanix dans Citrix Studio

1. Pour les Delivery Controller locaux, choisissez **Configuration > Hébergement > Ajouter une connexion et des ressources** dans la configuration locale Citrix Studio. Pour les Delivery Controller cloud, choisissez **Gérer > Hébergement > Ajouter une connexion et des ressources** dans la console Studio Web sur Citrix Cloud pour créer une connexion à l'hyperviseur Nutanix.
2. Dans l'assistant **Ajouter une connexion et des ressources**, sélectionnez le type de connexion Nutanix AHV sur la page **Connexion**, puis spécifiez l'adresse et les informations d'identification de l'hyperviseur, ainsi qu'un nom pour la connexion. Sur la page **Réseau**, sélectionnez un réseau pour l'unité d'hébergement.

   Par exemple, dans la configuration locale Citrix Studio :



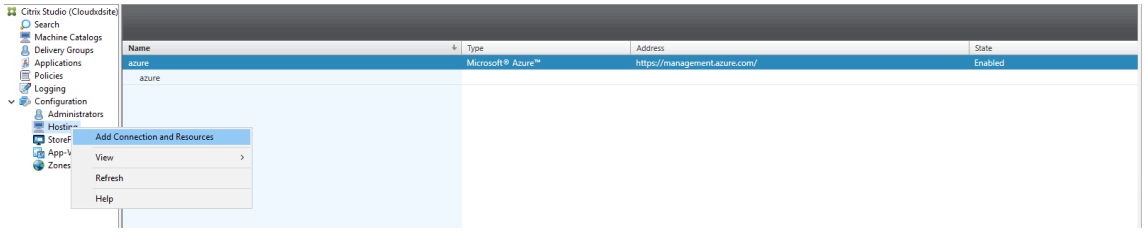
Par exemple, dans la console Studio Web sur Citrix Cloud :



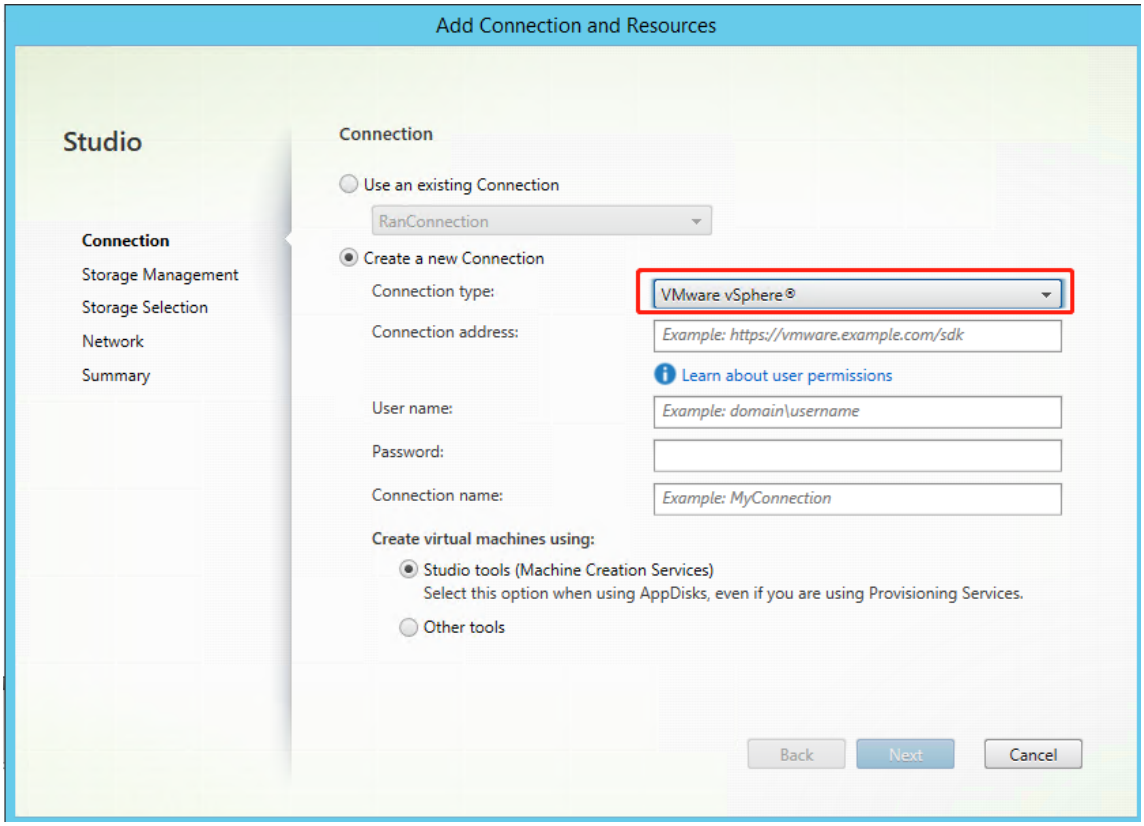
3. Sur la page **Réseau**, sélectionnez un réseau pour l'unité d'hébergement.

Créer une connexion d'hébergement vers VMware dans Citrix Studio

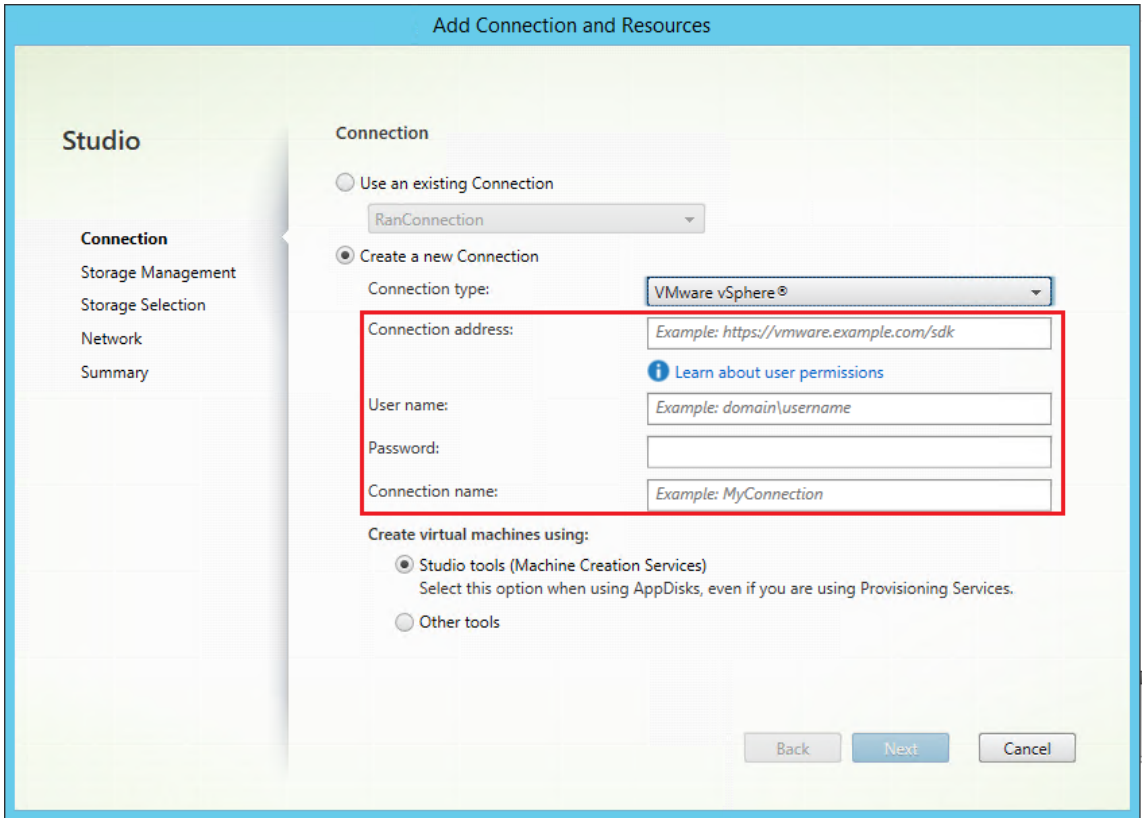
1. Installez vCenter Server dans l'environnement vSphere. Pour plus d'informations, consultez la section VMware vSphere.
2. Dans Citrix Studio, sélectionnez **Configuration > Hébergement > Ajouter une connexion et des ressources** pour créer une connexion à VMware vSphere.



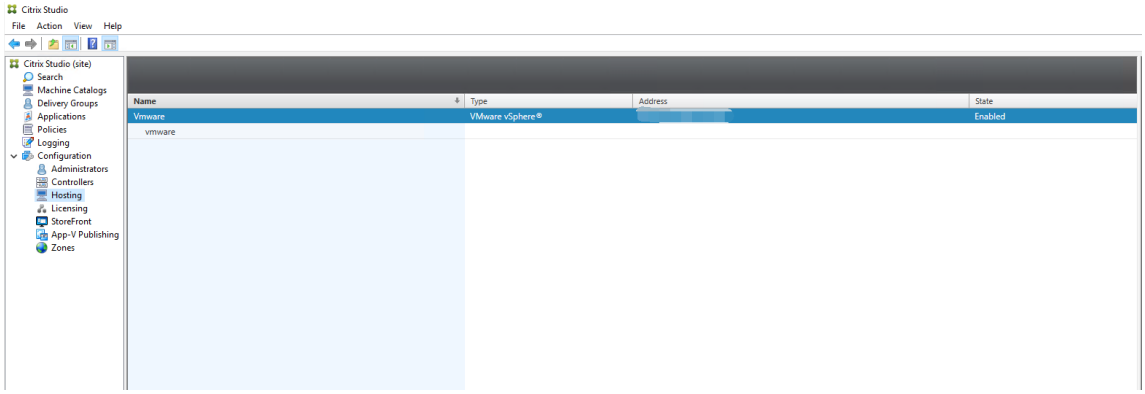
3. Sélectionnez le type de connexion VMware vSphere.



4. Saisissez l'adresse de connexion (l'adresse URL du serveur vCenter) de votre compte VMware, votre nom d'utilisateur et votre mot de passe ainsi que votre nom de connexion.



Une nouvelle connexion apparaît dans le panneau d'hébergement.



Étape 3 : préparer une image principale

(Pour Citrix Hypervisor uniquement) Étape 3a : installer Citrix VM Tools Installez le composant Citrix VM Tools sur la VM modèle pour que chaque VM utilise l'interface de ligne de commande xe ou XenCenter. Les performances de la VM peuvent être lentes à moins que les outils ne soient installés. Sans les outils, vous ne pouvez pas effectuer les opérations suivantes :

- Arrêter, redémarrer ou suspendre une VM correctement
- Afficher les données de performances de la VM dans XenCenter

- Migrer une VM en cours d'exécution (via XenMotion).
- Créer des instantanés ou des instantanés avec de la mémoire (points de contrôle) et revenir aux instantanés
- Régler le nombre de vCPU sur une VM Linux en cours d'exécution

1. Exécutez la commande suivante pour monter le composant Citrix VM Tools nommé guest-tools.iso.

```
sudo mount /dev/cdrom /mnt
<!--NeedCopy-->
```

2. Exécutez la commande suivante pour installer le package xe-guest-utilities en fonction de votre distribution Linux.

   Pour RHEL/CentOS/Rocky Linux :

```
sudo rpm -i /mnt/Linux/xe-guest-utilities_{
 package-version }
 _all.rpm
<!--NeedCopy-->
```

   Pour Ubuntu/Debian :

```
sudo dpkg -i /mnt/Linux/xe-guest-utilities_{
 package-version }
 _all.deb
<!--NeedCopy-->
```

   Pour SUSE :

```
sudo rpm -i /mnt/Linux/xe-guest-utilities_{
 package-version }
 _all.rpm
<!--NeedCopy-->
```

3. Vérifiez l'état de la virtualisation de la VM modèle dans l'onglet **General** de XenCenter. Si le composant Citrix VM Tools est correctement installé, l'état de la virtualisation est défini sur **Optimized**.

(Pour Azure, AWS et GCP) Étape 3b : configurer cloud-init pour Ubuntu 18.04

1. Pour vous assurer que le nom d'hôte du VDA soit préservé lorsqu'une VM est redémarrée ou arrêtée, exécutez la commande suivante :

```
echo "preserve_hostname: true" > /etc/cloud/cloud.cfg.d/99
   _hostname.cfg
<!--NeedCopy-->
```


Assurez-vous que les lignes suivantes sont présentes sous la section **system_info** du fichier /etc/cloud/cloud.cfg :

```
system_info:
   network:
       renderers: ['netplan', 'eni', 'sysconfig']
<!--NeedCopy-->
```

2. Pour utiliser SSH pour accéder à distance aux machines virtuelles créées avec MCS sur AWS, activez l'authentification par mot de passe car aucun nom de clé n'est attaché à ces machines virtuelles. Au besoin, procédez comme suit.

   - Modifiez le fichier de configuration `cloud-init`, /etc/cloud/cloud.cfg. Assurez-vous que la ligne **ssh_pwauth: true** est présente. Supprimez la ligne **set-password** et les lignes suivantes si elles existent ou ajoutez des commentaires.

     ```
     users:
     - default
     <!--NeedCopy-->
     ```

   - Si vous souhaitez utiliser l'utilisateur par défaut `ec2-user` ou `ubuntu` créé par `cloud-init`, vous pouvez modifier le mot de passe utilisateur à l'aide de la commande `passwd`. Conservez le nouveau mot de passe pour une utilisation ultérieure pour vous connecter aux machines virtuelles créées avec MCS.

   - Modifiez le fichier `/etc/ssh/sshd_config` pour vous assurer que la ligne suivante est présente :

     ```
     PasswordAuthentication yes
     <!--NeedCopy-->
     ```

     Enregistrez le fichier et exécutez la commande `sudo service sshd restart`.

Étape 3c : installer le package du Linux VDA sur la VM modèle

> **Remarque :**
>
> Pour utiliser un VDA en cours d'exécution comme VM modèle, ignorez cette étape.
>
> Avant d'installer le package Linux VDA sur la machine virtuelle modèle, installez .NET Runtime 6.0.

Selon votre distribution Linux, exécutez la commande suivante pour configurer l'environnement du Linux VDA :

Pour RHEL/CentOS/Rocky Linux :

```
sudo yum –y localinstall <PATH>/<Linux VDA RPM>
<!--NeedCopy-->
```


> **Remarque :**
>
> Pour RHEL et CentOS, vous devez installer le référentiel EPEL avant de pouvoir installer le Linux VDA et exécuter `deploymcs.sh`. Pour plus d'informations sur l'installation d'EPEL, consultez les instructions sur https://docs.fedoraproject.org/en-US/epel/.

Pour Ubuntu/Debian :

```
sudo dpkg  – i  <PATH>/<Linux VDA DEB>

apt-get install -f
<!--NeedCopy-->
```

Pour SUSE :

```
sudo zypper  – i install <PATH>/<Linux VDA RPM>
<!--NeedCopy-->
```

Étape 3d : activer les référentiels pour installer le package tdb-tools **Pour un serveur RHEL 7 :**

```
subscription-manager repos --enable=rhel-7-server-optional-rpms
<!--NeedCopy-->
```

Pour un poste de travail RHEL 7 :

```
subscription-manager repos --enable=rhel-7-workstation-optional-rpms
<!--NeedCopy-->
```

Étape 3e : (sur SUSE) installer manuellement ntfs-3g Sur la plate-forme SUSE, aucun référentiel ne fournit ntfs-3g. Téléchargez le code source, compilez, puis installez ntfs-3g manuellement :

1. Installez le système de compilation GCC (GNU Compiler Collection) et le package de création :

   ```
   sudo zypper install gcc
   sudo zypper install make
   <!--NeedCopy-->
   ```

2. Téléchargez le package ntfs-3g.
3. Décompressez le package ntfs-3g :

   ```
   sudo tar -xvzf ntfs-3g_ntfsprogs-<package version>.tgz
   <!--NeedCopy-->
   ```

4. Entrez le chemin d'accès au package ntfs-3g :


```
sudo cd ntfs-3g_ntfsprogs-<package version>
<!--NeedCopy-->
```

5. Installez ntfs-3g :

```
./configure
make
make install
<!--NeedCopy-->
```

Étape 3f: modifier les fichiers de configuration MCS

1. Modifiez les variables dans `/etc/xdl/mcs/mcs.conf`.

   - **Pour les scénarios de non-appartenance à un domaine**

     Vous pouvez utiliser les valeurs des variables par défaut ou modifier les variables selon vos besoins :

     `DOTNET_RUNTIME_PATH`=**path-to-install-dotnet-runtime **
     `DESKTOP_ENVIRONMENT`= **gnome | mate **
     `REGISTER_SERVICE`=**Y | N**
     `ADD_FIREWALL_RULES`=**Y | N**
     `VDI_MODE`=**Y | N**
     `START_SERVICE`=**Y | N**

   - **Pour les scénarios avec appartenance à un domaine**

     Vous pouvez définir les variables suivantes si nécessaire :

     - `Use_AD_Configuration_Files_Of_Current_VDA` : détermine s'il faut utiliser les fichiers de configuration liés à AD existants (/etc/krb5.conf, /etc/sssd.conf et /etc/samba/smb.conf) du VDA en cours d'exécution. Si la valeur Y est définie, les fichiers de configuration sur les machines créées avec MCS sont les mêmes que ceux sur le VDA en cours d'exécution. Cependant, vous devez toujours configurer les variables `dns` et `AD_INTEGRATION`. La valeur par défaut est N, ce qui signifie que les modèles de configuration sur l'image principale déterminent les fichiers de configuration sur les machines créées avec MCS.
     - `dns` : définit l'adresse IP de chaque serveur DNS. Vous pouvez configurer jusqu'à quatre serveurs DNS.
     - `NTP_SERVER` : définit l'adresse IP de votre serveur NTP. Sauf indication contraire, il s'agit de l'adresse IP de votre contrôleur de domaine.
     - `WORKGROUP` : définit le nom du groupe de travail sur le nom NetBIOS (sensible à la casse) que vous avez configuré dans AD. Sinon, MCS utilise la partie du nom de do-

maine qui suit immédiatement le nom d'hôte de la machine comme nom de groupe de travail. Par exemple, si le compte de la machine est **user1.lvda.citrix.com** , MCS utilise **lvda** comme nom de groupe de travail alors que **Citrix** est le bon choix. Assurez-vous de définir correctement le nom du groupe de travail.

- `AD_INTEGRATION` : définit Winbind, SSSD, PBIS ou Centrify. Pour une matrice des distributions Linux et des méthodes de jonction de domaine prises en charge par MSC, consultez la section Distributions prises en charge dans cet article.
- `CENTRIFY_DOWNLOAD_PATH` : définit le chemin de téléchargement du package Server Suite Free (anciennement Centrify Express). La valeur prend effet uniquement lorsque vous définissez la variable `AD_INTEGRATION` sur Centrify.
- `CENTRIFY_SAMBA_DOWNLOAD_PATH` : définit le chemin d'accès au téléchargement du package Centrify Samba. La valeur prend effet uniquement lorsque vous définissez la variable `AD_INTEGRATION` sur Centrify.
- `PBIS_DOWNLOAD_PATH` : définit le chemin d'accès au téléchargement du package PBIS. La valeur prend effet uniquement lorsque vous définissez la variable `AD_INTEGRATION` sur PBIS.
- `UPDATE_MACHINE_PW` : active ou désactive l'automatisation des mises à jour des mots de passe des comptes de machines. Pour plus d'informations, consultez Automatiser les mises à jour du mot de passe du compte de machine
- Variables de configuration de Linux VDA :

  `DOTNET_RUNTIME_PATH`=**path-to-install-dotnet-runtime **
  `DESKTOP_ENVIRONMENT`= **gnome | mate **
  `SUPPORT_DDC_AS_CNAME`=**Y | N**
  `VDA_PORT`=**port-number**
  `REGISTER_SERVICE`=**Y | N**
  `ADD_FIREWALL_RULES`=**Y | N**
  `HDX_3D_PRO`=**Y | N**
  `VDI_MODE`=**Y | N**
  `SITE_NAME`=**dns-site-name | '<none>'**
  `LDAP_LIST`=**'list-ldap-servers'| '<none>'**
  `SEARCH_BASE`=**search-base-set | '<none>'**
  `FAS_LIST`=**'list-fas-servers'| '<none>'**
  `START_SERVICE`=**Y | N**
  `TELEMETRY_SOCKET_PORT`=**port-number**
  `TELEMETRY_PORT`=**port-number**

2. Sur la machine modèle, ajoutez des lignes de commande au fichier `/etc/xdl/mcs/mcs_local_setting.reg` pour écrire ou mettre à jour les valeurs de registre selon les

besoins. Cette action empêche la perte de données et de paramètres chaque fois qu'une machine provisionnée par MCS redémarre.

Chaque ligne du fichier /etc/xdl/mcs/mcs_local_setting.reg est une commande permettant de définir ou de modifier une valeur de registre.

Par exemple, vous pouvez ajouter les lignes de commande suivantes au fichier /etc/xdl/mcs/mcs_local_setting.reg pour écrire ou modifier une valeur de registre respectivement :

```
create -k "HKLM\System\CurrentControlSet\Control\Citrix\
    VirtualChannels\Clipboard\ClipboardSelection" -t "REG_DWORD" -v
     "Flags" -d "0x00000003" --force
<!--NeedCopy-->
```

```
update -k "HKLM\System\CurrentControlSet\Control\Citrix\
    VirtualChannels\Clipboard\ClipboardSelection" -v "Flags" -d "0
    x00000003"
<!--NeedCopy-->
```

Étape 3g : créer une image principale

1. Exécutez /opt/Citrix/VDA/sbin/deploymcs.sh.
2. (Si vous utilisez un VDA en cours d'exécution en tant que VM modèle ou dans les scénarios dans lesquels le domaine n'est pas joint, ignorez cette étape.) Sur la VM modèle, mettez à jour les modèles de configuration pour personnaliser les fichiers /etc/krb5.conf, /etc/samba/smb.conf et /etc/sssd/sssd.conf sur toutes les VM créées.

   Pour les utilisateurs Winbind, mettez à jour les modèles /etc/xdl/ad_join/winbind_krb5.conf.tmpl et /etc/xdl/ad_join/winbind_smb.conf.tmpl.

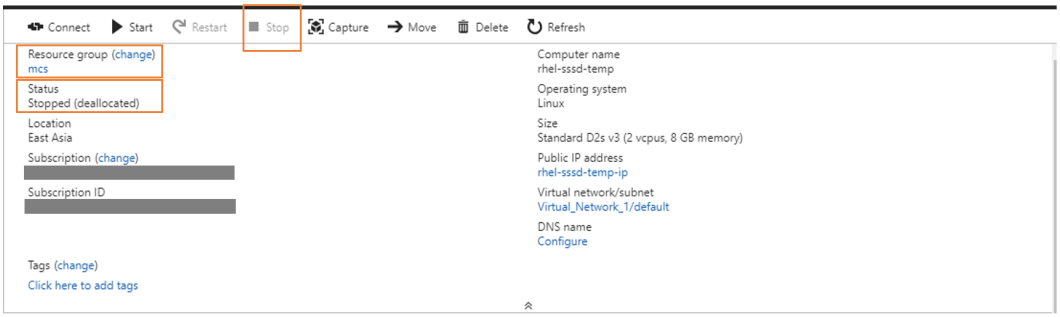
   Pour les utilisateurs SSSD, mettez à jour les modèles /etc/xdl/ad_join/sssd.conf.tmpl, /etc/xdl/ad_join/sssd_krb5.conf.tmpl et /etc/xdl/ad_join/sssd_smb.conf.tmpl.

   Pour les utilisateurs Centrify, mettez à jour les modèles /etc/xdl/ad_join/centrify_krb5.conf.tmpl et /etc/xdl/ad_join/centrify_smb.conf.tmpl.

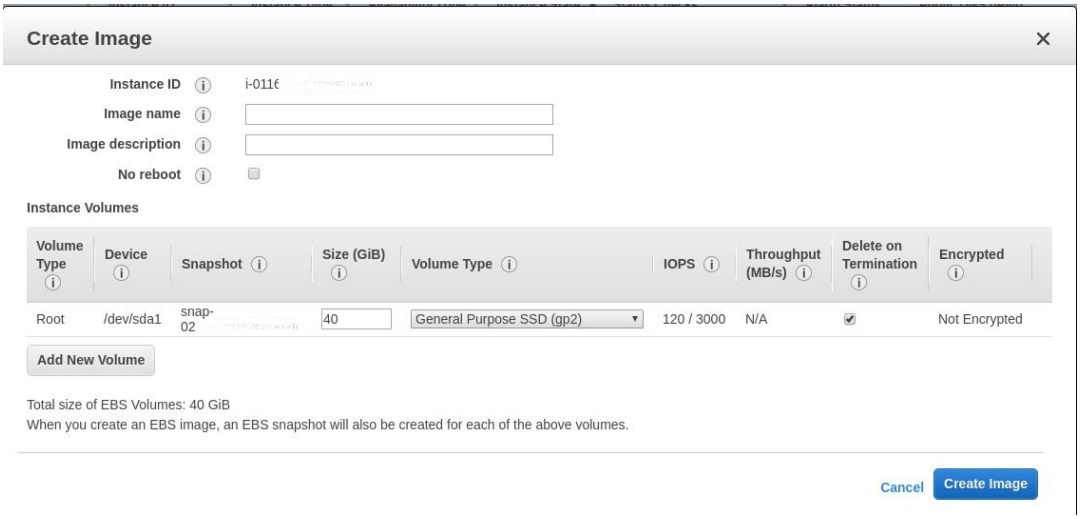
   > **Remarque :**
   >
   > Conservez le format existant utilisé dans les fichiers de modèle et utilisez des variables telles que $WORKGROUP, $REALM, $realm, ${new_hostname} et $AD_FQDN.

3. Créez et nommez un instantané de votre image principale en fonction du cloud public que vous utilisez.

- **(Pour Citrix Hypervisor, GCP et VMware vSphere)** Installez les applications sur la VM modèle et arrêtez-la. Créez et nommez un instantané de l'image principale.
- **(Pour Azure)** Installez les applications sur la VM modèle et fermez la VM modèle à partir du portail Azure. Assurez-vous que l'état de l'alimentation de la VM modèle est défini sur **Arrêté (libéré)**. Mémorisez le nom du groupe de ressources. Vous avez besoin du nom pour localiser votre image principale sur Azure.



- **(Pour AWS)** Installez les applications sur la VM modèle et fermez la VM modèle à partir du portail AWS EC2. Assurez-vous que l'état de l'instance de la VM modèle est défini sur **Arrêté**. Cliquez avec le bouton droit de la souris sur la VM modèle et sélectionnez **Image > Créer une image**. Entrez les informations requises et définissez les paramètres nécessaires. Cliquez sur **Créer une image**.



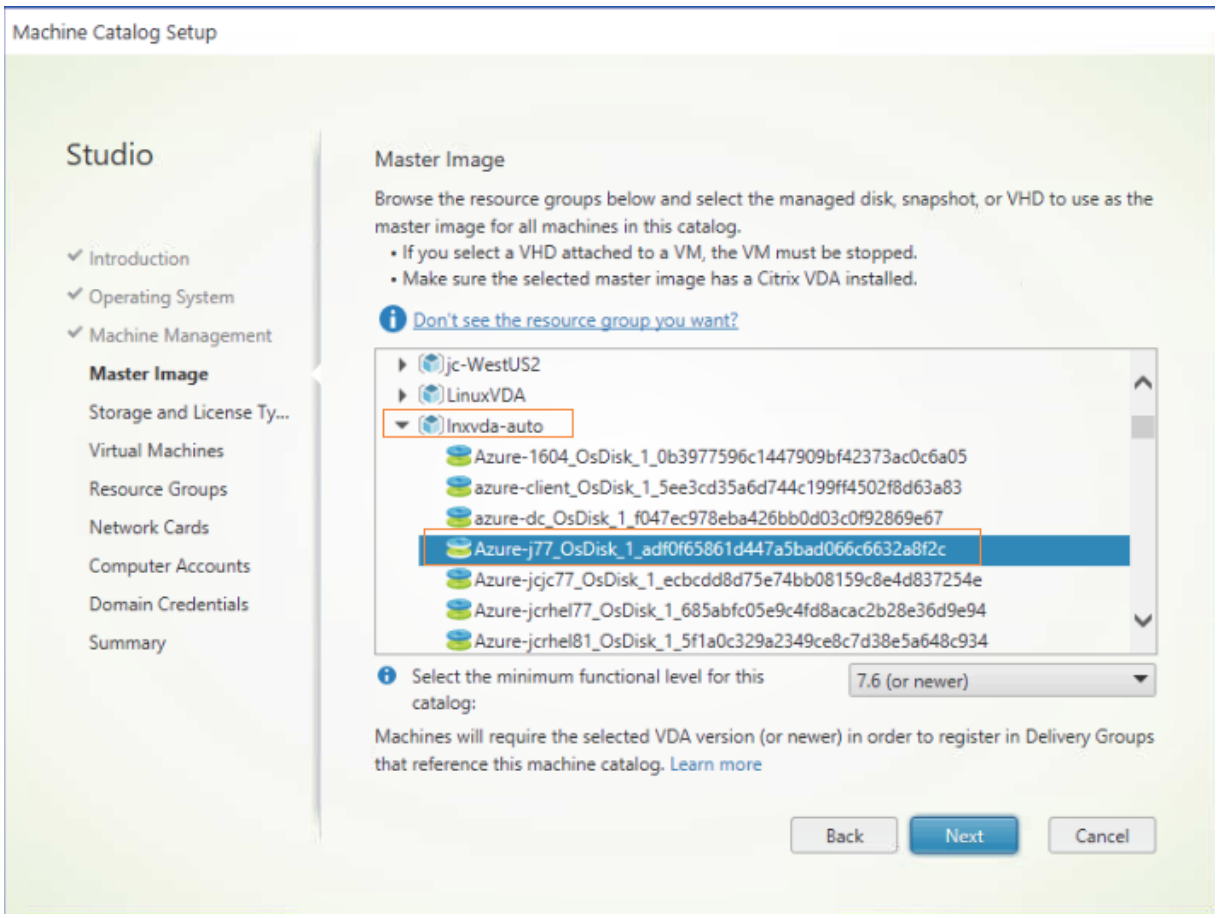
- **(Pour Nutanix)** Sur Nutanix AHV, arrêtez la VM modèle. Créez et nommez un instantané de l'image principale.

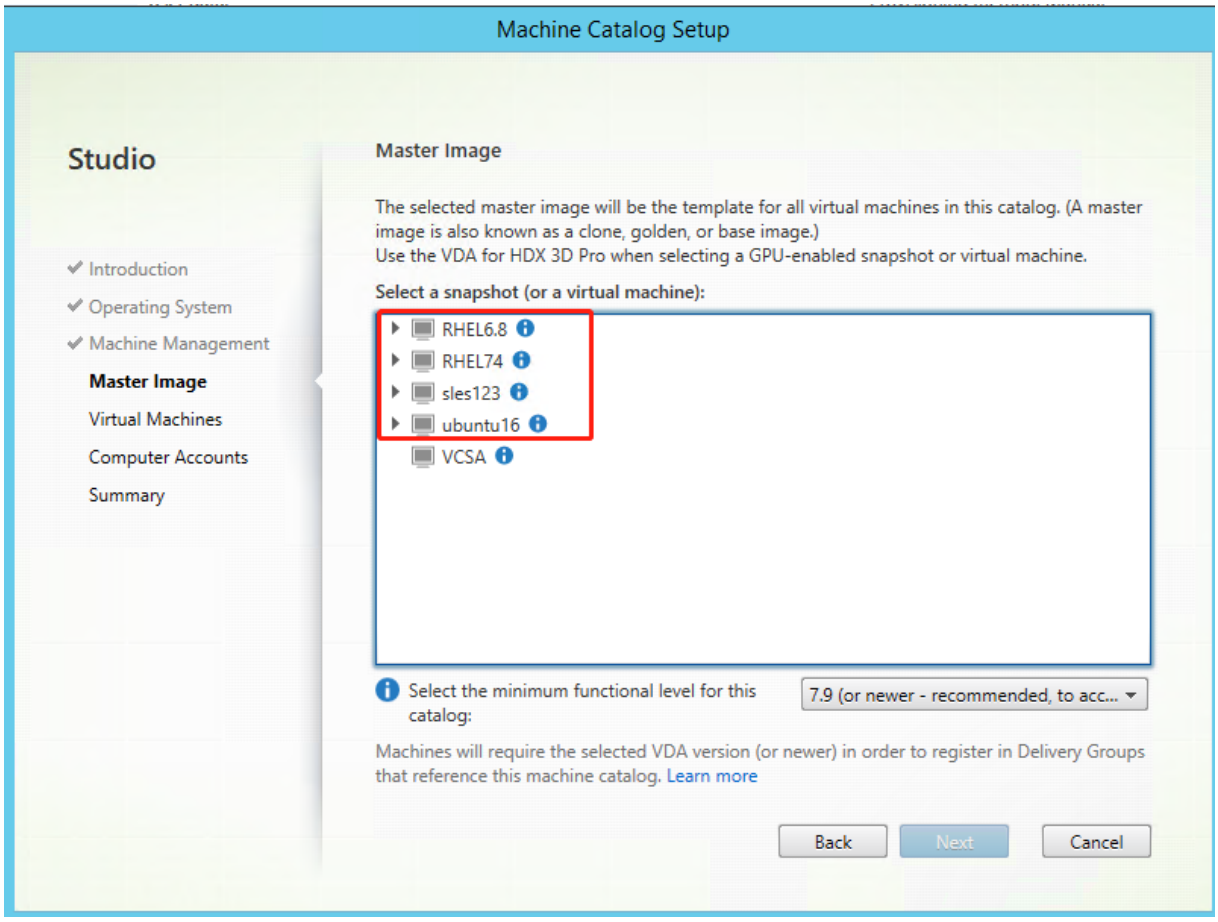
> **Remarque :**
>
> Les noms des instantanés Acropolis doivent être précédés de `XD_` pour pouvoir être utilisés dans Citrix Virtual Apps and Desktops. Utilisez la console Acropolis pour renommer vos instantanés, le cas échéant. Si vous renommez un instantané,

> redémarrez l'assistant **Créer un catalogue** pour afficher une liste actualisée.

Étape 4 : créer un catalogue de machines

Dans Citrix Studio, créez un catalogue de machines et spécifiez le nombre de VM à créer dans le catalogue. Lorsque vous créez le catalogue de machines, sélectionnez votre image principale. Voici quelques exemples :





Sur la page **Conteneur** unique à Nutanix, sélectionnez le conteneur que vous avez spécifié précédemment pour la VM modèle. Sur la page **Image principale**, sélectionnez l'instantané d'image. Sur la page **Machines virtuelles**, vérifiez le nombre de processeurs virtuels et le nombre de cœurs par vCPU.

> **Remarque :**
>
> Si le processus de création de votre catalogue de machines sur le Delivery Controller prend beaucoup de temps, accédez à Nutanix Prism et mettez sous tension manuellement la machine dont le nom est précédé du préfixe **Preparation**. Cette approche permet de poursuivre le processus de création.

Effectuez d'autres tâches de configuration si nécessaire. Pour plus d'informations, consultez l'article Créer un catalogue de machines à l'aide de Studio.

Étape 5 : créer un groupe de mise à disposition

Un groupe de mise à disposition est une collection de machines sélectionnées à partir d'un ou de plusieurs catalogues de machines. Il spécifie quels utilisateurs peuvent utiliser ces machines, ainsi

que les applications et bureaux disponibles auprès de ces utilisateurs. Pour plus d'informations, consultez la section Créer des groupes de mise à disposition.

Utiliser MCS pour mettre à jour votre Linux VDA

Pour utiliser MCS pour la mise à jour de votre Linux VDA, procédez comme suit :

1. Vérifiez que vous avez installé .NET Runtime 6.0 avant de mettre à jour votre Linux VDA vers la version actuelle.
2. Mettez à jour votre Linux VDA sur la machine modèle :

> **Remarque :**
>
> Vous pouvez également utiliser la fonctionnalité Mise à jour automatique de Linux VDA pour planifier des mises à jour logicielles automatiques. Pour ce faire, ajoutez des lignes de commande au fichier etc/xdl/mcs/mcs_local_setting.reg sur la machine modèle.
> Par exemple, vous pouvez ajouter les lignes de commande suivantes :

```
create -k "HKLM\System\CurrentControlSet\Control\Citrix\
    SelfUpdate" -t "REG_DWORD" -v "fEnabled" -d "0x00000001" –
    force

create -k "HKLM\System\CurrentControlSet\Control\Citrix\
    SelfUpdate" -t "REG_SZ" -v "ScheduledTime" -d "Immediately"
     – force

create -k "HKLM\System\CurrentControlSet\Control\Citrix\
    SelfUpdate" -t "REG_SZ" -v "Url" -d "<Your-Azure-Container-
    Url>" – force

create -k "HKLM\System\CurrentControlSet\Control\Citrix\
    SelfUpdate" -t "REG_SZ" -v "CaCertificate" -d "<Local-
    Certificate-Path-of-PortalAzureCom>" --force
<!--NeedCopy-->
```

Pour RHEL 7 et CentOS 7 :

```
sudo rpm -U XenDesktopVDA-<version>.el7_x.x86_64.rpm
<!--NeedCopy-->
```

Pour RHEL 8 et Rocky Linux 8 :

```
sudo rpm -U XenDesktopVDA-<version>.el8_x.x86_64.rpm
<!--NeedCopy-->
```

Pour SUSE :

```
sudo rpm -U XenDesktopVDA-<version>.sle12_x.x86_64.rpm
<!--NeedCopy-->
```


Pour Ubuntu 18.04 :

```
sudo dpkg -i xendesktopvda_<version>.ubuntu18.04_amd64.deb
<!--NeedCopy-->
```

Pour Ubuntu 20.04 :

```
sudo dpkg -i xendesktopvda_<version>.ubuntu20.04_amd64.deb
<!--NeedCopy-->
```

Pour Ubuntu 22.04 :

```
sudo dpkg -i xendesktopvda_<version>.ubuntu22.04_amd64.deb
<!--NeedCopy-->
```

3. Modifiez /etc/xdl/mcs/mcs.conf et /etc/xdl/mcs/mcs_local_setting.reg.
4. Prenez un nouvel instantané.
5. Dans Citrix Studio, sélectionnez le nouvel instantané pour la mise à jour de votre catalogue de machines. Attendez avant que chaque machine redémarre. Ne redémarrez pas une machine manuellement.

Automatiser les mises à jour du mot de passe du compte de machine

Par défaut, les mots de passe du compte de machine expirent 30 jours après la création du catalogue de machines. Pour empêcher l'expiration du mot de passe et automatiser les mises à jour du mot de passe du compte de machine, procédez comme suit :

1. Ajoutez l'entrée suivante dans /etc/xdl/mcs/mcs.conf avant d'exécuter /opt/Citrix/VDA/sbin/deployymcs.sh.

   ```
   UPDATE_MACHINE_PW="enabled"
   ```

2. Après avoir exécuté /opt/Citrix/VDA/sbin/deployymcs.sh, ouvrez /etc/cron.d/mcs_update_password_cronjo pour définir l'heure et la fréquence de mise à jour. Le paramètre par défaut met à jour les mots de passe du compte de machine chaque semaine à 2 h 30, le dimanche.

Après chaque mise à jour du mot de passe du compte de machine, le cache des tickets sur le Delivery Controller n'est plus valide et l'erreur suivante peut apparaître dans /var/log/xdl/jproxy.log :

```
[ERROR] - AgentKerberosServiceAction.Run: GSSException occurred.
 Error: Failure unspecified at GSS-API level (Mechanism level:
Checksum failed)
```

Pour éliminer l'erreur, videz le cache des tickets régulièrement. Vous pouvez planifier une tâche de nettoyage du cache sur tous les Delivery Controller ou sur le contrôleur de domaine.

Activer FAS sur les VM créées par MCS

Vous pouvez activer FAS sur les VM créées par MCS qui s'exécutent sur les distributions suivantes :

	Winbind	SSSD	Centrify	PBIS
RHEL 8	Oui	Non	Non	Oui
Rocky Linux 8	Oui	Non	Non	Non
RHEL 7, CentOS 7	Oui	Oui	Non	Oui
Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04	Oui	Non	Non	Non
Debian 11.3	Oui	Non	Non	Non
SUSE 15.3	Oui	Non	Non	Non

Activer FAS lorsque vous préparez une image principale sur la VM modèle

1. Importez le certificat d'autorité de certification racine.

```
sudo cp root.pem /etc/pki/CA/certs/
<!--NeedCopy-->
```

2. Exécutez ctxfascfg.sh. Pour plus d'informations, consultez la section Exécuter ctxfascfg.sh.
3. Définissez les variables dans `/etc/xdl/mcs/mcs.conf`.

> **Remarque :**
>
> définissez toutes les variables nécessaires dans `/etc/xdl/mcs/mcs.conf` car ces variables sont appelées au démarrage de la VM.

   a) Définissez la valeur de `Use_AD_Configuration_Files_Of_Current_VDA` sur Y.
   b) Définissez la variable `FAS_LIST` sur l'adresse de votre serveur FAS ou sur plusieurs adresses de serveur FAS. Séparez les différentes adresses avec des points-virgules et mettez-les entre guillemets simples, par exemple `FAS_LIST='<FAS_SERVER_FQDN>;<FAS_SERVER_FQDN>'`.
   c) Définissez les autres variables selon vos besoins, par exemple `VDI_MODE`.

4. Exécutez le script `/opt/Citrix/VDA/sbin/deploymcs.sh`.

Activer FAS sur une VM créée par MCS

Si FAS n'est pas activé sur la machine modèle comme décrit précédemment, vous pouvez activer FAS sur chaque machine virtuelle créée par MCS.

Pour activer FAS sur une machine virtuelle créée par MCS, procédez comme suit :

1. Définissez les variables dans /etc/xdl/mcs/mcs.conf.

   > **Remarque :**
   >
   > définissez toutes les variables nécessaires dans `/etc/xdl/mcs/mcs.conf` car ces variables sont appelées au démarrage de la VM.

   a) Définissez la valeur de `Use_AD_Configuration_Files_Of_Current_VDA` sur Y.
   b) Définissez la variable `FAS_LIST` sur l'adresse de votre serveur FAS.
   c) Définissez les autres variables selon vos besoins, par exemple `VDI_MODE`.

2. Importez le certificat d'autorité de certification racine.

   ```
   sudo cp root.pem /etc/pki/CA/certs/
   <!--NeedCopy-->
   ```

3. Exécutez le script `/opt/Citrix/VDA/sbin/ctxfascfg.sh`. Pour plus d'informations, consultez la section Exécuter ctxfascfg.sh.

Utiliser Citrix Provisioning pour créer des machines virtuelles Linux

December 16, 2022

Cet article fournit des informations sur le streaming de machines cibles Linux. Cette fonctionnalité vous permet de provisionner des bureaux virtuels Linux directement dans l'environnement Citrix Virtual Apps and Desktops.

Les distributions Linux suivantes sont prises en charge :

- Ubuntu 22.04
- Ubuntu 20.04
- Ubuntu 18.04
- RHEL 8.6
- Rocky Linux 8.6
- RHEL 8.4
- RHEL 7.9
- SUSE 15.3

> **Important :**
>
> - Nous vous recommandons d'utiliser le package d'installation le plus récent de Citrix Provisioning. Utilisez le package basé sur votre distribution Linux. Citrix Provisioning Server 2109 ou versions ultérieures est nécessaire pour utiliser Linux Streaming Agent 2109 et versions ultérieures.
> - Lorsque vous utilisez Citrix Provisioning pour streamer des machines cibles Linux, créez une partition de démarrage distincte sur l'image disque partagée unique de façon à ce que les machines provisionnées puissent démarrer comme prévu.
> - Évitez de formater une partition avec un fichier **btrfs**. GRUB2 rencontre un problème intrinsèque lors de la recherche de partitions **btrfs**. **GRUB** signifie **GRand Unified Bootloader**.

Pour de plus amples informations, veuillez consulter Streaming de machines cibles Linux dans la documentation de Citrix Provisioning.

Configurer des Delivery Controller pour XenDesktop 7.6 et versions antérieures

December 16, 2022

XenDesktop 7.6 et les versions antérieures requièrent des modifications pour prendre en charge le Linux VDA. Pour ces versions, un correctif ou un script de mise à jour est requis. Les instructions d'installation et de vérification sont décrites dans cet article.

Mettre à jour la configuration d'un Delivery Controller

Pour XenDesktop 7.6 SP2, appliquez le correctif Update 2 pour mettre à jour le broker pour Linux Virtual Desktop. Les correctifs Update 2 sont disponibles ici :

CTX142438 : correctif Update 2 - pour Delivery Controller 7.6 (32 bits) –Anglais

Pour les versions antérieures à XenDesktop 7.6 SP2, vous pouvez utiliser le script PowerShell appelé **Update-BrokerServiceConfig.ps1** pour mettre à jour la configuration du Broker Service. Ce script est disponible dans le package suivant :

- citrix-linuxvda-scripts.zip

Répétez les étapes suivantes sur chaque Delivery Controller de la batterie de serveurs :

1. Copiez le script **Update-BrokerServiceConfig.ps1** sur la machine Delivery Controller.

2. Ouvrez une console Windows PowerShell dans le contexte de l'administrateur local.
3. Accédez au dossier contenant le script **Update-BrokerServiceConfig.ps1**.
4. Exécutez le script **Update-BrokerServiceConfig.ps1** :

```
.\Update-BrokerServiceConfig.ps1
<!--NeedCopy-->
```

> **Conseil :**
>
> Par défaut, PowerShell est configuré pour empêcher l'exécution des scripts PowerShell. Si le script ne réussit pas à s'exécuter, modifiez la stratégie d'exécution PowerShell avant d'essayer à nouveau :
>
> ```
> Set-ExecutionPolicy Unrestricted
> <!--NeedCopy-->
> ```

Le script **Update-BrokerServiceConfig.ps1** met à jour le fichier de configuration du Broker Service en utilisant de nouveaux points de terminaison WCF requis par le Linux VDA et redémarre le Broker Service. Le script détermine automatiquement l'emplacement du fichier de configuration du Broker Service. Une copie de sauvegarde du fichier de configuration d'origine est créée dans le même répertoire avec l'extension **.prelinux** ajoutée au nom du fichier.

Ces modifications n'ont pas d'impact sur la négociation des VDA Windows configurés pour utiliser la même batterie de Delivery Controller. Une seule batterie de Delivery Controller peut gérer et négocier les sessions pour les VDA Windows et Linux en toute facilité.

Vérifier la configuration d'un Delivery Controller

Lorsque les modifications de configuration requises ont été appliquées à un Delivery Controller, la chaîne **EndpointLinux** apparaît cinq fois dans le fichier **%PROGRAMFILES%\Citrix\Broker\Service\BrokerServi**

À partir de l'invite de commande de Windows, connectez-vous en tant qu'administrateur local pour vérifier les éléments suivants :

```
cd "%PROGRAMFILES%"\Citrix\Broker\Service\
findstr EndpointLinux BrokerService.exe.config
<!--NeedCopy-->
```

Paramètres de stratégie et du serveur LDAP

December 16, 2022

Paramètres de stratégie dans Citrix Studio

Pour configurer des stratégies dans Citrix Studio, procédez comme suit :

1. Ouvrez **Citrix Studio**.
2. Sélectionnez le panneau **Stratégies**.
3. Cliquez sur **Créer une stratégie**.
4. Définissez la stratégie en fonction de la liste de stratégies prises en charge.

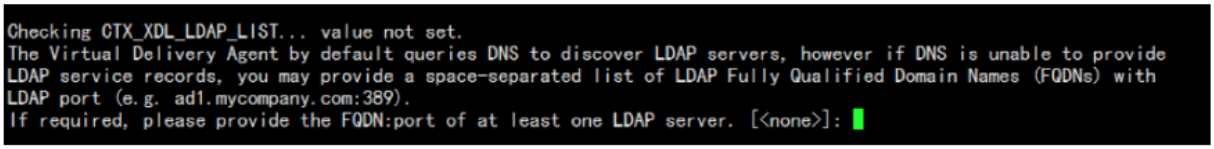
Paramètre du serveur LDAP sur le VDA

Le paramètre du serveur LDAP sur le Linux VDA est facultatif pour les environnements à domaine unique, mais obligatoire pour les environnements comportant plusieurs domaines et forêts. Le paramètre est requis par le service de stratégie pour effectuer une recherche LDAP dans ces environnements.

Après l'installation du package Linux VDA, exécutez la commande suivante :

```
/opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

Saisissez tous les serveurs LDAP dans le format recommandé : liste de noms de domaines complets (FQDN) séparés par des espaces avec le port LDAP (par exemple, ad1.mycompany.com:389 ad2.mycompany.com:389).



Vous pouvez également exécuter la commande **ctxreg** pour écrire ce paramètre directement sur le registre :

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
   VirtualDesktopAgent" -t "REG_SZ" -v "ListOfLDAPServers" -d "ad1.
   mycompany.com:389 ad2.mycomany.com:389" --force
<!--NeedCopy-->
```

Configurer

December 16, 2022

Cette section détaille les fonctionnalités du Linux VDA, notamment la description des fonctionnalités, la configuration et le dépannage.

Administration

December 16, 2022

Cette section contient les rubriques suivantes :

- CEIP
- HDX Insight
- Intégration avec Citrix Telemetry Service
- Mise à jour automatique du Linux VDA pour Citrix DaaS Standard pour Azure
- Mesures pour les sessions Linux et les machines virtuelles Linux
- Collecte de journaux
- Observation de session
- Démon du service de surveillance
- Outils et utilitaires
- Autres
  - Prise en charge de l'application Citrix Workspace pour HTML5
  - Créer un environnement virtuel Python3
  - Intégrer NIS avec Active Directory
  - IPv6
  - LDAPS
  - **Xauthority**

Programme d'amélioration de l'expérience du client Citrix (CEIP)

December 16, 2022

Si vous participez au programme CEIP, des informations d'utilisation et des statistiques anonymes sont envoyées à Citrix pour améliorer la qualité et les performances des produits Citrix. En outre, une copie des données anonymes est envoyée à Google Analytics (GA) pour une analyse rapide et efficace. GA est désactivé par défaut.

Paramètres de registre

Par défaut, vous participez automatiquement au programme CEIP lorsque vous installez le Linux VDA. Le premier chargement de données se produit approximativement sept jours après l'installation du Linux VDA. Vous pouvez modifier ce paramètre par défaut dans le registre.

- **CEIPSwitch**

Paramètre de Registre qui active ou désactive le programme CEIP (valeur par défaut = 0) :

Emplacement : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Nom : **CEIPSwitch**

Valeur : 1 = désactivé, 0 = activé

Si elle n'est pas spécifiée, le programme CEIP est activé.

Vous pouvez exécuter la commande suivante sur un client pour désactiver le programme CEIP.

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
     Citrix\CEIP" -v "CEIPSwitch" -d "1"
2 <!--NeedCopy-->
```

- **GASwitch**

Paramètre de Registre qui active ou désactive GA (valeur par défaut = 1) :

Emplacement : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Nom : **GASwitch**

Valeur : 1 = désactivé, 0 = activé

Si elle n'est pas spécifiée, GA est désactivé.

Vous pouvez exécuter la commande suivante sur un client pour activer GA :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
     Citrix\CEIP" -v "GASwitch" -d "0"
2 <!--NeedCopy-->
```

- **DataPersistPath**

Paramètre de Registre qui contrôle le chemin d'accès des données persistantes (défaut = /var/xdl/-ceip) :

Emplacement : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Nom : DataPersistPath

Valeur : chaîne

Vous pouvez exécuter la commande suivante pour définir ce chemin d'accès :


```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
   Citrix\CEIP" -v "DataPersistPath" -d "your_path"
<!--NeedCopy-->
```

Si le chemin d'accès configuré n'existe pas ou n'est pas accessible, les données sont enregistrées dans le chemin d'accès par défaut.

Données CEIP collectées depuis le Linux VDA

Le tableau suivant présente un exemple de types d'informations anonymes collectées. Les données ne contiennent aucun détail permettant d'identifier le client.

Point de données	Nom de la clé	Description
GUID de machine	**machine_guid**	Identification de la machine d'où les données proviennent
Solution Active Directory	**ad_solution**	Chaîne de texte indiquant la méthode de jonction du domaine de la machine
Version du noyau Linux	**kernel_version**	Chaîne de texte indiquant la version du noyau de la machine
Version LVDA	**vda_version**	Chaîne de texte indiquant la version installée du Linux VDA
Mise à jour LVDA ou nouvelle installation	**update_or_fresh_install**	Chaîne de texte indiquant que le package Linux VDA actuel est en cours de mise à jour ou d'installation
Méthode d'installation de LVDA	install_method	Chaîne de texte indiquant que le package Linux VDA actuel est installé à l'aide de MCS, PVS, Easy Install ou d'une installation manuelle.
HDX 3D Pro activé ou non	**hdx_3d_pro**	Chaîne de texte indiquant si HDX 3D Pro est activé sur la machine
Mode VDI activé ou non	**vdi_mode**	Chaîne de texte indiquant si le mode VDI est activé
Paramètres régionaux système	**system_locale**	Chaîne de texte indiquant les paramètres régionaux de cette machine

Point de données	Nom de la clé	Description
Dernière heure de redémarrage des services LVDA principaux	**ctxhdx ctxvda**	Dernière heure de redémarrage des services `ctxhdx` et `ctxvda`, au format jj-hh:mm:ss, par exemple, 10-17:22:19
Type de GPU	**gpu_type**	Indique le type de processeur graphique de la machine
Cœurs d'UC	**cpu_cores**	Entier indiquant le nombre de cœurs d'UC de la machine
Fréquence du processeur	**cpu_frequency**	Nombre flottant indiquant la fréquence du processeur en MHz
Taille de la mémoire physique	**memory_size**	Entier indiquant la taille de la mémoire physique en Ko
Nombre de sessions lancées	**session_launch**	Entier indiquant le nombre de sessions lancées (connexions ou reconnexions) sur la machine au moment où ce point de données est collecté
Version et nom du système d'exploitation Linux	**os_name_version**	Chaîne de texte indiquant le nom et la version du système d'exploitation Linux de la machine
Clé de session	**session_key**	Identification de la session d'où les données proviennent
Type de ressource	**resource_type**	Chaîne de texte indiquant le type de ressource de la session lancée : bureau ou `<appname>`
Période active de session	**active_session_time**	Utilisé pour enregistrer les périodes actives de la session. Une session peut contenir plusieurs périodes actives car la session peut se déconnecter/se reconnecter.
Durée de session	**session_duration_time**	Utilisé pour enregistrer la durée de la session de l'ouverture à la fermeture de session

Point de données	Nom de la clé	Description
Type de client Receiver	**receiver_type**	Entier indiquant le type d'application Citrix Workspace utilisé pour lancer la session
Version du client Receiver	**receiver_version**	Chaîne de texte indiquant la version de l'application Citrix Workspace utilisée pour lancer la session
Nombre d'impressions	**printing_count**	Entier indiquant le nombre de fois que la session utilise la fonction d'impression
Nombre de redirections USB	**usb_redirecting_count**	Entier indiquant le nombre de fois que la session utilise un périphérique USB
Type de fournisseur **Gfx**	**gfx_provider_type**	Chaîne de texte indiquant le type de fournisseur de graphiques de la session
Nombre d'observations	**shadow_count**	Entier indiquant le nombre de fois que la session a été observée
Langue sélectionnée par l'utilisateur	**ctxism_select**	Chaîne longue composée qui contient toutes les langues sélectionnées par les utilisateurs
Nombre de redirections de carte à puce	**scard_redirecting_count**	Entier indiquant le nombre de fois que la redirection de carte à puce est utilisée pour les ouvertures de session et l'authentification utilisateur pour les applications de session

HDX Insight

April 18, 2024

Vue d'ensemble

Le Linux VDA prend en charge partiellement la fonctionnalité HDX Insight.

Installation

Aucun package dépendant ne doit être installé.

Utilisation

HDX Insight analyse les messages ICA transmis via Citrix ADC entre l'application Citrix Workspace et le Linux VDA. Toutes les données HDX Insight proviennent du canal virtuel NSAP et sont envoyées non compressées. Le canal virtuel NSAP est activé par défaut.

Les commandes suivantes désactivent et activent le canal virtuel NSAP, respectivement :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP" -d "0x00000000"
     --force
2 <!--NeedCopy-->
```

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP" -d "0x00000001"
     --force
2 <!--NeedCopy-->
```

Résolution des problèmes

Aucun point de données n'est affiché

Deux causes peuvent être à l'origine du problème :

- HDX Insight n'est pas configuré correctement.

  Par exemple, AppFlow n'est pas activé sur le Citrix ADC ou une instance incorrecte de Citrix ADC est configurée sur Citrix ADM.

- Le canal virtuel de contrôle ICA n'est pas démarré sur le Linux VDA.

  ```
  ps aux | grep -i ctxctl
  ```

  Si `ctxctl` n'est pas exécuté, contactez votre administrateur pour signaler un bogue à Citrix.

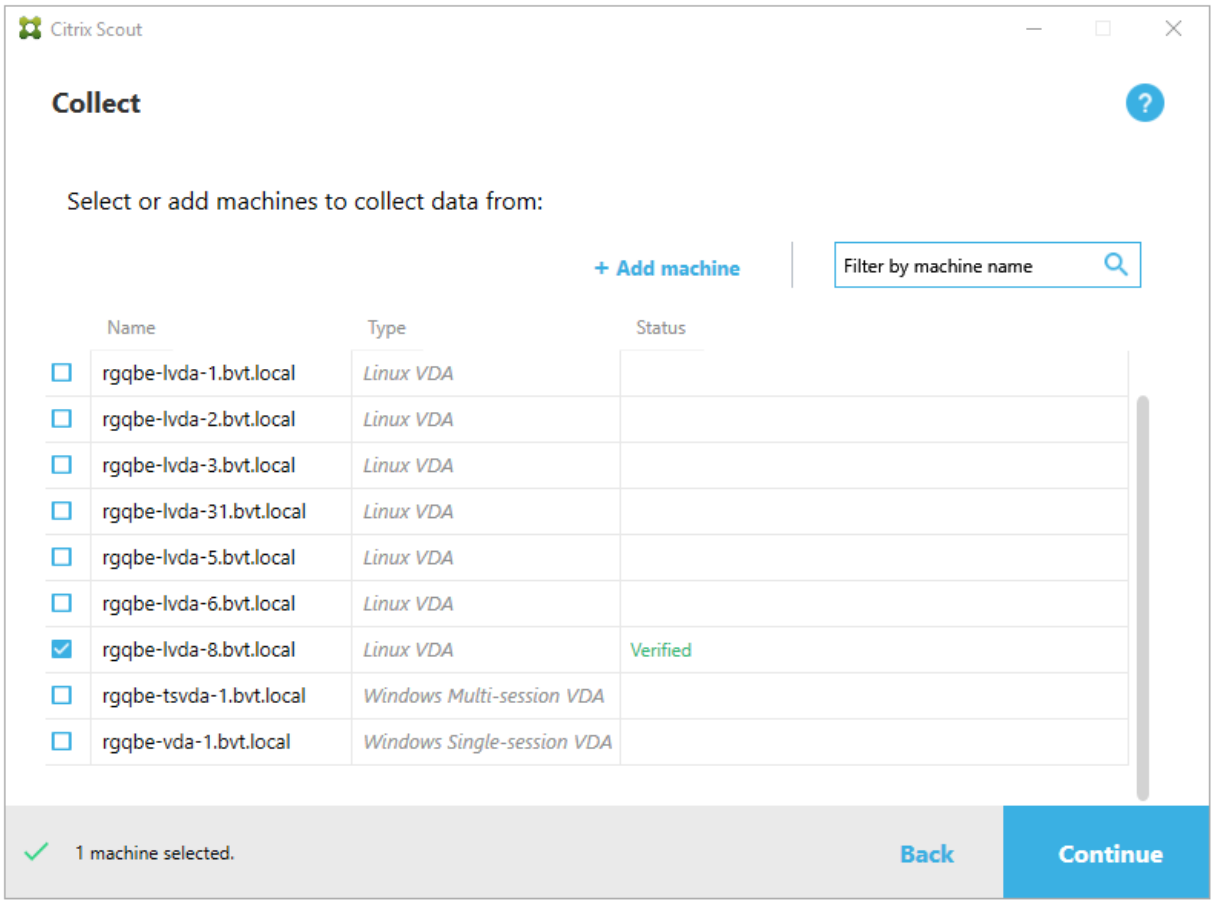
Aucun point de données d'application n'est affiché

Vérifiez que le canal virtuel transparent est activé et qu'une application transparente est exécutée.

Intégration avec Citrix Telemetry Service

December 16, 2022

Avec Citrix Telemetry Service (`ctxtelemetry`) intégré au logiciel VDA Linux, vous pouvez exécuter Citrix Scout, qui utilise ensuite le script /opt/Citrix/vda/bin/xdlcollect.sh, pour collecter des journaux sur le VDA Linux.



> **Remarque :**
>
> après la mise à niveau à partir de Linux VDA 1912 et versions antérieures, vous devez réexécuter /opt/Citrix/VDA/sbin/ctxsetup.sh pour configurer les variables du service de télémétrie Citrix (`ctxtelemetry`). Pour de plus amples informations sur les variables, consultez la section Easy Install.

Activer et désactiver le service de télémétrie Citrix

- Pour activer le service, exécutez la commande **sudo systemctl enable ctxtelemetry.socket**.
- Pour désactiver le service, exécutez **sudo systemctl disable ctxtelemetry.socket**.

Ports

Le service de télémétrie Citrix (`ctxtelemetry`), par défaut, utilise le port TCP/IP 7503 pour écouter Citrix Scout. Il utilise le port TCP/IP 7502 sur le Delivery Controller pour communiquer avec Citrix Scout.

Vous pouvez utiliser les ports par défaut ou modifier les ports via les variables suivantes lorsque vous installez le VDA Linux.

- **CTX_XDL_TELEMETRY_SOCKET_PORT** : port socket permettant d'écouter Citrix Scout. Le port par défaut est 7503.
- **CTX_XDL_TELEMETRY_PORT** : port de communication avec Citrix Scout. Le port par défaut est 7502.

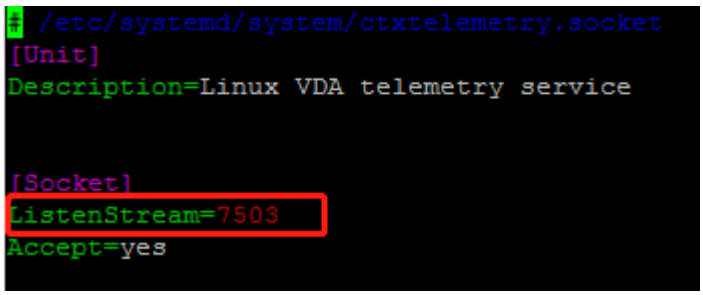
Pour modifier les ports après avoir installé votre VDA, procédez comme suit :

1. Pour modifier un port de communication avec Scout, exécutez la commande suivante.

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
   VirtualDesktopAgent" -v "TelemetryServicePort" -d <port number>
    -t REG_DWORD
<!--NeedCopy-->
```

2. Pour modifier le port de socket pour l'écoute de Scout, exécutez la commande suivante pour ouvrir et modifier le fichier ctxtelemetry.socket.

```
sudo vi /etc/systemd/system/ctxtelemetry.socket
<!--NeedCopy-->
```



3. Exécutez les commandes suivantes pour redémarrer le port de socket.

```
sudo systemctl daemon-reload
sudo systemctl stop ctxtelemetry.socket
sudo systemctl start ctxtelemetry.socket
<!--NeedCopy-->
```

4. Activez les nouveaux ports dans votre configuration de pare-feu.

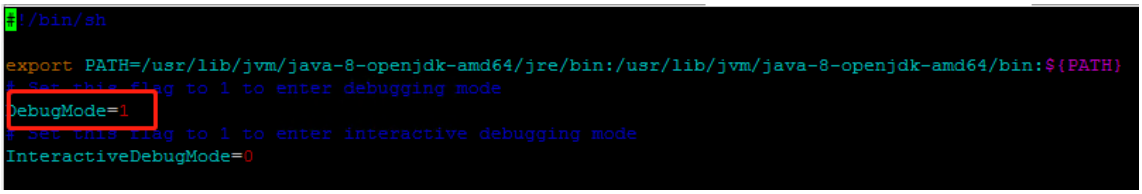
   Si vous utilisez Ubuntu, par exemple, exécutez la commande **sudo ufw allow 7503** pour activer le port 7503.

Mode débogage

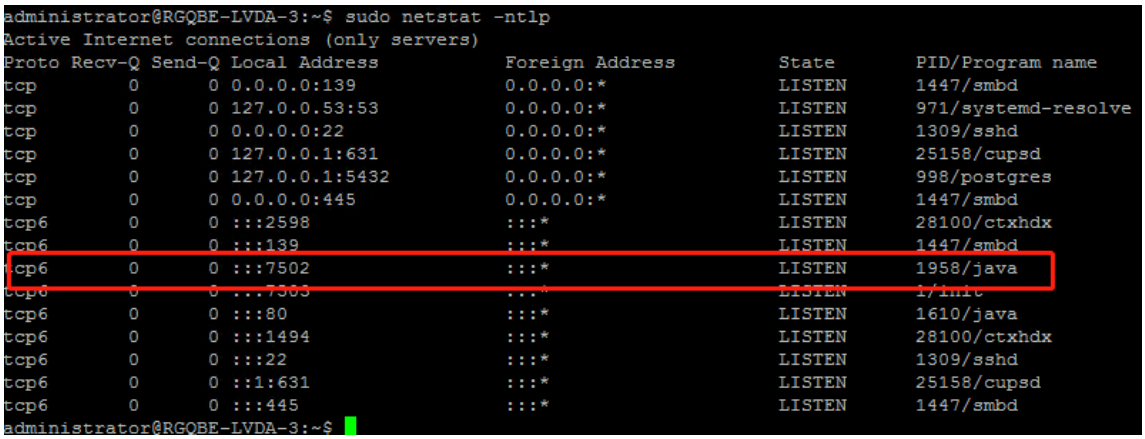
Si le service de télémétrie Citrix ne fonctionne pas comme prévu, vous pouvez activer le mode de débogage pour en déterminer les causes.

1. Pour activer le mode de débogage, exécutez la commande suivante pour ouvrir le fichier `ctxtelemetry`, puis modifiez la valeur DebugMode sur 1.

```
sudo vi /opt/Citrix/VDA/sbin/ctxtelemetry
<!--NeedCopy-->
```



2. Arrêtez manuellement le service de télémétrie Citrix ou attendez 15 minutes que le service s'arrête automatiquement.



   Dans cet exemple, vous pouvez exécuter les commandes suivantes pour arrêter le service de télémétrie Citrix.

```
sudo netstat -ntlp
Kill -9 1958
<!--NeedCopy-->
```

3. Pour redémarrer le service de télémétrie Citrix, sélectionnez votre VDA Linux sur Scout et recherchez telemetry-debug.log dans /var/log/xdl/.

Délai d'attente du service

Le démon `systemd` qui ouvre le port socket démarre par défaut et utilise peu de ressources. Le service de télémétrie Citrix s'arrête par défaut et démarre uniquement lorsqu'il existe une demande de

collecte de journaux à partir du Delivery Controller. Une fois la collecte des journaux terminée, le service attend les nouvelles demandes de collecte pendant 15 minutes et s'arrête à nouveau s'il n'y en a pas. Vous pouvez configurer le délai d'attente via la commande suivante. La valeur minimale est de 10 minutes. Si vous définissez une valeur inférieure à 10 minutes, la valeur minimale, 10 minutes, est appliquée. Après avoir défini le délai d'attente, arrêtez et redémarrez le service.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent" -v "TelemetryServiceIdleTimeoutInMinutes" -d <
     number> -t REG_DWORD
2 <!--NeedCopy-->
```

Tests de vérification

Avant le démarrage d'une collecte, des tests de vérification sont exécutés automatiquement pour chaque machine sélectionnée. Ces tests garantissent que les conditions requises sont remplies. Si un test échoue pour une machine, Scout affiche un message avec actions correctives proposées. Pour plus d'informations sur les tests de vérification, consultez la section Tests de vérification de la documentation Citrix Scout.

Mise à jour automatique de Linux VDA via Azure

May 30, 2024

Cette fonctionnalité permet de mettre à jour automatiquement votre logiciel Linux VDA, immédiatement ou à une heure planifiée. Cela est utile lorsque vous créez des VDA Linux dans Citrix DaaS Standard pour Azure (anciennement Citrix Virtual Apps and Desktops Standard pour Azure). Vous n'avez pas besoin de privilèges d'administrateur sur les machines virtuelles dans Azure. Pour plus d'informations, consultez Créer des Linux VDA dans Citrix DaaS Standard pour Azure.

Configuration

Pour utiliser cette fonctionnalité, procédez comme suit :

Étape 1 : charger les informations de mise à jour et les nouveaux packages VDA sur votre conteneur Azure

Étape 1a : créer un conteneur sous votre compte de stockage Azure et définir le niveau d'accès à votre conteneur sur **Blob (Accès en lecture anonyme pour les objets blobs uniquement)**

> **Remarque :**
>
> Les conteneurs et objets blobs Azure sont exclusivement détenus et gérés par les clients. Citrix n'est pas responsable des problèmes de sécurité liés à ces derniers. Pour garantir la sécurité des données et la rentabilité, définissez le niveau d'accès à votre conteneur sur **Privé (Pas d'accès anonyme)** après chaque **mise à jour automatique**.

Étape 1b : incorporer les informations de mise à jour de votre VDA dans un fichier JSON nommé UpdateInfo.json Pour obtenir un exemple de format de fichier, consultez le bloc suivant :

```
{

 "Version": "21.04.200.4",
"Distributions":[
{

"TargetOS": "RHEL7_9",
"PackageName": "",
"PackageHash": ""
 }
 ,
{

"TargetOS": "UBUNTU18_04",
"PackageName": "xendesktopvda_21.04.200.4-1.ubuntu18.04_amd64.deb",
"PackageHash": "4148
   cc3f25d3717e3cbc19bd953b42c72bd38ee3fcd7f7034c2cd6f2b15b3c5a"
 }
 ,
{

"TargetOS": "UBUNTU20_04",
"PackageName": "",
"PackageHash": ""
 }

]
 }

<!--NeedCopy-->
```

Où **Version** indique la nouvelle version du VDA et **Distributions** est un tableau d'objets de mise à jour. Chaque objet contient trois éléments :

- **TargetOS** : doit être RHEL7_9 (pour RHEL 7, CentOS 7 et Amazon Linux 2), UBUNTU18_04 ou UBUNTU20_04. Le service `ctxmonitorservice` ne reconnaît aucune autre distribution.
- **PackageName** : nom complet du package VDA de la version spécifiée.
- **PackageHash** : valeur SHA-256 que vous calculez à l'aide de la commande `shasum -a 256 <pkgname>`.

Étape 1c : charger le fichier JSON et la nouvelle version des packages Linux VDA sur votre conteneur Azure

Étape 2 : activer la fonction de mise à jour automatique sur l'image principale ou sur chaque VDA

Par défaut, la **mise à jour automatique** est désactivée. Si vous créez des VDA Linux dans Citrix DaaS Standard pour Azure, l'activation des fonctionnalités doit être effectuée sur l'image principale. Sinon, activez directement la fonctionnalité sur chaque VDA cible.

Pour activer la **mise à jour automatique**, exécutez des commandes similaires aux suivantes pour modifier la clé de registre sur HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\SelfUpdate.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
     Control\Citrix\SelfUpdate" -t "REG_DWORD" -v "fEnabled" -d "0
     x00000001" --force
2
3 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
     Control\Citrix\SelfUpdate" -t "REG_SZ" -v "ScheduledTime" -d "
     Immediately" --force
4
5 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
     Control\Citrix\SelfUpdate" -t "REG_SZ" -v "Url" -d "<Your-Azure-
     Container-Url>" --force
6
7 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
     Control\Citrix\SelfUpdate" -t "REG_SZ" -v "CaCertificate" -d "<Local
     -Certificate-Path-of-PortalAzureCom>" --force
8 <!--NeedCopy-->
```

Le tableau suivant décrit les paramètres de registre.

Paramètre de registre	Description
fEnabled	Ce paramètre est requis. Par défaut, la valeur est 0, ce qui signifie que la **mise à jour automatique** est désactivée. Vous pouvez définir ce paramètre sur 1 pour activer la **mise à jour automatique**.
Url	Ce paramètre est requis. Il définit l'URL de votre conteneur Azure pour obtenir les informations de mise à jour et les nouveaux packages VDA.

Paramètre de registre	Description
ScheduledTime	Ce paramètre est requis. Vous pouvez le définir sur **Immediate** ou **NextStart**. **Immediately** signifie l'exécution immédiate d'une mise à jour après le téléchargement des packages VDA. Cette option est appropriée lorsque la vitesse de téléchargement est élevée et que votre mise à jour est urgente. Toutefois, cela peut également perturber l'expérience utilisateur si des sessions actives sont en cours lorsque vous téléchargez le package. **NextStart** signifie l'exécution d'une mise à jour au prochain démarrage de `ctxmonitorservice`. Cette option est appropriée lorsque la vitesse de téléchargement n'est pas élevée et que votre mise à jour n'est pas urgente.
CaCertificate	Ce paramètre est facultatif. Il définit le chemin complet d'un certificat PEM pour vérifier l'URL de votre conteneur Azure. Pour les objets blobs Azure, il peut s'agir du certificat de portal.azure.com récupéré depuis le navigateur, puis converti au format PEM. Pour des raisons de sécurité, nous vous recommandons d'ajouter ce paramètre de registre. Cependant, il n'est pris en charge que sur Ubuntu. Sur RHEL, il ne lie pas certaines bibliothèques NSS pour la commande `curl`. Assurez-vous de définir les principes du moindre privilège sur le certificat.

Au redémarrage de `ctxmonitorservice`, le service interroge d'abord **Url** pour obtenir le fichier UpdateInfo.json et récupère la version de mise à jour à partir du fichier JSON. Ensuite, `ctxmonitorservice` compare la version de mise à jour avec la version actuelle. Si la version actuelle est antérieure, le service télécharge la nouvelle version du package VDA depuis Azure et l'enregistre localement. Après cela, il exécute une mise à jour en fonction du paramètre **Scheduled-Time**. Pour un déploiement local, vous pouvez redémarrer `ctxmonitorservice` directement pour déclencher la mise à jour. Toutefois, dans Citrix DaaS Standard pour Azure, où vous ne disposez pas de privilèges d'administrateur sur les machines virtuelles, `ctxmonitorservice` ne peut être redémarré qu'après le redémarrage de la machine VDA. Si une mise à jour échoue, votre VDA est

restauré à la version existante.

> **Remarque :**
>
> - Les paramètres de registre que vous avez configurés sur l'image principale ne peuvent pas être modifiés.
> - Si toutes les machines virtuelles d'un environnement téléchargent un package en même temps, le réseau local peut être encombré.
> - Les données utilisateur sont perdues en cas d'échec d'une mise à jour et d'une restauration.
> - Si une mise à jour échoue mais que la restauration réussit, les utilisateurs du même réseau peuvent avoir des versions différentes de Linux VDA. Ce cas n'est pas optimal.
> - Une mise à jour prend généralement plusieurs minutes. Il n'y a pas d'indicateur d'état dans Citrix Studio.

Mesures pour les sessions Linux et les machines virtuelles Linux

December 16, 2022

Le tableau suivant répertorie certaines mesures disponibles pour les machines virtuelles Linux et les sessions Linux.

Mesure	Min. Version du VDA requise	Description	Remarques
Mesure	Min. Version du VDA requise	Description	Remarques
Durée d'ouverture de session	2109	Il s'agit d'une mesure du processus d'ouverture de session calculée à partir du moment où un utilisateur se connecte depuis l'application Citrix Workspace jusqu'au moment où une session est prête à être utilisée. Pour afficher la mesure d'une session, accédez à l'onglet Surveiller de Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). La console Surveiller 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. Dans l'onglet Surveiller, cliquez sur **Afficher la tendance historique** dans la section **Durée moyenne d'ouverture de session**. Sur la page **Performances d'ouverture de session**, définissez les conditions de filtre et cliquez sur **Appliquer** pour afficher les mesures.	Disponible uniquement dans l'onglet Surveiller.

Mesure	Min. Version du VDA requise	Description	Remarques
Nombre de reconnexions automatiques de sessions	2109	Pour afficher le nombre de reconnexions automatiques dans une session, accédez à la vue **Tendances**. Définissez les conditions et cliquez sur **Appliquer** pour affiner les résultats de recherche. 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. 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.	Disponible à la fois dans Citrix Director et dans l'onglet Surveiller.

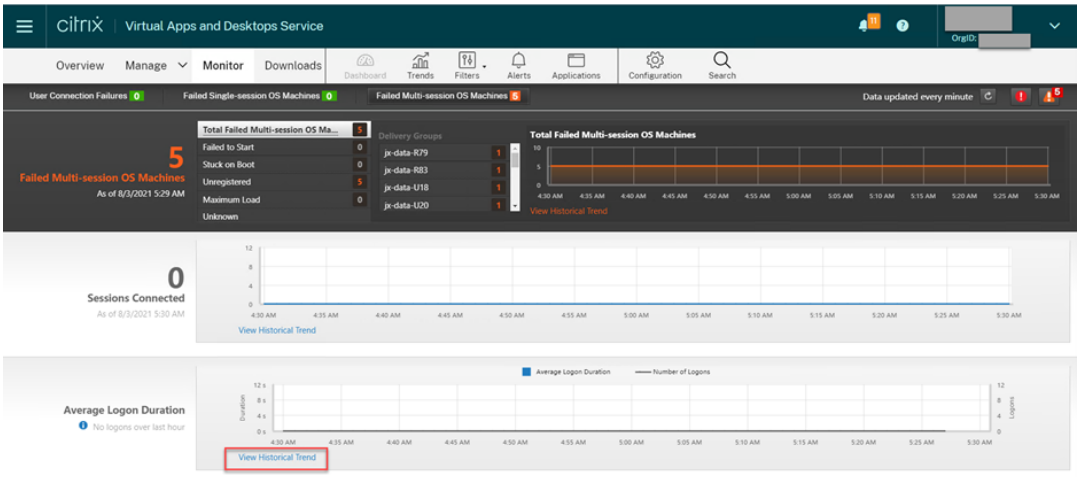
Mesure	Min. Version du VDA requise	Description	Remarques
Délai d'inactivité	2103	Pour accéder à cette mesure, ouvrez la boîte de dialogue **Toutes les sessions** en sélectionnant **Filtres > Sessions > Toutes les sessions**.	Disponible à la fois dans Citrix Director et dans l'onglet Surveiller.
Mesures d'une VM Linux	2103	Les mesures suivantes sont disponibles pour les VM Linux : nombre de cœurs de processeur, taille de la mémoire, capacité du disque dur et utilisation actuelle et historique du processeur et de la mémoire	Disponible à la fois dans Citrix Director et dans l'onglet Surveiller.
Protocol	1909	Le protocole de transport d'une session Linux apparaît comme UDP ou TCP dans le panneau **Détails de la session**.	Disponible à la fois dans Citrix Director et dans l'onglet Surveiller.

Mesure	Min. Version du VDA requise	Description	Remarques
RTT ICA	1903	La durée des boucles (RTT) ICA est le temps écoulé entre le moment où vous appuyez sur une touche jusqu'à ce que la réponse apparaisse sur le point de terminaison. Pour afficher les mesures RTT ICA, créez les stratégies de **Calcul des boucles ICA** et **Intervalle de calcul des boucles ICA** dans Citrix Studio.	Disponible à la fois dans Citrix Director et dans l'onglet Surveiller.

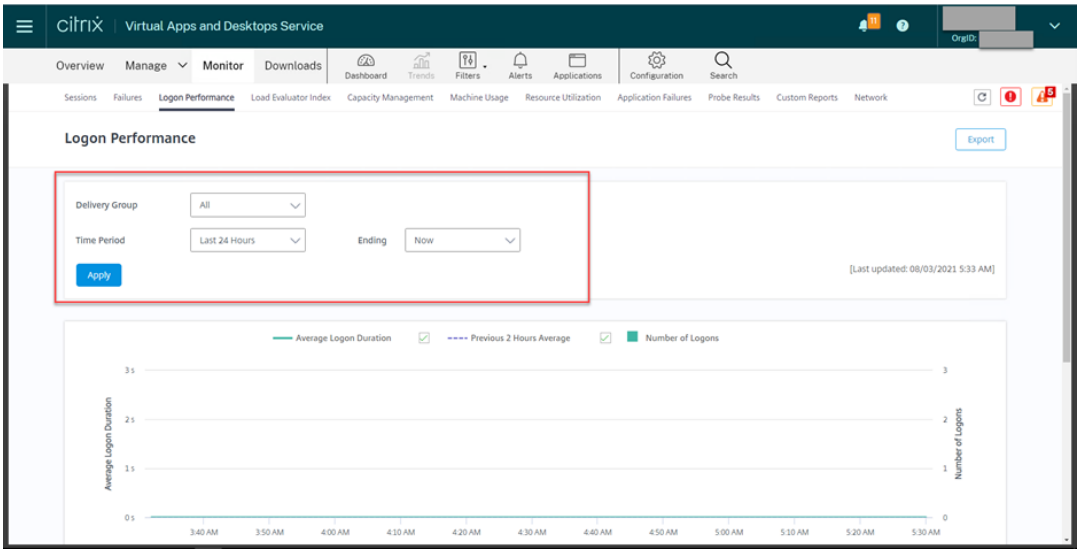
Exemples d'accès aux différentes mesures dans Citrix Director et l'onglet Surveiller

- Durée d'ouverture de session

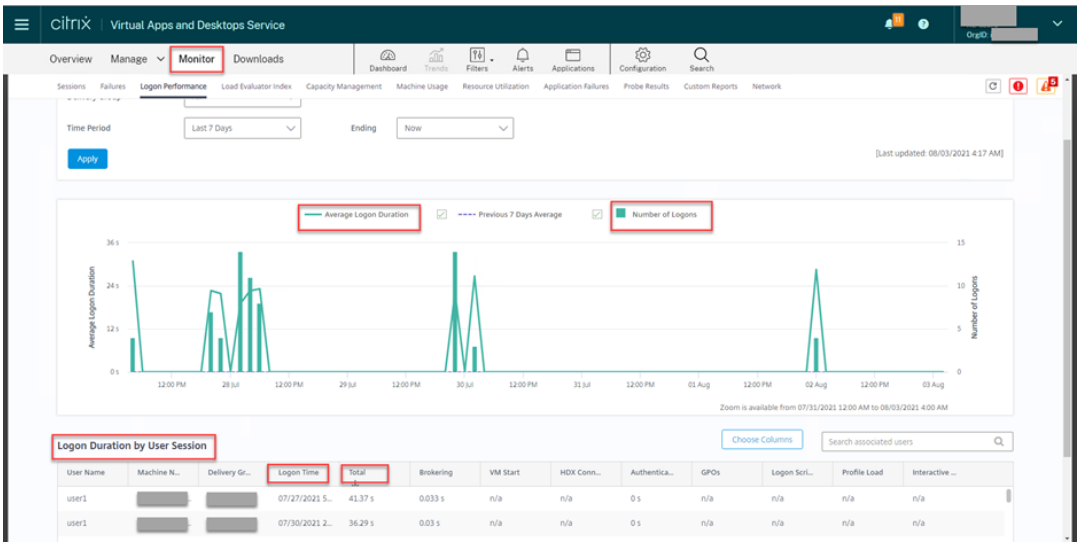
1. Dans l'onglet Surveiller de Citrix DaaS, cliquez sur **Afficher la tendance historique** dans la section **Durée moyenne d'ouverture de session**.



2. Sur la page **Performances d'ouverture de session**, définissez les conditions de filtre.



3. Cliquez sur **Appliquer** pour afficher les mesures de durée d'ouverture de session.

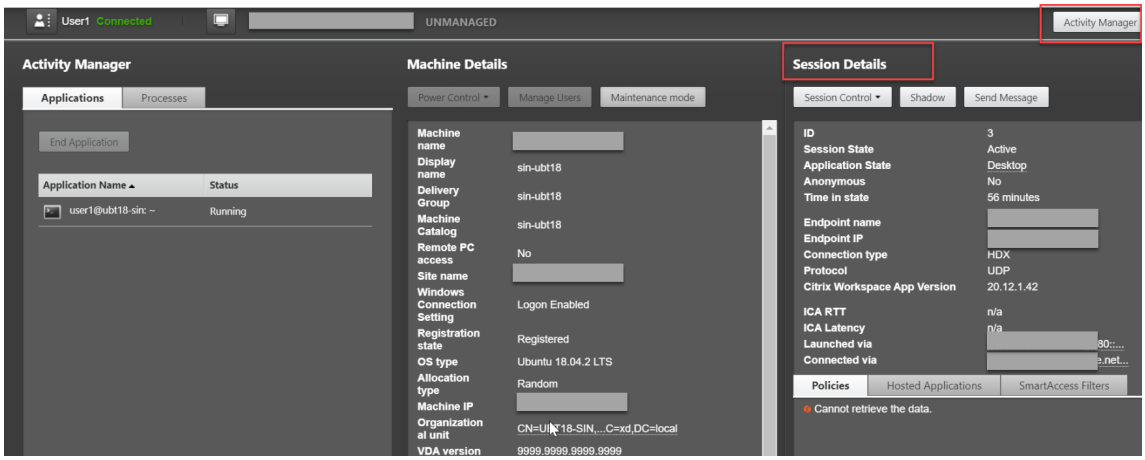


- Nombre de cœurs d'UC, taille de mémoire, capacité du disque dur, et utilisation actuelle et historique de l'UC et de la mémoire d'une VM Linux

  Pour accéder aux mesures d'une machine virtuelle Linux, recherchez la VM dans Citrix Director ou dans l'onglet Monitor et vérifiez le panneau **Détails de la machine**. Par exemple :

- RTT ICA, protocole

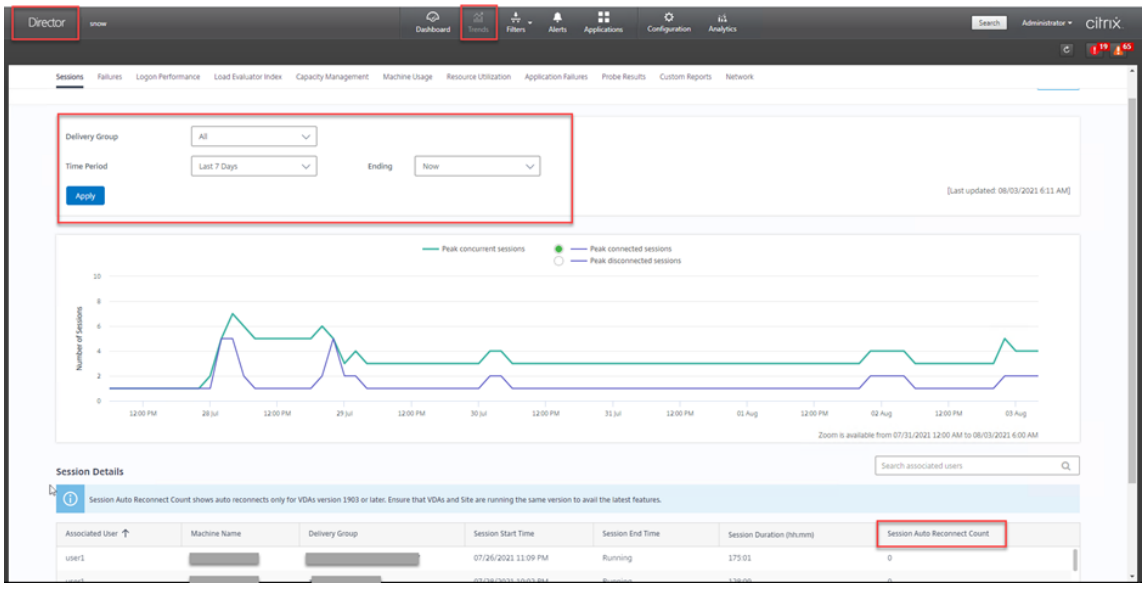
Pour afficher les mesures d'une session Linux, ouvrez la page **Toutes les sessions** en sélectionnant **Filtres > Sessions > Toutes les sessions** ou accédez au panneau **Détails de la session**. Pour accéder au panneau **Détails de la session**, ouvrez la page **Toutes les sessions** et cliquez sur une session cible pour accéder à la vue **Gestionnaire d'activités**. Par exemple :



- Nombre de reconnexions automatiques de sessions

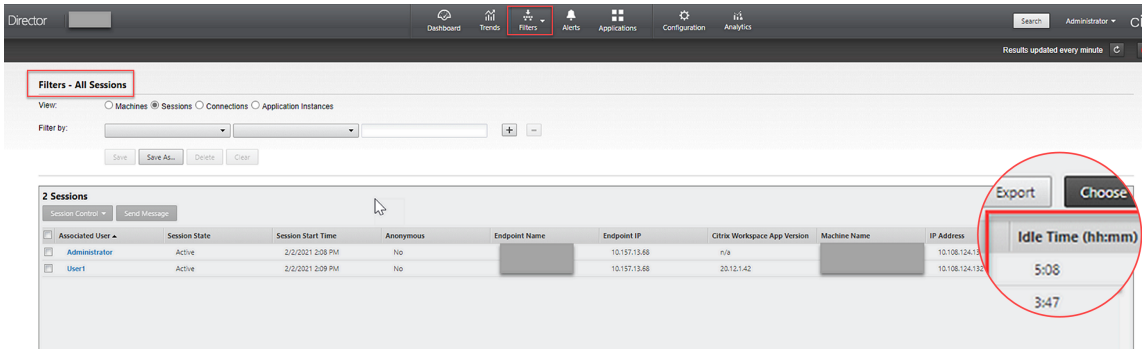
  Pour afficher le nombre de reconnexions automatiques dans une session, accédez à la vue **Tendances**. Définissez les conditions et cliquez sur **Appliquer** pour affiner les résultats de recherche.

  La colonne **Nombre de reconnexions automatiques de sessions** affiche le nombre de reconnexions automatiques dans une session. Par exemple :



- Délai d'inactivité

  Par exemple :



Collecte de journaux

December 16, 2022

Vue d'ensemble

La collecte de journaux est activée par défaut pour le Linux VDA.

Configuration

Le démon `ctxlogd` et l'utilitaire `setlog` sont inclus dans le package du Linux VDA. Par défaut, le démon `ctxlogd` démarre après l'installation et la configuration du Linux VDA.

Le démon ctxlogd

Tous les autres services qui font l'objet d'un suivi dépendent du démon `ctxlogd`. Vous pouvez arrêter le démon `ctxlogd` si vous ne souhaitez pas que le Linux VDA fasse l'objet d'un suivi.

L'utilitaire setlog

La collecte de journaux est configurée à l'aide de l'utilitaire `setlog`, qui se trouve sous **/opt/Citrix/VDA/bin/**. Seul l'utilisateur racine est autorisé à l'exécuter. Vous pouvez utiliser l'interface utilisateur ou exécuter des commandes pour afficher et modifier les configurations. Pour obtenir de l'aide sur l'utilitaire `setlog`, exécutez la commande suivante :

```
1 setlog help
2 <!--NeedCopy-->
```


Valeurs Par défaut, **Log Output Path** est défini sur **/var/log/xdl/hdx.log**, **Max Log Size** est défini sur 200 Mo, et vous pouvez enregistrer jusqu'à deux anciens fichiers journaux sous **Log Output Path**.

Afficher les valeurs `setlog` actuelles :

```
setlog values

log_path (Log Output Path) = /var/log/xdl/hdx.log

log_size (Max Log Size (MiB)) = 200

log_count (Max Old Log Files) = 2
<!--NeedCopy-->
```

Afficher ou définir une valeur `setlog` unique :

```
setlog value <name> [<value>]
<!--NeedCopy-->
```

Par exemple :

```
setlog value log_size 100
<!--NeedCopy-->
```

Niveaux Par défaut, les niveaux de journalisation sont définis sur **warning** (non sensibles à la casse).

Pour afficher les niveaux de journalisation définis pour différents composants, exécutez la commande suivante :

```
setlog levels
<!--NeedCopy-->
```

Pour définir tous les niveaux de journalisation (y compris Disabled, Inherited, Verbose, Information, Warnings, Errors, et Fatal Errors), exécutez la commande suivante :

```
setlog level <class> [<level>]
<!--NeedCopy-->
```

Niveau de journalisation	Paramètre de commande (non sensible à la casse)
Désactivé	aucun
Inherited	inherit
Verbose	verbose
Information	info

Niveau de journalisation	Paramètre de commande (non sensible à la casse)
Warnings	warning
Errors	error
Fatal Errors	fatal

La variable **<class>** spécifie un composant de l'agent Linux VDA. Pour couvrir tous les composants, définissez-la sur « all » : Par exemple :

```
setlog level all error
<!--NeedCopy-->
```

Indicateurs Par défaut, les indicateurs sont définis comme suit :

```
setlog flags

DATE = true

TIME = true

NAME = true

PID = true

TID = false

SID = true

UID = false

GID = false

CLASS = false

LEVEL = false

FUNC = true

FILE = false
<!--NeedCopy-->
```

Afficher les indicateurs actuels :

```
setlog flags
<!--NeedCopy-->
```

Afficher ou définir un indicateur de journalisation unique :


```
setlog flag <flag> [<state>]
<!--NeedCopy-->
```

Restaurer paramètres par défaut Rétablir les paramètres par défaut de tous les niveaux, de tous les indicateurs et de toutes les valeurs :

```
setlog default
<!--NeedCopy-->
```

> **Important :**
>
> Le service `ctxlogd` est configuré à l'aide du fichier **/var/xdl/.ctxlog**, que seuls les utilisateurs root peuvent créer. Les autres utilisateurs ne disposent pas d'un accès en écriture à ce fichier. Nous recommandons aux utilisateurs root de ne pas accorder l'accès en écriture à d'autres utilisateurs. Si cette consigne n'est pas respectée, `ctxlogd` peut être configuré de manière arbitraire ou malveillante, ce qui peut affecter les performances des serveurs et par conséquent l'expérience utilisateur.

Résolution des problèmes

Le démon `ctxlogd` échoue et vous ne pouvez pas redémarrer le service `ctxlogd` lorsque le fichier **/var/xdl/.ctxlog** est manquant (s'il a été supprimé accidentellement par exemple).

/var/log/messages :

```
Apr 1 02:28:21 RH72 citrix-ctxlogd[17881]: Failed to open logging
   configuration file.

Apr 1 02:28:21 RH72 systemd: ctxlogd.service: main process exited, code
   =exited, status=1/FAILURE

Apr 1 02:28:21 RH72 systemd: Unit ctxlogd.service entered failed state.

Apr 1 02:28:21 RH72 systemd: ctxlogd.service failed.
<!--NeedCopy-->
```

Pour résoudre ce problème, exécutez `setlog` en tant qu'utilisateur racine pour créer le fichier **/var/xdl/.ctxlog**. Redémarrez le service `ctxlogd` dont dépendent d'autres services.

Observation de session

April 18, 2024

L'observation de sessions permet aux administrateurs de domaine d'afficher les sessions ICA d'utilisateurs dans un intranet. La fonctionnalité utilise noVNC pour se connecter aux sessions ICA.

> **Remarque :**
>
> Pour utiliser cette fonctionnalité, utilisez `Citrix Director` 7.16 ou une version ultérieure.

Installation et configuration

Dépendances

Deux nouvelles dépendances, `python-websockify` et `x11vnc`, sont nécessaires pour l'observation de session. Installez manuellement `python-websockify` et `x11vnc` après avoir installé le Linux VDA.

Pour RHEL 7.x et Amazon Linux2 :

Exécutez les commandes suivantes pour installer `python-websockify` et `x11vnc` (`x11vnc` version 0.9.13 ou ultérieure).

```
sudo pip3 install websockify
sudo yum install x11vnc
<!--NeedCopy-->
```

Pour résoudre `python-websockify` et `x11vnc`, activez les packages supplémentaires pour Enterprise Linux (EPEL) et les référentiels RPM facultatifs sur RHEL 7.x :

- EPEL

  Le référentiel EPEL est requis pour `x11vnc`. Pour activer le référentiel EPEL, exécutez la commande suivante :

  ```
  yum install https://dl.fedoraproject.org/pub/epel/epel-release-
     latest-7.noarch.rpm
  <!--NeedCopy-->
  ```

- RPM facultatifs

  Exécutez la commande suivante pour activer le référentiel de `RPMs` facultatifs pour l'installation de certains packages de dépendances de `x11vnc` :

  ```
  subscription-manager repos --enable rhel-7-server-optional-rpms
     --enable rhel-7-server-extras-rpms
  <!--NeedCopy-->
  ```

Pour RHEL 8.x et Rocky Linux 8 :

Exécutez les commandes suivantes pour installer `python-websockify` et `x11vnc` (`x11vnc` version 0.9.13 ou ultérieure).


```
sudo pip3 install websockify
sudo yum install x11vnc
<!--NeedCopy-->
```

Pour résoudre `x11vnc`, activez les référentiels EPEL et CodeReady Linux Builder :

```
dnf install -y --nogpgcheck https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm

subscription-manager repos --enable "codeready-builder  -for-rhel-8-x86_64-rpms"
<!--NeedCopy-->
```

Pour Ubuntu :

Exécutez les commandes suivantes pour installer `python-websockify` et `x11vnc` (`x11vnc` version 0.9.13 ou ultérieure).

```
sudo pip3 install websockify
sudo apt-get install x11vnc
<!--NeedCopy-->
```

Pour SUSE :

Exécutez les commandes suivantes pour installer `python-websockify` et `x11vnc` (`x11vnc` version 0.9.13 ou ultérieure).

```
sudo pip3 install websockify
sudo zypper install x11vnc
<!--NeedCopy-->
```

Pour Debian :

Exécutez les commandes suivantes pour installer `python-websockify` et `x11vnc` (`x11vnc` version 0.9.13 ou ultérieure).

```
sudo pip3 install websockify
sudo apt-get install x11vnc
<!--NeedCopy-->
```

Port

La fonctionnalité d'observation de session sélectionne automatiquement les ports disponibles entre 6001 et 6099 pour établir des connexions entre le Linux VDA et `Citrix Director`. Par conséquent, le nombre de sessions ICA que vous pouvez observer simultanément est limité à 99. Assurez-vous que suffisamment de ports sont disponibles pour répondre à vos besoins, en particulier pour l'observation multi-sessions.

Registre

Le tableau suivant répertorie les registres associés :

Registre	Description	Valeur par défaut
EnableSessionShadowing	Active ou désactive la fonctionnalité d'observation de session	1 (activé)
ShadowingUseSSL	Détermine si vous souhaitez crypter la connexion entre le Linux VDA et Citrix Director	0 (désactivé)

Exécutez la commande `ctxreg` sur le Linux VDA pour modifier les valeurs de Registre. Par exemple, pour désactiver l'observation de session, exécutez la commande suivante :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
     VirtualDesktopAgent" -v "EnableSessionShadowing" -d 0x00000000
```

SSL

La connexion noVNC entre le Linux VDA et Citrix Director utilise le protocole WebSocket. Pour l'observation de session, le choix entre `ws://` ou `wss://` dépend du registre « ShadowingUseSSL » mentionné précédemment. Par défaut, `ws://` est choisi. Toutefois, pour des raisons de sécurité, nous vous recommandons d'utiliser `wss://` et d'installer des certificats sur chaque client Citrix Director et sur chaque serveur Linux VDA. Citrix décline toute responsabilité en matière de sécurité en ce qui concerne l'observation de session de Linux VDA avec l'utilisation de `ws://`.

Obtenir des certificats SSL serveur et racine Les certificats doivent être signés par une autorité de certification (AC).

Un certificat de serveur distinct (y compris la clé) est requis pour chaque serveur Linux VDA sur lequel vous souhaitez configurer SSL. Un certificat de serveur identifie une machine. Vous devez donc connaître le nom de domaine complet (FQDN) de chaque serveur. Vous pouvez utiliser un certificat générique pour la totalité du domaine. Dans ce cas, vous devez connaître au moins le nom de domaine.

Un certificat racine est également requis pour chaque client Citrix Director qui communique avec le Linux VDA. Les autorités de certification émettant des certificats de serveur émettent aussi les certificats racines.

Vous pouvez installer des certificats de serveur et de client à partir des autorités de certification suivantes :

- Une autorité de certification fournie avec votre système d'exploitation
- Une autorité de certification d'entreprise (une autorité de certification que votre organisation met à votre disposition)
- Une autorité de certification non fournie avec votre système d'exploitation

Consultez l'équipe des experts en sécurité de votre organisation afin de trouver parmi les méthodes celle requise pour l'obtention des certificats.

Important :

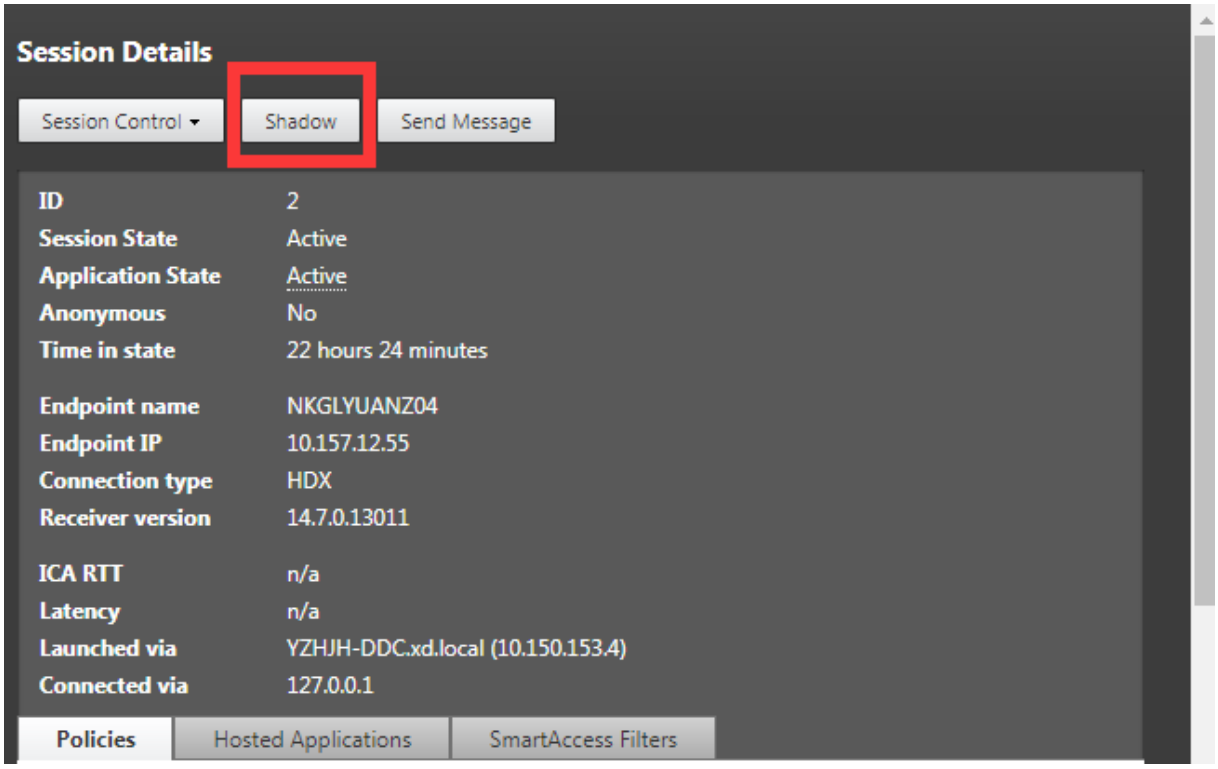
- Le nom commun d'un certificat de serveur doit être le nom de domaine complet exact du Linux VDA ou, au moins, les caractères générique + domaine corrects. Par exemple, vda1.basedomain.com ou * .basedomain.com.
- Les algorithmes de hachage, y compris SHA1 et MD5, sont trop faibles pour les signatures dans les certificats numériques pour certains navigateurs. SHA-256 est donc spécifié comme standard minimum.

Installer un certificat racine sur chaque client Citrix Director L'observation de session utilise le même magasin de certificats qu'IIS (reposant sur le registre). Par conséquent, vous pouvez installer les certificats à l'aide d'IIS ou du composant logiciel enfichable MMC (Microsoft Management Console). Après avoir reçu un certificat d'une autorité de certification, vous pouvez redémarrer l'assistant Certificat de serveur Web d'IIS. L'assistant installe alors le certificat. Vous pouvez également afficher et importer des certificats sur l'ordinateur en utilisant la console MMC et ajouter le certificat en tant que composant logiciel enfichable autonome. Internet Explorer et Google Chrome importent les certificats installés sur votre système d'exploitation par défaut. Pour Mozilla Firefox, vous devez importer vos certificats SSL racine dans l'onglet **Autorités** du gestionnaire de certificats.

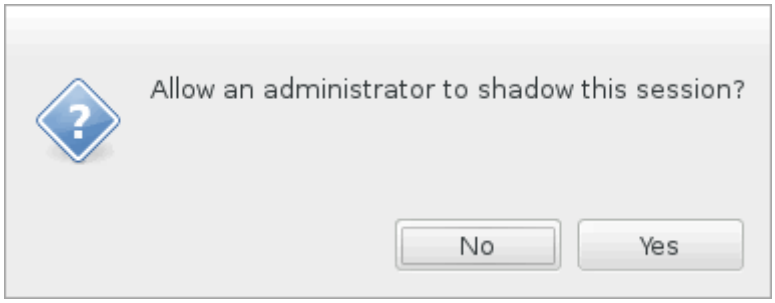
Installer un certificat de serveur et sa clé sur chaque serveur Linux VDA Appelez les certificats de serveur « shadowingcert.* » et le fichier de clé « shadowingkey.* » (* peut indiquer le format, par exemple, shadowingcert.pem et shadowingkey.key). Placez les certificats de serveur et les fichiers de clés sous le chemin d'accès **/etc/xdl/shadowingssl** et protégez-les correctement avec des autorisations restreintes. Si le nom ou le chemin est incorrect, le Linux VDA est incapable de trouver un certificat ou un fichier de clé spécifique et, par conséquent, cela entraîne une défaillance de la connexion avec `Citrix Director`.

Utilisation

Dans `Citrix Director`, recherchez la session cible et cliquez sur **Observer** dans la vue **Détails de la session** pour envoyer une demande d'observation à l'agent Linux VDA.



Une fois que la connexion s'initialise, une confirmation s'affiche sur le client de session ICA (pas le client `Citrix Director`) pour demander l'autorisation d'observer la session.



Si l'utilisateur clique sur **Oui**, une fenêtre s'affiche du côté `Citrix Director`, indiquant que la session ICA est en cours d'observation.

Pour de plus amples informations sur l'utilisation, veuillez consulter la documentation de Citrix Director.

Limitations

- L'observation de session est conçue pour une utilisation dans un intranet uniquement. Elle ne fonctionne pas pour les réseaux externes même en se connectant via Citrix Gateway. Citrix décline toute responsabilité en ce qui concerne l'observation de session de Linux VDA dans un réseau externe.
- Lorsque l'observation de session est activée, un administrateur de domaine peut uniquement afficher les sessions ICA, et n'a pas l'autorisation d'écrire dessus ou de le contrôler.
- Une fois qu'un administrateur a cliqué sur **Observer** depuis `Citrix Director`, une confirmation s'affiche pour demander l'autorisation à l'utilisateur d'observer la session. Une session peut être observée uniquement lorsque l'utilisateur de la session en donne l'autorisation.
- La confirmation mentionnée précédemment a un délai d'expiration, qui est de 20 secondes. Une demande d'observation échoue lorsque ce délai est écoulé.
- Une session peut être observée par un seul administrateur. Par exemple, si l'administrateur B envoie une demande d'observation pour une session que l'administrateur A est en train d'observer, la confirmation d'obtention de l'autorisation de l'utilisateur réapparaît sur la machine utilisateur. Si l'utilisateur accepte, la connexion d'observation pour l'administrateur A s'arrête et une nouvelle connexion d'observation est créée pour l'administrateur B. Si un administrateur envoie une autre demande d'observation pour la même session, une nouvelle connexion d'observation peut également être créée.
- Pour utiliser l'observation de session, installez `Citrix Director` 7.16 ou version ultérieure.
- Un client `Citrix Director` utilise un nom de domaine complet plutôt qu'une adresse IP pour se connecter au serveur Linux VDA cible. Par conséquent, le client `Citrix Director` doit pouvoir résoudre le nom de domaine complet du serveur Linux VDA.

Dépannage

Si l'observation de session échoue, effectuez le débogage à la fois sur le client `Citrix Director` et sur le Linux VDA.

Sur le client Citrix Director

À l'aide des outils de développement du navigateur, vérifiez les journaux de sortie dans l'onglet **Console**. Ou vérifiez la réponse de l'API ShadowLinuxSession dans l'onglet **Réseau**. Si la confirmation de l'obtention de l'autorisation de l'utilisateur s'affiche mais que la connexion ne parvient pas à être établie, envoyez une commande ping manuelle au nom de domaine complet du VDA pour vérifier que `Citrix Director` peut résoudre le nom de domaine complet. En cas de problème avec la connexion `wss://`, vérifiez vos certificats.

Sur le Linux VDA

Vérifiez que la confirmation d'obtention de l'autorisation de l'utilisateur s'affiche en réponse à une requête d'observation. Si ce n'est pas le cas, vérifiez les fichiers vda.log et hdx.log à la recherche d'indices. Pour obtenir le fichier vda.log, procédez comme suit :

1. Recherchez le fichier /etc/xdl/ctx-vda.conf. Supprimez les marques de commentaire sur la ligne suivante pour activer la configuration vda.log :

   ```
   Log4jConfig="/etc/xdl/log4j.xml"
   ```

2. Ouvrez le fichier /etc/xdl/log4j.xml, localisez la partie com.citrix.dmc et remplacez « info » par « trace » comme suit :

   ```
   <!-- Broker Agent Plugin - Director VDA plugin Logger -->

    <logger name="com.citrix.dmc">

      <level value="trace"/>

    </logger>
   <!--NeedCopy-->
   ```

3. Exécutez la commande `service ctxvda restart` pour redémarrer le service `ctxvda`.

En cas d'erreur lors de l'établissement de la connexion, procédez comme suit :

1. Recherchez toute limitation de pare-feu qui empêche l'observation de session d'ouvrir le port.
2. Vérifiez que les certificats et les fichiers de clés sont correctement nommés et placés sous le bon chemin pour un scénario SSL.
3. Vérifiez qu'il reste suffisamment de ports entre 6001 et 6099 pour les nouvelles demandes d'observation.

Démon du service de surveillance

December 16, 2022

Le démon du service de surveillance surveille les services clés en effectuant des analyses périodiques. Lors de la détection des exceptions, le démon redémarre ou arrête les processus de service et nettoie les données résiduelles du processus pour libérer les ressources. Les exceptions détectées sont enregistrées dans le fichier **/var/log/xdl/ms.log**.

Configuration

Le démon du service de surveillance démarre automatiquement lorsque vous démarrez le VDA.

Vous pouvez configurer la fonctionnalité via les fichiers **scanningpolicy.conf**, **rulesets.conf** et **whitelist.conf** sous **/opt/Citrix/VDA/sbin** avec des privilèges d'administrateur.

Pour que les modifications apportées aux fichiers **scanningpolicy.conf**, **rulesets.conf**et **whitelist.conf** prennent effet, exécutez la commande suivante pour redémarrer le démon du service de surveillance.

```
service ctxmonitorservice restart
<!--NeedCopy-->
```

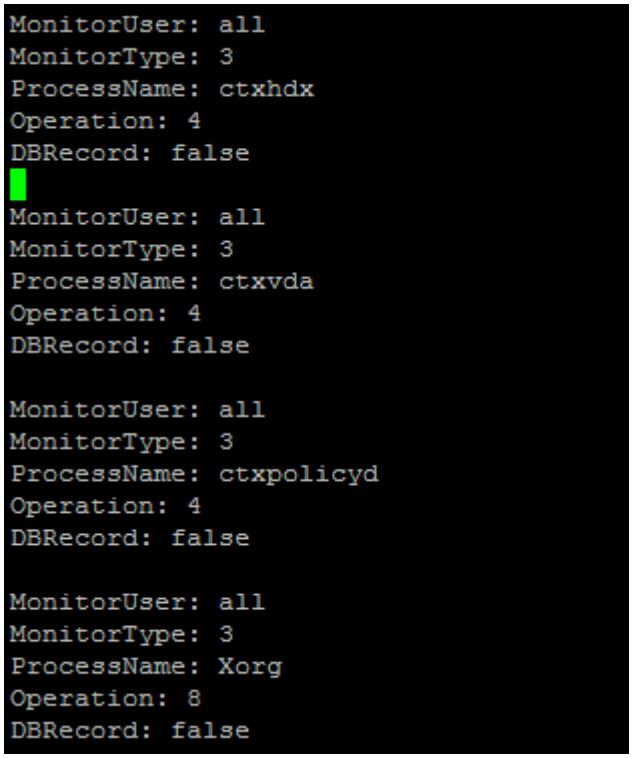
- **scanningpolicy.conf**

  Ce fichier de configuration active ou désactive le démon du service de surveillance. Il définit l'intervalle de détection du service et spécifie si les exceptions détectées doivent être réparées.

  - MonitorEnable : true/false (valeur par défaut : true)
  - DetectTime : 20 (unité : secondes ; valeur par défaut : 20 ; valeur minimum : 5)
  - AutoRepair : true/false (valeur par défaut : true)
  - MultBalance : false
  - ReportAlarm : false

- **rulesets.conf**

  Ce fichier de configuration spécifie les services cibles à surveiller. Il existe quatre services surveillés par défaut, comme indiqué dans la capture d'écran suivante.



Pour configurer chaque service à surveiller, définissez les champs suivants.

- **MonitorUser** : all
- **MonitorType** : 3
- **ProcessName** : <> (le nom du processus ne peut pas être vide et doit avoir une correspondance exacte)
- **Operation** : 1/2/4/8 (1 = arrêter le service lorsque des exceptions sont détectées ; 2 = supprimer le service lorsque des exceptions sont détectées ; 4 = redémarrer le service ; 8 = effacer les valeurs résiduelles du processus Xorg)
- **DBRecord** : false

- **whitelist.conf**

  Les services cibles spécifiés dans le fichier **rulesets.conf** doivent également être configurés dans le fichier **whitelist.conf**. La configuration de la liste blanche est un filtre secondaire pour la sécurité.

  Pour configurer la liste blanche, incluez uniquement les noms de processus (qui doivent avoir une correspondance exacte) dans le fichier **whitelist.conf**. Pour obtenir un exemple, consultez la capture d'écran suivante.


```
ctxcdmd
ctxcdmmount
ctxcdmstat
ctxceip
ctxclipboard
ctxconnect
ctxcredentialctl
ctxctl
ctxcupsd
ctxdisconnect
ctxeuem
ctxfiletransfer
ctxgfx
ctxhdx
ctxism
ctxlogd
ctxlogin
ctxmonitorservice
ctxmrvc
ctxpolicyd
ctxscardsd
ctxvhcid
ctxvda
Xorg
```

> **Remarque :**
>
> Avant d'arrêter les services `ctxvda`, `ctxhdx` et `ctxpolicyd`, exécutez la commande `service ctxmonitorservice stop` pour arrêter le démon du service de surveillance. Sinon, le démon du service de surveillance redémarre les services que vous avez arrêtés.

Outils et utilitaires

May 3, 2023

Utilitaire permettant d'interroger les données de session

Nous fournissons un utilitaire (`ctxsdcutil`) permettant d'interroger les données de session sur chaque Linux VDA. Pour interroger les données suivantes de toutes les sessions ou d'une session spécifique hébergée sur un VDA, exécutez la commande `/opt/Citrix/VDA/bin/ctxsdcutil -q <all | SessionID> [-c]`. L'argument `[-c]` signifie que les données sont interrogées toutes les secondes.

- **Bande passante de session - entrée**

- **Bande passante de session - sortie**
- **Vitesse de ligne de session en sortie**
- **Latence - dernière enregistrée**
- **Durée des boucles**
- **Bande passante de sortie de ThinWire**
- **Bande passante de sortie de l'audio**
- **Bande passante de sortie de l'imprimante**
- **Bande passante d'entrée du lecteur**
- **Bande passante de sortie du lecteur**

Le script Bash xdlcollect

Le script Bash `xdlcollect` utilisé pour collecter les journaux est intégré dans le logiciel Linux VDA et se trouve dans **/opt/Citrix/VDA/bin**. Après avoir installé Linux VDA, vous pouvez exécuter la commande `bash /opt/Citrix/VDA/bin/xdlcollect.sh` pour collecter les journaux. Une fois la collecte des journaux terminée, un fichier journal compressé est généré dans le même dossier que le script. Le script Bash `xdlcollect` peut vous demander s'il faut charger le fichier journal compressé sur Citrix Insight Services (CIS). Si vous acceptez, `xdlcollect` renvoie upload_ID une fois le chargement terminé. Le téléchargement ne supprime pas le fichier journal compressé de votre machine locale. Les autres utilisateurs peuvent utiliser upload_ID pour accéder au fichier journal dans CIS.

XDPing

L'outil **XDPing** pour Linux est une application de ligne de commande. Il automatise le processus de vérification des problèmes de configuration courants dans un environnement Linux VDA.

L'outil **XDPing** Linux effectue plus de 150 tests individuels sur le système, qui sont généralement classés comme suit :

- Vérifier si la configuration système du VDA Linux est respectée
- Identifier et afficher les informations de la machine, y compris les distributions Linux
- Vérifier la compatibilité du noyau Linux
- Vérifier les problèmes de distribution Linux connus qui peuvent avoir un impact sur le fonctionnement du VDA Linux
- Vérifier le mode de sécurité Security-Enhanced Linux (SELinux) et sa compatibilité
- Identifier les interfaces réseau et vérifier les paramètres réseau

- Vérifier le partitionnement du stockage et l'espace disque disponible
- Vérifier la configuration du nom d'hôte et du nom de domaine de la machine
- Vérifier la configuration DNS et effectuer des tests de recherche
- Identifier les hyperviseurs sous-jacents et vérifier la configuration de la machine virtuelle. Prise en charge de :
  - Citrix Hypervisor
  - Microsoft HyperV
  - VMware vSphere
- Vérifier les paramètres d'heure et vérifier si la synchronisation de l'heure réseau est opérationnelle
- Vérifier si le service PostgreSQL est correctement configuré et opérationnel
- Vérifier si le pare-feu est activé et si les ports requis sont ouverts
- Vérifier la configuration de Kerberos et effectuer des tests d'authentification
- Vérifier l'environnement de recherche LDAP pour Group Policy Engine Service
- Vérifier si l'intégration Active Directory est correctement configurée et que la machine actuelle est jointe au domaine. Prise en charge de :
  - Samba Winbind
  - Dell Quest Authentication Services
  - Centrify DirectControl
  - SSSD
- Vérifier l'intégrité de l'objet ordinateur Linux dans Active Directory
- Vérifier la configuration du module d'authentification enfichable (PAM)
- Vérifier le modèle de l'image mémoire
- Vérifier si les packages requis par le VDA Linux sont installés
- Identifier le package du VDA Linux et vérifier l'intégrité de l'installation
- Vérifier l'intégrité de la base de données de registre PostgreSQL
- Vérifier si les services du VDA Linux sont correctement configurés et opérationnels
- Vérifier l'intégrité de la configuration VDA et HDX
- Analyser la configuration de chaque Delivery Controller pour vérifier que le Broker Service est accessible, opérationnel et réactif
- Vérifier si la machine est enregistrée auprès de la batterie du Delivery Controller
- Vérifier l'état de chaque session HDX active ou déconnectée
- Analyser les fichiers journaux pour les erreurs et avertissements liés au VDA Linux
- Vérifier si la version de Xorg est adaptée

Utiliser l'outil XDPing Linux

> **Remarque :**
>
> L'exécution de ctxsetup.sh n'installe pas **XDPing**. Vous pouvez exécuter `sudo /opt/Citrix/VDA/bin/xdping` pour installer **XDPing**.
> Cette commande crée également un environnement virtuel Python3 requis pour **XDPing**. Si cette commande ne parvient pas à créer un environnement virtuel Python3, créez-le manuellement en suivant les instructions de la section Créer un environnement virtuel Python3.
>
> Pour résoudre les erreurs de connexion SSL que vous pouvez rencontrer lors de l'utilisation de l'outil pip, envisagez d'ajouter les hôtes approuvés suivants au fichier /etc/pip.conf :
> ```
> [global]
> trusted-host =
> pypi.org
> files.pythonhosted.org
> ```

L'outil **XDPin**g est fourni avec l'exécutable unique nommé `xdping` qui est exécuté à partir de l'interface de commande.

Pour afficher les options de ligne de commande, utilisez l'option `-h` :

```
1 sudo /opt/Citrix/VDA/bin/xdping -h
2 <!--NeedCopy-->
```

Pour exécuter la suite complète de tests, exécutez `xdping` sans aucune option de ligne de commande :

```
1 sudo /opt/Citrix/VDA/bin/xdping
2 <!--NeedCopy-->
```

Pour vérifier l'environnement avant d'installer le package du VDA Linux, exécutez les tests `preflight` :

```
1 sudo /opt/Citrix/VDA/bin/xdping --preflight
2 <!--NeedCopy-->
```

Pour exécuter uniquement des catégories de test spécifiques, par exemple les tests liés à l'heure et à Kerberos, utilisez l'option `-T` :

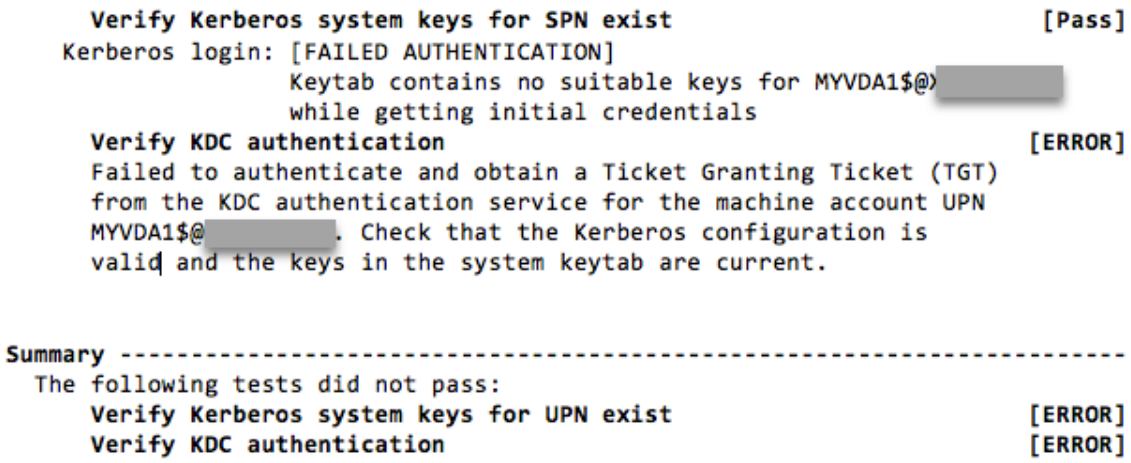
```
1 sudo /opt/Citrix/VDA/bin/xdping -T time,kerberos
2 <!--NeedCopy-->
```

Pour analyser un contrôleur XenDesktop spécifique :

```
1 sudo /opt/Citrix/VDA/bin/xdping -d myddc.domain.net
2 <!--NeedCopy-->
```

Exemple de sortie Voici un exemple de sortie lors de l'exécution du test Kerberos :


```
sudo xdping -T kerberos

Root User ------------------------------------------------------------------
    User:         root
    EUID:         0
      Verify user is root                                              [Pass]

Kerberos -------------------------------------------------------------------
    Kerberos version: 5
      Verify Kerberos available                                        [Pass]
      Verify Kerberos version 5                                        [Pass]
    KRB5CCNAME:    [Not set]
                   Distro default FILE:/tmp/krb5cc_%{uid}
    KRB5CCNAME type: [Supported]
    KRB5CCNAME format: [Default]
      Verify KRB5CCNAME cache type                                     [Pass]
      Verify KRB5CCNAME format                                         [Pass]
    Configuration file: /etc/krb5.conf [Exists]


  Verify Kerberos configuration file found                             [Pass]
Keytab file:  /etc/krb5.keytab [Exists]
Default realm: XD2.LOCAL
Default realm KDCs: [NONE SPECIFIED]
Default realm domains: [NONE SPECIFIED]
DNS lookup realm: [Enabled]
DNS lookup KDC: [Enabled]
Weak crypto:  [Disabled]
Clock skew limit:  300 s
  Verify system keytab file exists                                     [Pass]
  Verify default realm set                                             [Pass]
  Verify default realm in upper-case                                   [Pass]
  Verify default realm not EXAMPLE.COM                                 [Pass]
  Verify default realm domain mappings                                 [Pass]
  Verify default realm master KDC configured                           [Pass]
  Verify Kerberos weak crypto disabled                                 [Pass]
  Verify Kerberos clock skew setting                                   [Pass]
Default ccache: [Not set]
                Distro default FILE:/tmp/krb5cc_%{uid}
Default ccache type: [Supported]
Default ccache format: [Default]
  Verify default credential cache cache type                           [Pass]
  Verify default credential cache format                               [Pass]
UPN system key [MYVDA1$@          ]: [MISSING]
SPN system key [host/r                l]: [Exists]
  Verify Kerberos system keys for UPN exist                          [ERROR]
  No system keys were found for the user principal name (UPN) of
  the machine account. For the Linux VDA to mutually authenticate
  with the Delivery Controller, the system keytab file must
  contain keys for both the UPN and host-based SPN of the machine
  account.
```

Autres

December 16, 2022

Cette section contient les rubriques suivantes :

- Prise en charge de l'application Citrix Workspace pour HTML5
- Créer un environnement virtuel Python3
- Intégrer NIS avec Active Directory
- IPv6
- LDAPS
- **Xauthority**

Prise en charge de l'application Citrix Workspace pour HTML5

December 16, 2022

Vous pouvez utiliser l'application Citrix Workspace pour HTML5 pour accéder directement aux applications et aux bureaux virtuels Linux sans connecter votre client à Citrix Gateway. Pour plus d'informations sur l'application Citrix Workspace pour HTML5, consultez la documentation Citrix.

Activer cette fonctionnalité

Cette fonction est désactivée par défaut. Pour l'activer, procédez comme suit :

1. Dans Citrix StoreFront, activez l'application Citrix Workspace pour HTML5.

   Pour obtenir la procédure détaillée, reportez-vous à l'étape 1 de l'article CTX208163 du centre de connaissances.

2. Activez les connexions WebSocket.

   a) Dans Citrix Studio, définissez la stratégie **Connexions WebSockets** sur **Autorisé**.

   Vous pouvez également définir les autres stratégies WebSocket. Pour obtenir la liste complète des stratégies WebSocket, consultez Paramètres de stratégie WebSockets.

   b) Sur le VDA, redémarrez le service `ctxvda` et le service `ctxhdx`, dans cet ordre, pour que votre paramètre prenne effet.

   c) Sur le VDA, exécutez la commande suivante pour vérifier si l'écouteur WebSocket est en cours d'exécution.

   ```
   netstat -an | grep 8008
   ```

   Lorsque l'écouteur WebSocket est en cours d'exécution, le résultat de la commande est similaire au suivant :

   ```
   tcp 0 0 :::8008 :::* LISTEN
   ```

Remarque : vous pouvez également activer le chiffrement TLS pour sécuriser les connexions WebSocket. Pour de plus amples informations sur l'activation du cryptage TLS, consultez la section Sécuriser les sessions utilisateur en utilisant TLS.

Créer un environnement virtuel Python3

November 24, 2023

Si vous vous connectez au réseau, vous pouvez exécuter `sudo /opt/Citrix/VDA/bin/xdping` ou `/opt/Citrix/VDA/sbin/enable_ldaps.sh` pour créer un environnement virtuel Python3. Toutefois, si les commandes ne parviennent pas à créer un environnement virtuel Python3, vous pouvez le créer manuellement même sans connexion réseau. Cet article détaille les conditions préalables et les étapes à suivre pour créer un environnement virtuel Python3 sans connexion réseau.

Conditions préalables

- Vous devez disposer de privilèges d'administrateur pour accéder au répertoire /opt/Citrix/VDA/sbin/ctxpython3.
- Les fichiers wheel des packages Python3 sont installés. Vous pouvez télécharger les fichiers wheel à partir de https://pypi.org/.

Créer un environnement virtuel Python3

Procédez comme suit pour créer un environnement virtuel Python3 :

1. Installez les dépendances Python3.

   Pour Amazon Linux 2 :

   ```
   yum -y install python3 python3-devel krb5-devel gcc
   <!--NeedCopy-->
   ```

   Pour RHEL et Rocky Linux :

   ```
   yum -y install python36-devel krb5-devel gcc
   <!--NeedCopy-->
   ```

   > **Remarque :**
   >
   > Vous devrez peut-être activer un référentiel spécifique pour installer certaines dépendances. Pour RHEL 7, exécutez la commande `subscription-manager repos --enable rhel-7-server-optional-rpms`. Pour RHEL 8, exécutez la commande `subscription-manager repos --enable=rhel-8-for-x86_64-appstream-rpms`.

   Pour Debian et Ubuntu :

   ```
   apt-get -y install python3-dev python3-pip python3-venv libkrb5-
      dev
   <!--NeedCopy-->
   ```

   Pour SUSE :

   ```
   zypper -n install lsb-release python3-devel python3-setuptools
      krb5-devel gcc libffi-devel libopenssl-devel
   <!--NeedCopy-->
   ```

2. Créez un environnement virtuel Python3.

> **Remarque :**
>
> pour résoudre les erreurs de connexion SSL que vous pouvez rencontrer lors de l'utilisation de l'outil pip, envisagez d'ajouter les hôtes approuvés suivants au fichier /etc/pip.conf :
> [global]
> trusted-host =
> pypi.org
> files.pythonhosted.org

Pour Amazon Linux 2, Debian, RHEL, Rocky Linux, Ubuntu :

```
sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
<!--NeedCopy-->
```

Pour SUSE :

```
export PATH=$PATH:/usr/lib/mit/bin:/usr/lib/mit/sbin

sudo mkdir -p /usr/lib/mit/include/gssapi/

sudo ln -s /usr/include/gssapi/gssapi_ext.h/usr/lib/mit/include/
   gssapi/gssapi_ext.h

sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
<!--NeedCopy-->
```

3. Installez les dépendances LDAPS.

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install --
   upgrade pip==21.3.1

sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
   cffi==1.15.0 cryptography==36.0.2 decorator==5.1.1 gssapi
   ==1.7.3 ldap3==2.9.1 pyasn1==0.4.8 pycparser==2.21 six==1.16.0
<!--NeedCopy-->
```

4. Installez les dépendances **XDPing**.

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install --
   upgrade pip==21.3.1

sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
   asn1crypto==1.5.1 cffi==1.15.0 cryptography==36.0.2 decorator
   ==5.1.1 gssapi==1.7.3 ldap3==2.9.1 netifaces==0.11.0 packaging
   ==21.3 pg8000==1.26.0 psutil==5.9.0 pyasn1==0.4.8 pycparser
   ==2.21 pyparsing==3.0.8 scramp==1.4.1 six==1.16.0 termcolor
   ==1.1.0

sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install /
   opt/Citrix/VDA/sbin/ctxpython3/packages/xdping-*.whl
<!--NeedCopy-->
```


Intégrer NIS avec Active Directory

December 16, 2022

Cet article décrit comment intégrer NIS avec Windows Active Directory (AD) sur le Linux VDA à l'aide de SSSD. Le Linux VDA est considéré comme un composant de Citrix Virtual Apps and Desktops. Par conséquent, il s'intègre sans problème à l'environnement Windows Active Directory.

L'utilisation de NIS au lieu d'AD comme fournisseur d'UID et de GID requiert que les informations de compte (nom d'utilisateur et mot de passe) soient les mêmes dans AD et NIS.

> **Remarque :**
>
> L'authentification est toujours effectuée par le serveur Active Directory. NIS+ n'est pas pris en charge. Si vous utilisez NIS comme fournisseur d'UID et de GID, les attributs POSIX du serveur Windows ne sont plus utilisés.
>
> **Conseil :**
>
> Cette méthode de déploiement de Linux VDA est obsolète et n'est utilisée que pour des scénarios particuliers. Pour une distribution RHEL/CentOS, suivez les instructions indiquées dans la section Installer Linux Virtual Delivery Agent pour RHEL/CentOS. Pour une distribution Ubuntu, suivez les instructions indiquées dans la section Installer Linux Virtual Delivery Agent pour Ubuntu.

Présentation de SSSD

SSSD est un démon système. Sa fonction principale consiste à offrir un accès pour l'identification et l'authentification de ressources distantes par le biais d'une infrastructure commune qui peut fournir une mise en cache et un accès en mode déconnecté au système. Il propose des modules PAM et NSS et prendra en charge à l'avenir les interfaces D-BUS qui permettront d'obtenir davantage d'informations utilisateur. Il offre également une meilleure base de données pour stocker les comptes utilisateur locaux ainsi que les données utilisateur supplémentaires.

Intégrer NIS à Active Directory

Pour intégrer NIS à AD, procédez comme suit :

Étape 1 : Ajouter l'agent Linux VDA en tant que client NIS

Configurez le client NIS :

```
yum -y install ypbind rpcbind oddjob-mkhomedir
<!--NeedCopy-->
```


Définissez le domaine NIS :

```
ypdomainname nis.domain
echo "NISDOMAIN=nis.domain" >> /etc/sysconfig/network
<!--NeedCopy-->
```

Ajoutez l'adresse IP pour le serveur et le client NIS dans **/etc/hosts** :

```
{ NIS server IP address }    server.nis.domain nis.domain
```

Configurez NIS par `authconfig` :

```
sudo authconfig --enablenis --nisdomain=nis.domain --nisserver=server.
   nis.domain --enablemkhomedir --update
<!--NeedCopy-->
```

nis.domain représente le nom de domaine du serveur NIS. **server.nis.domain** représente le nom d'hôte du serveur NIS, qui peut également être l'adresse IP du serveur NIS.

Configurez les services NIS :

```
sudo systemctl start rpcbind ypbind

sudo systemctl enable rpcbind ypbind
<!--NeedCopy-->
```

Assurez-vous que la configuration NIS est correcte :

```
ypwhich
<!--NeedCopy-->
```

Vérifiez que les informations de compte sont disponibles à partir du serveur NIS :

```
getent passwd nisaccount
<!--NeedCopy-->
```

> **Remarque :**
>
> **nisaccount** représente le compte NIS réel sur le serveur NIS. Assurez-vous que l'UID, le GID, le répertoire de base et le shell d'ouverture de session sont correctement configurés.

Étape 2 : Rejoindre le domaine et créer un fichier keytab hôte avec Samba

SSSD ne fournit pas de fonctions de client Active Directory pour rejoindre le domaine et gérer le fichier keytab système. Plusieurs méthodes sont disponibles, y compris :

- `adcli`
- `realmd`
- `Winbind`

- Samba

Les informations contenues dans cette section décrivent l'approche Samba uniquement. Pour realmd, reportez-vous à la documentation RHEL ou CentOS du fournisseur. Ces étapes doivent être suivies avant la configuration de SSSD.

Rejoindre le domaine et créer un fichier keytab hôte avec Samba :

Sur le client Linux avec des fichiers correctement configurés :

- /etc/krb5.conf
- /etc/samba/smb.conf :

Configurez la machine pour l'authentification Kerberos et Samba :

```
1 sudo authconfig --smbsecurity=ads --smbworkgroup=domain --smbrealm=
     REALM --krb5realm=REALM --krb5kdc=fqdn-of-domain-controller --update
2 <!--NeedCopy-->
```

Où **REALM** est le nom du domaine Kerberos en majuscules et **domain** est le nom NetBIOS du domaine.

Si des recherches DNS sur le nom de domaine et de serveur KDC sont requises, ajoutez les options suivantes à la commande précédente :

```
--enablekrb5kdcdns --enablekrb5realmdns
```

Ouvrez **/etc/samba/smb.conf** et ajoutez les entrées suivantes dans la section **[Global]**, mais après la section générée par l'outil **authconfig** :

```
kerberos method = secrets and keytab
winbind offline logon = no
```

Pour rejoindre le domaine Windows, votre contrôleur de domaine doit être accessible et vous devez disposer d'un compte utilisateur Active Directory avec les autorisations nécessaires pour ajouter des ordinateurs au domaine.

```
1 sudo net ads join REALM -U user
2 <!--NeedCopy-->
```

REALM est le nom de domaine Kerberos en majuscules, et **user** est un utilisateur de domaine disposant des autorisations nécessaires pour ajouter les ordinateurs au domaine.

Étape 3 : Configurer SSSD

La configuration de SSSD comprend les étapes suivantes :

- Installez les packages **sssd-ad** et **sssd-proxy** sur la machine cliente Linux.

- Apportez des modifications de configuration à plusieurs fichiers (par exemple, **sssd.conf**).
- Démarrez le service **sssd**.

/etc/sssd/sssd.conf Exemple de configuration **sssd.conf** (des options supplémentaires peuvent être ajoutées si nécessaire) :

```
[sssd]
config_file_version = 2
domains = EXAMPLE
services = nss, pam

[domain/EXAMPLE]
# Uncomment if you need offline logins
# cache_credentials = true
re_expression = (((?P<domain>[^\\]+)\\(?P<name>.+$))|((?P<name>[^@]+)@(?P<domain>.+$))|(^(?P<name>[^@\\]+)$))
id_provider = proxy
proxy_lib_name = nis
auth_provider = ad
access_provider = ad

# Should be specified as the long version of the Active Directory domain.
ad_domain = EXAMPLE.COM

# Kerberos settings
krb5_ccachedir = /tmp
krb5_ccname_template = FILE:%d/krb5cc_%U

# Uncomment if service discovery is not working
# ad_server = server.ad.example.com

# Comment out if the users have the shell and home dir set on the AD side
default_shell = /bin/bash
fallback_homedir = /home/%d/%u

# Uncomment and adjust if the default principal SHORTNAME$@REALM is not available
# ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
<!--NeedCopy-->
```

Remplacez **ad.example.com**, **server.ad.example.com** par les valeurs correspondantes. Pour plus de détails, reportez-vous à la page **sssd-ad**(5) - Linux man.

Définissez les autorisations et les propriétaires de fichier sur **sssd.conf** :

```
chown root:root /etc/sssd/sssd.conf
chmod 0600 /etc/sssd/sssd.conf
restorecon /etc/sssd/sssd.conf
```


Étape 4 : Configurer NSS/PAM

RHEL/CentOS :

Utilisez **authconfig** pour activer SSSD. Installez **oddjob-mkhomedir** pour vous assurer que la création du répertoire de base est compatible avec SELinux :

```
authconfig --enablesssd --enablesssdauth --enablemkhomedir --update

sudo systemctl start sssd

sudo systemctl enable sssd
<!--NeedCopy-->
```

> **Conseil :**
>
> Lors de la configuration des paramètres de Linux VDA, n'oubliez pas qu'il n'y a aucun paramètre spécial pour le client Linux VDA dans SSSD. Pour des solutions supplémentaires dans le script **ctxsetup.sh**, utilisez la valeur par défaut.

Étape 5 : Vérifier la configuration de Kerberos

Pour vous assurer que Kerberos est correctement configuré pour être utilisé avec l'agent Linux VDA, vérifiez que le fichier **keytab** système a été créé et contient des clés valides :

```
sudo klist -ke
<!--NeedCopy-->
```

Cette commande affiche la liste des clés disponibles pour les différentes combinaisons de noms principaux et de suites de chiffrement. Exécutez la commande **kinit** Kerberos pour authentifier la machine auprès du contrôleur de domaine à l'aide de ces clés :

```
sudo kinit  – k MACHINE$@REALM
<!--NeedCopy-->
```

Les noms de machine et de domaine doivent être spécifiés en majuscules. Le signe dollar ($) doit être placé dans une séquence d'échappement avec une barre oblique inverse (\) pour empêcher le remplacement shell. Dans certains environnements, le nom de domaine DNS est différent du nom de domaine Kerberos. Assurez-vous que le nom de domaine est utilisé. Si cette commande réussit, aucun résultat n'est affiché.

Vérifiez que le ticket TGT pour le compte de machine a été mis en cache à l'aide de :

```
sudo klist -ke
<!--NeedCopy-->
```


Étape 6 : Vérifier l'authentification utilisateur

Utilisez la commande **getent** pour vérifier que le format d'ouverture de session est pris en charge et que NSS fonctionne :

```
sudo getent passwd DOMAIN\username
<!--NeedCopy-->
```

Le paramètre **DOMAIN** indique la version courte du nom de domaine. Si un autre format d'ouverture de session est nécessaire, vérifiez en utilisant d'abord la commande **getent**.

Les formats d'ouverture de session pris en charge sont :

- Nom d'ouverture de session de niveau inférieur : `DOMAIN\username`
- Nom d'utilisateur principal (UPN) : `username@domain.com`
- Format du suffixe NetBIOS : `username@DOMAIN`

Pour vérifier que le module PAM SSSD est correctement configuré, ouvrez une session à l'aide d'un compte d'utilisateur de domaine sur le Linux VDA. Le compte d'utilisateur de domaine n'a pas été utilisé auparavant.

```
sudo ssh localhost  – l DOMAIN\username

id -u
<!--NeedCopy-->
```

Vérifiez qu'un fichier cache d'identification Kerberos correspondant a été créé pour le **uid** renvoyé par la commande :

```
ls /tmp/krb5cc_{
 uid }

<!--NeedCopy-->
```

Vérifiez que les tickets dans le cache d'identification de Kerberos de l'utilisateur sont valides et n'ont pas expiré :

```
klist
<!--NeedCopy-->
```

IPv6

December 16, 2022

Le Linux VDA prend en charge IPv6 pour s'aligner avec Citrix Virtual Apps and Desktops. Lors de l'utilisation de cette fonctionnalité, considérez ce qui suit :

- Pour les environnements double pile, IPv4 est utilisé sauf si le protocole IPv6 est explicitement activé.
- Si le protocole IPv6 est activé dans un environnement IPv4, le Linux VDA ne fonctionnera pas.

> **Important :**
>
> - L'environnement réseau entier doit être IPv6, et pas uniquement pour le Linux VDA.
> - Centrify ne prend pas en charge IPv6 pur.

Aucune tâche de configuration spéciale n'est requise pour IPv6 lors de l'installation du Linux VDA.

Configurer le protocole IPv6 pour le Linux VDA

Avant de modifier la configuration du Linux VDA, assurez-vous que votre machine virtuelle Linux a précédemment fonctionné dans un réseau IPv6. Deux clés de registre sont associées à la configuration d'IPv6 :

```
1 " HKLM\Software\Policies\Citrix\VirtualDesktopAgent " -t " REG_DWORD "
    -v " OnlyUseIPv6ControllerRegistration "
2 " HKLM\Software\Policies\Citrix\VirtualDesktopAgent " -t " REG_DWORD "
    -v " ControllerRegistrationIPv6Netmask "
3 <!--NeedCopy-->
```

OnlyUseIPv6ControllerRegistration doit être défini sur 1 pour activer IPv6 sur Linux VDA :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Policies\
    Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "
    OnlyUseIPv6ControllerRegistration" -d "0x00000001" --force
2 <!--NeedCopy-->
```

Si l'agent Linux VDA comporte plusieurs interfaces réseau, **ControllerRegistrationIPv6Netmask** peut être utilisé pour spécifier l'interface à utiliser pour l'enregistrement de Linux VDA :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Policies\
    Citrix\VirtualDesktopAgent" -t "REG_SZ" -v "
    ControllerRegistrationIPv6Netmask " -d "{
2  IPv6 netmask }
3  " --force
4 <!--NeedCopy-->
```

Remplacez **{IPv6 netmask}** par le masque réseau réel (par exemple, 2000::/64).

Pour plus d'informations sur le déploiement IPv6 dans Citrix Virtual Apps and Desktops, consultez la section Prise en charge d'IPv4/IPv6.

Résolution des problèmes

Vérifiez l'environnement réseau IPv6 de base et utilisez ping6 pour vérifier si AD et Delivery Controller sont accessibles.

LDAPS

December 16, 2022

LDAPS est la version sécurisée du protocole LDAP (Lightweight Directory Access Protocol) avec lequel les communications LDAP sont cryptées à l'aide de TLS/SSL.

Par défaut, les communications LDAP entre les applications du client et du serveur ne sont pas cryptées. LDAPS vous permet de protéger le contenu de la requête LDAP entre le Linux VDA et les serveurs LDAP.

Les composants Linux VDA suivants ont des dépendances avec LDAPS :

- Agent broker : enregistrement de l'agent Linux VDA auprès du Delivery Controller
- Service de stratégie : évaluation de la stratégie

La configuration de LDAPS implique les actions suivantes :

- Activer LDAPS sur le serveur Active Directory (AD)/LDAP
- Exporter l'autorité de certification racine pour les clients
- Activer ou désactiver LDAPS sur le Linux VDA
- Configurer LDAPS pour les plates-formes tierces
- Configurer SSSD
- Configurer Winbind
- Configurer Centrify
- Configurer Quest

> **Remarque :**
>
> Vous pouvez exécuter la commande suivante pour définir un cycle de surveillance pour vos serveurs LDAP. La valeur par défaut est 15 minutes. Définissez la valeur sur au moins 10 minutes.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent" -v "ListOfLDAPServersMonitorPeroid" -t "
     REG_DWORD" -d "0x0000000f" --force
2 <!--NeedCopy-->
```


Activer LDAPS sur le serveur AD/LDAP

Vous pouvez activer LDAP sur SSL (LDAPS) en installant un certificat correctement formaté provenant d'une autorité de certification (CA) Microsoft ou d'une autorité de certification autre que Microsoft.

> **Conseil :**
>
> LDAPS est automatiquement activé lorsque vous installez une autorité de certification racine d'entreprise sur un contrôleur de domaine.

Pour de plus amples informations sur la manière d'installer le certificat et de vérifier la connexion LDAPS, consultez l'article Comment faire pour activer le protocole LDAP sur SSL avec une autorité de certification tierce.

Lorsque vous disposez d'une hiérarchie d'autorité de certification à plusieurs niveaux, vous ne disposerez pas automatiquement du certificat approprié pour l'authentification LDAPS sur le contrôleur de domaine.

Pour de plus amples informations sur la manière d'activer LDAPS pour les contrôleurs de domaine à l'aide d'une hiérarchie d'autorité de certification à plusieurs niveaux, consultez l'article LDAP over SSL (LDAPS) Certificate.

Activer l'autorité de certification racine pour le client

Le client doit utiliser un certificat provenant d'une autorité de certification approuvée par le serveur LDAP. Pour activer l'authentification LDAPS pour le client, importez le certificat d'autorité de certification racine sur le keystore approuvé.

Pour de plus amples informations sur la manière d'exporter l'autorité de certification racine, consultez l'article Comment faire pour exporter le certificat d'autorité de Certification racine sur le site Web de support de Microsoft.

Activer ou désactiver LDAPS sur le Linux VDA

Pour activer ou désactiver LDAPS sur le Linux VDA, exécutez le script suivant (vous devez être connecté en tant qu'administrateur) :

La syntaxe de cette commande comprend les éléments suivants :

- Activer LDAP sur SSL/TLS avec le certificat d'autorité de certification racine fourni :

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enable pathToRootCA
<!--NeedCopy-->
```

- Activer LDAP sur SSL/TLS avec liaison de canal :


```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enablecb pathToRootCA
<!--NeedCopy-->
```

> **Remarque :**
>
> Le certificat d'autorité de certification racine pour la liaison de canal doit être au format PEM. Si l'activation de LDAPS ne crée pas un environnement virtuel Python3 correctement, créez-le manuellement en suivant les instructions de la section Créer un environnement virtuel Python3.
>
> Pour résoudre les erreurs de connexion SSL que vous pouvez rencontrer lors de l'utilisation de l'outil pip, envisagez d'ajouter les hôtes approuvés suivants au fichier /etc/pip.conf :
>
> ```
> [global]
> trusted-host =
> pypi.org
> files.pythonhosted.org
> ```

- Retour à LDAP sans SSL/TLS

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Disable
<!--NeedCopy-->
```

Le keystore Java dédié à LDAPS se trouve dans **/etc/xdl/.keystore**. Clés de registre affectées :

```
HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServers

HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServersForPolicy

HKLM\Software\Citrix\VirtualDesktopAgent\UseLDAPS

HKLM\Software\Policies\Citrix\VirtualDesktopAgent\Keystore

HKLM\Software\Citrix\VirtualDesktopAgent\EnableChannelBinding
<!--NeedCopy-->
```

Configurer LDAPS pour une plate-forme tierce

Outre les composants Linux VDA, plusieurs composants logiciels tiers conformes au VDA peuvent également nécessiter le protocole LDAP sécurisé, comme SSSD, Winbind, Centrify et Quest. Les sections suivantes décrivent comment configurer le protocole LDAP sécurisé avec LDAPS, STARTTLS ou SASL (signer et sceller).

> **Conseil :**
>
> Ces composants logiciels ne préfèrent pas tous utiliser le port SSL 636 pour garantir un protocole

> LDAP sécurisé. De plus, la plupart du temps, LDAPS (LDAP sur SSL sur le port 636) ne peut pas coexister avec STARTTLS sur le port 389.

SSSD

Configurez le trafic LDAP sécurisé SSSD sur le port 636 ou 389 conformément aux options. Pour plus d'informations, consultez la page SSSD LDAP Linux man page.

Winbind

La requête LDAP Winbind utilise la méthode ADS. Winbind prend uniquement en charge la méthode StartTLS sur le port 389. Les fichiers de configuration affectés sont **/etc/samba/smb.conf** et **/etc/openldap/ldap.conf** (pour RHEL) ou **/etc/ldap/ldap.conf** (pour Ubuntu). Modifiez les fichiers comme suit :

- smb.conf

  ```
  ldap ssl = start tls
  ldap ssl ads = yes
  client ldap sasl wrapping = plain
  ```

- ldap.conf

  ```
  TLS_REQCERT never
  ```

LDAP sécurisé peut également être configuré par SASL GSSAPI (signer et sceller), mais il ne peut pas coexister avec TLS/SSL. Pour utiliser le cryptage SASL, modifiez la configuration du fichier **smb.conf** :

```
ldap ssl = off
ldap ssl ads = no
client ldap sasl wrapping = seal
```

Centrify

Centrify ne prend pas en charge LDAPS sur le port 636. Toutefois, il fournit un cryptage sécurisé sur le port 389. Pour de plus amples informations, consultez le site Centrify.

Quest

Quest Authentication Service ne prend pas en charge LDAPS sur le port 636, mais il offre un cryptage sécurisé sur le port 389 à l'aide d'une autre méthode.

Résolution des problèmes

Les problèmes suivants peuvent se produire lors de l'utilisation de cette fonctionnalité :

- **Disponibilité du service LDAPS**

  Vérifiez que la connexion LDAPS est disponible sur le serveur AD/LDAP. Le port par défaut est 636.

- **Échec de l'enregistrement du Linux VDA lorsque LDAPS est activé**

  Vérifiez que le serveur LDAP et les ports sont configurés correctement. Vérifiez le certificat d'autorité de certification racine et assurez-vous qu'il correspond au serveur AD/LDAP.

- **Modification incorrecte du registre effectuée accidentellement**

  Si vous avez mis à jour les clés liées à LDAPS par accident sans utiliser **enable_ldaps.sh**, cela peut rompre la dépendance des composants LDAPS.

- **Le trafic LDAP n'est pas crypté via SSL/TLS à partir de Wireshark ou tout autre outil de gestion du réseau**

  Par défaut, LDAPS est désactivé. Exécutez **/opt/Citrix/VDA/sbin/enable_ldaps.sh** pour le forcer.

- **Il n'existe aucun trafic LDAPS depuis Wireshark ou tout autre outil d'analyse du réseau**

  Le trafic LDAP/LDAPS se produit lors de l'enregistrement du Linux VDA et de l'évaluation de la stratégie de groupe.

- **Impossible de vérifier la disponibilité de LDAPS en exécutant ldp Connect sur le serveur Active Directory**

  Utilisez le nom de domaine complet (FQDN) Active Directory au lieu de l'adresse IP.

- **Impossible d'importer le certificat d'autorité de certification racine en exécutant le script /opt/Citrix/VDA/sbin/enable_ldaps.sh**

  Fournissez le chemin d'accès complet du certificat d'autorité de certification, et vérifiez que le type de certificat d'autorité de certification racine est correct. Il est supposé être compatible avec la plupart des types de keystore Java pris en charge. S'il n'est pas répertorié dans la liste, vous pouvez convertir le type. Nous recommandons le format PEM codé en base64 si vous rencontrez un problème avec le format du certificat.

- **Impossible d'afficher le certificat d'autorité de certification racine avec la commande -list de Keytool**

  Lorsque vous activez LDAPS en exécutant `/opt/Citrix/VDA/sbin/enable_ldaps.sh`, le certificat est importé sur /etc/xdl/.keystore, et le mot de passe est défini pour protéger le

keystore. Si vous avez oublié le mot de passe, vous pouvez réexécuter le script pour créer un keystore.

Xauthority

December 16, 2022

Le Linux VDA prend en charge les environnements qui utilisent le déport d'affichage X11 interactif (y compris `xterm` et `gvim`). Cette fonctionnalité fournit un mécanisme de sécurité nécessaire pour sécuriser les communications entre XClient et XServer.

Deux méthodes permettent de sécuriser l'autorisation pour cette communication sécurisée :

- **Xhost**. Par défaut, Xhost permet uniquement au XClient localhost de communiquer avec XServer. Si vous choisissez d'autoriser un XClient distant à accéder à XServer, la commande Xhost doit être exécutée pour accorder l'autorisation sur la machine spécifique. Vous pouvez aussi utiliser **xhost +** pour autoriser n'importe quel XClient à se connecter à XServer.
- **Xauthority**. Le fichier `.Xauthority` se trouve dans le répertoire de base de chaque utilisateur. Il est utilisé pour stocker les informations d'identification dans les cookies utilisés par xauth pour l'authentification de XServer. Lorsqu'une instance XServer (Xorg) est lancée, le cookie est utilisé pour authentifier les connexions à cet affichage spécifique.

Fonctionnement

Lorsque Xorg démarre, un fichier `.Xauthority` est transmis à Xorg. Le fichier `.Xauthority` contient les éléments suivants :

- Numéro d'affichage
- Protocole de demande distante
- Numéro de cookie

Vous pouvez accéder à ce fichier à l'aide de la commande `xauth`. Par exemple :

```
# xauth -f ~/.Xauthority

# > list

# > us01msip06:107  MIT-MAGIC-COOKIE-1
      fb228d1b695729242616c5908f11624b
<!--NeedCopy-->
```

Si **XClient** se connecte à Xorg à distance, deux conditions doivent être préalablement remplies :

- Définissez la variable d'environnement **DISPLAY** vers le XServer distant.
- Obtenez le fichier `.Xauthority` qui contient l'un des numéros de cookie dans Xorg.

Configurer Xauthority

Pour activer **Xauthority** sur Linux VDA pour le déport d'affichage X11, vous devez créer les deux clés de registre suivantes :

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "
    XauthEnabled" -d "0x00000001" --force

sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "ListenTCP"
     -d "0x00000001" --force
<!--NeedCopy-->
```

Après avoir activé **Xauthority**, transmettez le fichier `.Xauthority` à **XClient** manuellement, ou en montant un répertoire de base partagé :

- Transmettre le fichier `.Xauthority` à XClient manuellement

  Après le lancement d'une session ICA, le Linux VDA génère le fichier `.Xauthority` pour le XClient et stocke le fichier dans le répertoire de base de la session utilisateur. Vous pouvez copier ce fichier `.Xauthority` sur la machine XClient distante et définir les variables d'environnement **DISPLAY** et **XAUTHORITY**. `DISPLAY` est le numéro d'affichage stocké dans le fichier `.Xauthority` et `XAUTHORITY` est le chemin d'accès au fichier **Xauthority**. Pour un exemple, reportez-vous à la commande suivante :

  ```
  export DISPLAY={
  Display number stored in the Xauthority file }


  export XAUTHORITY={
  the file path of .Xauthority }

  <!--NeedCopy-->
  ```

  > **Remarque :**
  >
  > Si la variable d'environnement **XAUTHORITY** n'est pas définie, le fichier `~/.Xauthority` est utilisé par défaut.

- Transmettre le fichier `.Xauthority` à XClient en montant un répertoire de base partagé

  La façon la plus pratique consiste à monter un répertoire de base partagé pour la session utilisateur. Lorsque le Linux VDA démarre une session ICA, le fichier `.Xauthority` est créé dans le

répertoire de base de la session utilisateur. Si ce répertoire de base est partagé avec le XClient, l'utilisateur n'a pas besoin de transmettre manuellement ce fichier `.Xauthority` à XClient. Après avoir correctement défini les variables d'environnement **DISPLAY** et **XAUTHORITY**, l'interface utilisateur est affichée dans le bureau XServer automatiquement.

Résolution des problèmes

Si **Xauthority** ne fonctionne pas, suivez la procédure de dépannage ci-dessous :

1. En tant qu'administrateur avec privilège root, récupérez tous les cookies Xorg :

   ```
   ps aux | grep -i xorg
   <!--NeedCopy-->
   ```

   Cette commande affiche le processus Xorg et les paramètres transmis à Xorg lors du démarrage. Un autre paramètre affiche le fichier `.Xauthority` utilisé. Par exemple :

   ```
   /var/xdl/xauth/.Xauthority110
   <!--NeedCopy-->
   ```

   Affichez les cookies à l'aide de la commande **Xauth** :

   ```
   Xauth -f /var/xdl/xauth/.Xauthority110
   <!--NeedCopy-->
   ```

2. Utilisez la commande `Xauth` pour afficher les cookies contenus dans ~/`.Xauthority`. Pour le même numéro d'affichage, les cookies affichés doivent être identiques dans les fichiers `.Xauthority` de Xorg et de XClient.
3. Si les cookies sont identiques, vérifiez l'accessibilité du port d'affichage à distance en utilisant l'adresse IP du Linux VDA et le numéro d'affichage du bureau publié.

   Par exemple, exécutez la commande suivante sur la machine XClient :

   ```
   telnet 10.158.11.11 6160
   <!--NeedCopy-->
   ```

   Le numéro de port est la somme de 6000 + \<numéro d'affichage\>.

   Si l'opération telnet échoue, il est possible que le pare-feu bloque la requête.

Authentification

December 16, 2022

Cette section contient les rubriques suivantes :

- Authentification avec Azure Active Directory
- Authentification Single Sign-On double-hop
- Service d'authentification fédérée
- Pas d'authentification unique
- Cartes à puce
- Sessions non authentifiées par des utilisateurs anonymes

Authentification avec Azure Active Directory

December 16, 2022

> **Remarque :**
>
> Cette fonctionnalité n'est disponible que pour les VDA hébergés sur Azure.

En fonction de vos besoins, vous pouvez déployer deux types de Linux VDA dans Azure :

- VM jointes à Azure AD DS. Les machines virtuelles sont jointes à un domaine géré par les services de domaine (DS) Azure Active Directory (AAD). Les utilisateurs utilisent leurs informations d'identification de domaine pour se connecter aux machines virtuelles.
- VM n'appartenant pas à un domaine. Les machines virtuelles s'intègrent au service d'identité AAD pour fournir l'authentification des utilisateurs. Les utilisateurs utilisent leurs informations d'identification AAD pour se connecter aux machines virtuelles.

Pour plus d'informations sur AAD DS et AAD, consultez cet article Microsoft.

Cet article explique comment activer et configurer le service d'identité AAD sur des VDA n'appartenant pas à un domaine.

Distributions prises en charge

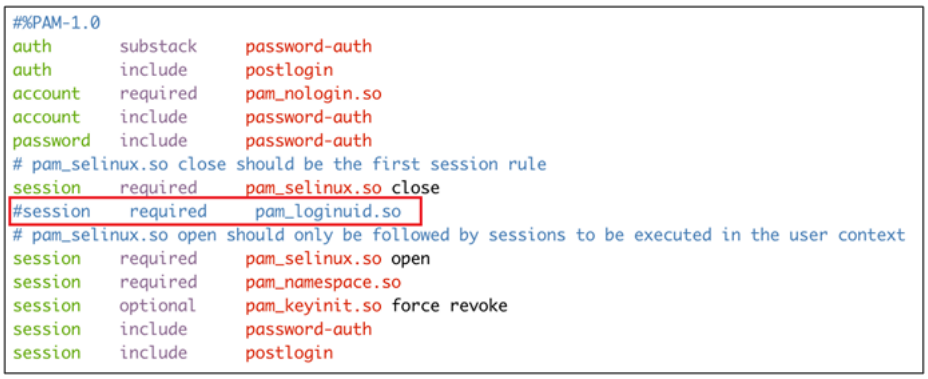
- Ubuntu 22.04, 20.04, 18.04
- RHEL 8.6, 8.4, 7.9
- SUSE 15.3

Pour plus d'informations, veuillez consulter l'article Microsoft.

Problèmes connus et solutions

Sur Red Hat 8.3 et 7.9, le module PAM (Pluggable Authentication Module) `pam_loginuid.so` ne parvient pas à définir `loginuid` après l'authentification utilisateur AAD. Ce problème empêche les utilisateurs AAD d'accéder aux sessions VDA.

Pour contourner ce problème, dans `/etc/pam.d/remote`, commentez la ligne `Session required pam_loginuid.so`. Reportez-vous à la capture d'écran suivante pour un exemple.

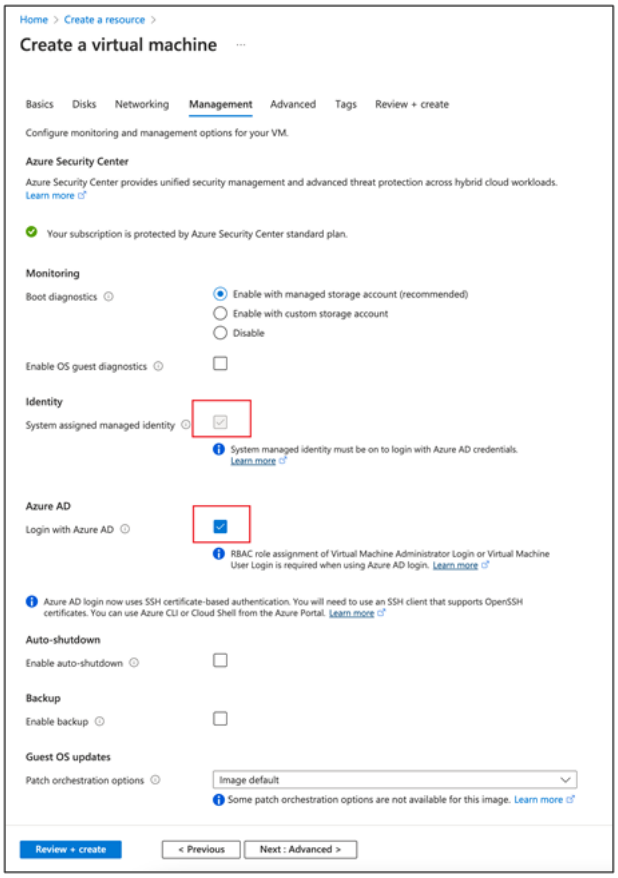


```
#%PAM-1.0
auth       substack     password-auth
auth       include      postlogin
account    required     pam_nologin.so
account    include      password-auth
password   include      password-auth
# pam_selinux.so close should be the first session rule
session    required     pam_selinux.so close
#session    required     pam_loginuid.so
# pam_selinux.so open should only be followed by sessions to be executed in the user context
session    required     pam_selinux.so open
session    required     pam_namespace.so
session    optional     pam_keyinit.so force revoke
session    include      password-auth
session    include      postlogin
```

Étape 1 : Créer une VM modèle sur le portail Azure

Créez une VM modèle et installez l'interface de ligne de commande Azure sur la machine virtuelle.

1. Sur le portail Azure, créez une VM modèle. Assurez-vous de sélectionner **Se connecter avec Azure AD** dans l'onglet **Gestion** avant de cliquer sur **Examiner et créer**.



2. Installez l'interface de ligne de commande Azure sur la VM modèle.
   Pour plus d'informations, veuillez consulter l'article Microsoft.

Étape 2 : préparer une image principale sur la VM modèle

Pour préparer une image principale, suivez l'**Étape 3 : préparer une image principale** dans Utiliser MCS pour créer des machines virtuelles Linux sur Azure.

Étape 3 : Définir la VM modèle sur le mode non joint au domaine

Après avoir créé une image principale, procédez comme suit pour définir la machine virtuelle en mode non joint au domaine :

1. Exécutez le script suivant à partir de l'invite de commandes.

```
Modify /var/xdl/mcs/mcs_util.sh
<!--NeedCopy-->
```

2. Localisez `function read_non_domain_joined_info()`, puis remplacez la valeur `NonDomainJoined` par 2. Consultez le bloc de code dans l'exemple suivant.


```
function read_non_domain_joined_info()
{

log "Debug: Enter read_non_domain_joined_info"
# check if websocket enabled
TrustIdentity=`cat ${
 id_disk_mnt_point }
 ${
 ad_info_file_path }
  | grep '[TrustIdentity]' | sed 's/\s//g'`
if [ "$TrustIdentity" == "[TrustIdentity]" ]; then
NonDomainJoined=2
fi
...
 }

<!--NeedCopy-->
```

3. Enregistrez la modification.
4. Arrêtez la VM modèle.

Étape 4 : Créer les machines virtuelles Linux à partir de la VM modèle

Une fois que la VM modèle n'appartenant pas à un domaine est prête, procédez comme suit pour créer des machines virtuelles :

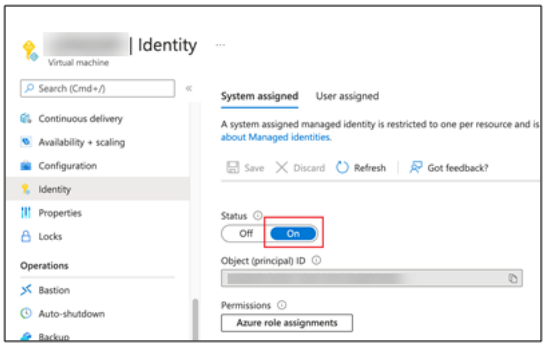
1. Connectez-vous à Citrix Cloud.
2. Double-cliquez sur Citrix DaaS, puis accédez à la console de gestion Configuration complète.
3. Dans **Catalogues de machines**, choisissez d'utiliser Machine Creation Services pour créer les machines virtuelles Linux à partir de la VM modèle. Pour plus d'informations, consultez VDA n'appartenant pas à un domaine dans le document Citrix DaaS.

Étape 5 : Attribuer des comptes utilisateurs AAD aux machines virtuelles Linux

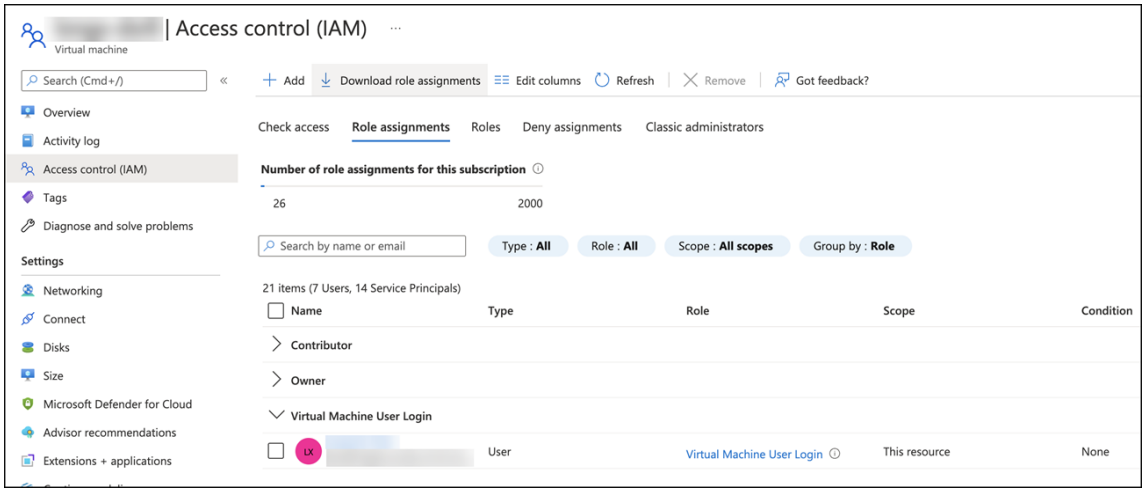
Après avoir créé les machines virtuelles n'appartenant pas à un domaine, attribuez-leur des comptes utilisateur AAD.

Pour attribuer des comptes utilisateur AAD à une machine virtuelle, procédez comme suit :

1. Accédez à la machine virtuelle à l'aide d'un compte administrateur.
2. Dans l'onglet **Identify > System assigned**, activez **System Identity**.



3. Dans l'onglet **Access control (IAM) > Role assignments**, localisez la zone **Virtual Machine User Login**, puis ajoutez les comptes utilisateur AAD selon vos besoins.



Se connecter à des VDA n'appartenant pas à un domaine

Les utilisateurs finaux de votre organisation peuvent se connecter à un VDA n'appartenant pas à un domaine de deux manières. Les étapes détaillées sont les suivantes :

1. Démarrez l'application Workspace, puis connectez-vous à l'espace de travail en saisissant le nom d'utilisateur et le mot de passe AAD. La page Workspace s'affiche.
2. Double-cliquez sur un bureau n'appartenant pas à un domaine. La page AAD LOGIN s'affiche.

   La page varie en fonction du mode de connexion défini sur le VDA : code d'appareil ou compte/-mot de passe AAD. Par défaut, les VDA Linux authentifient les utilisateurs AAD à l'aide du mode de connexion Code d'appareil comme suit. En tant qu'administrateur, vous pouvez définir le mode de connexion sur Compte/mot de passe AAD si nécessaire. Consultez la section suivante pour connaître les étapes détaillées.

3. Selon les instructions à l'écran, connectez-vous à la session de bureau de l'une des manières suivantes :

   - Scannez le code QR et saisissez-le.
   - Saisissez le nom d'utilisateur et le mot de passe AAD.

Passer au mode de connexion Compte/mot de passe AAD

Par défaut, les VDA Linux authentifient les utilisateurs AAD avec des codes d'appareil. Consultez cet article Microsoft pour plus de détails. Pour passer au mode de connexion *Compte/mot de passe AAD*, procédez comme suit :

Exécutez la commande suivante sur le VDA, localisez la clé `AADAcctPwdAuthEnable` et définissez sa valeur sur `0x00000001`.

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
   Services\CitrixBrokerAgent\WebSocket" -t "REG_DWORD" -v "
   AADAcctPwdAuthEnable" -d "0x00000001" --force

<!--NeedCopy-->
```

> **Remarque :**
>
> Cette approche ne fonctionne pas avec les comptes Microsoft ou les comptes pour lesquels l'authentification à deux facteurs est activée.

Authentification Single Sign-On double-hop

December 16, 2022

Les informations d'identification utilisateur peuvent être entrées pour accéder à un magasin StoreFront dans le module AuthManager de l'application Citrix Workspace pour Linux et Citrix Receiver pour Linux 13.10. Après l'injection, vous pouvez utiliser le client pour accéder à des bureaux et applications virtuels à partir d'une session de bureau virtuel Linux, sans entrer les informations d'identification de l'utilisateur une deuxième fois.

> **Remarque :**
>
> cette fonctionnalité est prise en charge sur l'application Citrix Workspace pour Linux et Citrix Receiver pour Linux 13.10.

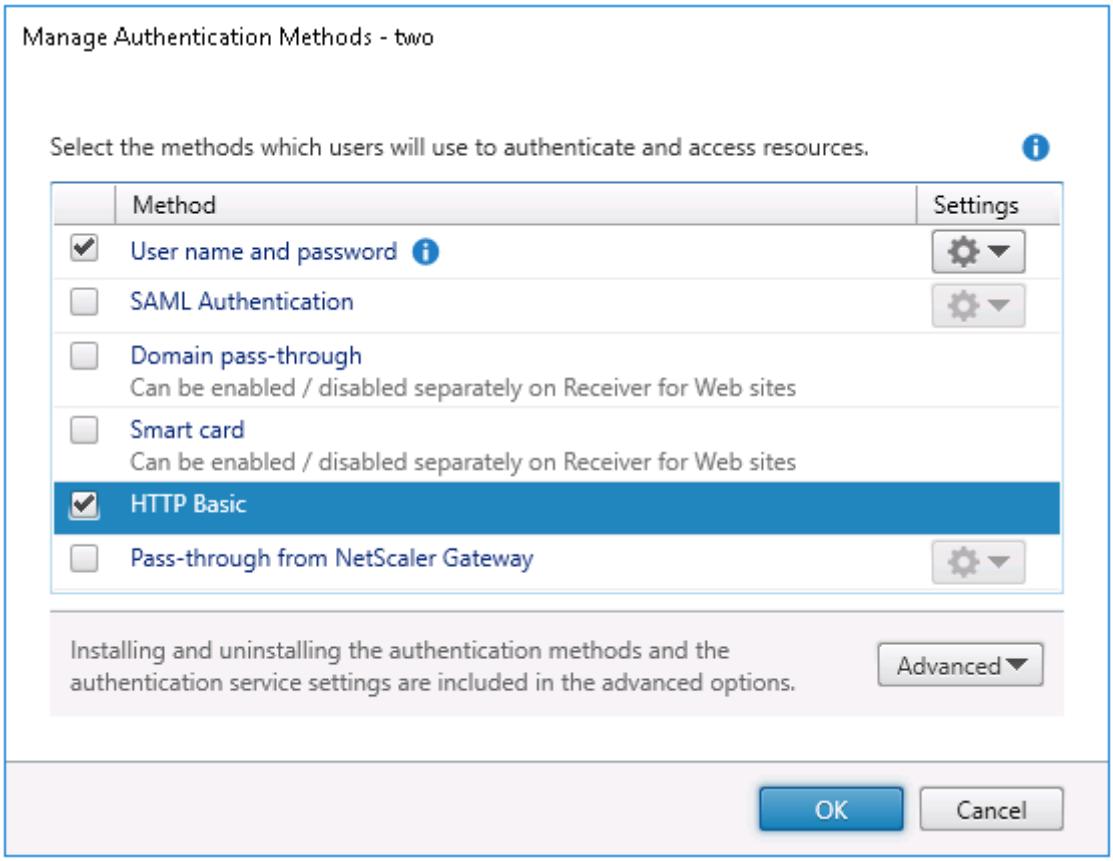
Pour activer la fonctionnalité :

1. Sur le Linux VDA, installez l'application Citrix Workspace pour Linux ou Citrix Receiver pour Linux 13.10.

   Téléchargez l'application depuis la page de téléchargement Citrix pour l'application Citrix Workspace ou pour Citrix Receiver.

   Le chemin d'installation par défaut est /opt/Citrix/ICAClient/. Si vous installez l'application sur un chemin d'accès différent, définissez la variable d'environnement ICAROOT pour qu'elle pointe vers le chemin d'installation réel.

2. Dans la console de gestion Citrix StoreFront, ajoutez la méthode d'authentification **HTTP basique** pour le magasin cible.



3. Ajoutez la clé suivante au fichier de configuration AuthManager ($ICAROOT/config/AuthManConfig.xml) pour autoriser l'authentification HTTP basique :

```
<Protocols>
     <HTTPBasic>
         <Enabled>True</Enabled>
    </HTTPBasic>
</Protocols>
<!--NeedCopy-->
```

4. Exécutez les commandes suivantes pour installer le certificat racine dans le répertoire spécifié.


```
cp rootcert.pem $ICAROOT/keystore/cacerts/
$ICAROOT/util/ctx_rehash  $ICAROOT/keystore/cacerts/
<!--NeedCopy-->
```

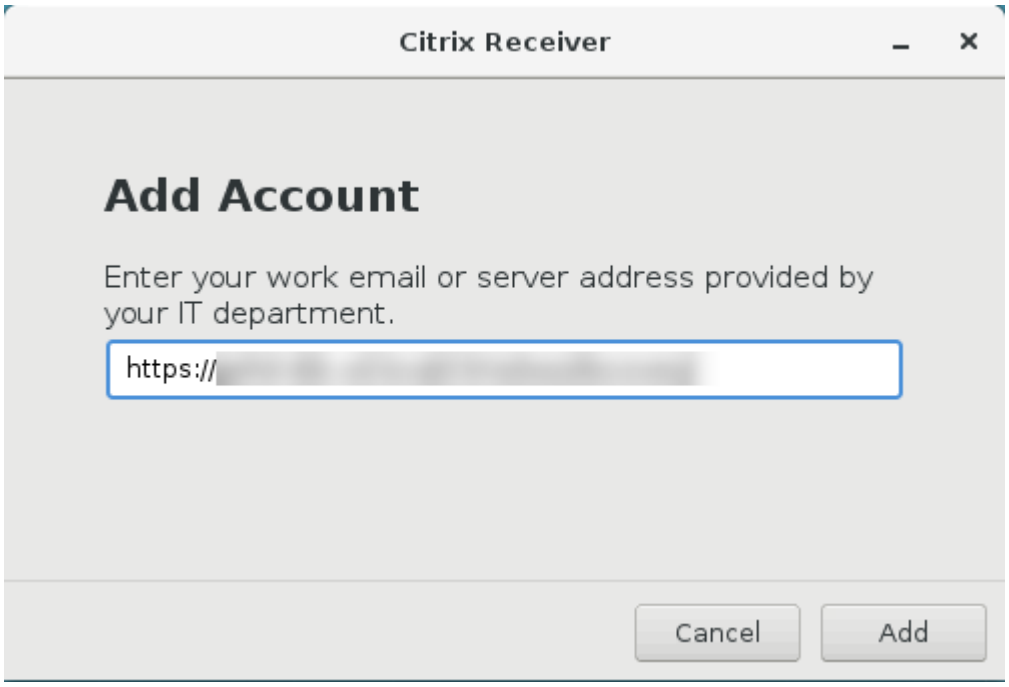
5. Exécutez la commande suivante pour activer la fonctionnalité :

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
   CurrentControlSet\Control\Citrix" -v "LurSsonEnabled" -d "0
   x00000001"
<!--NeedCopy-->
```

6. Lancez une session de bureau virtuel Linux et démarrez l'application Citrix Workspace pour Linux ou Citrix Receiver pour Linux 13.10 dans cette session.

   Vous êtes invité à saisir un compte de magasin lorsque vous démarrez l'application Citrix Workspace pour la première fois. Ensuite, vous serez automatiquement connecté au magasin que vous avez spécifié précédemment.

   > **Remarque :**
   >
   > entrez une URL HTTPS comme compte de magasin.



Service d'authentification fédérée

February 9, 2024

Vous pouvez utiliser le service d'authentification fédérée (FAS) pour authentifier les utilisateurs qui ouvrent une session sur un Linux VDA. Le Linux VDA utilise le même environnement Windows que le VDA Windows pour la fonctionnalité d'ouverture de session de FAS. Pour plus d'informations sur la configuration de l'environnement Windows pour FAS, consultez Service d'authentification fédérée. Cet article fournit des informations supplémentaires spécifiques au Linux VDA.

> **Remarque :**
>
> - Le Linux VDA ne prend pas en charge la stratégie **Comportement en session**.
> - Le Linux VDA utilise des connexions courtes pour transmettre des données avec des serveurs FAS.
> - À compter de la version 2206, vous pouvez personnaliser le port FAS côté Linux VDA via CTX_XDL_FAS_LIST dans le fichier ctxsetup.sh. Pour plus d'informations, consultez l'article sur l'installation de Linux VDA correspondant à votre distribution.

Configurer FAS sur le Linux VDA

Prise en charge de FAS sur RHEL 8 et Rocky Linux 8

FAS dépend du module pam_krb5, qui est obsolète sur RHEL 8 et Rocky Linux 8. Pour utiliser FAS sur RHEL 8 et Rocky Linux 8, créez le module pam_krb5 comme suit :

1. Téléchargez le code source pam_krb5-2.4.8-6 à partir du site Web suivant :

   https://centos.pkgs.org/7/centos-x86_64/pam_krb5-2.4.8-6.el7.x86_64.rpm.html.

2. Créez et installez le module pam_krb5 sur RHEL 8 et Rocky Linux 8.

```
yum install make gcc krb5-devel pam-devel autoconf libtool
rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio -div
tar xvzf pam_krb5-2.4.8.tar.gz
cd pam_krb5-2.4.8
./configure --prefix=/usr
make
make install
<!--NeedCopy-->
```

3. Vérifiez que pam_krb5.so existe sous /usr/lib64/security/.

```
ls -l /usr/lib64/security | grep pam_krb5
<!--NeedCopy-->
```


Définir les serveurs FAS

Pour utiliser FAS dans une nouvelle installation Linux VDA, tapez le nom de domaine complet de chaque serveur FAS lorsque vous exécutez ctxinstall.sh ou ctxsetup.sh. Comme le Linux VDA ne prend pas en charge la stratégie de groupe AD, vous pouvez fournir une liste de serveurs FAS séparés par des points-virgules. Si une adresse de serveur est supprimée, remplissez son espace vide avec la chaîne de texte **<none>** et ne modifiez pas l'ordre des adresses de serveur.

Pour mettre à niveau une installation Linux VDA existante, vous pouvez réexécuter `ctxsetup.sh` pour définir les serveurs FAS. Vous pouvez également exécuter les commandes suivantes pour définir les serveurs FAS et redémarrer le service `ctxvda` pour que vos paramètres prennent effet.

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
    VirtualDesktopAgent\Authentication\UserCredentialService" -t "REG_SZ
    " -v "Addresses" -d "<Your-FAS-Server-List>" --force

service ctxjproxy restart

service ctxvda restart
<!--NeedCopy-->
```

Pour mettre à jour les serveurs FAS via `ctxreg`, exécutez les commandes suivantes :

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
    VirtualDesktopAgent\Authentication\UserCredentialService" -v "
    Addresses" -d "<Your-FAS-Server-List>"

service ctxjproxy restart

service ctxvda restart
<!--NeedCopy-->
```

Installation des certificats

Pour la vérification des certificats des utilisateurs, installez le certificat d'autorité de certification racine et tous les certificats intermédiaires sur le VDA. Par exemple, pour installer le certificat d'autorité de certification racine, vous pouvez obtenir le certificat racine AD depuis l'étape précédente **Récupérer le certificat CA à partir de l'autorité de certification Microsoft (sur AD)** ou télécharger son format DER à partir du serveur de l'autorité de certification racine `http://CA-SERVER/certsrv`.

> **Remarque :**
>
> Les commandes suivantes s'appliquent également à la configuration d'un certificat intermédiaire.

Vous pouvez exécuter une commande similaire à la suivante pour convertir un fichier DER (.crt, .cer, .der) en PEM.

```
sudo openssl x509 -inform der -in root.cer -out root.pem
<!--NeedCopy-->
```

Installez ensuite le certificat d'autorité de certification racine dans le répertoire `openssl` en exécutant la commande suivante :

```
sudo cp root.pem /etc/pki/CA/certs/
<!--NeedCopy-->
```

> **Remarque :**
>
> ne placez pas le certificat d'autorité de certification racine sous le chemin d'accès **/root**. Sinon, FAS n'a pas l'autorisation de lecture sur le certificat d'autorité de certification racine.

Exécuter ctxfascfg.sh

Exécutez le script ctxfascfg.sh pour configurer FAS :

```
sudo /opt/Citrix/VDA/sbin/ctxfascfg.sh
<!--NeedCopy-->
```

Les variables d'environnement sont ajoutées pour pouvoir exécuter `ctxfascfg.sh` en mode silencieux :

- **CTX_FAS_ADINTEGRATIONWAY=winbind | sssd | centrify | pbis** : indique la méthode d'intégration d'Active Directory, qui est `CTX_EASYINSTALL_ADINTEGRATIONWAY` lorsque `CTX_EASYINSTALL_ADINTEGRATIONWAY` est spécifié. Si `CTX_EASYINSTALL_ADINTEGRATIONWAY` n'est pas spécifié, `CTX_FAS_ADINTEGRATIONWAY` utilise son propre paramètre de valeur.
- **CTX_FAS_CERT_PATH =<certificate path>** : spécifie le chemin complet qui stocke le certificat racine et tous les certificats intermédiaires.
- **CTX_FAS_KDC_HOSTNAME :** spécifie le nom d'hôte du centre de distribution de clés lorsque vous sélectionnez PBIS.
- **CTX_FAS_PKINIT_KDC_HOSTNAME :** spécifie le nom d'hôte KDC PKINIT, qui correspond à CTX_FAS_KDC_HOSTNAME, sauf indication contraire.

Choisissez la méthode d'intégration Active Directory correcte, puis tapez le chemin correct des certificats (par exemple, `/etc/pki/CA/certs/`).

Le script installe ensuite les packages krb5-pkinit et pam_krb5 et définit les fichiers de configuration pertinents.

Limitation

- FAS prend en charge des plateformes Linux et des méthodes d'intégration AD limitées. Reportez-vous à la matrice suivante :

	Winbind	SSSD	Centrify	PBIS
Amazon Linux 2	Oui	Oui	Oui	Oui
Debian 11.3	Oui	Oui	Oui	Oui
RHEL 8.6, RHEL 8.4	Oui	Oui	Oui	Oui
RHEL 7.9 / CentOS 7.9	Oui	Oui	Oui	Oui
Rocky Linux 8	Oui	Oui	Non	Non
SLES 15.3	Oui	Oui	Oui	Non
Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04	Oui	Oui	Oui	Oui

- FAS ne prend pas encore en charge l'écran de verrouillage. Si vous cliquez sur le bouton de verrouillage dans une session, vous ne pouvez plus vous reconnecter à la session en utilisant FAS.
- Cette version ne prend en charge que les déploiements FAS courants décrits dans l'article Vue d'ensemble de l'architecture du Service d'authentification fédérée, dont **Windows 10 Azure AD Join** est exclu.

Dépannage

Avant de résoudre les problèmes dans FAS, assurez-vous que le Linux VDA est installé et configuré correctement afin qu'une session non FAS puisse être lancée dans le magasin commun en utilisant l'authentification par mot de passe.

Si les sessions non FAS fonctionnent correctement, définissez le niveau de journalisation HDX de la classe **Login** sur VERBOSE et le niveau de journalisation VDA sur TRACE. Pour plus d'informations sur l'activation de la consignation de trace pour Linux VDA, consultez l'article du centre de connaissances CTX220130.

Erreur de configuration du serveur FAS

Le lancement d'une session à partir du magasin FAS échoue.

Vérifiez **/var/log/xdl/hdx.log** et recherchez le journal des erreurs semblable au suivant :

```
2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user: [Logon Type] Federated Authentication Logon.

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: entry

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: connect_fas: start connect to server 0

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: connect_fas0: failed to connect: Connection refused.

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: failed to connect to server [0], please confirm if fas service list is well configurated in condb

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: exit, 43

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user: failed to validate fas credential

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: LoginBoxValidate: failed validation of user 'user1@CTXDEV.LOCAL', INVALID_PARAMETER

<!--NeedCopy-->
```

Solution Exécutez la commande suivante pour vérifier que la valeur de Registre Citrix « HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent\Authentication\UserCredentialService » est définie sur <Your-FAS-Server-List>.

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep "UserCredentialService"
<!--NeedCopy-->
```

Si le paramètre existant est incorrect, suivez l'étape précédente Définir les serveurs FAS pour le définir à nouveau.

Configuration du certificat d'autorité de certification incorrecte

Le lancement d'une session à partir du magasin FAS échoue. Une fenêtre grise apparaît et disparaît quelques secondes plus tard.

Vérifiez **/var/log/xdl/hdx.log** et recherchez le journal des erreurs semblable au suivant :

```
2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
   get_logon_certificate: entry

2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin: check_caller:
   current process: pid [30656], name [/opt/Citrix/VDA/bin/ctxlogin]

2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
   get_public_certificate: entry

2021-01-28 01:47:46.211 <P30656:S5> citrix-ctxlogin: query_fas: waiting
    for response...

2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin: query_fas: query
   to server success

2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin:
   get_public_certificate: exit

2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin: fas_base64_decode:
    input size 1888

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: fas_base64_decode:
    output size 1415

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin:
   get_logon_certificate: get logon certificate success

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: cache_certificate:
    cache certificate success

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin:
   get_logon_certificate: exit, 0

2021-01-28 01:47:48.060 <P30656:S5> citrix-ctxlogin: validate_user:
   pam_authenticate err,can retry for user user1@CTXDEV.LOCAL
<!--NeedCopy-->
```


Solution Vérifiez que vous avez correctement défini le chemin complet qui stocke le certificat d'autorité de certification racine et tous les certificats intermédiaires dans /etc/krb5.conf. Le chemin d'accès complet est similaire au suivant :

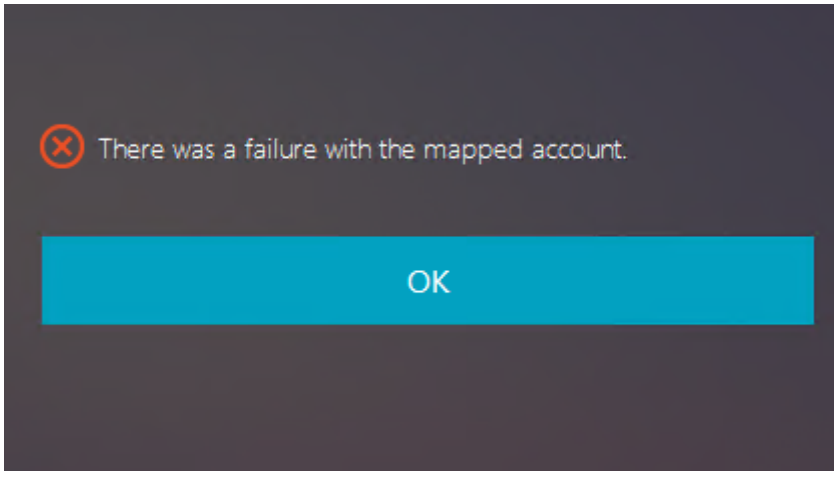
```
 [realms]

EXAMPLE.COM = {


    ......

    pkinit_anchors = DIR:/etc/pki/CA/certs/

    ......

 }

<!--NeedCopy-->
```

Si le paramètre existant est incorrect, suivez l'étape précédente Installation des certificats pour le définir à nouveau.

Vous pouvez également vérifier si le certificat d'autorité de certification racine est valide.

Erreur de mappage du compte fictif

FAS est configuré par l'authentification SAML. L'erreur suivante peut survenir après qu'un utilisateur ADFS entre le nom d'utilisateur et le mot de passe sur la page de connexion ADFS.

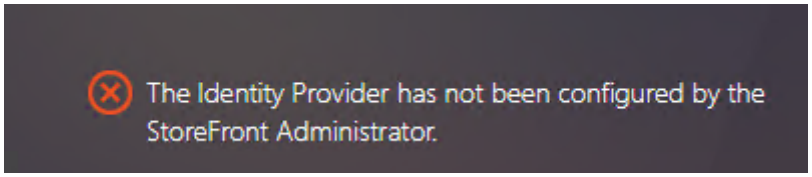


Cette erreur indique que l'utilisateur ADFS a été vérifié, mais qu'aucun utilisateur fictif n'est configuré sur AD.

Solution Définissez le compte fictif sur AD.

ADFS non configuré

L'erreur suivante se produit lors d'une tentative d'ouverture de session au magasin FAS :



Le problème se produit lorsque le magasin FAS est configuré pour utiliser l'authentification SAML mais que le déploiement ADFS est manquant.

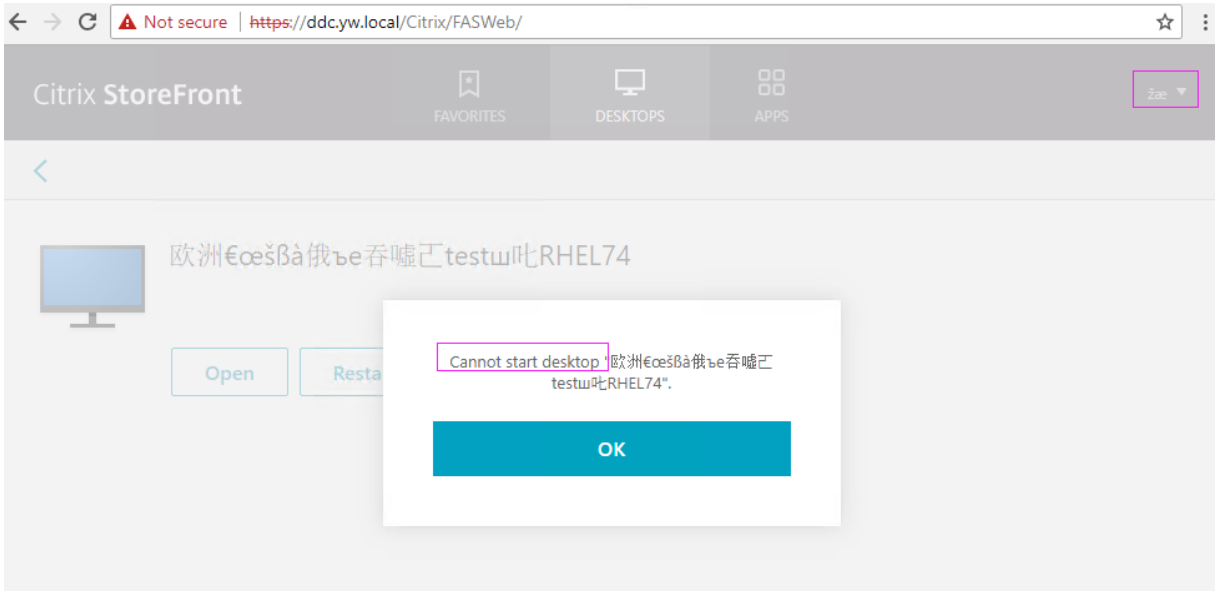
Solution Déployez le fournisseur d'identité ADFS du Service d'authentification fédérée. Pour plus d'informations, consultez la section Déploiement ADFS du Service d'authentification fédérée.

Informations connexes

- Les déploiements FAS courants sont décrits dans l'article Vue d'ensemble de l'architecture du Service d'authentification fédérée.
- Des informations pratiques sont disponibles dans le chapitre Configuration avancée du Service d'authentification fédérée.

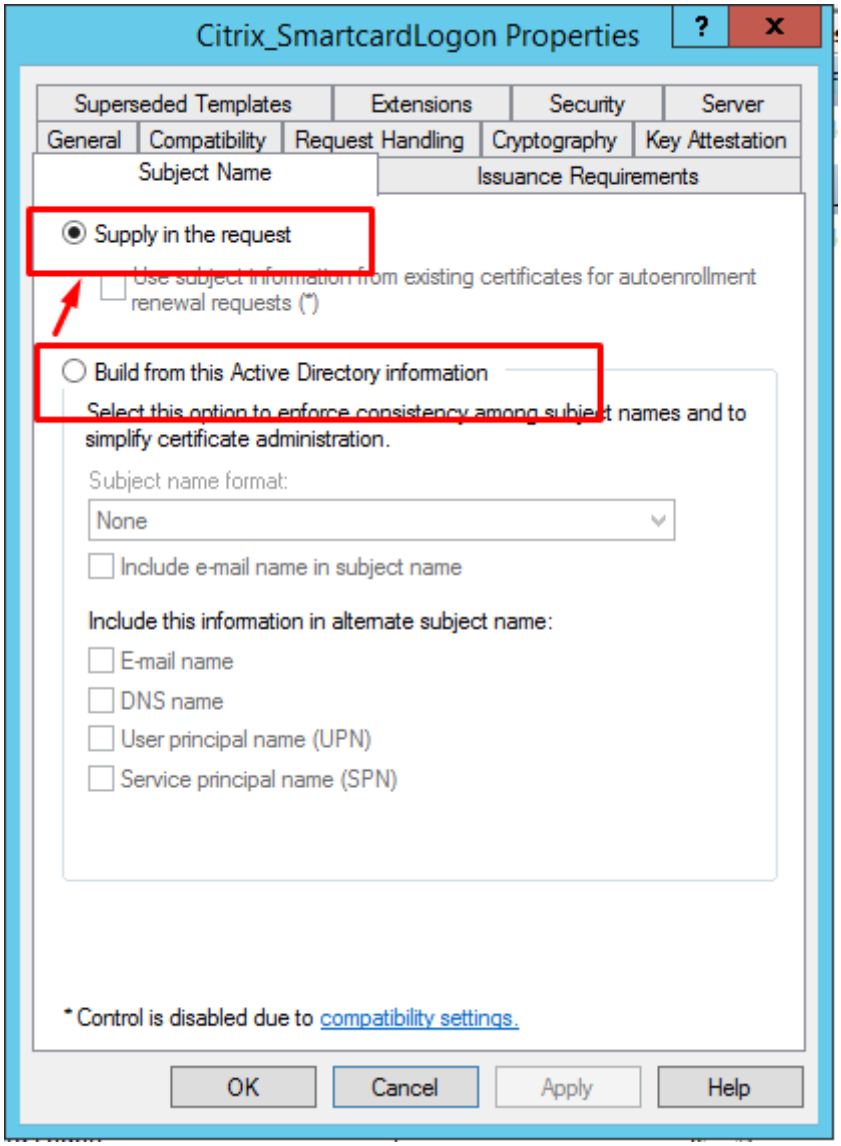
Problème connu

Lorsque FAS est utilisé, la tentative de lancement d'une session de bureau ou d'application publiée avec des caractères non anglais peut échouée.



Solution

Cliquez avec le bouton droit sur **Manage Templates** dans l'outil d'autorité de certification pour modifier le modèle **Citrix_SmartcardLogon** à partir de **Build from this Active Directory information** vers **Supply in the request** :



Pas d'authentification unique

December 16, 2022

Cet article fournit des conseils pour activer l'authentification non SSO sur le Linux VDA.

Vue d'ensemble

Par défaut, l'authentification unique (SSO) est activée sur le Linux VDA. Les utilisateurs se connectent à l'application Citrix Workspace et aux sessions VDA à l'aide d'un ensemble d'informations d'identification.

Pour que les utilisateurs se connectent aux sessions VDA à l'aide d'un ensemble d'informations d'identification différent, désactivez l'authentification unique sur le Linux VDA. Le tableau suivant répertorie les combinaisons de méthodes d'authentification des utilisateurs prises en charge dans les scénarios sans authentification unique.

Application Citrix Workspace	Session VDA
nom d'utilisateur	nom d'utilisateur
carte à puce	nom d'utilisateur
nom d'utilisateur	carte à puce

Désactiver l'authentification unique (SSO)

Exécutez la commande suivante sur votre Linux VDA :

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
     Control\Citrix\WinStations\tcp" -t "REG_DWORD" -v "
     fPromptForDifferentUser" -d "0x00000001" --force
2 <!--NeedCopy-->
```

Cartes à puce

December 23, 2022

Vous pouvez utiliser une carte à puce connectée à la machine cliente pour vous authentifier lors de la connexion à une session de bureau virtuel Linux. Cette fonctionnalité est implémentée via la redirection de carte à puce sur le canal virtuel de la carte à puce ICA. Vous pouvez également utiliser la carte à puce dans la session. Parmi les cas d'utilisation :

- Ajouter une signature numérique à un document
- Chiffrer ou déchiffrer un e-mail
- S'authentifier auprès d'un site Web

L'agent Linux VDA utilise la même configuration que l'agent Windows VDA pour cette fonctionnalité. Pour plus d'informations, veuillez consulter la section Configurer l'environnement de carte à puce.

> **Remarque :**
>
> L'utilisation d'une carte à puce mappée dans une session Linux VDA pour se connecter à Citrix Gateway n'est pas prise en charge.

Conditions préalables

La disponibilité de l'authentification pass-through avec des cartes à puce dépend des conditions suivantes :

- Votre Linux VDA est installé sur l'une des distributions suivantes :
  - RHEL 8
  - RHEL 7/CentOS 7
  - Rocky Linux 8
  - Ubuntu 22.04
  - Ubuntu 20.04
  - Ubuntu 18.04
  - Debian 11.3

  Une fois l'installation du VDA terminée, vérifiez que votre VDA peut s'enregistrer auprès du Delivery Controller et que les sessions de bureau Linux publiées peuvent être lancées avec succès à l'aide des informations d'identification Windows.
- Des cartes à puce prises en charge par OpenSC sont utilisées. Pour de plus amples informations, consultez la section S'assurer que OpenSC prend en charge votre carte à puce.
- L'application Citrix Workspace pour Windows est utilisée.

S'assurer que OpenSC prend en charge votre carte à puce

OpenSC est un pilote de carte à puce largement utilisé sur RHEL 7.4+. Remplacement entièrement compatible de CoolKey, OpenSC prend en charge de nombreux types de cartes à puce (consultez la page Smart Card Support in Red Hat Enterprise Linux).

Dans cet article, la carte à puce YubiKey est utilisée comme exemple pour illustrer la configuration. YubiKey est un périphérique USB CCID PIV tout-en-un qui peut facilement être acheté auprès d'Amazon ou d'autres revendeurs. Le pilote OpenSC prend en charge YubiKey.

Si votre organisation a besoin d'une autre carte à puce plus avancée, préparez une machine physique avec une distribution Linux prise en charge sur laquelle le package OpenSC est installé. Pour plus d'informations sur l'installation d'OpenSC, consultez la section Installer le pilote de la carte à puce. Insérez votre carte à puce et exécutez la commande suivante pour vérifier qu'OpenSC prend en charge votre carte à puce :


```
pkcs11-tool --module opensc-pkcs11.so --list-slots
<!--NeedCopy-->
```

Configuration

Préparer un certificat racine

Un certificat racine est utilisé pour vérifier le certificat sur la carte à puce. Suivez les étapes suivantes pour télécharger et installer un certificat racine.

1. Obtenez un certificat racine au format PEM, généralement auprès de votre serveur d'autorité de certification.

   Vous pouvez exécuter une commande similaire à la suivante pour convertir un fichier DER (*.crt, *.cer, *.der) en PEM. Dans l'exemple de commande suivant, **certnew.cer** est un fichier DER.

   ```
   openssl x509 -inform der -in certnew.cer -out certnew.pem
   <!--NeedCopy-->
   ```

2. Installez le certificat racine dans le répertoire `openssl`. Le fichier **certnew.pem** est utilisé à titre d'exemple.

   ```
   cp certnew.pem <path where you install the root certificate>
   <!--NeedCopy-->
   ```

   Pour créer un chemin d'accès pour l'installation du certificat racine, exécutez `sudo mdkir -p <path where you install the root certificate>`.

Créez le module pam_krb5 sur RHEL 8 et Rocky Linux 8

L'authentification par carte à puce dépend du module pam_krb5, qui est obsolète sur RHEL 8 et Rocky Linux 8. Pour utiliser l'authentification par carte à puce sur RHEL 8 et Rocky Linux 8, créez le module pam_krb5 comme suit :

1. Téléchargez le code source pam_krb5-2.4.8-6 à partir de https://centos.pkgs.org/7/centos-x86_64/pam_krb5-2.4.8-6.el7.x86_64.rpm.html.
2. Créez et installez le module pam_krb5 sur RHEL 8 et Rocky Linux 8.

   ```
   yum install -y opensc pcsc-lite pcsc-lite-libs pcsc-lite-ccid nss-
       tools
   yum install gcc krb5-devel pam-devel autoconf libtool
   rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio  – div
   tar xvzf pam_krb5-2.4.8.tar.gz
   cd pam_krb5-2.4.8
   ```



```
./configure --prefix=/usr
make
make install
<!--NeedCopy-->
```

3. Vérifiez que pam_krb5.so existe sous /usr/lib64/security/.

```
ls -l /usr/lib64/security | grep pam_krb5
<!--NeedCopy-->
```

Configurer l'environnement de la carte à puce

Vous pouvez utiliser le script ctxsmartlogon.sh pour configurer l'environnement de carte à puce ou effectuer la configuration manuellement.

(Option 1) Utiliser le script ctxsmartlogon.sh pour configurer l'environnement de carte à puce

> **Remarque :**
>
> Le script ctxsmartlogon.sh ajoute des informations PKINIT au domaine par défaut. Vous pouvez modifier ce paramètre via le fichier de configuration **/etc/krb5.conf**.

Avant d'utiliser les cartes à puce pour la première fois, exécutez le script ctxsmartlogon.sh pour configurer l'environnement de la carte à puce.

> **Conseil :**
>
> Si vous avez utilisé SSSD pour rejoindre un domaine, redémarrez le service SSSD après avoir exécuté ctxsmartlogon.sh.

```
sudo /opt/Citrix/VDA/sbin/ctxsmartlogon.sh
<!--NeedCopy-->
```

Les résultats ressemblent à ce qui suit :


```
#************************************************************************
# ctxsmartlogon.sh sets up smart card logon for the Linux VDA, which
# includes automatic installation of the necessary packages and changes to
# the configuration files.
#
# Note:
# The ctxsmartlogon.sh adds pkinit information to the default realm. You can
# change this setting through the /etc/krb5.conf configuration file.
#************************************************************************
Step 1:Enable smart card logon.
  Do you want enable smart card logon? (y/n)[y] y
Step 2:Select the Active Directory integration method.
  Please select which Active Directory integration method to use:
     1: Winbind
     2: SSSD
     3: Centrify
  Select one of the above options (1-3)[1] 1
Step 3:Install dependent packages.
  Installing, please wait...
    [krb5-pkinit][pam_krb5] already installed.
    [pcsc-lite][pcsc-lite-ccid][pcsc-lite-libs][coolkey] already installed.
  Packages installed. [Success]
Step 4:Configure krb5.conf.
  Specify the path to the root CA (e.g., /etc/pki/CA/certs/root.pem):/etc/pki/CA/certs/root.pem
  /etc/krb5.conf configure successfully.
Step 5:Configure PAM files.
  Specify the path to the smart card PKCS11 driver (e.g., /usr/lib64/pkcs11/libcoolkeypk11.so):/usr/lib64/pkcs11/libcoolkeypk11.so
  /etc/pam.d/ctxfsc configure successfully.
  /etc/pam.d/smartcard-auth configure successfully.
ctxsmartlogon.sh executed successfully. SmartCard is ready.
```

Vous pouvez également désactiver les cartes à puce en exécutant le script ctxsmartlogon.sh :

```
1 sudo /opt/Citrix/VDA/sbin/ctxsmartlogon.sh
2 <!--NeedCopy-->
```

Les résultats ressemblent à ce qui suit :

```
#************************************************************************
# ctxsmartlogon.sh sets up smart card logon for the Linux VDA, which
# includes automatic installation of the necessary packages and changes to
# the configuration files.
#
# Note:
# The ctxsmartlogon.sh adds pkinit information to the default realm. You can
# change this setting through the /etc/krb5.conf configuration file.
#************************************************************************
Step 1:Enable smart card logon.
  Do you want enable smart card logon? (y/n)[y] n
ctxsmartlogon.sh exit.
```

(Option 2) Configurer manuellement l'environnement de carte à puce Le Linux VDA utilise le même environnement de carte à puce que le VDA Windows. Dans l'environnement, plusieurs composants doivent être configurés, notamment le contrôleur de domaine, l'autorité de certification Microsoft (CA), Internet Information Services, Citrix StoreFront et l'application Citrix Workspace. Pour plus d'informations sur la configuration basée sur la carte à puce YubiKey, consultez l'article CTX206156 du centre de connaissances.

Avant de passer à l'étape suivante, assurez-vous que :

- Vous avez correctement configuré tous les composants.
- Vous avez téléchargé la clé privée et le certificat utilisateur sur la carte à puce.

- Vous pouvez vous connecter avec succès au VDA à l'aide de la carte à puce.

Installer les packages PC/SC Lite PCSC Lite est une mise en œuvre de la spécification PC/SC (Personal Computer/Smart Card) sous Linux. Il fournit une interface de carte à puce Windows pour communiquer avec les cartes à puce et les lecteurs. La redirection de carte à puce dans le Linux VDA est implémentée au niveau PC/SC.

Exécutez la commande suivante pour installer les packages PC/SC Lite :

RHEL 8, Rocky Linux 8, RHEL 7/CentOS 7 :

```
yum install pcsc-lite pcsc-lite-ccid pcsc-lite-libs
<!--NeedCopy-->
```

Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04, Debian 11.3 :

```
apt-get install -y libpcsclite1 libccid
<!--NeedCopy-->
```

Installer le pilote de la carte à puce OpenSC est un pilote de carte à puce largement utilisé. Si CoolKey n'est pas installé, exécutez la commande suivante pour l'installer :

RHEL 8, Rocky Linux 8, RHEL 7/CentOS 7 :

```
yum install opensc
<!--NeedCopy-->
```

Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04, Debian 11.3 :

```
apt-get install -y opensc
<!--NeedCopy-->
```

Installer les modules PAM pour l'authentification par carte à puce Exécutez la commande suivante pour installer les modules pam_krb5 et krb5-pkinit.

RHEL 7/CentOS 7 :

```
yum install pam_krb5 krb5-pkinit
<!--NeedCopy-->
```

RHEL 8, Rocky Linux 8 :

```
yum install krb5-pkinit
<!--NeedCopy-->
```

Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04 :


```
apt-get install libpam-krb5 krb5-pkinit
<!--NeedCopy-->
```

Debian 11.3 :

```
apt-get install -y libpam-krb5 krb5-pkinit
<!--NeedCopy-->
```

Le module pam_krb5 est un module d'authentification enfichable (PAM). Les applications compatibles PAM peuvent utiliser pam_krb5 pour vérifier les mots de passe et obtenir des tickets d'attribution de tickets auprès du centre de distribution de clés (KDC). Le module krb5-pkinit contient le plugin PKINIT qui permet aux clients d'obtenir les informations d'identification initiales depuis le KDC à l'aide d'une clé privée et d'un certificat.

Configurer le module pam_krb5 Le module pam_krb5 interagit avec le KDC pour obtenir des tickets Kerberos à l'aide des certificats de la carte à puce. Pour activer l'authentification pam_krb5 dans PAM, exécutez la commande suivante :

```
authconfig --enablekrb5 --update
<!--NeedCopy-->
```

Dans le fichier de configuration **/etc/krb5.conf**, ajoutez des informations PKINIT en fonction du domaine réel.

> **Remarque :**
>
> L'option **pkinit_cert_match** spécifie les règles de correspondance auxquelles le certificat client doit répondre avant qu'il ne soit utilisé pour tenter l'authentification PKINIT. La syntaxe des règles de correspondance est :
>
> **relation-operator component-rule...**
>
> où **relation-operator** peut être **&&**, ce qui signifie que toutes les règles du composant doivent correspondre, ou **||**, ce qui signifie qu'une seule règle doit correspondre.

Voici un exemple de fichier krb5.conf générique :

```
EXAMPLE.COM = {


    kdc = KDC.EXAMPLE.COM

    auth_to_local = RULE:[1:$1@$0]

    pkinit_anchors = FILE:<path where you install the root certificate
       >/certnew.pem

    pkinit_kdc_hostname = KDC.EXAMPLE.COM
```



```
11
12      pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature
13
14      pkinit_eku_checking = kpServerAuth
15
16    }
17
18  <!--NeedCopy-->
```

Le fichier de configuration ressemble à ce qui suit une fois que vous avez ajouté les informations PKINIT.

```
CTXDEV.LOCAL = {
     kdc = ctx-ad.ctxdev.local
     auth_to_local = RULE:[1:$1@$0]
     pkinit_kdc_hostname = ctx-ad.ctxdev.local
     pkinit_anchors = FILE:/etc/pki/CA/certs/certnew.pem
     pkinit_eku_checking = kpServerAuth
     pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature
}
```

Configurer l'authentification PAM Les fichiers de configuration PAM indiquent les modules qui sont utilisés pour l'authentification PAM. Pour ajouter pam_krb5 en tant que module d'authentification, ajoutez la ligne suivante au fichier **/etc/pam.d/smartcard-auth** :

```
auth [success=done ignore=ignore default=die] pam_krb5.so preauth_options
=X509_user_identity=PKCS11:<path to the pkcs11 driver>/opensc-pkcs11.
so
```

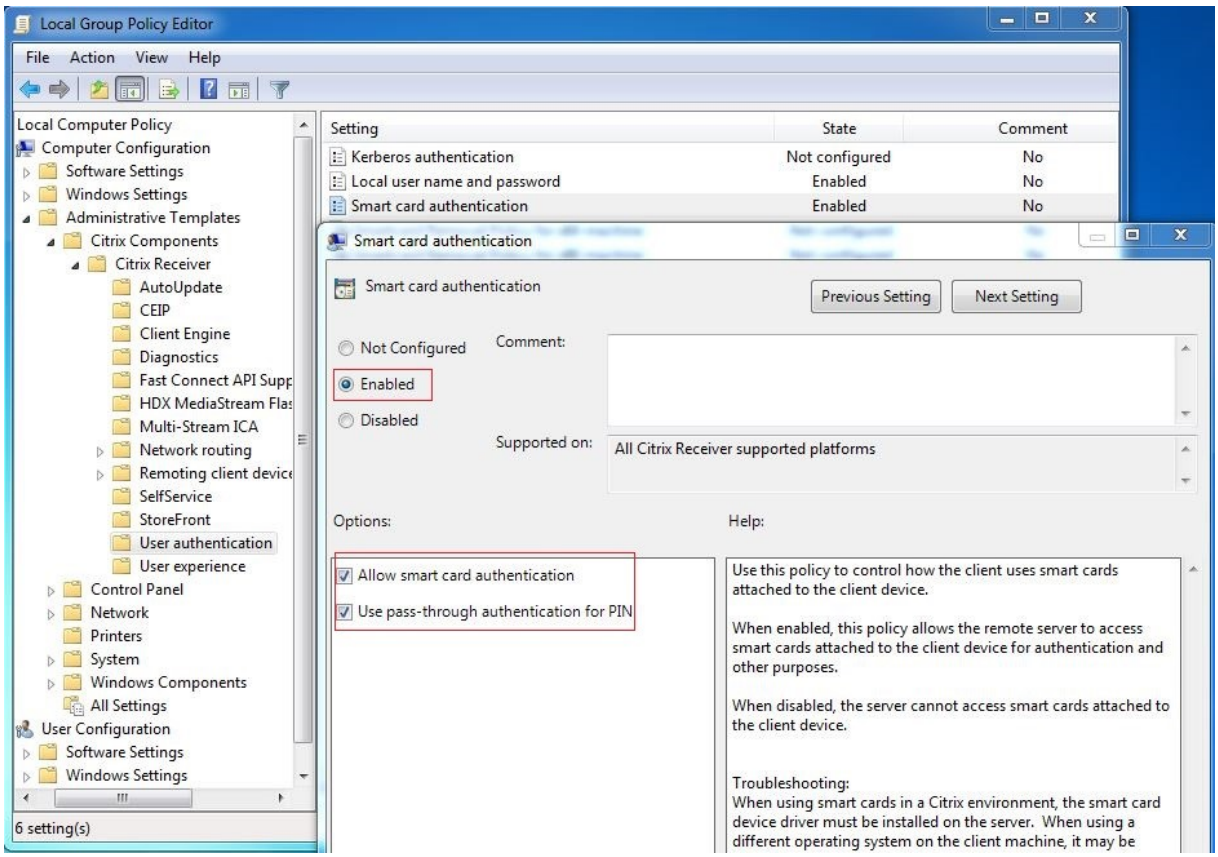
Le fichier de configuration ressemble à ce qui suit après les modifications si SSSD est utilisé.

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        [success=done ignore=ignore default=die]  pam_krb5.so preauth_opt=X509_user_identity=PKCS11:/usr/lib/x86_64-linux-gnu/pkcs11/opensc-pkcs11.so
auth        sufficient    pam_permit.so
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     [default=bad success=ok auth_err=ignore user_unknown=ignore ignore=ignore]  pam_krb5.so
account     required      pam_permit.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
#session     optional      pam_oddjob_mkhomedir.so umask=0077
session     optional      pam_mkhomedir.so umask=0077
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
session     optional      pam_sss.so
session     optional      pam_krb5.so
```


(Facultatif) Single Sign-On avec cartes à puce

Citrix Single Sign-On (SSO) est une fonctionnalité qui implémente l'authentification unique lors du lancement de bureaux virtuels et d'applications. Cette fonctionnalité réduit le nombre de fois que les utilisateurs entrent leur code PIN. Pour utiliser l'authentification SSO avec le Linux VDA, configurez l'application Citrix Workspace. La configuration est la même avec le VDA Windows. Pour plus d'informations, consultez l'article CTX133982 du centre de connaissances.

Activez l'authentification par carte à puce comme suit lors de la configuration de la stratégie de groupe dans l'application Citrix Workspace.



Connexion par carte à puce rapide

La carte à puce rapide constitue une amélioration par rapport à la redirection de carte à puce PC/SC HDX existante. Elle améliore les performances lorsque les cartes à puce sont utilisées dans des environnements WAN à latence élevée. Pour plus d'informations, veuillez consulter la section Cartes à puce.

Le Linux VDA prend en charge les cartes à puce rapides sur les versions suivantes de l'application Citrix Workspace :

- Citrix Receiver pour Windows 4.12
- Application Citrix Workspace 1808 pour Windows et versions ultérieures

Activer une connexion par carte à puce rapide sur le client La connexion par carte à puce rapide est activée par défaut sur le VDA et désactivée par défaut sur le client. Sur le client, pour activer la connexion par carte à puce rapide, incluez le paramètre suivant dans le fichier default.ica du site StoreFront associé :

```
[WFClient]
SmartCardCryptographicRedirection=On
<!--NeedCopy-->
```

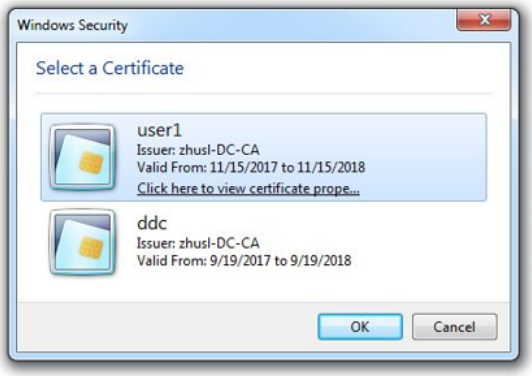
Désactiver une connexion par carte à puce rapide sur le client Pour désactiver la connexion par carte à puce rapide sur le client, supprimez le paramètre **SmartCardCryptographicRedirection** dans le fichier default.ica du site StoreFront associé.

Utilisation

Se connecter au Linux VDA en utilisant une carte à puce

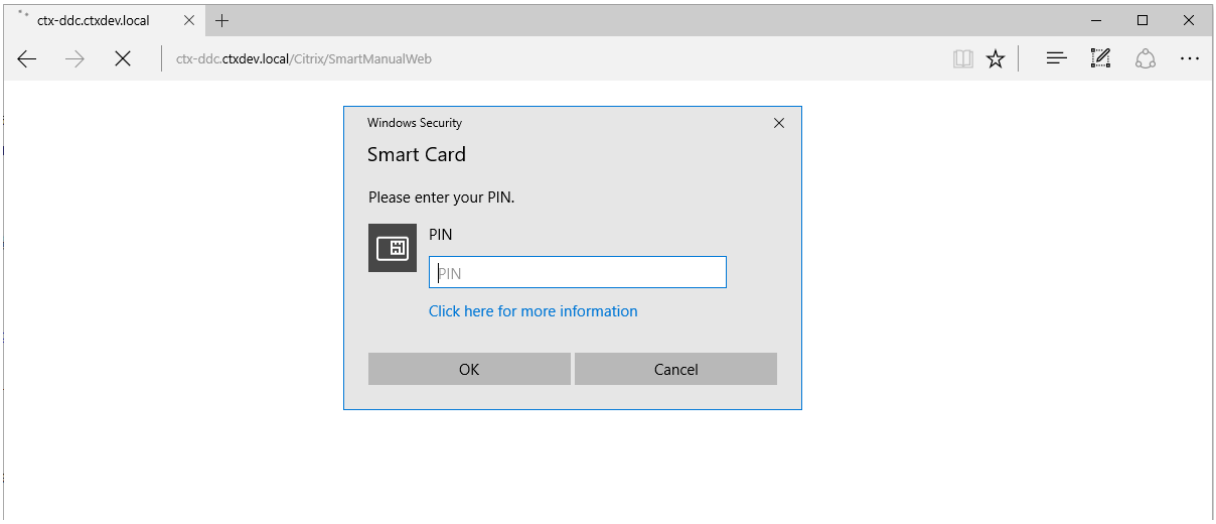
Vous pouvez utiliser une carte à puce pour vous connecter au Linux VDA dans les scénarios SSO et non SSO.

- Dans le scénario SSO, vous êtes automatiquement connecté à StoreFront avec le certificat et le code PIN de la carte à puce mis en cache. Lorsque vous lancez une session de bureau virtuel Linux dans StoreFront, le code PIN est transmis au Linux VDA pour l'authentification par carte à puce.
- Dans le scénario non SSO, vous êtes invités à sélectionner un certificat et à entrer un code PIN pour vous connecter à StoreFront.



Lorsque vous lancez une session de bureau virtuel Linux dans StoreFront, une boîte de dialogue de connexion au Linux VDA apparaît comme suit. Le nom d'utilisateur est extrait du certificat dans la carte à puce et vous devez le saisir de nouveau pour l'authentification de connexion.

Le comportement est le même avec le VDA Windows.



Se reconnecter à une session en utilisant une carte à puce

Pour vous reconnecter à une session, assurez-vous que la carte à puce est connectée à la machine cliente. Sinon, une fenêtre de mise en cache grise apparaît du côté du Linux VDA et se ferme rapidement car la ré-authentification échoue si la carte à puce n'est pas connectée. Aucune autre invite ne s'affiche dans ce cas pour vous rappeler de connecter la carte à puce.

Du côté de StoreFront, cependant, si une carte à puce n'est pas connectée lorsque vous vous reconnectez à une session, le site Web StoreFront peut afficher une alerte comme suit.

Limitation

Stratégie de retrait de carte à puce

Actuellement, le Linux VDA utilise uniquement le comportement par défaut pour le retrait de la carte à puce. Lorsque vous retirez la carte à puce après vous être connecté au Linux VDA, la session reste connectée et l'écran de session n'est pas verrouillé.

Prise en charge des autres cartes à puce et de la bibliothèque PKCS#11

Citrix fournit une solution générique de redirection de carte à puce. Bien que seule la carte à puce OpenSC soit répertoriée dans notre liste de prise en charge, vous pouvez essayer d'utiliser d'autres cartes à puce et la bibliothèque PKCS #11. Pour passer à votre carte à puce spécifique ou à la bibliothèque PKCS#11 :

1. Remplacez toutes les instances `opensc-pkcs11.so` par votre bibliothèque PKCS#11.
2. Pour définir le chemin d'accès de votre bibliothèque PKCS#11 sur le Registre, exécutez la commande suivante :

   ```
   /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
      CurrentControlSet\Control\Citrix\VirtualChannels\Scard" -v "
      PKCS11LibPath" -d "PATH"
   <!--NeedCopy-->
   ```

   où **PATH pointe vers** votre bibliothèque PKCS #11 telle que /usr/lib64/pkcs11/opensc-pkcs11.so
3. Désactivez la connexion par carte à puce rapide sur le client.

Sessions non authentifiées par des utilisateurs anonymes

April 18, 2024

Utilisez les informations de cet article pour configurer des sessions non authentifiées. Aucun paramètre spécial n'est requis lors de l'installation de Linux VDA pour utiliser cette fonctionnalité.

> **Remarque :**
>
> Lorsque vous configurez des sessions non authentifiées, n'oubliez pas que le pré-lancement de session n'est pas pris en charge. Le prélancement de session n'est pas non plus pris en charge sur l'application Citrix Workspace pour Android.

Créer un magasin non authentifié

Vous devez créer un magasin non authentifié à l'aide de StoreFront pour prendre en charge une session non authentifiée sur l'agent Linux VDA.

Autoriser les utilisateurs non authentifiés dans un groupe de mise à disposition

Après la création d'un magasin non authentifié, activez les utilisateurs non authentifiés dans un groupe de mise à disposition pour prendre en charge une session non authentifiée. Pour activer les utilisateurs non authentifiés dans un groupe de mise à disposition, suivez les instructions de la documentation Citrix Virtual Apps and Desktops.

Définir le délai d'inactivité de sessions non authentifiées

Une session non authentifiée a un délai d'inactivité par défaut de 10 minutes. Cette valeur est configurée avec le paramètre de registre **AnonymousUserIdleTime**. Utilisez l'outil **ctxreg** pour modifier cette valeur. Par exemple, pour définir ce paramètre de registre sur cinq minutes, procédez comme suit :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
    CurrentControlSet\Control\Citrix" -v AnonymousUserIdleTime -d 0
    x00000005
2 <!--NeedCopy-->
```

Définir le nombre maximal d'utilisateurs non authentifiés

Pour définir le nombre maximal d'utilisateurs non authentifiés, utilisez la clé de registre **MaxAnonymousUserNumber**. Ce paramètre limite le nombre de sessions non authentifiées s'exécutant simultanément sur un seul agent Linux VDA. Utilisez l'outil **ctxreg** pour configurer ce paramètre de registre. Par exemple, pour définir la valeur sur 32 bits :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
    CurrentControlSet\Control\Citrix" -v MaxAnonymousUserNumber -d 0
    x00000020
2 <!--NeedCopy-->
```

> **Important :**
>
> Limitez le nombre de sessions non authentifiées. Le lancement d'un trop grand nombre de sessions simultanées peut entraîner des problèmes sur le VDA, y compris la saturation de la mémoire.

Résolution des problèmes

Tenez compte des éléments suivants lors de la configuration de sessions non authentifiées :

- **Impossible de se connecter à une session non authentifiée**.

Vérifiez que le registre a été mis à jour comme suit (défini sur 0):

```
sudo /opt/Citrix/VDA/bin/ctxreg read -k "HKLM\System\CurrentControlSet
    \Control\Citrix" -v MaxAnonymousUserNumber
<!--NeedCopy-->
```

Vérifiez que le service **ncsd** est en cours d'exécution et qu'il est configuré pour activer le cache **passwd** :

```
ps uax | grep nscd
cat /etc/nscd.conf | grep 'passwd' | grep 'enable-cache'
<!--NeedCopy-->
```

Définissez la variable du cache **passwd** sur **no** s'il est activé, puis redémarrez le service **ncsd**. Vous devrez peut-être réinstaller le Linux VDA après la modification de cette configuration.

- **Le bouton de l'écran de verrouillage est affiché dans une session non authentifiée avec KDE**.

Le bouton et le menu de l'écran de verrouillage sont désactivés par défaut dans une session non authentifiée. Toutefois, ils peuvent toujours être visibles dans KDE. Dans KDE, pour désactiver le bouton et le menu de l'écran de verrouillage pour un utilisateur spécifique, ajoutez les lignes suivantes au fichier de configuration **$Home/.kde/share/config/kdeglobals**. Par exemple :

```
[KDE Action Restrictions]
action/lock_screen=false
<!--NeedCopy-->
```

Toutefois, si le paramètre `KDE Action Restrictions` est configuré comme non modifiable dans un fichier `kdeglobals` global volumineux tel que `/usr/share/kde-settings/kde-profile/default/share/config/kdeglobals`, la configuration utilisateur n'a aucun effet.

Pour résoudre ce problème, modifiez le fichier `kdeglobals` à l'échelle du système pour supprimer la balise `[$i]` dans la section `[KDE Action Restrictions]`, ou utilisez directement la configuration à l'échelle du système pour désactiver le bouton et le menu de l'écran de verrouillage. Pour de plus amples informations sur la configuration KDE, consultez la page KDE System Administration/Kiosk/Keys.

Fichier

December 16, 2022

Cette section contient les rubriques suivantes :

- Copier-coller de fichiers
- Transfert de fichiers

Copier-coller de fichiers

December 16, 2022

Les utilisateurs peuvent copier et coller des fichiers entre une session et un client local à l'aide du menu contextuel ou des raccourcis clavier. Cette fonctionnalité nécessite Citrix Virtual Apps and Desktops 2006 ou version ultérieure et l'application Citrix Workspace 1903 ou ultérieure pour Windows.

Pour copier et coller des fichiers avec succès, assurez-vous que :

- Le nombre maximal de fichiers ne dépasse pas 20.
- La taille maximale des fichiers ne dépasse pas 200 Mo.
- Le gestionnaire de fichiers Nautilus est disponible sur la machine sur laquelle vous avez installé le Linux VDA.

Distributions Linux prises en charge

La **fonction de copier-coller des fichiers** est disponible pour toutes les distributions Linux prises en charge par le Linux VDA.

Stratégies pertinentes

Les stratégies de presse-papiers suivantes sont pertinentes pour la configuration de la fonctionnalité. Pour plus d'informations sur les stratégies de presse-papiers, consultez la section Liste des stratégies prises en charge.

- Redirection de Presse-papiers client
- Mode de mise à jour de la sélection du Presse-papiers
- Mode de mise à jour de la sélection principale

> **Remarque :**
>
> Pour désactiver la fonction de copier-coller des fichiers, définissez la stratégie de **Redirection du Presse-papiers client** sur **Interdit** dans Citrix Studio.

Limitations

- La fonction Couper n'est pas prise en charge. Les opérations Couper d'un fichier sont traitées comme une opération de copie.
- La fonction Glisser-déposer n'est pas prise en charge.
- La copie des répertoires n'est pas prise en charge.
- Le copier-coller des fichiers doit être effectué de manière séquentielle. Ce n'est qu'une fois que le fichier précédent a été copié et collé avec succès que le fichier suivant peut être copié.

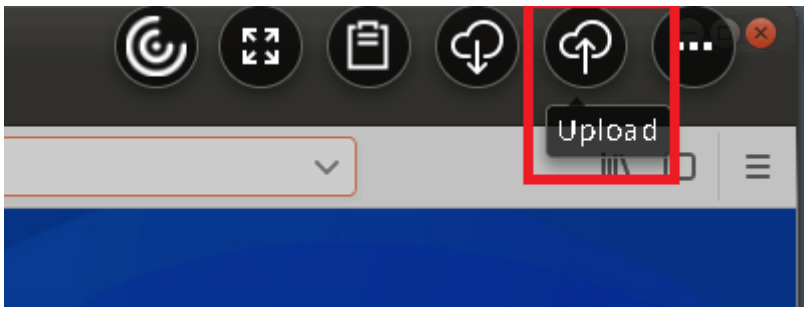
Transfert de fichiers

December 16, 2022

Le transfert de fichiers est pris en charge entre le Linux VDA et le périphérique client. Cette fonctionnalité est disponible lorsque le périphérique client exécute un navigateur Web qui prend en charge l'attribut sandbox HTML5. L'attribut sandbox HTML5 permet aux utilisateurs d'accéder à des applications et des bureaux virtuels à l'aide de l'application Citrix Workspace pour HTML5 ou pour Chrome.

> **Remarque :**
>
> le transfert de fichiers est disponible pour l'application Citrix Workspace pour HTML5 et Chrome.

Dans les sessions d'application et de bureau publiées, le transfert de fichiers permet le chargement et le téléchargement de fichiers entre le VDA Linux et la machine cliente. Pour télécharger des fichiers depuis la machine cliente vers le VDA Linux, cliquez sur l'icône **Charger** dans la barre d'outils de l'application Citrix Workspace et sélectionnez le fichier souhaité dans les boîtes de dialogue de fichiers. Pour télécharger des fichiers à partir du VDA Linux sur la machine cliente, cliquez sur l'icône **Télécharger**. Vous pouvez ajouter des fichiers lors du chargement ou du téléchargement. Vous pouvez transférer jusqu'à 100 fichiers en même temps.



> **Remarque :**
>
> pour charger et télécharger des fichiers entre le VDA Linux et la machine cliente, activez la barre d'outils de l'application Citrix Workspace.
> Vous pouvez utiliser une version de l'application Citrix Workspace qui vous permet de glisser-déposer des fichiers.

Le téléchargement automatique est une amélioration du transfert de fichiers. Les fichiers que vous téléchargez ou déplacez vers le répertoire **Enregistrer sur mon appareil** sur le VDA sont automatiquement transférés sur la machine cliente.

> **Remarque :**
>
> Le téléchargement automatique nécessite que les stratégies **Autoriser le transfert de fichiers entre le bureau et le client** et **Télécharger des fichiers depuis le bureau** soient définies sur **Autorisé**.

Voici quelques cas d'utilisation pour le téléchargement automatique :

- Télécharger des fichiers vers le répertoire **Enregistrer sur mon appareil**

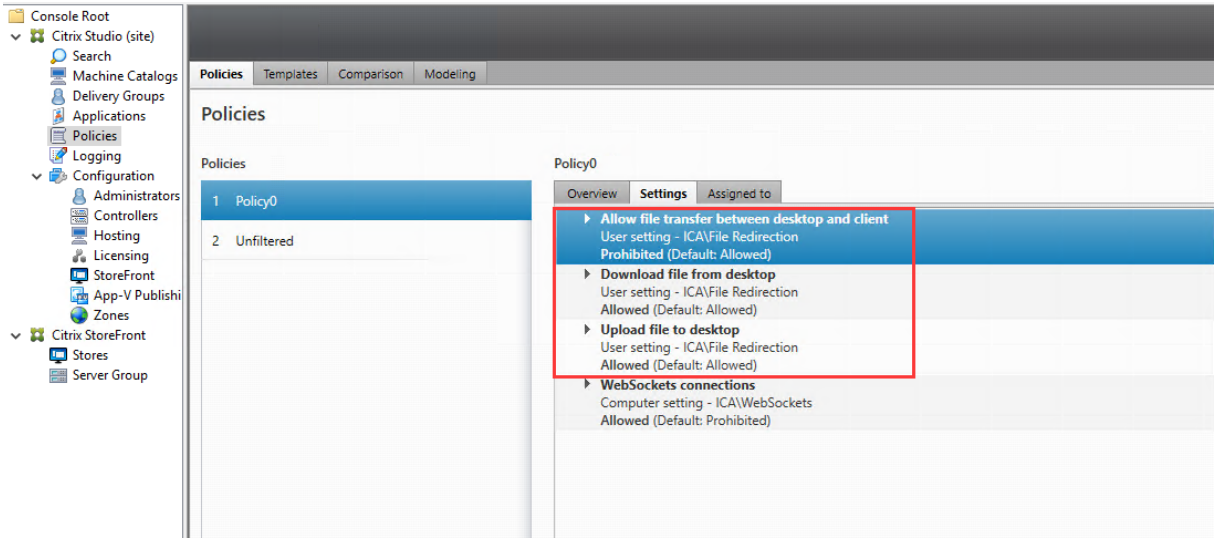
  Dans les sessions d'applications de bureau et de navigateur Web publiées, les fichiers que vous téléchargez à partir de sites Web peuvent être enregistrés dans le répertoire **Enregistrer sur mon appareil** du VDA pour un transfert automatique vers la machine cliente. Pour effectuer le téléchargement automatique, définissez le répertoire de téléchargement par défaut du navigateur Web en session sur **Enregistrer sur mon appareil** et définissez un répertoire de téléchargement local dans le navigateur Web qui exécute votre application Citrix Workspace pour HTML5 ou Chrome.

- Déplacer ou copier des fichiers vers **Enregistrer sur mon appareil**

  Dans les sessions de bureau publiées, choisissez les fichiers cibles et déplacez-les ou copiez-les dans le répertoire **Enregistrer sur mon appareil** pour qu'ils soient disponibles sur la machine cliente.

Stratégies de transfert de fichiers

Vous pouvez utiliser Citrix Studio pour définir les stratégies de transfert de fichiers. Par défaut, le transfert de fichiers est activé.



Descriptions des stratégies :

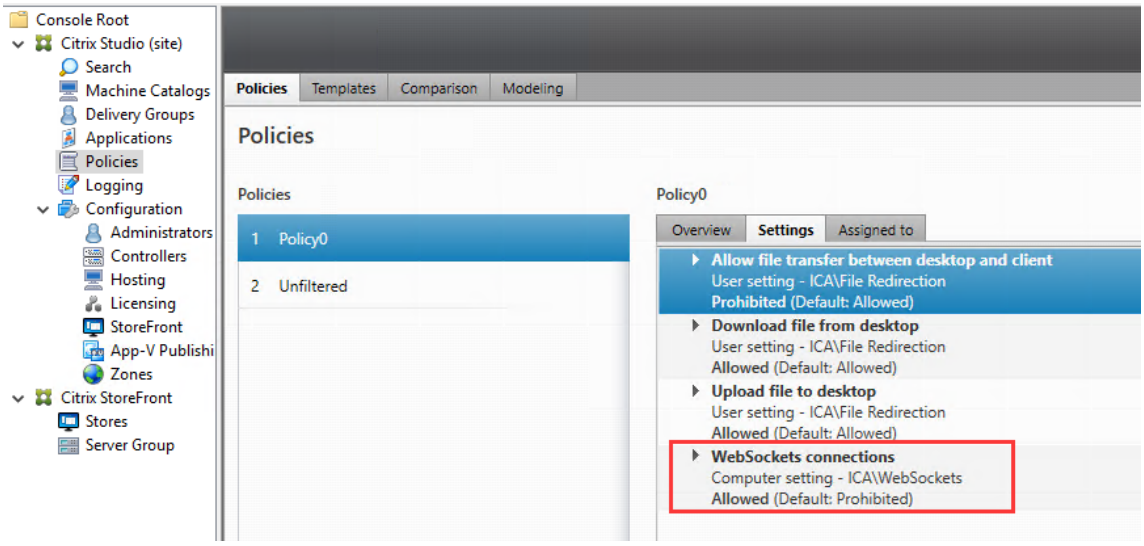
- **Autoriser le transfert de fichiers entre le bureau et le client.** Autorise ou empêche les utilisateurs de transférer des fichiers entre une session Citrix Virtual Apps and Desktops et leurs appareils.
- **Télécharger des fichiers depuis le bureau.** Autorise ou empêche les utilisateurs de télécharger des fichiers depuis une session Citrix Virtual Apps and Desktops vers leurs appareils.
- **Charger des fichiers sur le bureau.** Autorise ou empêche les utilisateurs de charger des fichiers depuis leurs appareils sur une session Citrix Virtual Apps and Desktops.

> **Remarque :**
>
> pour vous assurer que les stratégies **Télécharger des fichiers depuis le bureau** et **Charger des fichiers sur le bureau** prennent effet, définissez l'option **Autoriser le transfert de fichiers entre le bureau et le client** sur **Autorisé**.

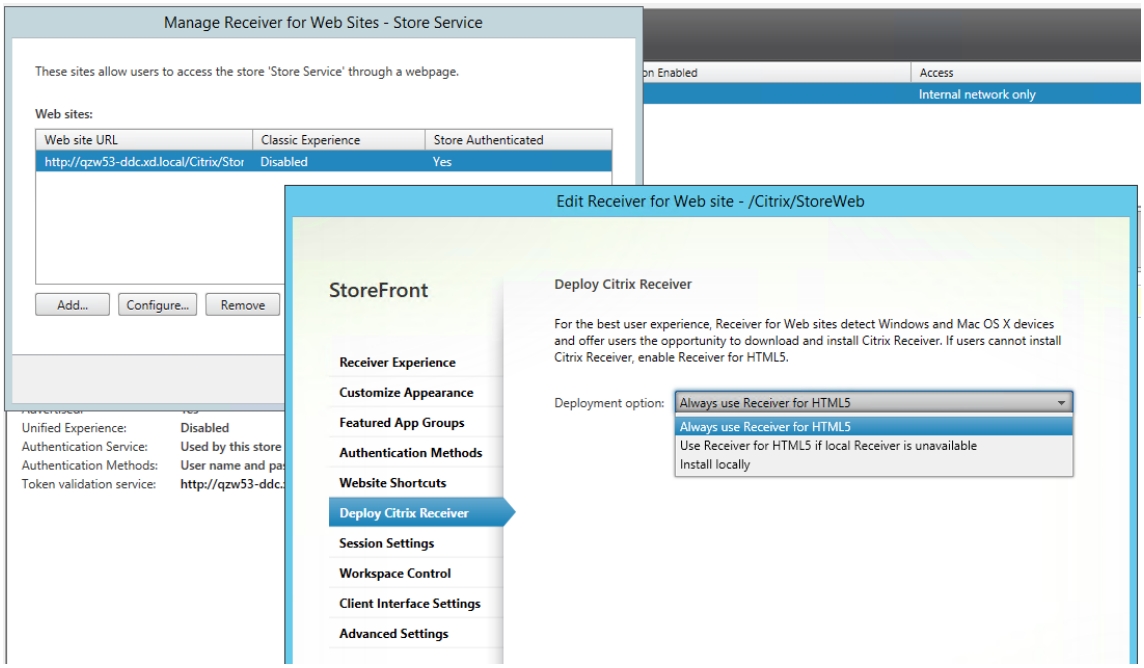
Utilisation

Pour utiliser la fonctionnalité de transfert de fichiers via l'application Citrix Workspace pour HTML5 :

1. Dans Citrix Studio, définissez la stratégie **Connexions WebSockets** sur **Autorisé**.



2. Dans Citrix Studio, activez le transfert de fichiers via les stratégies de transfert de fichiers décrites précédemment.
3. Dans la console de gestion Citrix StoreFront, cliquez sur **Magasins**, sélectionnez le nœud **Gérer les sites Receiver pour Web** et activez Citrix Receiver pour HTML5 en sélectionnant l'option **Toujours utiliser Receiver pour HTML5**.



4. Lancez une session de bureau virtuel ou d'application de navigateur Web. Effectuez un ou plusieurs transferts de fichiers entre le VDA Linux et votre machine cliente.

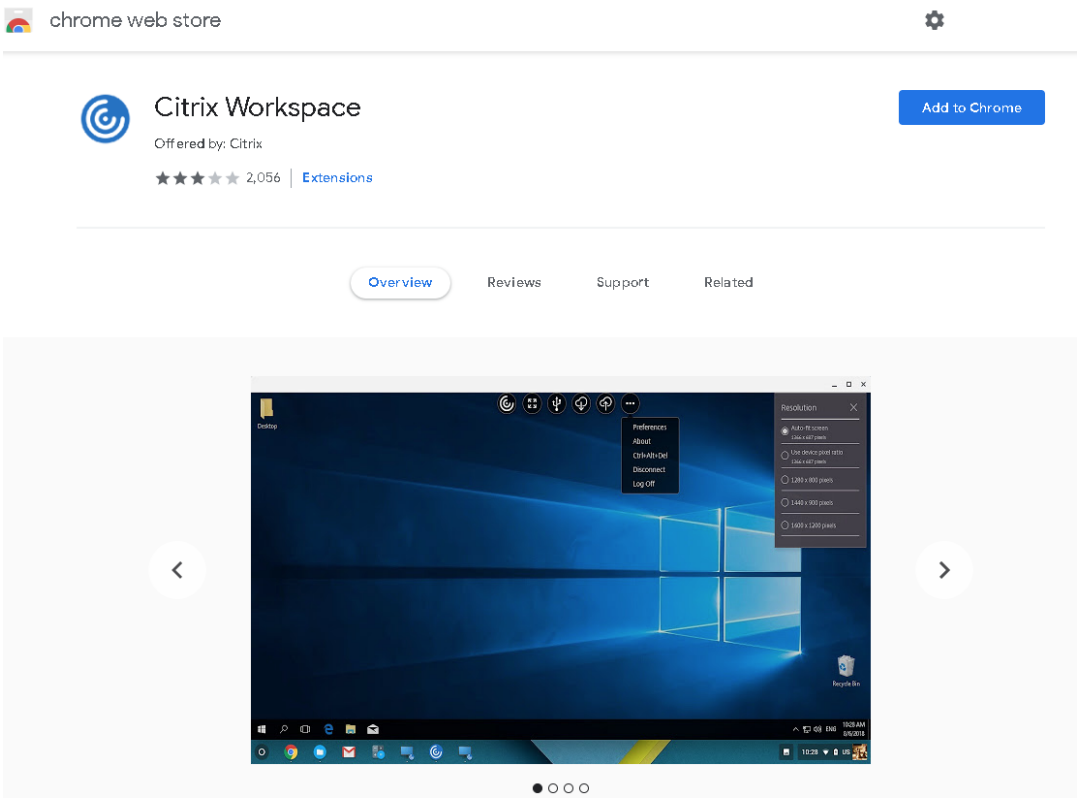
Pour utiliser la fonctionnalité de transfert de fichiers via l'application Citrix Workspace pour Chrome :

1. Activez le transfert de fichiers via les stratégies de transfert de fichiers décrites précédemment.
2. Obtenez l'application Citrix Workspace à partir de Chrome Web Store.

   Ignorez cette étape si vous avez déjà ajouté l'application Citrix Workspace pour Chrome à la page des applications Chrome.

   a) Tapez **Citrix Workspace for Chrome** dans la zone de recherche de Google Chrome. Cliquez sur l'icône de recherche.

   b) Parmi les résultats de la recherche, cliquez sur l'URL du Chrome Web Store où l'application Citrix Workspace est disponible.



   c) Cliquez sur **Ajouter à Chrome** pour ajouter l'application Citrix Workspace à Google Chrome.

3. Cliquez sur l'application Citrix Workspace pour Chrome sur la page des applications Chrome.
4. Tapez l'URL de votre magasin StoreFront pour la connexion.

   Ignorez cette étape si vous avez déjà saisi l'URL.

5. Lancez une session de bureau virtuel ou d'application. Effectuez un ou plusieurs transferts de fichiers entre le VDA Linux et votre machine cliente.

Graphiques

December 16, 2022

Cette section contient les rubriques suivantes :

- Mise à l'échelle DPI automatique
- Affichage de l'état de la batterie client
- Configuration et réglage précis des graphiques
- Partage d'écran HDX
- Cartes graphiques non vGPU
- Filigrane de session
- Affichage progressif Thinwire

Mise à l'échelle DPI automatique

April 18, 2024

Le Linux VDA prend en charge la mise à l'échelle DPI automatique. Lorsqu'un utilisateur ouvre une session d'application ou de bureau virtuel, la valeur DPI de la session change automatiquement pour correspondre au paramètre DPI du côté client.

Quelques points à prendre en compte sur cette fonctionnalité :

- Cette fonctionnalité nécessite que vous activiez la correspondance DPI pour Citrix Workspace. Dans le cas de l'application Citrix Workspace pour Windows, assurez-vous que l'option **Non, utiliser la résolution native** est sélectionnée. Pour plus d'informations sur la configuration de la mise à l'échelle DPI pour l'application Citrix Workspace pour Windows, consultez la section Mise à l'échelle DPI.
- Pour qu'elle fonctionne dans des scénarios multi-écrans, chaque moniteur doit être configuré avec le même paramètre DPI. Les scénarios DPI mixtes ne sont pas pris en charge Si les moniteurs sont configurés avec des paramètres DPI différents, le Linux VDA applique la plus petite valeur DPI à tous les écrans.
- La fonctionnalité est activée pour MATE, GNOME, GNOME Classic et KDE. Lorsque vous utilisez KDE ou MATE, tenez compte des points suivants :
  - Pour les bureaux virtuels Linux s'exécutant dans un environnement de bureau KDE :

    * Nous recommandons d'utiliser KDE Plasma 5 ou une version ultérieure.
    * La modification des paramètres DPI côté client pendant l'exécution des sessions oblige les utilisateurs à se déconnecter puis à se reconnecter.
  - Pour les bureaux virtuels Linux s'exécutant dans un environnement de bureau MATE :
    * Seuls les facteurs d'échelle de 1 et 2 sont pris en charge.
    * La modification des paramètres DPI côté client pendant l'exécution des sessions oblige les utilisateurs à se déconnecter puis à se reconnecter.

- La valeur DPI de la session virtuelle change automatiquement en fonction du paramètre DPI du côté client. Actuellement, la fonctionnalité prend uniquement en charge les facteurs d'échelle de type entier, par exemple 100 % et 200 %. Si le facteur d'échelle configuré côté client est de type fractionnaire, le paramètre DPI de la session virtuelle passe à un facteur d'échelle entier conformément au tableau suivant. Exemple : si le facteur d'échelle est de 125 %, la valeur DPI passe à 100 %.

Facteur d'échelle côté client	DPI de la session distante
Inférieur ou égal à 174 %	96 (1 x 96)
175 %–274 %	192 (2 x 96)
275 %–399 %	288 (3 x 96)
Supérieur ou égal à 400 %	384 (4 x 96)

Affichage de l'état de la batterie client

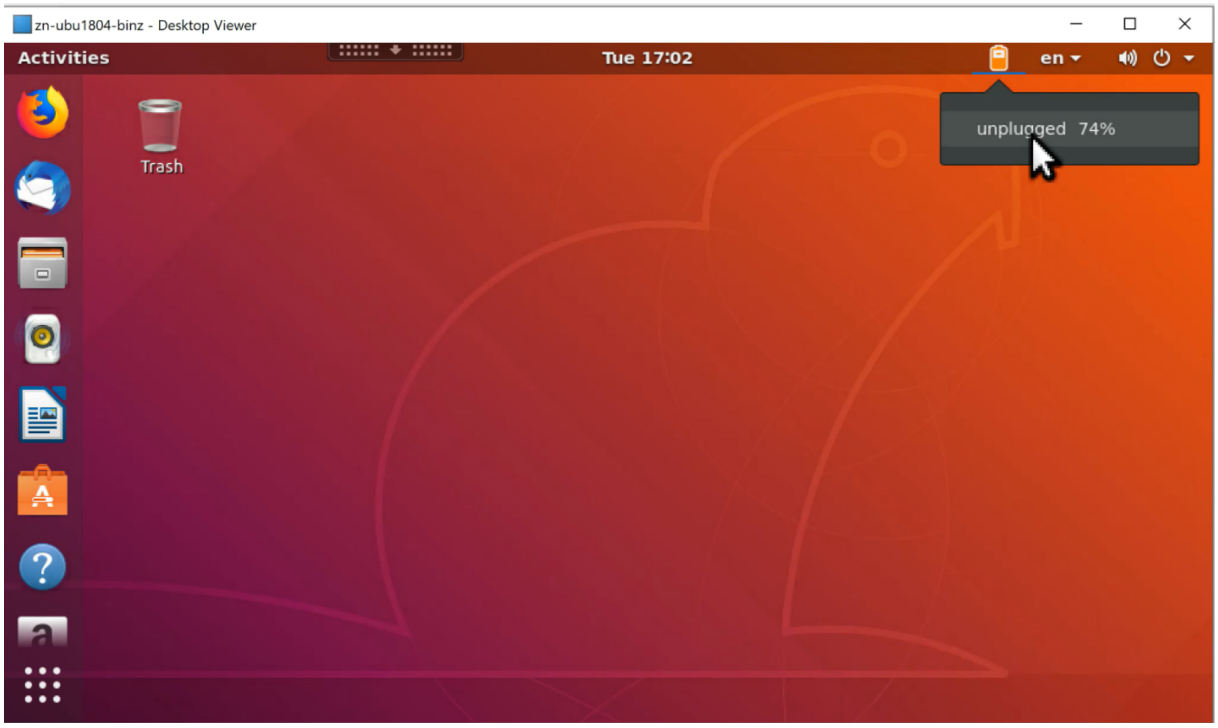
December 16, 2022

Le Linux VDA peut rediriger et afficher l'état de la batterie des machines clientes dans les bureaux virtuels. Cette fonctionnalité est activée par défaut et disponible pour les versions suivantes de l'application Citrix Workspace :

- Application Citrix Workspace pour iOS
- Application Citrix Workspace pour Linux
- Application Citrix Workspace pour Mac (la version 2204.1 n'est pas prise en charge)
- Application Citrix Workspace pour Windows (la version 2204.1 n'est pas prise en charge)

Vue d'ensemble

Lorsque les utilisateurs ouvrent un bureau virtuel, ils peuvent voir une icône de batterie dans la barre d'état système Linux. Cette icône indique l'état de la batterie de leurs appareils clients. Pour vérifier le pourcentage d'autonomie restante de la batterie, cliquez sur l'icône de la batterie. Pour obtenir un exemple, consultez la capture d'écran suivante :



Différentes icônes de batterie indiquent différents états. Pour en savoir plus, consultez le tableau suivant :

Icône de batterie	État de charge	Niveau d'autonomie restante	Pourcentage d'autonomie restante
	En cours de charge, indiqué par un symbole « + »	Élevé, indiqué par une couleur verte	=80 %
	En cours de charge, indiqué par un symbole « + »	Moyen, indiqué par une couleur ambrée	= 20 % et <80 %
	En cours de charge, indiqué par un symbole « + »	Faible, indiqué par une couleur rouge	< 20 %

Icône de batterie	État de charge	Niveau d'autonomie restante	Pourcentage d'autonomie restante
	Pas en cours de charge, indiqué par un symbole « + »	Élevé, indiqué par une couleur verte	=80 %
	Pas en cours de charge, indiqué par un symbole « + »	Moyen, indiqué par une couleur ambrée	= 20 % et <80 %
	Pas en cours de charge, indiqué par un symbole « + »	Faible, indiqué par une couleur rouge	< 20 %
	Inconnu	Inconnu	Inconnu

Configuration

L'affichage de l'état de la batterie client est activé par défaut.

Pour désactiver cette fonctionnalité, exécutez la commande suivante :

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\
   Control\Citrix\VirtualChannels\MrVc"  -v "Enabled" -d "0x00000000"
<!--NeedCopy-->
```

Pour activer cette fonctionnalité, exécutez la commande suivante :

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\
   Control\Citrix\VirtualChannels\MrVc"  -v "Enabled" -d "0x00000001"
<!--NeedCopy-->
```

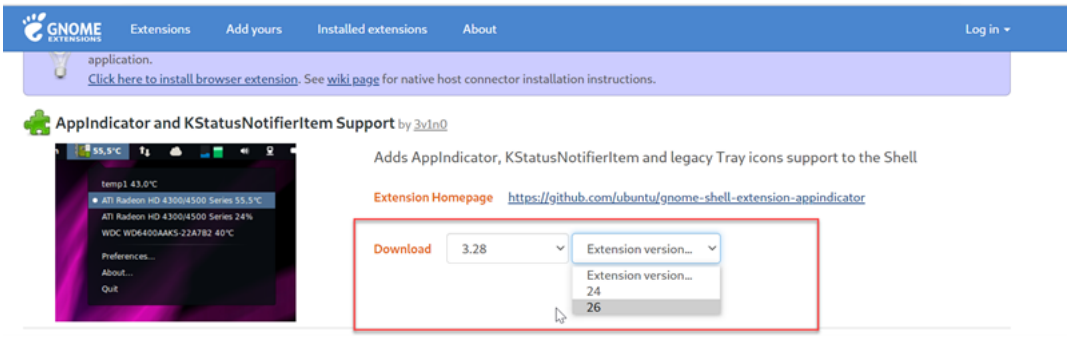
> **Remarque :**
>
> Les commandes précédentes ont un impact sur la fonction de clavier logiciel, qui partage le canal virtuel du récepteur mobile (MRVC) avec l'affichage de l'état de la batterie du client.

En fonction de votre distribution, suivez les étapes supplémentaires suivantes :

1. Si vous utilisez RHEL 8.x ou SUSE 15.x installé avec GNOME, installez une extension compatible pour votre shell GNOME pour activer la prise en charge d'AppIndicator :

a) Exécutez la commande `gnome-shell --version` pour vérifier votre version du shell GNOME.

b) Téléchargez une extension compatible pour votre shell GNOME depuis https://extensions.gnome.org/extension/615/appindicator-support. Par exemple, si votre version du shell est 3.28, vous pouvez sélectionner 24 ou 26 pour la version d'extension.



c) Décompressez le package téléchargé. Vérifiez que la valeur **uuid** dans le fichier **metadata.json** du package est définie sur **appindicatorsupport@rgcjonas.gmail.com**.

d) Exécutez la commande `mv` pour déplacer le répertoire **appindicatorsupport@rgcjonas.gmail.com** vers l'emplacement sous `/usr/share/gnome-shell/extensions/`.

e) Exécutez la commande `chmod a+r metadata.json` pour rendre le fichier **metadata.json** lisible pour d'autres utilisateurs.

> **Conseil :**
>
> Par défaut, le fichier **metadata.json** du répertoire **appindicatorsupport@rgcjonas.gmail.com** est lisible uniquement pour l'utilisateur racine. Pour prendre en charge le partage d'écran, assurez-vous que le fichier **metadata.json** est également lisible pour d'autres utilisateurs.

f) Installez l'outil GNOME Tweaks.

g) Dans l'environnement de bureau, rechargez votre shell GNOME en appuyant sur les touches `Alt+F2`, `r` et `Enter` dans cet ordre ou en exécutant la commande `killall -SIGQUIT gnome-shell`.

h) Dans l'environnement de bureau, exécutez Gnome Tweaks et activez **KStatusNotifierItem/AppIndicator Support** dans l'outil Tweaks.

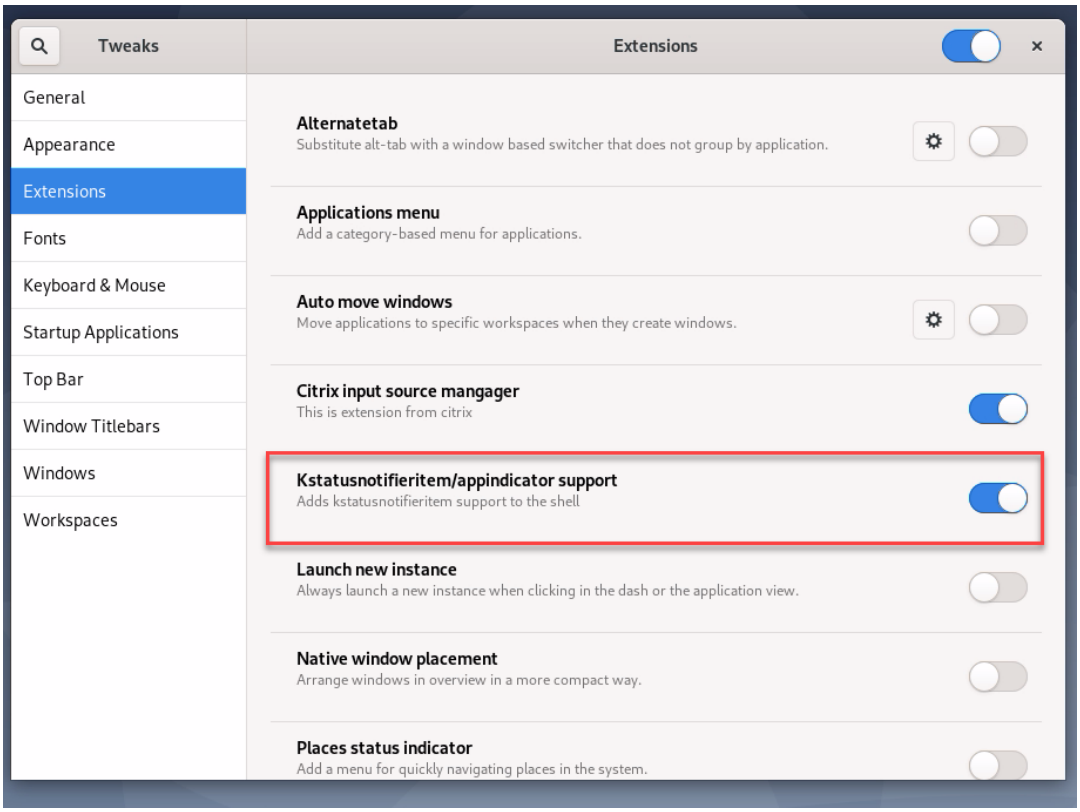
2. Si vous utilisez Debian 11.3 installé avec GNOME, procédez comme suit pour installer et activer les icônes de la barre d'état système GNOME :

a) Exécutez la commande `sudo apt install gnome-shell-extension-appindicator`. Vous devrez peut-être vous déconnecter, puis vous reconnecter pour que GNOME puisse voir l'extension.

b) Recherchez l'outil Tweaks dans l'écran **Activities**.

c) Sélectionnez **Extensions** dans l'outil Tweaks.

d) Activez **Kstatusnotifieritem/appindicator support**.



Configuration et réglage précis des graphiques

April 18, 2024

Cet article fournit des instructions pour configurer et ajuster les graphiques du Linux VDA.

Pour de plus amples informations, consultez les sections Configuration système requise et Présentation de l'installation.

Configuration

Optimiser pour la charge des graphiques 3D

Ce paramètre configure les valeurs par défaut appropriées qui conviennent le mieux aux charges de travail exigeant d'importantes ressources graphiques. Activez ce paramètre pour les utilisateurs dont

la charge de travail utilise des applications exigeant d'importantes ressources graphiques. Appliquez cette stratégie uniquement dans les cas où un processeur graphique est disponible pour la session. Tous les autres paramètres qui remplacent explicitement les paramètres par défaut définis par cette stratégie sont prioritaires.

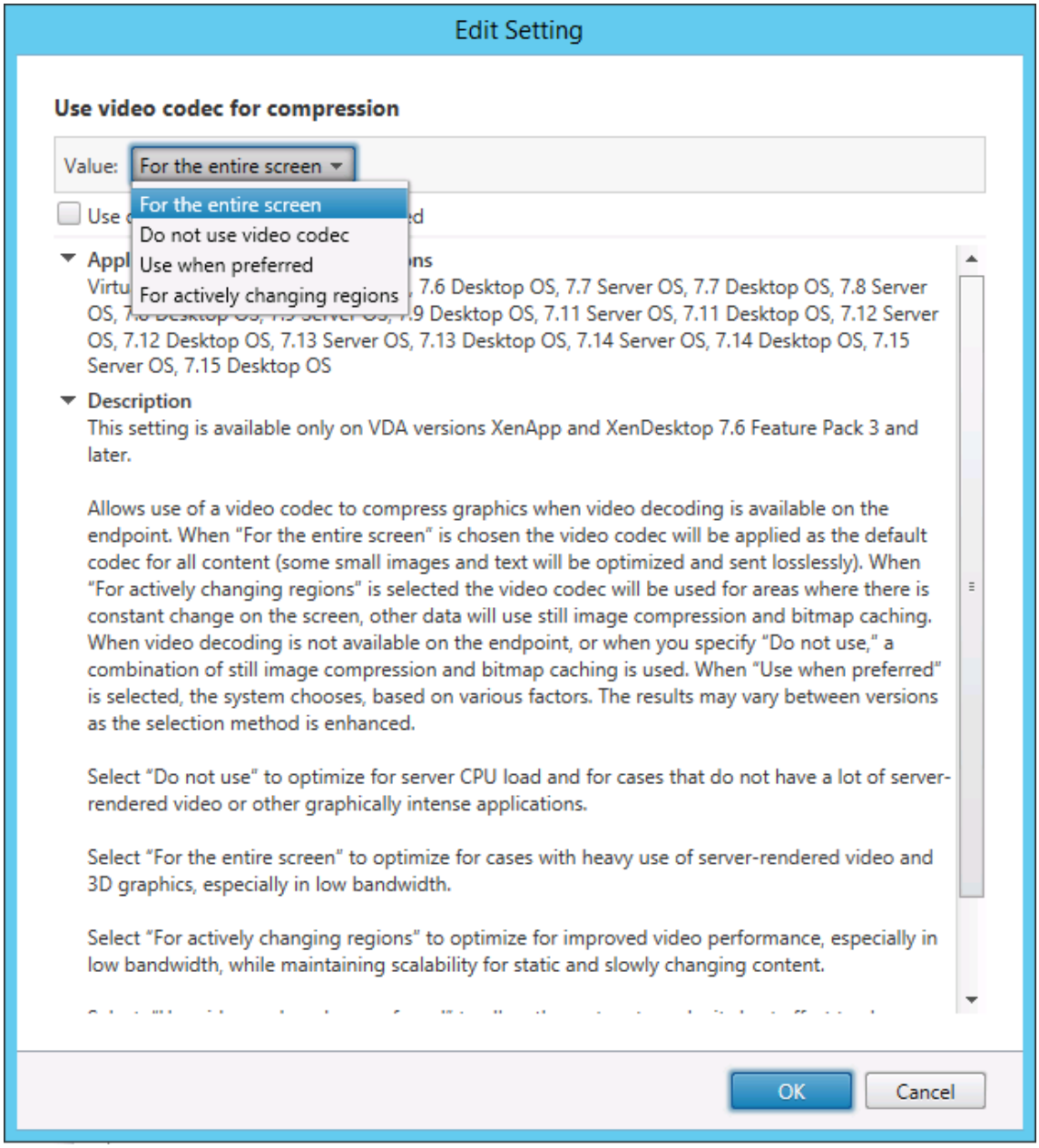
Par défaut, l'option **Optimiser pour la charge des graphiques 3D** est désactivée.

Codec vidéo pour la compression

Thinwire est la technologie de communication à distance d'écran utilisée dans le Linux VDA. Cette technologie permet aux graphiques générés sur une machine d'être transmis, généralement via un réseau, vers une autre machine.

La stratégie de graphiques **Utiliser codec vidéo pour la compression** définit le mode graphique par défaut et fournit les options suivantes pour différents cas d'utilisation :

- **Utiliser au choix**. Il s'agit du réglage par défaut. Aucune configuration supplémentaire n'est requise. Ce paramètre 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.
- **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, particulièrement dans les cas dans lesquels les graphiques 3D sont fortement sollicités. Le filigrane de session est pris en charge lorsque l'option **Pour l'écran entier** est sélectionnée ou lorsque l'option **Utiliser au choix** est sélectionnée et que l'option Optimiser pour la charge des graphiques 3D est activée.
- **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 uniquement dans la partie de l'écran sur laquelle l'image est en mouvement. L'utilisation sélective du codec vidéo H.264 permet à HDX Thinwire de détecter et de coder des parties de l'écran qui sont fréquemment mises à jour à l'aide du codec vidéo H.264. La compression d'images immobiles (JPEG, RLE) et la mise en cache de bitmaps continuent à être utilisées pour le reste de l'écran, y compris le texte et l'imagerie photographique. Les utilisateurs bénéficient d'une bande passante plus faible et d'une meilleure qualité pour le contenu vidéo, conjointement avec du texte sans perte ou à des images de haute qualité. Pour activer cette fonctionnalité, réglez la stratégie **Utiliser codec vidéo pour la compression** par **Utiliser au choix** (valeur par défaut) ou **Pour les zones changeant constamment**. Pour plus d'informations, veuillez consulter la section Paramètres de stratégie des graphiques.



D'autres paramètres de stratégie, y compris les paramètres de stratégie Affichage visuel suivants, peuvent être utilisés pour optimiser les performances de la communication à distance d'écran :

- **Nombre de couleurs préféré pour les graphiques simples**
- **Taux de trames cible**
- **Qualité visuelle**

Encodage matériel H.264

La stratégie **Utiliser le codage matériel pour le codec vidéo** permet d'utiliser l'accélération matérielle du GPU, s'il est disponible, pour compresser les éléments d'écran avec le codec vidéo. Si le matériel GPU n'est pas disponible, le VDA utilise le codage basé sur l'UC avec le codec vidéo logiciel.

L'accélération matérielle du GPU optimise l'utilisation des ressources matérielles et améliore considérablement les performances des images par seconde (FPS).

À partir de la version 2210, l'accélération matérielle du GPU couvre les modes graphiques suivants :

- Utiliser au choix
- Pour l'écran entier
- Pour les zones changeant constamment

Autoriser la compression visuelle sans perte

La stratégie **Autoriser la compression visuelle sans perte** permet d'utiliser une compression visuelle sans perte au lieu d'une véritable compression sans perte pour les graphiques. La compression visuellement sans perte améliore les performances par rapport à la compression vraie sans perte, mais engendre une perte mineure qui ne peut être remarquée à l'œil nu. Ce paramètre change la manière dont les valeurs du paramètre **Qualité visuelle** sont utilisées.

La stratégie **Autoriser la compression visuelle sans perte** est désactivée par défaut. Pour activer la compression visuelle sans perte, définissez **Autoriser la compression visuelle sans perte** sur **Activé** et la stratégie **Qualité visuelle** sur **Sans perte si possible**.

Si la stratégie **Utiliser codec vidéo pour la compression** est définie sur **Ne pas utiliser de codec vidéo**, la compression visuelle sans perte s'applique au codage d'image statique. Si la stratégie **Utiliser codec vidéo pour la compression** est définie sur un mode graphique autre que **Ne pas utiliser de codec vidéo**, la compression visuelle sans perte s'applique au codage H.264.

Les clients suivants prennent en charge le mode sélectif H.264 :

- Citrix Receiver pour Windows 4.9 à 4.12
- Citrix Receiver pour Linux 13.5 à 13.10
- Application Citrix Workspace 1808 pour Windows et versions ultérieures
- Application Citrix Workspace 1808 pour Linux et version ultérieure

Pour plus d'informations sur les paramètres de stratégie **Qualité visuelle** et **Utiliser codec vidéo pour la compression**, consultez la section Paramètres de stratégie Affichage visuel et Paramètres de stratégie Graphiques.

Prise en charge du codec vidéo H.265

À compter de la version 7.18, le Linux VDA prend en charge le codec vidéo H.265 pour l'accélération matérielle des graphiques et vidéos distants.

Vous pouvez utiliser cette fonctionnalité sur :

- Citrix Receiver pour Windows 4.10 à 4.12
- Application Citrix Workspace 1808 pour Windows et versions ultérieures

Pour bénéficier de cette fonctionnalité, activez-la à la fois sur le Linux VDA et sur votre client. Si le GPU de votre client ne prend pas en charge le décodage H.265 à l'aide de l'interface DXVA, le paramètre de stratégie de **décodage H.265 pour les graphiques** est ignoré et les sessions utilisent le codec vidéo H.264. Pour plus d'informations, consultez la section Codage vidéo H.265.

Pour activer le codage matériel H.265 sur le VDA :

1. Activez la stratégie **Utiliser le codage matériel pour le codec vidéo**.
2. Activez la stratégie **Optimiser pour la charge des graphiques 3D**.
3. Assurez-vous que la stratégie **Utiliser codec vidéo pour la compression** est définie par défaut ou définie sur **Pour l'écran entier**.
4. Assurez-vous que la stratégie **Qualité visuelle** n'est **PAS** définie sur **Sans perte si possible** ni sur **Toujours sans perte**.

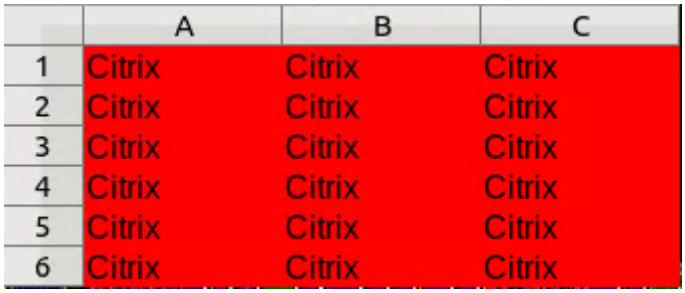
Pour activer le codage matériel H.265 sur votre client, consultez la section Codage vidéo H.265.

Prise en charge du codage logiciel YUV444

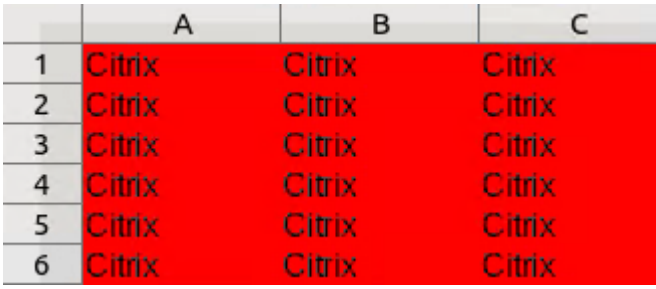
Le Linux VDA prend en charge le codage logiciel YUV444. Le schéma de codage YUV attribue à chaque pixel des valeurs de luminosité et de couleur. En YUV, Y représente la luminosité ou les valeurs « luma », et UV représente la couleur ou les valeurs « chroma ». Vous pouvez utiliser cette fonctionnalité sur Citrix Receiver pour Windows 4.10 à 4.12 et sur l'application Citrix Workspace 1808 pour Windows et versions ultérieures.

Chaque valeur unique Y, U ou V comprend 8 bits, ou un octet, de données. Le format de données YUV444 transmet 24 bits par pixel. Le format de données YUV422 partage les valeurs U et V entre deux pixels, ce qui permet un taux de transmission moyen de 16 bits par pixel. Le tableau suivant contient une comparaison intuitive entre YUV444 et YUV420.

YUV444



YUV420



Pour activer le codage logiciel YUV444 sur le VDA :

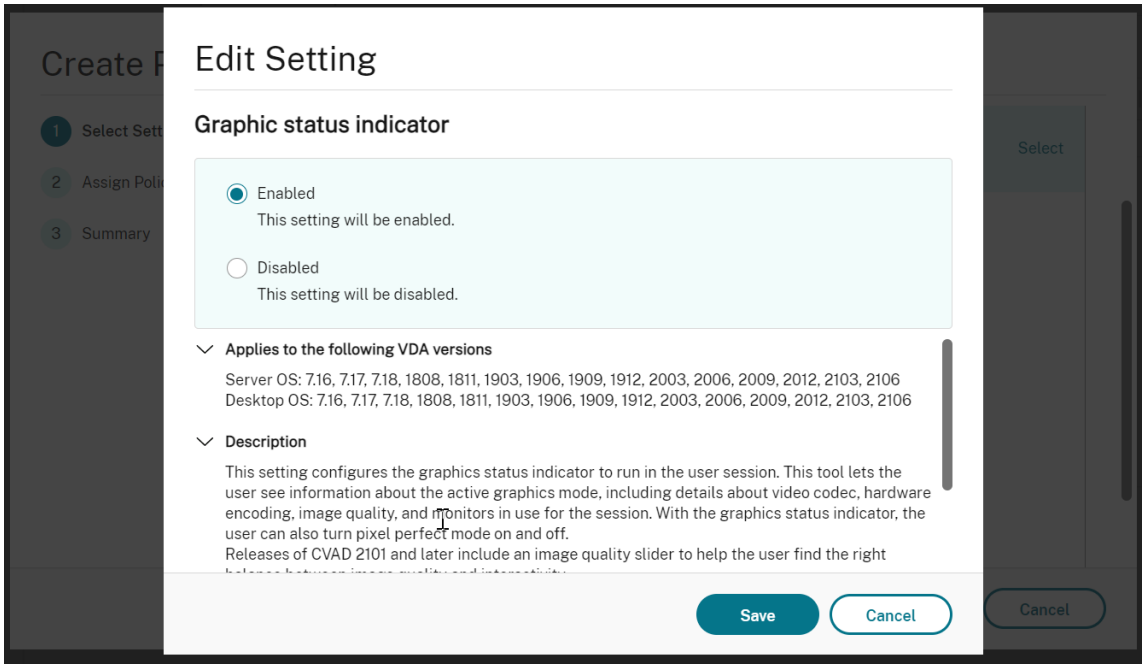
1. Assurez-vous que la stratégie **Utiliser codec vidéo pour la compression** est définie sur **Pour l'écran entier**.
2. Assurez-vous que la stratégie **Qualité visuelle** est définie sur **Toujours sans perte** ou **Sans perte si possible**

Curseur pour la qualité des graphiques

Nous avons inclus un curseur pour la qualité des graphiques dans l'outil d'indicateur d'état des graphiques qui s'exécute dans vos sessions Linux virtuelles. Le curseur permet de trouver le bon équilibre entre la qualité d'image et l'interactivité.

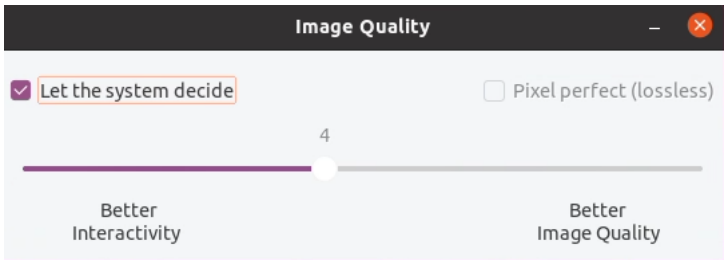
Pour utiliser le curseur, procédez comme suit :

1. Activez la stratégie **Indicateur d'état des graphiques** dans Citrix Studio.



2. Ouvrez le terminal et exécutez la commande `ctxslider`. L'interface utilisateur du curseur apparaît.

> **Remarque :**
>
> Si vous avez défini la stratégie **Qualité visuelle** sur **Toujours sans perte** ou **Sans perte si possible**, l'interface utilisateur du curseur ne s'affiche pas.



Les options suivantes sont désormais disponibles :

- Pour modifier la qualité de l'image, déplacez le curseur. Le curseur prend en charge une plage comprise entre 0 et 9.
- Pour utiliser les paramètres définis par le système, sélectionnez **Laisser le système décider**.
- Pour passer en mode sans perte, sélectionnez **Pixel parfait**.

Ajuster les débits moyens en fonction des estimations de bande passante

Citrix améliore le codage matériel HDX 3D Pro en ajustant les débits binaires moyens en fonction des estimations de bande passante.

Lorsque le codage matériel HDX 3D Pro est utilisé, le VDA peut estimer par intermittence la bande passante du réseau et ajuster les débits des images codées en conséquence. Cette nouvelle fonctionnalité fournit un mécanisme pour équilibrer la netteté et la fluidité.

Par défaut, cette fonction est activée. Pour le désactiver, exécutez la commande suivante :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
     CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
     DisableReconfigureEncoder" -d "0x00000001" --force
2 <!--NeedCopy-->
```

Outre l'utilisation de cette fonctionnalité, vous pouvez également exécuter les commandes suivantes pour régler la netteté et la fluidité. Les paramètres **AverageBitRatePercent** et **MaxBitRatePercent** définissent le pourcentage d'utilisation de la bande passante. Les valeurs les plus élevées que vous définissez, les graphiques plus nets et la fluidité moindre que vous obtenez. La plage de réglages recommandée est de 50 à 100.

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
     CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
     AverageBitRatePercent" -d "90" --force
2
3 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
     CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
     MaxBitRatePercent" -d "100" --force
4 <!--NeedCopy-->
```

Avec le réglage de débit binaire moyen, lorsque votre écran reste immobile, l'image la plus récente reste dans un état de mauvaise qualité car aucune nouvelle image n'est envoyée. L'amélioration de la netteté peut résoudre ce problème en reconfigurant et en envoyant immédiatement l'image la plus récente avec la plus haute qualité.

Pour une liste complète des stratégies prises en charge par Linux VDA Thinwire, consultez la Liste des stratégies prises en charge.

Pour plus d'informations sur la configuration de la prise en charge de moniteurs multiples sur Linux VDA, consultez CTX220128.

Traitement en parallèle

Thinwire peut améliorer le nombre d'images par seconde (FPS) en exécutant certaines tâches en parallèle, avec pour effet une charge liée à une consommation globale du processeur légèrement plus

élevée. Cette fonction est désactivée par défaut. Pour activer cette fonctionnalité, exécutez la commande suivante sur votre VDA :

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
   ParallelProcessing" -d "0x00000001" --force
<!--NeedCopy-->
```

Dépannage

Vérifier quel mode graphique est utilisé

Exécutez la commande suivante pour vérifier quel mode graphique est utilisé (**0** signifie TW+ ; **1** signifie codec vidéo plein écran) :

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep GraphicsMode
<!--NeedCopy-->
```

Le résultat se présente comme suit :

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "GraphicsMode"-d "0x00000000"--force
```

Vérifier si H.264 est utilisé

Exécutez la commande suivante pour vérifier si H.264 est en cours d'utilisation (**0** signifie qu'il n'est pas utilisé ; **1** signifie qu'il est utilisé) :

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H264
<!--NeedCopy-->
```

Le résultat se présente comme suit :

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "H264"-d "0x00000000"--force
```

Vérifier si H.265 est utilisé

Exécutez la commande suivante pour vérifier si H.265 plein écran est en cours d'utilisation (**0** signifie qu'il n'est pas utilisé ; **1** signifie qu'il est utilisé) :

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H265
<!--NeedCopy-->
```


Le résultat se présente comme suit :

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "H265"-d "0x00000000"--force
```

Vérifier quel schéma de codage YUV est utilisé

Exécutez la commande suivante pour vérifier quel schéma de codage YUV est utilisé (**0** signifie YUV420. **1** signifie YUV422. **2** signifie YUV444) :

Remarque : la valeur de YuvFormat n'a de sens que lorsqu'un codec vidéo est utilisé.

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep YUVFormat
2 <!--NeedCopy-->
```

Le résultat se présente comme suit :

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "YUVFormat"-d "0x00000000"--force
```

Vérifier si le codage logiciel YUV444 est utilisé

Exécutez la commande suivante pour vérifier si le codage logiciel YUV444 est utilisé :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep Graphics
2 <!--NeedCopy-->
```

Lorsque YUV444 est utilisé, le résultat se présente comme suit :

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "GraphicsMode"-d "0x00000001"--force
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "H264"-d "0x00000001"--force
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "HardwareEncoding"-d "0x00000000"--force
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "YUVFormat"-d "0x00000002"--force
```

Vérifier si le codage matériel est utilisé pour 3D Pro

Exécutez la commande suivante (**0** signifie qu'il n'est pas utilisé ; **1** signifie qu'il est utilisé) :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep HardwareEncoding
2 <!--NeedCopy-->
```


Le résultat se présente comme suit :

```
create -k "HKLM\Software\Citrix\Ica\Session\1\Graphics"-t "REG_DWORD"
-v "HardwareEncoding"-d "0x00000001"--force
```

Une autre méthode consiste à utiliser la commande **nvidia-smi**. Les résultats se présentent comme suit lorsque le codage matériel est utilisé :

```
Tue Apr 12 10:42:03 2016
+-----------------------------------------------------+
| NVIDIA-SMI 361.28     Driver Version: 361.28        |
|-------------------------------+----------------------+----------------------+

| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
   Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
   Compute M. |
|===============================+======================+======================|

|   0  GRID K1             Off  | 0000:00:05.0     Off |
                      N/A |
| N/A   42C    P0    14W /  31W |    207MiB /  4095MiB |      8%
   Default |
+-------------------------------+----------------------+----------------------+


+-----------------------------------------------------------------------------+

| Processes:                                                       GPU
   Memory |
|  GPU       PID  Type  Process name
   Usage      |
|=============================================================================|

|    0      2164  C+G   /usr/local/bin/ctxgfx
   106MiB |
|    0      2187    G   Xorg
    85MiB |
+-----------------------------------------------------------------------------+

<!--NeedCopy-->
```

Vérifier que le pilote graphique NVIDIA GRID est correctement installé

Pour vérifier si le pilote graphique NVIDIA GRID est correctement installé, exécutez **nvidia-smi**. Le résultat se présente comme suit :

```
+-----------------------------------------------------+
| NVIDIA-SMI 352.70     Driver Version: 352.70        |
|-------------------------------+----------------------+----------------------+
```



```
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
   Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
   Compute M. |
|===============================+======================+======================|
|   0  Tesla M60           Off  | 0000:00:05.0     Off |
                    Off |
| N/A   20C    P0    37W / 150W |     19MiB /  8191MiB |      0%
   Default |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                       GPU
   Memory |
|  GPU       PID  Type  Process name
   Usage      |
|=============================================================================|
|  No running processes found
                                 |
+-----------------------------------------------------------------------------+
<!--NeedCopy-->
```

Définissez la configuration correcte pour la carte :

`etc/X11/ctx-nvidia.sh`

Problèmes d'actualisation des multi-écrans HDX 3D Pro

Si vous rencontrez des problèmes d'actualisation des écrans autres que l'écran principal, vérifiez que la licence NVIDIA GRID est disponible.

Vérifier les journaux d'erreurs Xorg

Le nom du fichier journal Xorg est similaire à **Xorg.{DISPLAY}.log** dans le dossier **/var/log/**.

Problèmes connus et limitations

Pour vGPU, la console locale Citrix Hypervisor affiche l'écran de la session de bureau ICA

Solution : désactivez la console VGA locale de la machine virtuelle en exécutant les commandes suivantes :

Pour Citrix Hypervisor 8.1 et versions ultérieures :


```
[root@xenserver ~]# xe vgpu-param-set uuid=vgpu-uuid extra_args=
   disable_vnc=1
<!--NeedCopy-->
```

Pour Citrix Hypervisor versions antérieures à 8.1 :

```
xe vm-param-set uuid=<vm-uuid> platform:vgpu_extra_args="disable_vnc=1"
<!--NeedCopy-->
```

Les fenêtres contextuelles du bureau Gnome 3 sont lentes lors de l'ouverture de session

Il s'agit d'une limitation du démarrage de session de bureau Gnome 3.

Certaines applications OpenGL/WebGL ne s'affichent pas correctement après le redimensionnement de l'application Citrix Workspace

Si vous redimensionnez la fenêtre de l'application Citrix Workspace, la résolution de l'écran est modifiée. Le pilote propriétaire NVIDIA modifie certains états internes et peut attendre des applications une réponse adaptée. Par exemple, l'élément de bibliothèque WebGL **lightgl.js** peut générer une erreur « `Rendering to this texture is not supported (incomplete frame buffer)` ».

Partage d'écran HDX

December 16, 2022

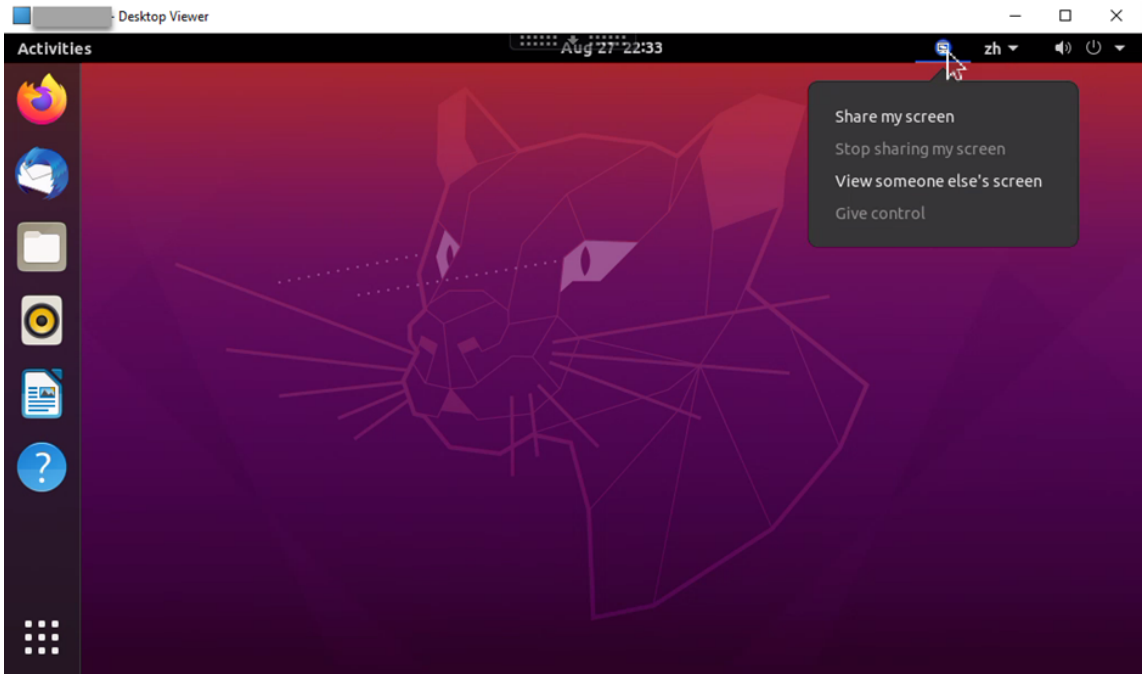
Vue d'ensemble

Le VDA Linux vous permet de partager l'écran de votre bureau virtuel avec les utilisateurs de session sur d'autres bureaux virtuels.

L'exemple suivant vous explique comment partager un écran et afficher l'écran d'un autre utilisateur.

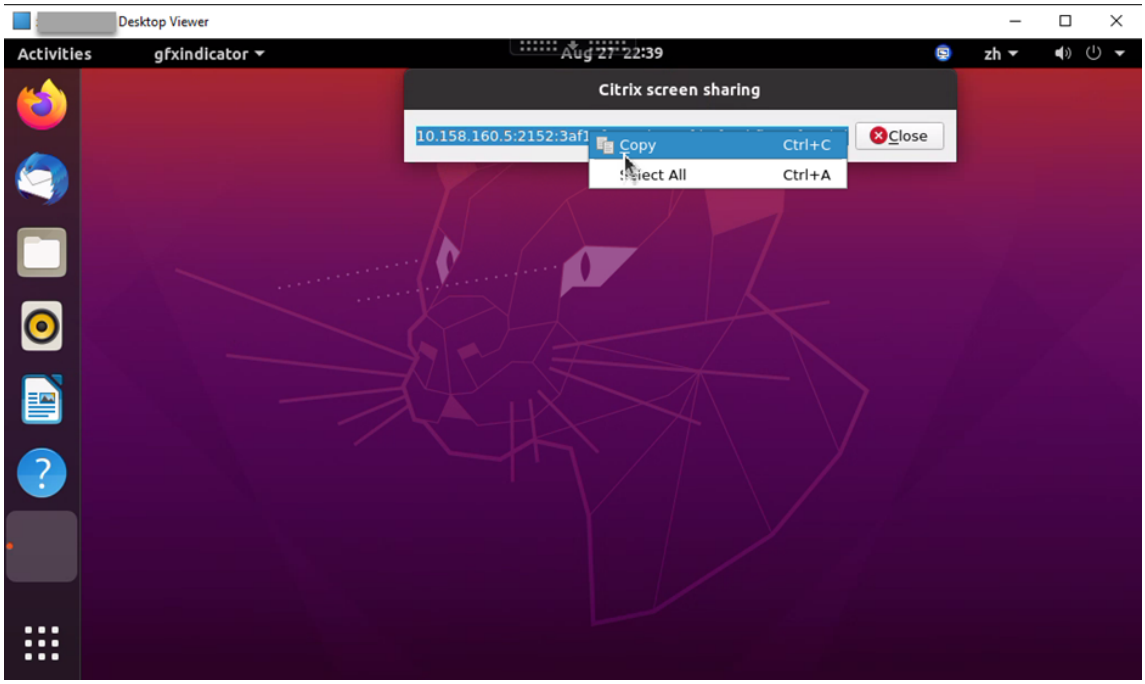
Pour partager un écran :

1. Dans la zone de notification de votre bureau virtuel, cliquez sur l'icône de **partage d'écran** et sélectionnez **Partager mon écran**.



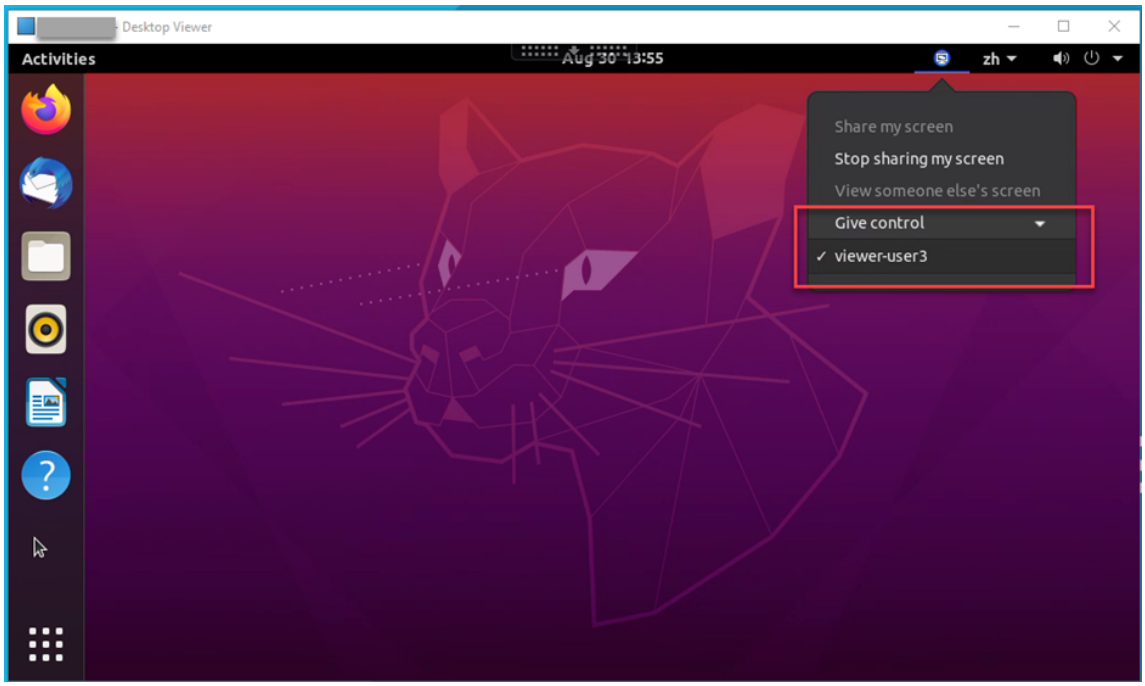
2. Cliquez sur **Copier et fermer**.

   Le code de partage d'écran actuel persiste jusqu'à ce que vous arrêtiez et recommenciez le partage de votre écran.

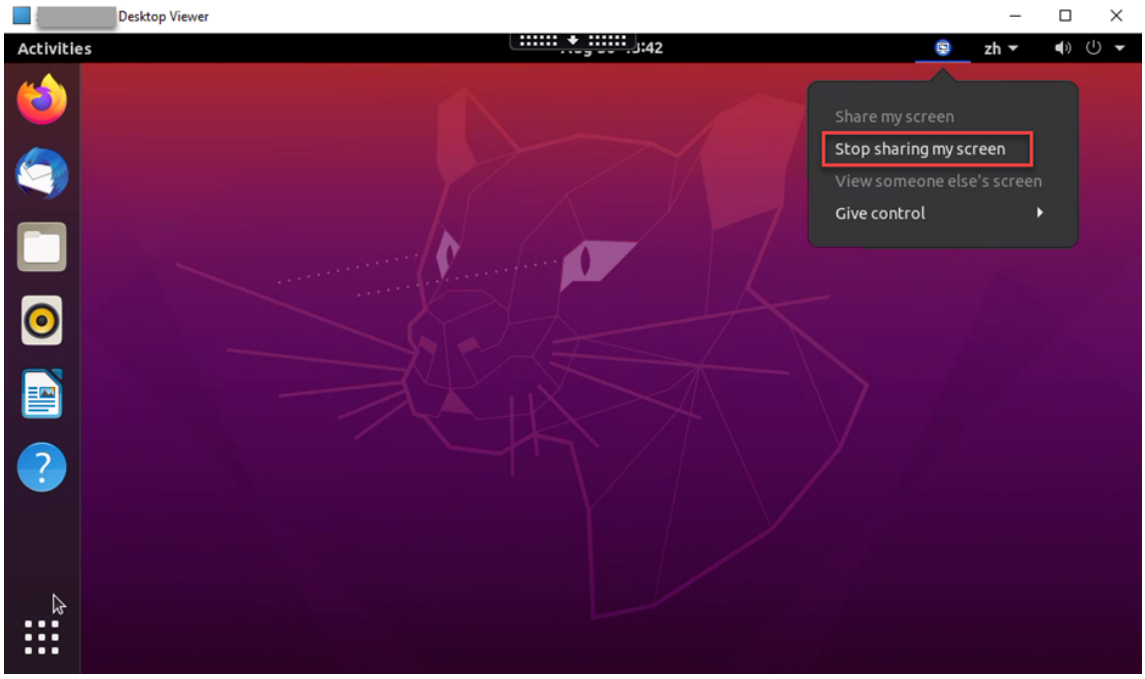


> **Conseil :**
>
> Lorsque vous partagez votre écran, une bordure rouge l'entoure, indiquant que le partage est en cours.

3. Partagez le code copié avec les utilisateurs de session sur d'autres bureaux virtuels avec lesquels vous souhaitez partager votre écran.
4. Pour autoriser un utilisateur à contrôler votre écran, sélectionnez **Donner le contrôle**, puis le nom de l'utilisateur. Pour retirer le contrôle, effacez le nom de l'utilisateur.

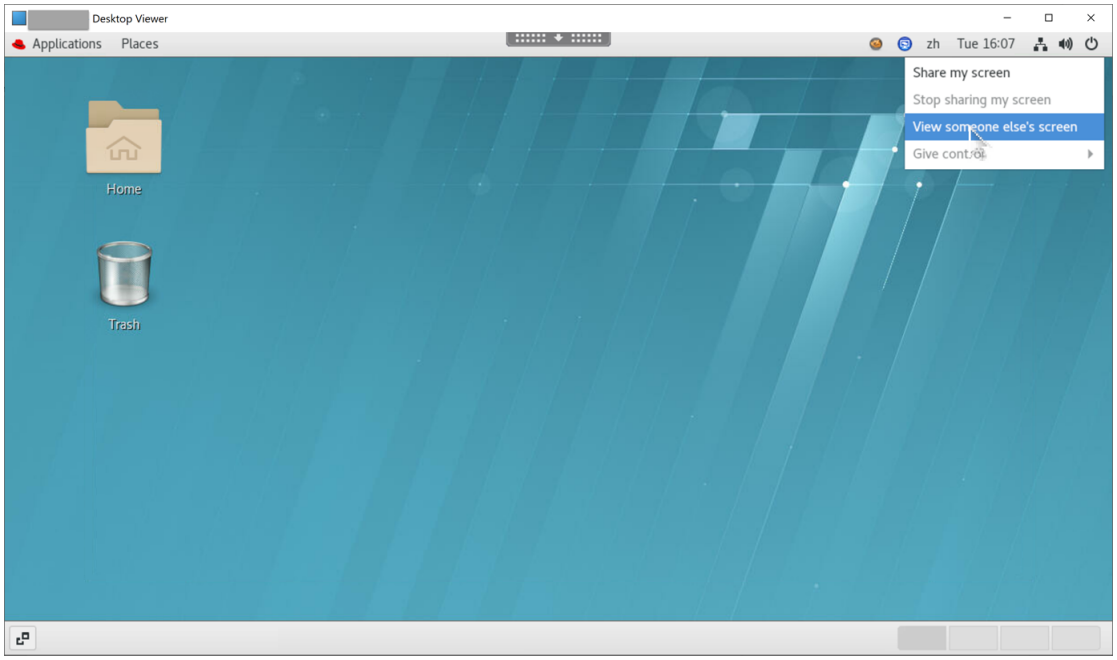


5. Pour arrêter le partage de votre écran, sélectionnez **Arrêter de partager mon écran**.

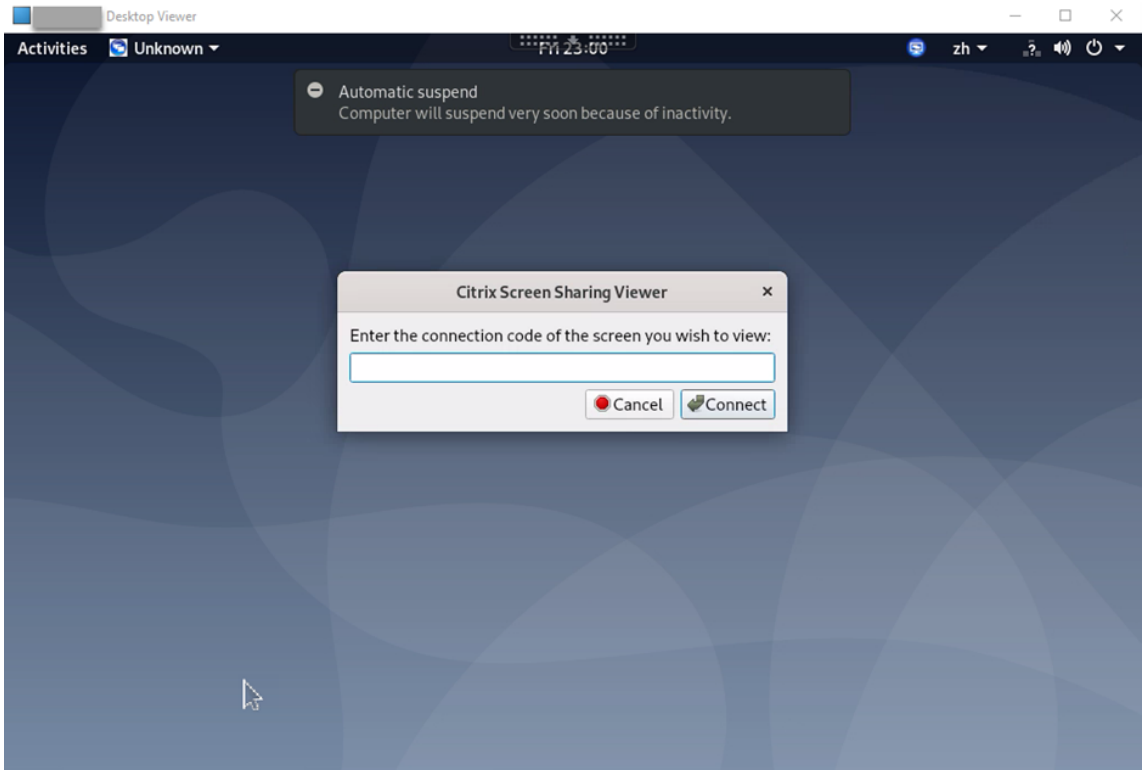


Pour afficher l'écran d'un autre utilisateur :

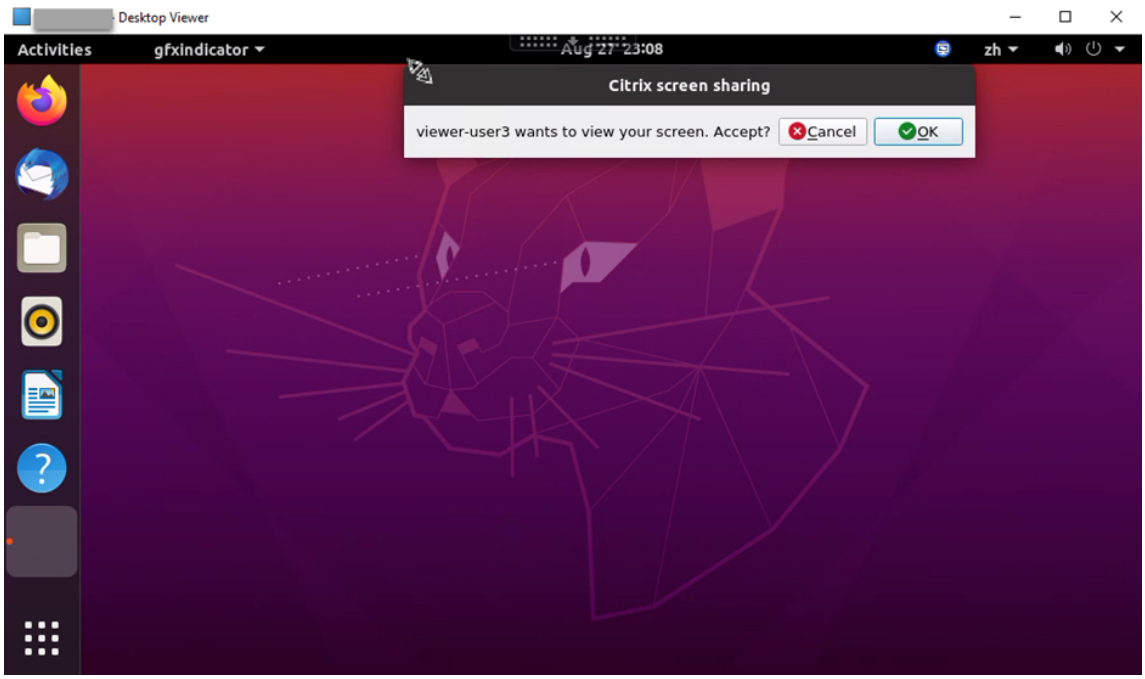
1. Dans la zone de notification de votre bureau virtuel, cliquez sur l'icône de **partage d'écran** et sélectionnez **Afficher l'écran de quelqu'un d'autre**.



2. Entrez le code de connexion de l'écran que vous souhaitez afficher, puis cliquez sur **Connecter**.

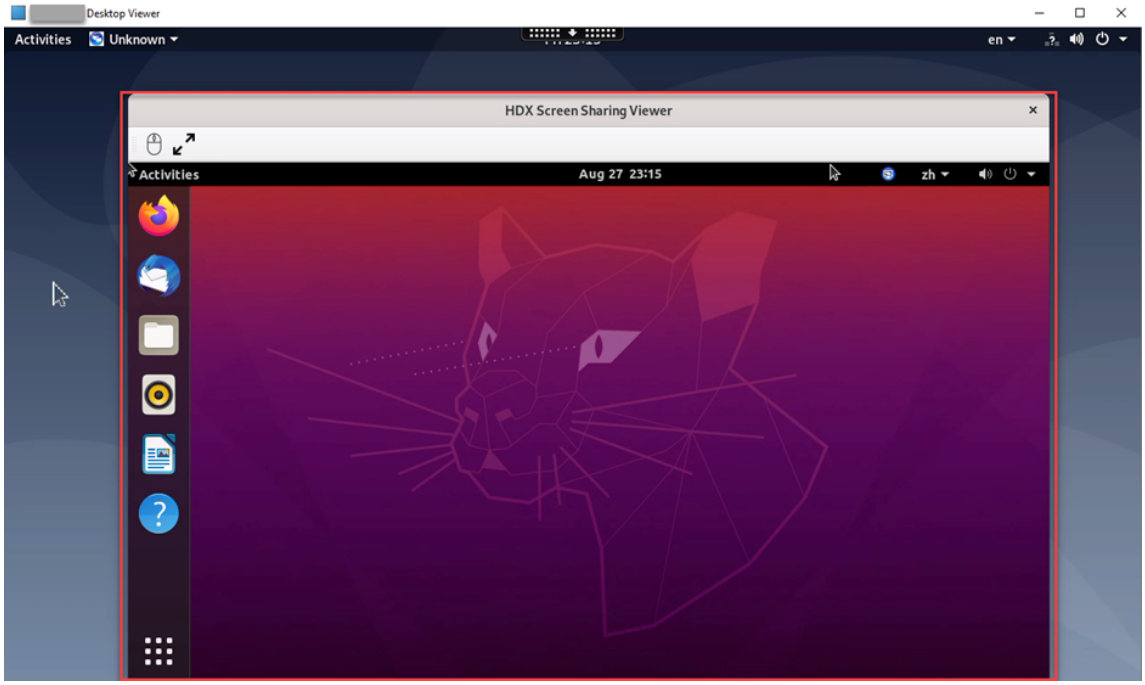


3. Attendez que l'utilisateur effectuant le partage d'écran accepte votre demande. Par exemple :



> **Conseil :**
>
> - Le système Linux émet une notification de votre demande à l'utilisateur effectuant le partage d'écran.
> - Si l'utilisateur effectuant le partage d'écran n'accepte pas votre demande dans les 30 secondes, votre demande expire et une invite apparaît.

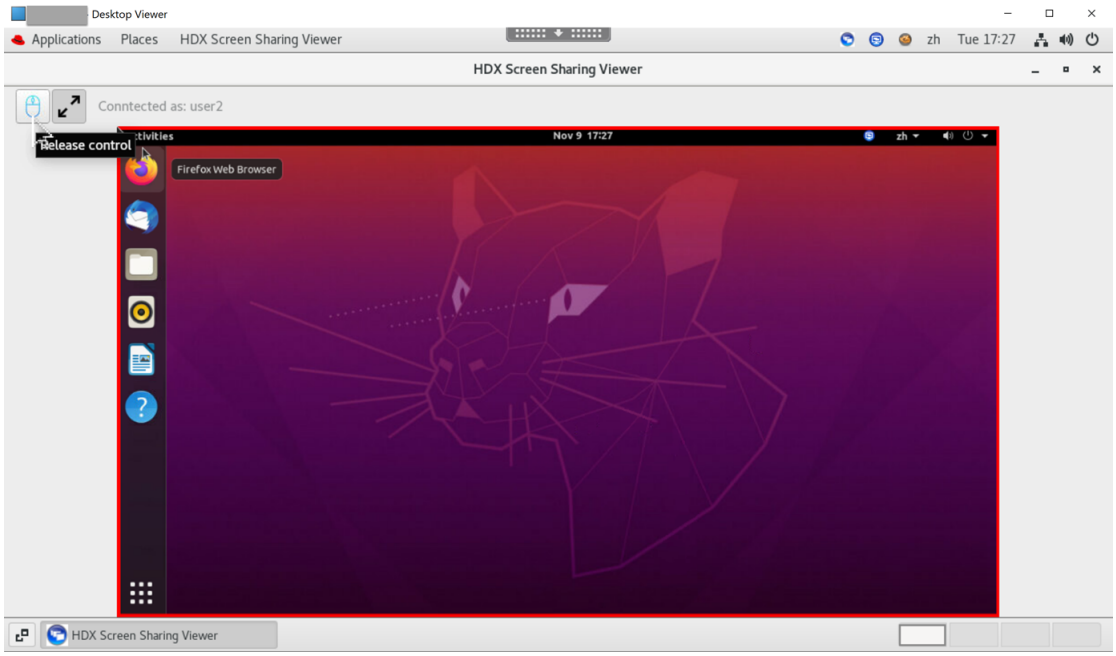
4. Une fois que l'utilisateur effectuant le partage d'écran a accepté votre demande en cliquant sur **OK**, l'écran partagé s'affiche dans votre fenêtre Desktop Viewer. Vous êtes connecté en tant qu'observateur avec un nom d'utilisateur attribué automatiquement.



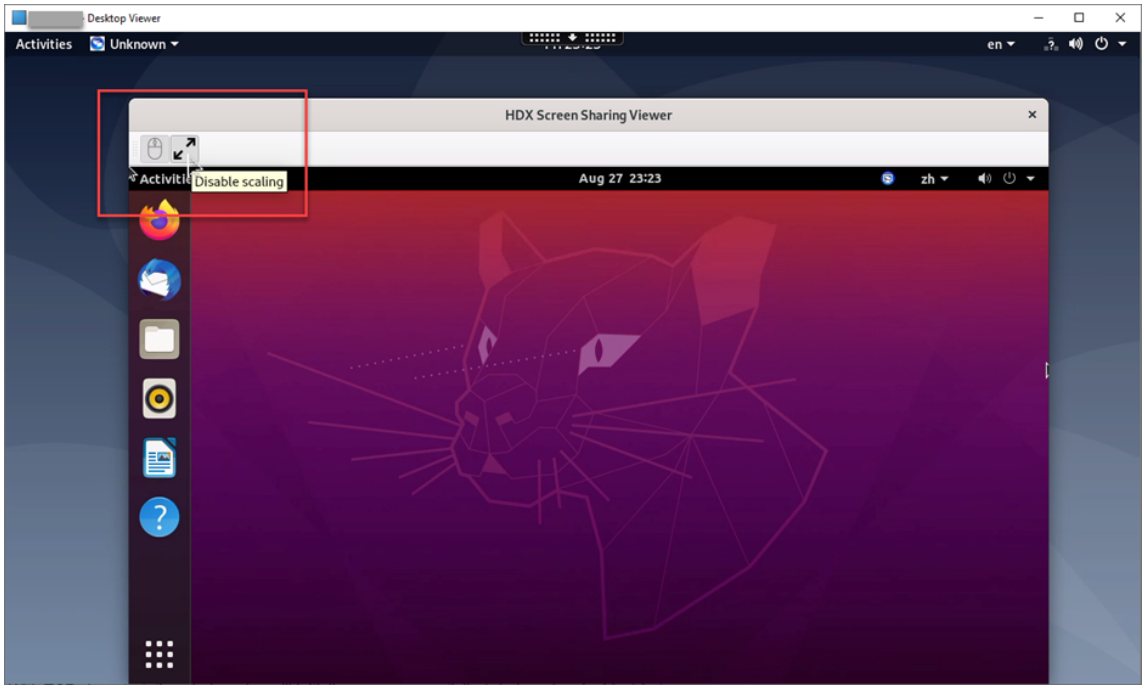
5. Pour demander le contrôle de l'écran partagé, cliquez sur l'icône de la souris dans le coin supérieur gauche.

   > **Conseil :**
   >
   > - Si l'utilisateur effectuant le partage d'écran n'accepte pas votre demande dans les 30 secondes, votre demande expire.
   > - Un seul observateur est autorisé à contrôler un écran partagé à la fois.

   Cliquez à nouveau sur l'icône de la souris pour abandonner le contrôle de l'écran partagé.



6. Pour désactiver ou activer la mise à l'échelle en fonction de la taille de la fenêtre, cliquez sur l'icône en regard de l'icône de la souris.



Configuration

La fonctionnalité de partage d'écran est désactivée par défaut. Pour l'activer, remplissez les paramètres suivants :

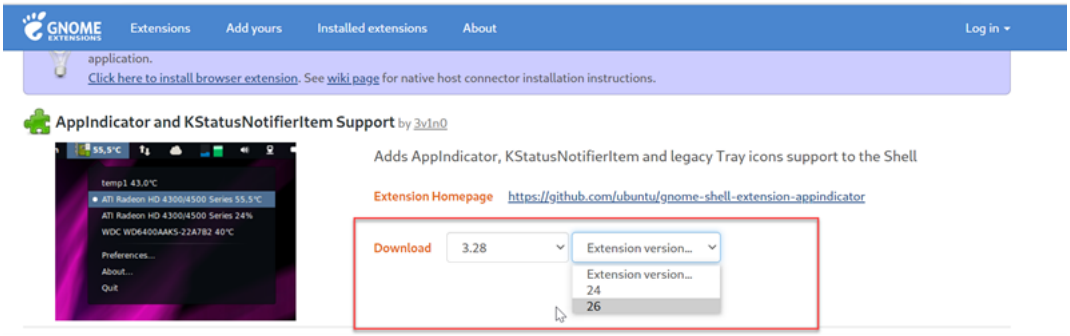
1. Activez la stratégie Indicateur d'état des graphiques dans Citrix Studio.
2. Pour Citrix Virtual Apps and Desktops 2112 et versions ultérieures, activez la stratégie **Partage d'écran** dans Citrix Studio.
3. (Facultatif) Pour Citrix Virtual Apps and Desktops 2109 et versions antérieures, activez le partage d'écran sur le Linux VDA en exécutant la commande suivante :

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Thinwire" -v "
   EnableScreenSharing" -d "0x00000001"
<!--NeedCopy-->
```

4. Autorisez les ports 52525 - 52625 dans votre pare-feu.
5. (Facultatif) Si vous utilisez RHEL 8.x, Debian 11 ou SUSE 15.x installé avec GNOME, installez une extension compatible pour votre shell GNOME pour activer la prise en charge d'AppIndicator :

   a) Exécutez la commande `gnome-shell --version` pour vérifier votre version du shell GNOME.

   b) Téléchargez une extension compatible pour votre shell GNOME depuis https://extensions.gnome.org/extension/615/appindicator-support. Par exemple, si votre version du shell est 3.28, vous pouvez sélectionner 24 ou 26 pour la version d'extension.



   c) Décompressez le package téléchargé. Vérifiez que la valeur **uuid** dans le fichier **metadata.json** du package est définie sur **appindicatorsupport@rgcjonas.gmail.com**.

   d) Exécutez la commande `mv` pour déplacer le répertoire **appindicatorsupport@rgcjonas.gmail.com** vers l'emplacement sous `/usr/share/gnome-shell/extensions/`.

   e) Exécutez la commande `chmod a+r metadata.json` pour rendre le fichier **metadata.json** lisible pour d'autres utilisateurs.

> **Conseil :**
>
> Par défaut, le fichier **metadata.json** du répertoire **appindicatorsupport@rgcjonas.gmail.com** est lisible uniquement pour l'utilisateur racine. Pour prendre en charge le partage d'écran, assurez-vous que le fichier **metadata.json** est également lisible pour d'

> autres utilisateurs.

f) Installez l'outil GNOME Tweaks.

g) Dans l'environnement de bureau, rechargez votre shell GNOME en appuyant sur les touches `Alt`+`F2`, `r` et `Enter` dans cet ordre ou en exécutant la commande `killall -SIGQUIT gnome-shell`.

h) Dans l'environnement de bureau, exécutez Gnome Tweaks et activez **KStatusNotifierItem/AppIndicator Support** dans l'outil Tweaks.

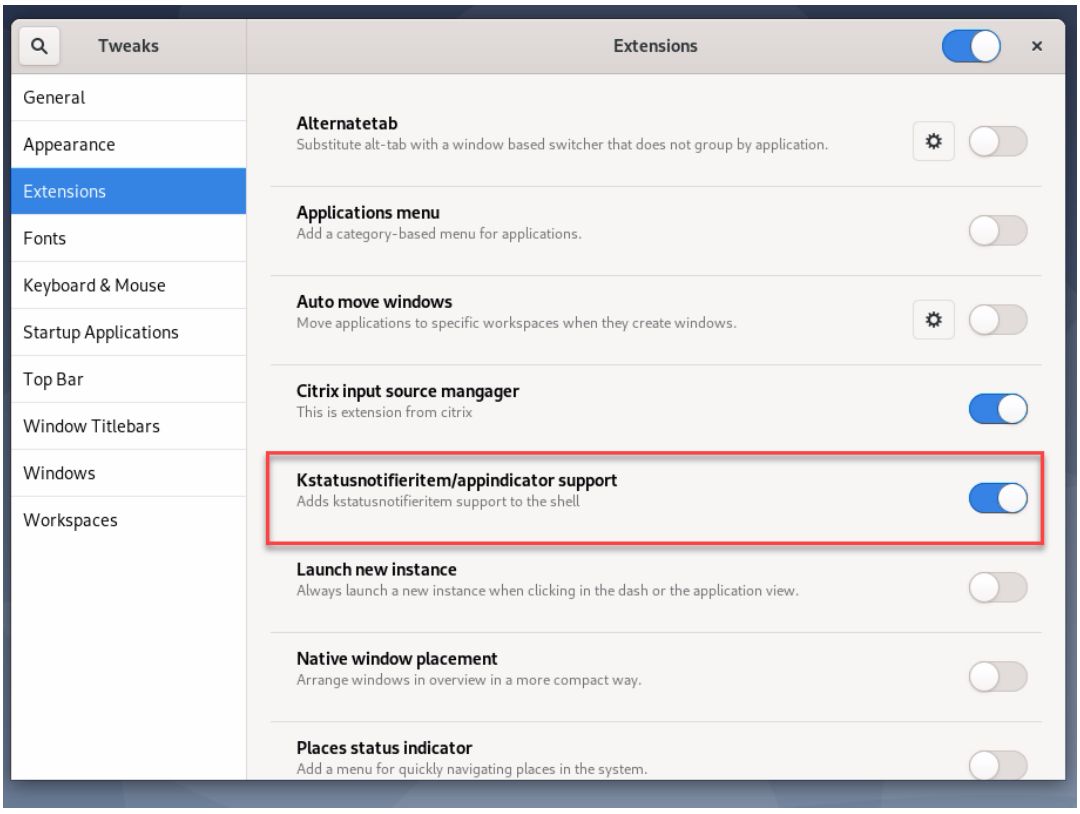
6. (Facultatif) Si vous utilisez Debian 11.3 installé avec GNOME, procédez comme suit pour installer et activer les icônes de la barre d'état système GNOME :

a) Exécutez la commande `sudo apt install gnome-shell-extension-appindicator`. Vous devrez peut-être vous déconnecter, puis vous reconnecter pour que GNOME puisse voir l'extension.

b) Recherchez l'outil Tweaks dans l'écran **Activities**.

c) Sélectionnez **Extensions** dans l'outil Tweaks.

d) Activez **Kstatusnotifieritem/appindicator support**.



Considérations

- La fonctionnalité de partage d'écran ne prend pas en charge le codec vidéo H.265.
- La fonctionnalité de partage d'écran n'est pas disponible pour les sessions d'application.
- Les utilisateurs de sessions de bureau peuvent partager les écrans de leurs sessions avec un maximum de 10 personnes par défaut. Le nombre maximum de personnes est configurable via `ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire"-v "ScreenSharingViewerMaxNum"-d <hex_value>`. Lorsque le nombre maximum est atteint, une invite apparaît lorsque les utilisateurs tentent d'accepter des demandes de connexion supplémentaires.

Cartes graphiques non vGPU

March 11, 2024

Les cartes graphiques non vGPU font référence aux cartes graphiques qui ne prennent pas en charge la solution NVIDIA Virtual GPU (vGPU). Cet article fournit des informations sur l'utilisation des cartes graphiques non vGPU.

Logiciels requis

Pour utiliser des cartes graphiques non vGPU, vous devez :

- Installer XDamage avant de commencer. En règle générale, XDamage existe sous forme d'extension de XServer.
- Définissez `CTX_XDL_HDX_3D_PRO` sur `Y` lors de l'installation de Linux VDA. Pour plus d'informations sur les variables d'environnement, consultez Étape 7 : définir l'environnement d'exécution afin de terminer l'installation.

Configuration

Modifier les fichiers de configuration Xorg

Pour les cartes graphiques NVIDIA Si vous utilisez un pilote NVIDIA, les fichiers de configuration sont installés et définis automatiquement.

Pour les autres cartes graphiques Vous devez modifier les quatre fichiers de configuration de modèle installés sous `/etc/X11/` :

- ctx-driver_name-1.conf
- ctx-driver_name-2.conf
- ctx-driver_name-3.conf
- ctx-driver_name-4.conf

En utilisant **ctx-driver_name-1.conf** en tant qu'exemple, suivez la procédure suivante pour modifier les fichiers de configuration de modèle :

1. Remplacez ***driver_name*** par le nom de votre pilote.

   Par exemple, si votre nom de pilote est `intel`, vous pouvez modifier le nom du fichier de configuration pour `ctx-intel-1.conf`.

2. Ajoutez les informations du pilote vidéo.

   Chaque fichier de configuration de modèle contient une section appelée « Machine », à laquelle un commentaire est ajouté. Cette section décrit les informations du pilote vidéo. Activez cette section avant d'ajouter les informations de votre pilote vidéo. Pour activer cette section :

   a) Consultez le guide de la carte fourni par le fabricant pour obtenir des informations sur la configuration. Un fichier de configuration natif peut être généré. Vérifiez que votre carte fonctionne dans un environnement local avec le fichier de configuration natif lorsque vous n'exécutez pas une session de Linux VDA.

   b) Copiez la section « Device » du fichier de configuration natif vers**ctx-driver_name-1.conf.**

3. Exécutez la commande suivante pour définir la clé de registre de façon à permettre au Linux VDA de reconnaître le nom du fichier de configuration défini à l'étape 1.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\System\
     CurrentControlSet\Control\Citrix\XDamage" -t "REG_SZ" -v "
     DriverName" -d "intel" --force
2 <!--NeedCopy-->
```

Activer les graphiques non vGPU

Cette fonctionnalité est désactivée par défaut. Vous pouvez exécuter la commande suivante pour l'activer en définissant la valeur XDamageEnabled sur 1.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\System\
     CurrentControlSet\Control\Citrix\XDamage" -t "REG_DWORD" -v "
     XDamageEnabled" -d "0x00000001" --force
2 <!--NeedCopy-->
```


Occultation de moniteur pour les VDA Remote PC Access

Le Linux VDA prend en charge l'occultation de moniteur physique pour les VDA Remote PC Access qui utilisent des cartes graphiques non vGPU. Cette amélioration décharge l'affichage graphique sur des moniteurs virtuels EVDI (Extensible Virtual Display Interface).

> **Remarque :**
>
> Le nombre maximal de moniteurs virtuels EVDI varie selon les distributions.

L'occultation de moniteur fonctionne pour les VDA Ubuntu 20.04 et Debian 11.3. Pour utiliser l'occultation de moniteur, effectuez les deux étapes suivantes :

1. Installez le package `evdi-dkms` basé sur votre distribution Linux :

```
sudo apt install evdi-dkms
<!--NeedCopy-->
```

2. Activez le déchargement de l'affichage graphique vers l'EVDI :

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
   Evdi" -d "0x00000001" --force
<!--NeedCopy-->
```

3. Si vous utilisez une carte graphique Intel, désactivez le gestionnaire d'affichage. Sinon, la carte Intel est occupée par le gestionnaire d'affichage et n'est pas disponible pour les sessions distantes Citrix.

```
sudo systemctl disable --now gdm
<!--NeedCopy-->
```

Dépannage

Pas de sortie graphique ou sortie illisible

Si vous pouvez exécuter des applications 3D localement et que toutes les configurations sont correctes, une sortie graphique manquante ou illisible est due à un bogue. Utilisez /opt/Citrix/VDA/bing/setlog et définissez GFX_X11 sur Détaillé afin de collecter les informations de trace à des fins de débogage.

Le codage matériel ne fonctionne pas

Cette fonctionnalité prend uniquement en charge le codage logiciel.

Filigrane de session

December 16, 2022

Le filigrane de session aide à dissuader et à suivre le vol de données. Les informations traçables apparaissent sur les bureaux 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 sous forme de calque de texte ou d'image PNG avec couche alpha. Le filigrane s'affiche sur l'intégralité de l'écran de session sans modifier le contenu du document d'origine.

> **Important :**
>
> le filigrane de session n'est pas un élément de sécurité. Cela n'empêche pas complètement le vol de données, mais elle offre un certain niveau de dissuasion et de traçabilité. Nous ne garantissons pas la traçabilité complète des informations lors de l'utilisation de cette fonctionnalité. Nous vous recommandons plutôt de combiner cette fonctionnalité avec d'autres solutions de sécurité, le cas échéant.

Le filigrane de session contient des informations utilisées pour le suivi du vol de données. Les données les plus importantes sont l'identité de l'utilisateur, suivie via ses informations d'identification de connexion, de la session 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 de filigrane de session suivants pour configurer l'emplacement et l'apparence du filigrane sur l'écran :

Paramètres de stratégie Filigrane de session

Activer le filigrane de session

Lorsque vous activez ce paramètre, l'affichage de la session comporte un filigrane opaque affichant des informations spécifiques à la session. Les autres paramètres de filigrane dépendent du paramètre activé.

Par défaut, le filigrane de session est désactivé.

Inclure adresse IP du client

Lorsque vous activez ce paramètre, la session affiche l'adresse IP du client actuel en tant que filigrane.

Par défaut, l'option **Inclure adresse IP du client** est désactivée.

Inclure l'heure de connexion

Lorsque vous activez ce paramètre, le filigrane de session affiche une heure de connexion. Le format est aaaa/mm/jj hh:mm. L'heure affichée est basée sur l'horloge système et le fuseau horaire.

Par défaut, l'option **Inclure l'heure de connexion** est désactivée.

Inclure nom d'utilisateur de connexion

Lorsque vous activez ce paramètre, la session affiche le nom d'utilisateur de connexion actuel en tant que filigrane. Le format d'affichage est NOMUTILISATEUR@NOMDOMAINE. Nous vous recommandons d'utiliser un nom d'utilisateur de 20 caractères maximum. Lorsqu'un nom d'utilisateur comporte plus de 20 caractères, des tailles de police plus petites ou des troncations peuvent se produire, ce qui réduit l'efficacité du filigrane.

Par défaut, l'option **Inclure nom d'utilisateur de connexion** est activée.

Inclure nom d'hôte du VDA

Lorsque vous activez ce paramètre, la session affiche le nom d'hôte du VDA de la session ICA en cours en tant que filigrane.

Par défaut, l'option **Inclure nom d'hôte du VDA** est activée.

Inclure adresse IP du VDA

Lorsque vous activez ce paramètre, la session affiche l'adresse IP du VDA de la session ICA en cours en tant que filigrane.

Par défaut, l'option **Inclure adresse IP du VDA** est désactivée.

Style de filigrane de session

Ce paramètre détermine si vous affichez un seul ou plusieurs filigranes. Choisissez **Multiple** ou **Simple** dans le menu déroulant **Valeur**.
Pour d'autres options de style, consultez la section **Texte personnalisé en filigrane** de cet article.

L'option **Multiple** permet d'afficher cinq filigranes dans la session. un dans le centre et quatre dans les coins.

L'option **Simple** permet d'afficher un seul filigrane au centre de la session.

Par défaut, le **style de filigrane de session** est défini sur **Multiple**.

Transparence du filigrane

Vous pouvez spécifier l'opacité du filigrane de 0 à 100. Plus la valeur spécifiée est grande, plus le filigrane est opaque.

Par défaut, la valeur est 17.

Texte personnalisé en filigrane

La valeur est vide par défaut. Vous pouvez taper une chaîne non vide, définir une syntaxe pour former une chaîne ou utiliser la combinaison des deux pour l'afficher dans le filigrane de la session. Les chaînes non vides peuvent contenir jusqu'à 25 caractères Unicode par ligne. Les chaînes plus longues sont tronquées à 25 caractères.

Par exemple, vous pouvez définir la stratégie sur la valeur suivante :

```
<date> <time><newline><username><style=single><fontsize=40><font=
Ubuntu><position=center><rotation=0><newline><serverip><newline><
clientip><newline>Citrix Linux VDA<newline>Version 2207
```

Pour obtenir une description de toutes les options de syntaxe, consultez le tableau suivant :

Option de syntaxe	Description	Paramètre valide (sensible à la casse)	Valeur par défaut	Remarques
`<style>`	Style de disposition du filigrane	`xstyle`, `single`, `tile`, `horizontal`	`xstyle`	-
`<position>`	Position du filigrane	`center`, `topleft`, `topright`, `bottomleft`, `bottomright`	`center`	Valide uniquement lorsque le style de disposition est défini sur **Unique**.
`<rotation>`	Rotation du filigrane selon un certain angle	-180–180	0	-
`<transparency>`	Opacité du filigrane	0–100	17	-

Option de syntaxe	Description	Paramètre valide (sensible à la casse)	Valeur par défaut	Remarques
<font>	-	Police prise en charge par le système	Sans	-
<fontsize>	-	20–50	0 (calculé automatiquement)	-
<fontzoom>	Pourcentage des tailles de police et d'image que vous définissez via <fontsize> et <image>	0 –	100	-
<image>	Filigrane PNG	Chemin d'accès à une image PNG sur le VDA	S.O.	Cette syntaxe configure un filigrane PNG. Seul le format PNG avec une couche alpha est pris en charge. Si un filigrane PNG est utilisé, seules les options de syntaxe <style>, <position>, <rotation>, <transparency> et <fontzoom> peuvent être appliquées.
<date>	Espace réservé pour la date de connexion à la session (AAAA/MM/JJ)	S.O.	S.O.	-

Option de syntaxe	Description	Paramètre valide (sensible à la casse)	Valeur par défaut	Remarques
<time>	Espace réservé pour l'heure de connexion à la session (HH:MM)	S.O.	S.O.	-
<domain>	Espace réservé pour le domaine du compte d'utilisateur	S.O.	S.O.	-
<username>	Espace réservé pour le nom d'utilisateur d'ouverture de session actuel (à l'exception du domaine du compte d'utilisateur)	S.O.	S.O.	-
<hostname>	Espace réservé pour le nom d'hôte du VDA	S.O.	S.O.	-
<clientip>	Espace réservé pour l'adresse IP du client	S.O.	S.O.	-
<serverip>	Espace réservé pour l'adresse IP du VDA	S.O.	S.O.	-

> **Remarque :**
>
> Si le **texte personnalisé en filigrane** est spécifié avec un paramètre de syntaxe valide, toutes les autres stratégies de filigrane de session, sauf **Activer le filigrane de session**, sont ignorées.
>
> Si vous laissez une option de syntaxe non spécifiée ou si vous la définissez sur une valeur non prise en charge, sa valeur par défaut est utilisée.

Limitations

- Le filigrane de session est pris en charge dans l'un des cas suivants :
  - Lorsque l'option **Utiliser codec vidéo pour la compression** est définie sur **Pour l'écran entier**.
  - Lorsque l'option **Utiliser codec vidéo pour la compression** est définie sur **Utiliser au choix** et que l'option Optimiser pour la charge des graphiques 3D est activée.
- Le filigrane de session n'est pas pris en charge dans les sessions dans lesquelles la redirection du contenu du navigateur est utilisée. Pour utiliser la fonction de filigrane de session, assurez-vous que la redirection du contenu du navigateur est désactivée.
- Le filigrane de session n'est pas pris en charge et n'apparaît pas si la session s'exécute en mode d'accélération matérielle plein écran (codage H.264 ou H.265) avec des pilotes NVIDIA d'ancienne génération (dans ce cas, NvCaptureType est défini sur 2 dans le Registre).
- Le filigrane n'est pas visible pour l'observation de session.
- Si vous appuyez sur la touche Impr. écran pour capturer un écran, l'écran capturé du côté VDA n'inclut pas le filigrane. Nous vous recommandons de prendre des mesures pour éviter que les captures d'écran ne soient copiées.

Affichage progressif Thinwire

December 16, 2022

L'interactivité de session peut se dégrader sur des connections à faible bande passante ou à latence élevée. Par exemple, le défilement d'une page Web peut devenir lent, ne pas répondre ou être saccadé. Les opérations de clavier et de souris peuvent être à la traîne des mises à jour graphiques.

Jusqu'à la version 7.17, vous pouviez utiliser les paramètres de stratégie pour réduire la consommation de bande passante en configurant la session sur une **faible** qualité visuelle ou en définissant une profondeur de couleur inférieure (graphiques 16 ou 8 bits). Cependant, vous aviez besoin de savoir qu'un utilisateur était sur une connexion faible. HDX Thinwire n'ajustait pas dynamiquement la qualité des images statiques en fonction des conditions du réseau.

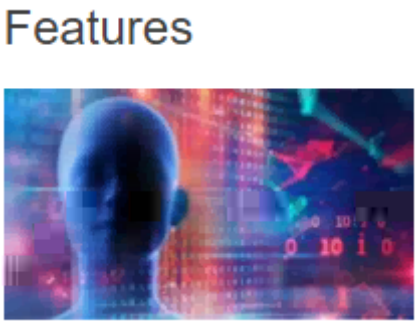
À partir de la version 7.18, HDX Thinwire passe en mode de mise à jour progressive par défaut dans l'un des cas suivants :

- La bande passante disponible est inférieure à 2 Mbits/s.
- La latence du réseau dépasse 200 ms.

Dans ce mode :

Par exemple, dans le graphique suivant où le mode de mise à jour progressive est actif, les lettres **F** et **e** disposent d'artefacts bleus et l'image est fortement compressée. Cette approche réduit considérablement la consommation de bande passante, ce qui permet de recevoir les images et le texte plus rapidement et améliore l'interactivité de la session.

Lorsque vous arrêtez d'interagir avec la session, les images et le texte dégradés sont progressivement affinés sans perte. Par exemple, dans le graphique suivant, les lettres ne contiennent plus d'artefacts bleus et la qualité de l'image est restaurée.



Pour les images, l'amélioration de la netteté utilise une méthode aléatoire de type bloc. Pour le texte, des lettres individuelles ou des parties de mots sont affinées. Le processus d'amélioration de la netteté se produit sur plusieurs trames. Cette approche évite d'introduire un retard avec une trame importante unique d'amélioration de la netteté.

Les images transitoires (vidéo) sont toujours gérées avec l'affichage adaptatif ou sélectif H.264.

Utilisation du mode progressif

Par défaut, le mode progressif attend les paramètres de la stratégie **Qualité visuelle** : **Élevé**, **Moyen** (par défaut) et **Faible**.

Le mode progressif est désactivé (non utilisé) lorsque :

- **Qualité visuelle** = **Toujours sans perte** ou **Sans perte si possible**
- **Nombre de couleurs préféré pour les graphiques simples** = 8 bits

- **Utiliser codec vidéo pour la compression** = **Pour l'écran entier** (lorsque le mode H.264 en plein écran est souhaité)

Lorsque le mode progressif est en veille, il est activé par défaut lorsque l'une des conditions suivantes se présente :

- La bande passante disponible est inférieure à 2 Mbits/s.
- La latence du réseau est supérieure à 200 ms.

Après un changement de mode, un minimum de 10 sec est passé dans ce mode, même si les conditions de réseau défavorables sont momentanées.

Changement du comportement du mode progressif

Vous pouvez modifier le comportement du mode progressif en exécutant la commande suivante :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\
     CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
     ProgressiveDisplay" -d "<value>" --force
2 <!--NeedCopy-->
```

Où <\value\> :

0 = Toujours désactivé (ne jamais utiliser)

1 = Automatique (bascule en fonction des conditions du réseau, valeur par défaut)

2 = Toujours activé

En mode automatique (1), vous pouvez exécuter les commandes suivantes pour modifier les seuils de basculement du mode progressif :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg  create -k "HKEY_LOCAL_MACHINE\SYSTEM\
     CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
     ProgressiveDisplayBandwidthThreshold" -d "<value>" --force
2 <!--NeedCopy-->
```

où <value> est le <seuil en Kbit/s> (par défaut = 2,048)

Exemple : 4096 = bascule en mode progressif si la bande passante descend sous 4 Mbits/s

```
1 sudo /opt/Citrix/VDA/bin/ctxreg  create -k "HKEY_LOCAL_MACHINE\SOFTWARE
     \CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
     ProgressiveDisplayLatencyThreshold" -d "<value>" --force
2 <!--NeedCopy-->
```

où <value> est le <seuil en ms> (par défaut = 200)

Exemple : 100 = bascule en mode progressif si le réseau descend sous 100 ms.

Clavier

December 16, 2022

Cette section contient les rubriques suivantes :

- Éditeur IME du client
- Synchronisation de l'interface utilisateur de l'éditeur IME client
- Synchronisation dynamique de la disposition du clavier
- Clavier logiciel
- Prise en charge des entrées en plusieurs langues

Éditeur IME

December 16, 2022

Vue d'ensemble

Les caractères codés sur deux octets, tels que les caractères chinois, japonais et coréen, doivent être saisis via un éditeur IME. Tapez ces caractères au moyen de tout éditeur IME compatible avec l'application Citrix Workspace du côté client, tel que l'éditeur IME CJK Windows natif.

Installation

Cette fonctionnalité est installée automatiquement lorsque vous installez le Linux VDA.

Utilisation

Ouvrez une session Citrix Virtual Apps ou Citrix Virtual Desktops comme d'habitude.

Modifiez votre méthode d'entrée conformément à ce qui est requis sur le client pour commencer à utiliser à la fonctionnalité d'éditeur IME client.

Problèmes connus

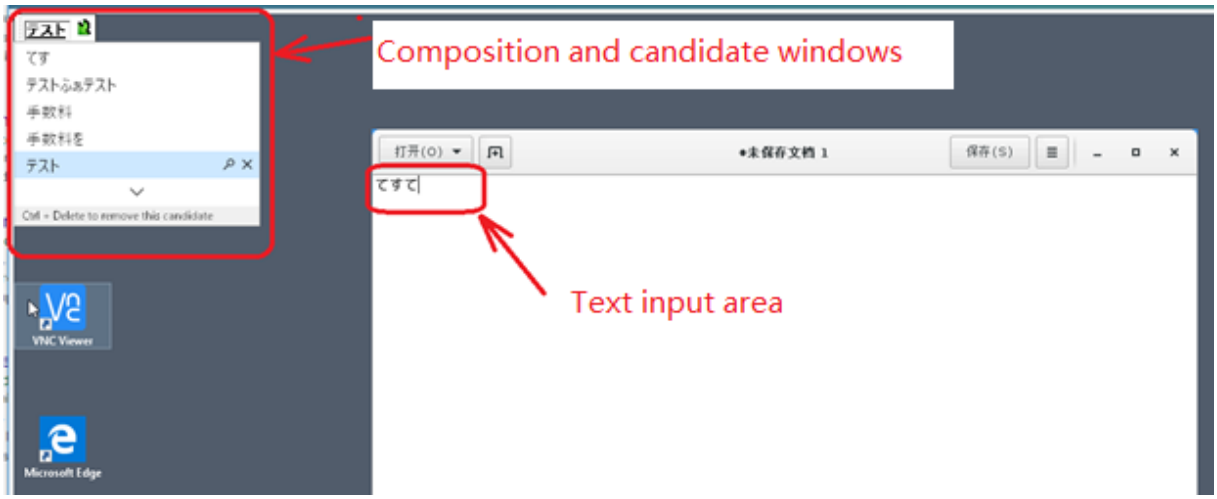
- Vous devez double-cliquer sur une cellule dans une feuille de calcul Google avant de pouvoir utiliser la fonctionnalité d'éditeur IME client pour saisir des caractères dans la cellule.
- La fonctionnalité d'éditeur IME client n'est pas automatiquement désactivé dans les champs de mot de passe.
- L'interface utilisateur de l'éditeur IME ne suit pas le curseur dans la zone de saisie.

Synchronisation de l'interface utilisateur de l'éditeur IME client

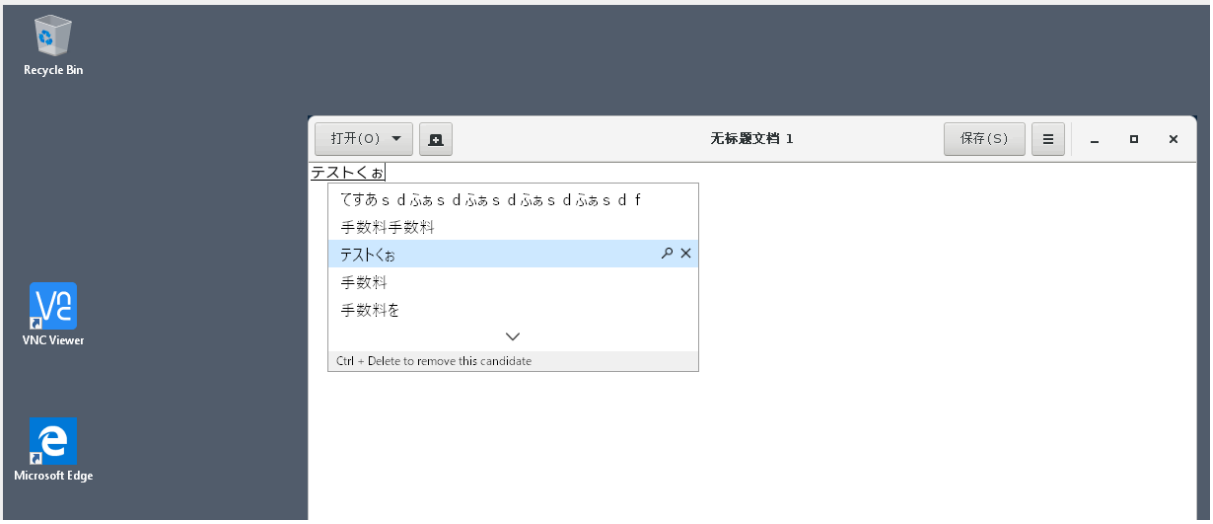
December 16, 2022

Vue d'ensemble

Jusqu'à présent, l'interface utilisateur de l'éditeur IME client (y compris la fenêtre de composition et la fenêtre candidate) était positionnée dans le coin supérieur gauche de l'écran. Celle-ci ne suivait pas le curseur et était parfois située loin du curseur dans la zone de saisie de texte.



Citrix améliore la convivialité et optimise davantage l'expérience avec l'éditeur IME client comme suit :



Conditions préalables à l'utilisation de la fonctionnalité

1. Activez Intelligent Input Bus (`IBus`) sur votre Linux VDA. Pour plus d'informations sur la manière d'activer `IBus` sur un système d'exploitation Linux, consultez la documentation du fournisseur du système d'exploitation. Par exemple :
   - Ubuntu : https://help.ubuntu.com/community/ibus
   - CentOS, RHEL : https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/7.0_release_notes/sect-red_hat_enterprise_linux-7.0_release_notes-internationalization-input_methods
   - Debian : https://wiki.debian.org/I18n/ibus
   - SUSE : https://documentation.suse.com/sles/15-SP2/html/SLES-all/cha-gnome-settings.html#sec-gnome-settings-lang
2. La fonctionnalité s'installe automatiquement, mais vous devez l'activer avant de pouvoir l'utiliser.

Activer et désactiver la fonctionnalité

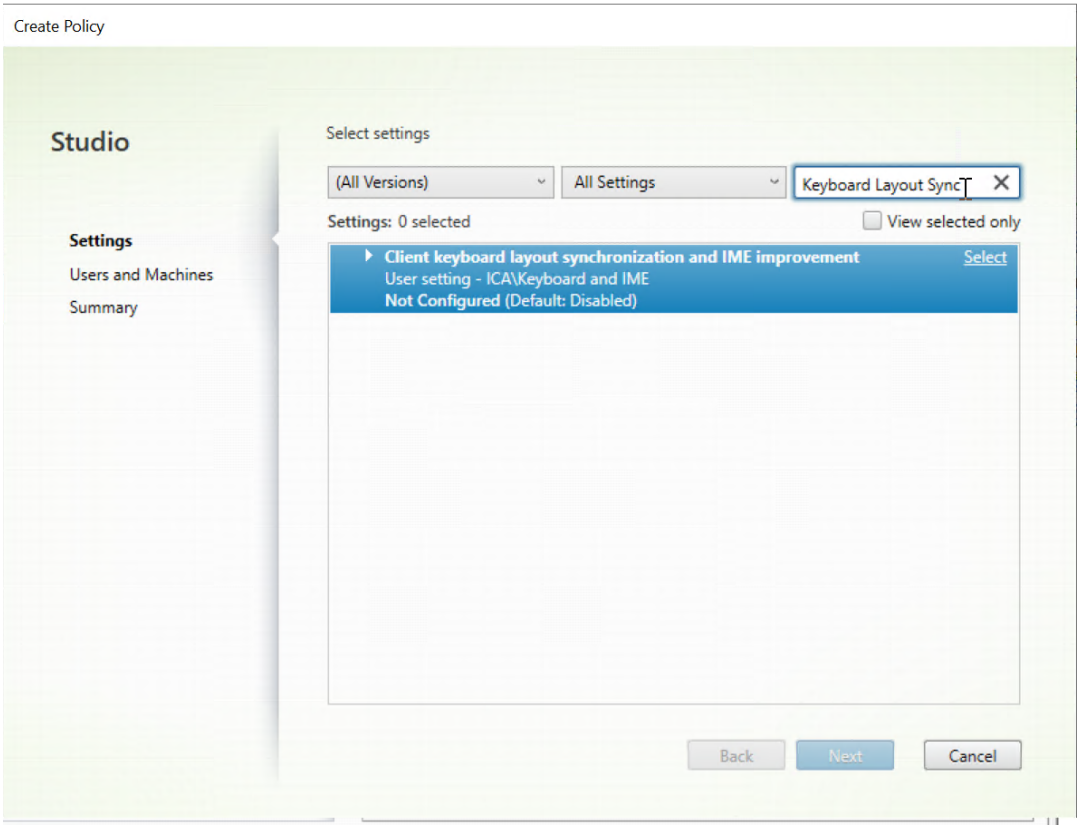
La fonctionnalité de synchronisation de l'interface utilisateur de l'éditeur IME client est désactivée par défaut. Pour activer ou désactiver la fonctionnalité, définissez la stratégie **Synchronisation de la disposition du clavier client et améliorations apportées à l'éditeur IME** ou modifiez le Registre via l'utilitaire `ctxreg`.

> **Remarque :**
>
> La stratégie **Synchronisation de la disposition du clavier client et améliorations apportées à l'éditeur IME** prend la priorité sur les paramètres du Registre et peut être appliquée aux objets

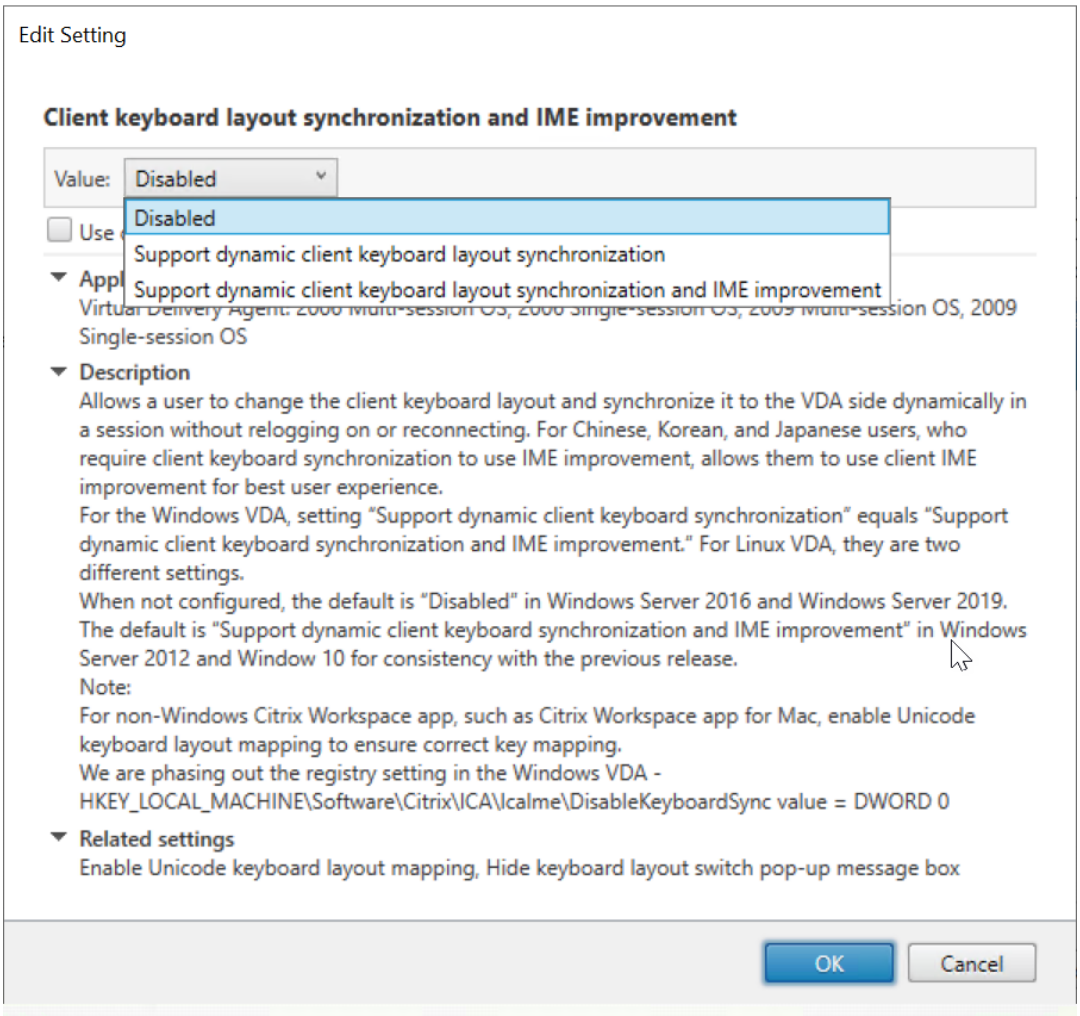
> utilisateur et ordinateur que vous spécifiez ou à tous les objets de votre site. Les paramètres du Registre sur un Linux VDA donné s'appliquent à toutes les sessions de ce VDA.

- Définissez la stratégie **Synchronisation de la disposition du clavier client et améliorations apportées à l'éditeur IME** pour activer ou désactiver la fonctionnalité de synchronisation de l'interface utilisateur de l'éditeur IME client :

  1. Dans Studio, cliquez avec le bouton droit sur **Stratégies** et sélectionnez **Créer une stratégie**.
  2. Recherchez la stratégie **Synchronisation de la disposition du clavier client et améliorations apportées à l'éditeur IME**.



  3. Cliquez sur **Sélectionner** en regard du nom de la stratégie.
  4. Définissez la stratégie.



Trois options sont disponibles :

- **Désactivé** : désactive la synchronisation dynamique de disposition du clavier et la synchronisation de l'interface utilisateur de l'éditeur IME client.
- **Prise en charge de la synchronisation dynamique de la disposition du clavier client** : active la synchronisation dynamique de la disposition du clavier indépendamment de la valeur DWORD de la clé de Registre **SyncKeyboardLayout** sur `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\LanguageBar`.
- **Prise en charge de la synchronisation dynamique de la disposition du clavier client et des améliorations apportées à l'éditeur IME** : permet la synchronisation dynamique de la disposition du clavier et la synchronisation de l'interface utilisateur de l'éditeur IME client, quelles que soient les valeurs DWORD des clés de Registre **SyncKeyboardLayout** et **SyncClientIME** sur `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\LanguageBar`.

- Modifiez le Registre via l'utilitaire `ctxreg` pour activer ou désactiver la fonctionnalité de syn-

chronisation de l'interface utilisateur de l'éditeur IME client :

Pour activer cette fonctionnalité, exécutez la commande suivante :

```
1  /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
       CurrentControlSet\Control\Citrix\LanguageBar" -v  "
       SyncClientIME" -d "0x00000001"
2  <!--NeedCopy-->
```

Pour désactiver cette fonctionnalité, exécutez la commande suivante :

```
1  /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
       CurrentControlSet\Control\Citrix\LanguageBar" -v "
       SyncClientIME" -d "0x00000000"
2  <!--NeedCopy-->
```

Synchronisation dynamique de la disposition du clavier

December 16, 2022

Auparavant, les dispositions de clavier sur le Linux VDA et sur la machine cliente devaient être les mêmes. Des problèmes de mappage des clés peuvent survenir, par exemple, lorsque la disposition du clavier passe de l'anglais au français sur la machine cliente, mais pas sur le VDA.

Citrix résout le problème en synchronisant automatiquement la disposition du clavier du VDA avec la disposition du clavier de la machine cliente. Chaque fois que la disposition du clavier de la machine cliente change, la disposition sur le VDA change en conséquence.

> **Remarque :**
>
> L'application Citrix Workspace pour HTML5 ne prend pas en charge la fonctionnalité de synchronisation dynamique de la disposition du clavier.

Configuration

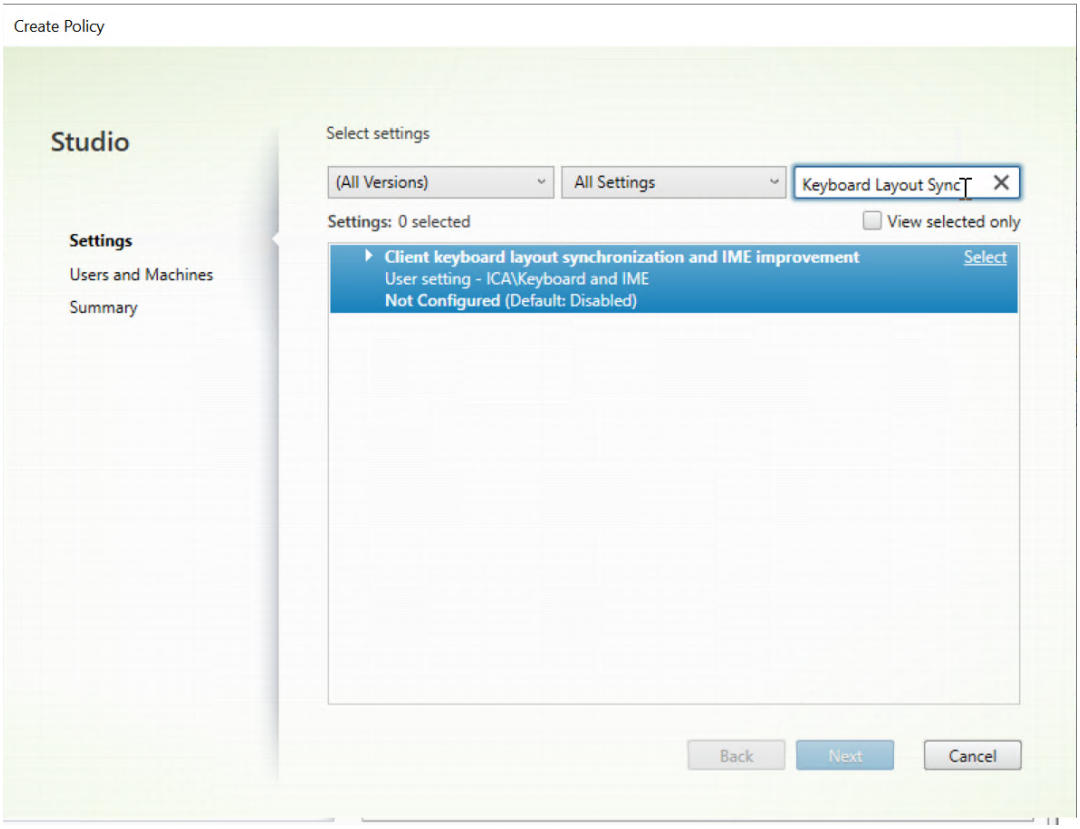
La fonctionnalité de synchronisation dynamique de la disposition du clavier est désactivée par défaut. Pour activer ou désactiver la fonctionnalité, définissez la stratégie **Synchronisation de la disposition du clavier client et améliorations apportées à l'éditeur IME** ou modifiez le Registre via l'utilitaire `ctxreg`.

> **Remarque :**
>
> La stratégie **Synchronisation de la disposition du clavier client et améliorations apportées à l'éditeur IME** prend la priorité sur les paramètres du Registre et peut être appliquée aux objets

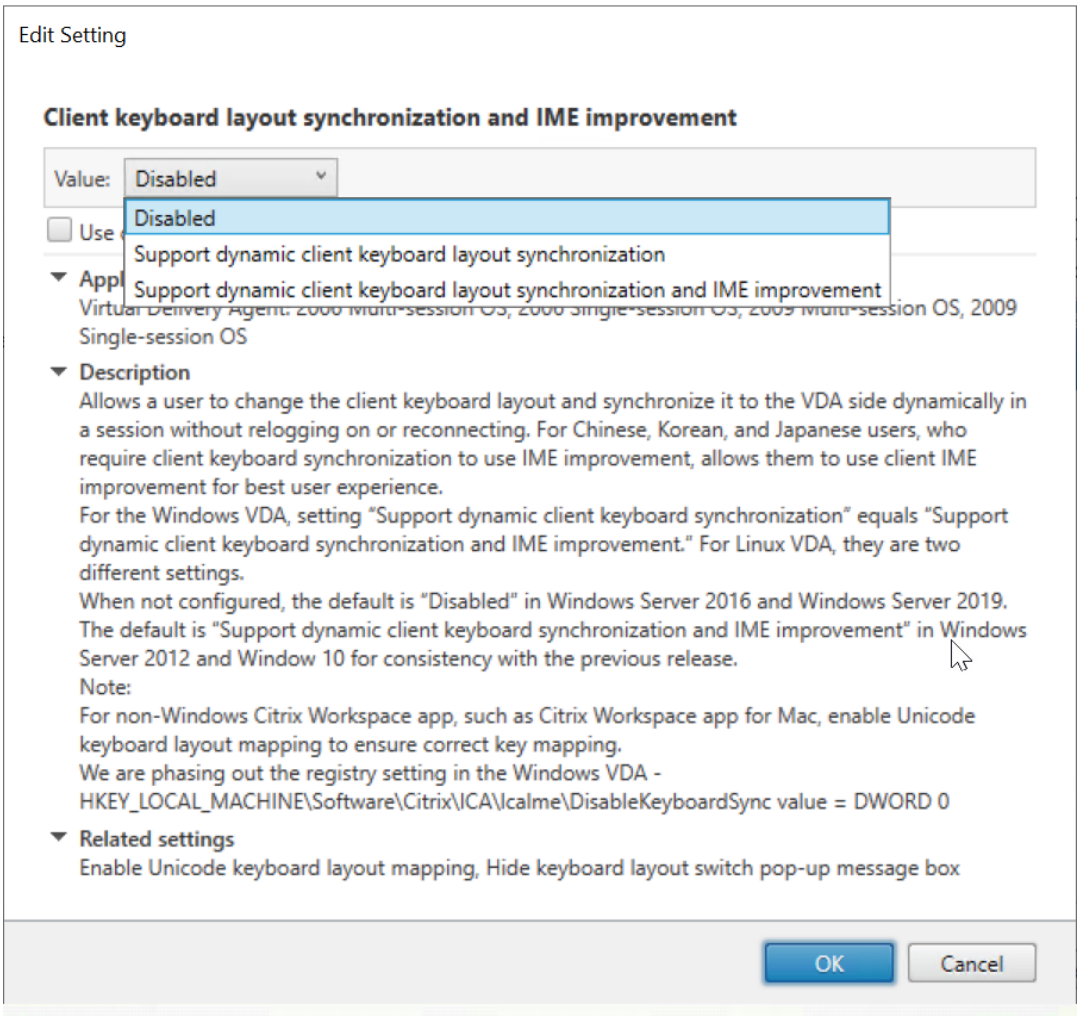
> utilisateur et ordinateur que vous spécifiez ou à tous les objets de votre site. Les paramètres du Registre sur un Linux VDA donné s'appliquent à toutes les sessions de ce VDA.

- Définissez la stratégie **Synchronisation de la disposition du clavier client et améliorations apportées à l'éditeur IME** pour activer ou désactiver la fonctionnalité de synchronisation dynamique de la disposition du clavier :

  1. Dans Studio, cliquez avec le bouton droit sur **Stratégies** et sélectionnez **Créer une stratégie**.
  2. Recherchez la stratégie **Synchronisation de la disposition du clavier client et améliorations apportées à l'éditeur IME**.



  3. Cliquez sur **Sélectionner** en regard du nom de la stratégie.
  4. Définissez la stratégie.



Trois options sont disponibles :

- **Désactivé** : désactive la synchronisation dynamique de disposition du clavier et la synchronisation de l'interface utilisateur de l'éditeur IME client.
- **Prise en charge de la synchronisation dynamique de la disposition du clavier client** : active la synchronisation dynamique de la disposition du clavier indépendamment de la valeur DWORD de la clé de Registre **SyncKeyboardLayout** sur `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\LanguageBar`.
- **Prise en charge de la synchronisation dynamique de la disposition du clavier client et des améliorations apportées à l'éditeur IME** : permet la synchronisation dynamique de la disposition du clavier et la synchronisation de l'interface utilisateur de l'éditeur IME client, quelles que soient les valeurs DWORD des clés de Registre **SyncKeyboardLayout** et **SyncClientIME** sur `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\LanguageBar`.

- Modifiez le Registre via l'utilitaire `ctxreg` pour activer ou désactiver la fonctionnalité de syn-

chronisation dynamique de la disposition du clavier :

Pour activer cette fonctionnalité, exécutez la commande :

```
1  /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
       CurrentControlSet\Control\Citrix\LanguageBar" -v "
       SyncKeyboardLayout" -d "0x00000001"
2  <!--NeedCopy-->
```

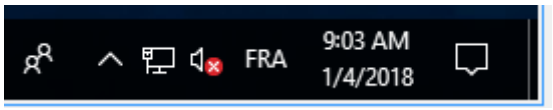
Pour désactiver cette fonctionnalité, exécutez la commande :

```
1  /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
       CurrentControlSet\Control\Citrix\LanguageBar" -v "
       SyncKeyboardLayout" -d "0x00000000"
2  <!--NeedCopy-->
```

Utilisation

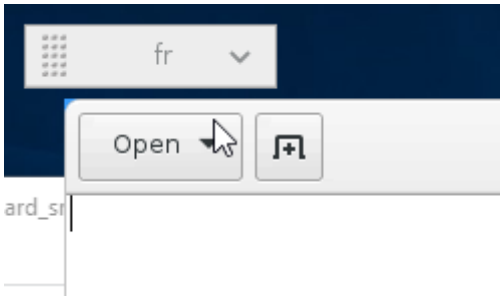
Lorsque cette fonctionnalité est activée, si la disposition du clavier change sur la machine cliente pendant une session, la disposition du clavier de la session change en conséquence.

Par exemple, si vous changez la disposition du clavier sur une machine cliente vers le français (FR) :

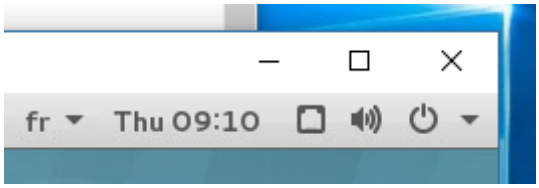


La disposition du clavier de la session Linux VDA devient également « fr ».

Dans une session d'application, ce changement automatique est visible si vous avez activé la barre de langue :



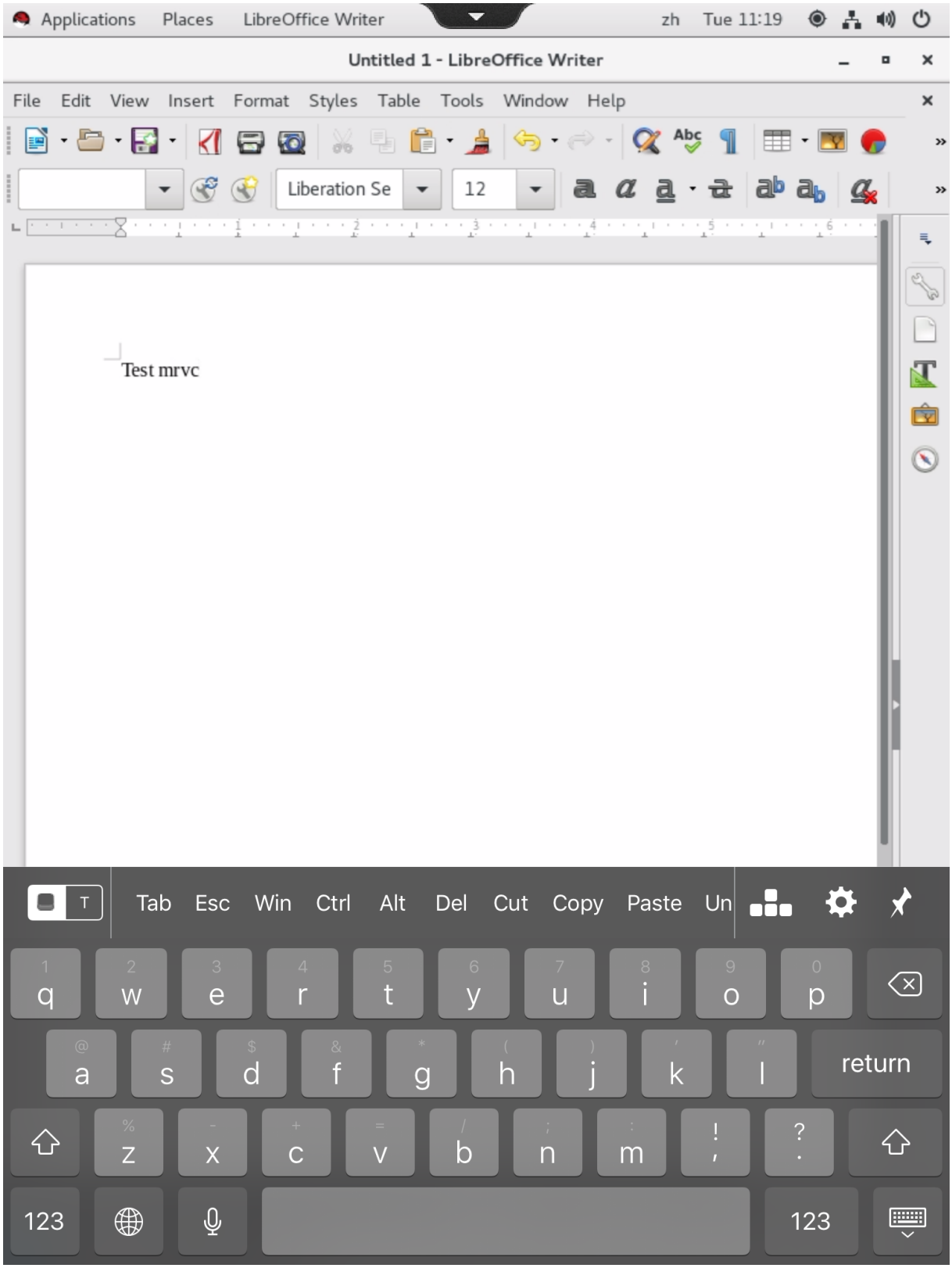
Dans une session de bureau, cette modification automatique est affichée dans la barre des tâches :



Clavier logiciel

December 16, 2022

La fonctionnalité de clavier logiciel est disponible dans une session d'application ou de bureau virtuel Linux. Le clavier logiciel s'affiche ou se masque automatiquement lorsque vous accédez à un champ de saisie ou le quittez.



> **Remarque :**
>
> La fonctionnalité est disponible pour RHEL 7.9, RHEL 8.4, RHEL 8.6, Rocky Linux 8, SUSE 15.3, Ubuntu 22.04, Ubuntu 20.04 et Ubuntu 18.04. Elle est prise en charge sur l'application Citrix Workspace pour iOS et Android.

Activer et désactiver la fonctionnalité

Cette fonction est désactivée par défaut. Utilisez l'utilitaire **ctxreg** pour activer ou désactiver cette fonctionnalité. La configuration de la fonctionnalité sur un Linux VDA donné s'applique à toutes les sessions sur ce VDA.

Pour activer la fonctionnalité :

1. Exécutez la commande :

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
   CurrentControlSet\Control\Citrix\VirtualChannels\MrVc"  -v "
   Enabled" -d "0x00000001"
<!--NeedCopy-->
```

2. Dans Citrix Studio, définissez la stratégie **Affichage automatique du clavier** sur **Autorisé**.
3. (Facultatif) Pour RHEL 7 et CentOS 7, exécutez la commande suivante pour configurer Intelligent Input Bus (`IBus`) en tant que service de messagerie instantanée par défaut :

```
echo "GTK_IM_MODULE=ibus" >>/etc/bashrc
<!--NeedCopy-->
```

Pour désactiver cette fonctionnalité, exécutez la commande suivante :

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\
   Control\Citrix\VirtualChannels\MrVc"  -v "Enabled" -d "0x00000000"
<!--NeedCopy-->
```

> **Remarque :**
>
> les paramètres précédents prennent effet lorsque vous vous connectez à une nouvelle session ou que vous fermez une session et que vous vous reconnectez à la session en cours.

Limitations

- La fonctionnalité peut ne pas fonctionner comme prévu avec Google Chrome, LibreOffice et d'autres applications.
- Pour afficher à nouveau le clavier logiciel après l'avoir masqué manuellement, cliquez sur un champ sans saisie, puis de nouveau sur le champ de saisie actuel.

- Le clavier logiciel peut ne pas apparaître lorsque vous cliquez depuis un champ de saisie vers un autre dans un navigateur Web. Pour contourner ce problème, cliquez sur un champ sans saisie, puis sur le champ de saisie cible.
- La fonctionnalité ne prend pas en charge les caractères Unicode et les caractères codés sur deux octets (tels que les caractères chinois, japonais et coréen).
- Le clavier logiciel n'est pas disponible pour les champs de saisie de mot de passe.
- Le clavier logiciel peut chevaucher le champ de saisie actuel. Dans ce cas, déplacez la fenêtre de l'application ou faites défiler l'écran vers le haut pour déplacer le champ de saisie vers une position accessible.
- En raison de problèmes de compatibilité entre l'application Citrix Workspace et les tablettes Huawei, le clavier logiciel apparaît sur les tablettes Huawei même si un clavier physique est connecté.

Prise en charge des entrées en plusieurs langues

December 16, 2022

Depuis la version 1.4 du Linux VDA, Citrix a ajouté la prise en charge des applications publiées. Les utilisateurs peuvent accéder à une application Linux souhaitée sans l'environnement de bureau Linux.

Toutefois, la barre de langue sur le Linux VDA n'était pas disponible pour l'application publiée, car elle est étroitement intégrée à l'environnement de bureau Linux. Par conséquent, les utilisateurs ne pouvaient pas saisir de texte dans une langue nécessitant un éditeur IME tel que le chinois, le japonais ou le coréen. Les utilisateurs ne pouvaient pas non plus basculer entre les dispositions de clavier pendant une session d'application.

Pour résoudre ces problèmes, cette fonctionnalité fournit une barre de langue pour les applications publiées acceptant la saisie de texte. La barre de langue permet aux utilisateurs de sélectionner un IME côté serveur et de basculer entre les dispositions de clavier durant une session d'application.

Configuration

Vous pouvez utiliser l'utilitaire **ctxreg** pour activer ou désactiver cette fonctionnalité (désactivée par défaut). La configuration de la fonctionnalité sur un serveur Linux VDA donné s'applique à toutes les applications publiées sur ce VDA.

La clé de configuration est « HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar » et le type est DWORD.

Pour activer cette fonctionnalité, exécutez la commande :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
     CurrentControlSet\Control\Citrix\LanguageBar" -v "Enabled" -d "0
     x00000001"
2 <!--NeedCopy-->
```

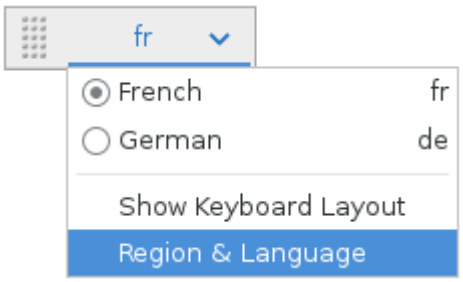
Pour désactiver cette fonctionnalité, exécutez la commande :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
     CurrentControlSet\Control\Citrix\LanguageBar" -v "Enabled" -d "0
     x00000000"
2 <!--NeedCopy-->
```

Utilisation

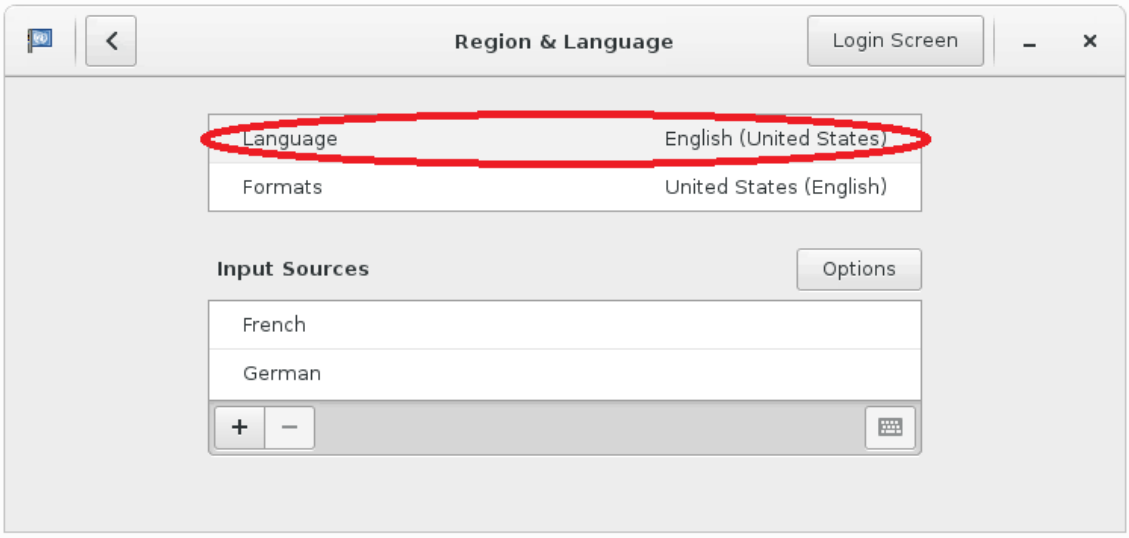
Son utilisation est simple.

1. Activez la fonctionnalité.
2. Accédez à une application publiée pouvant accepter la saisie de texte. Une barre de langue s'affiche dans la session, à côté de l'application.
3. Dans le menu déroulant, sélectionnez **Région et langue** pour ajouter la langue souhaitée (source d'entrée).



4. Sélectionnez l'IME ou la disposition du clavier dans le menu déroulant.
5. Saisissez une langue à l'aide de l'IME ou de la disposition du clavier sélectionné(e).

> **Remarque :**
>
> - Lorsque vous modifiez une disposition de clavier sur la barre de langue côté VDA, vérifiez que la même disposition de clavier est utilisée côté client (application Citrix Workspace).
> - Le package **accountsservice** doit être mis à niveau vers la version 0.6.37 ou ultérieure avant la configuration dans la boîte de dialogue **Région et langue**.



Multimédia

December 16, 2022

Cette section contient les rubriques suivantes :

- Fonctionnalités audio
- Redirection du contenu du navigateur
- Compression vidéo pour Webcam HDX

Fonctionnalités audio

August 7, 2023

Audio adaptatif

L'audio adaptatif est activé par défaut. Il prend en charge les clients de l'application Citrix Workspace suivants :

- Application Citrix Workspace pour Windows versions 2109 et ultérieures
- Application Citrix Workspace pour Linux versions 2109 et ultérieures
- Application Citrix Workspace pour Mac versions 2109 et ultérieures

L'audio adaptatif retourne à l'ancien format d'audio lorsque vous utilisez un client qui ne figure pas dans la liste.

Avec l'audio adaptatif, vous n'avez pas besoin de configurer manuellement les stratégies de qualité audio sur le VDA. L'audio adaptatif ajuste dynamiquement les débits d'échantillonnage audio en fonction des conditions du réseau afin de fournir une expérience audio de qualité supérieure.

Le tableau suivant affiche une comparaison entre l'audio adaptatif et l'ancien format d'audio :

Audio adaptatif	Ancien format d'audio
Taux d'échantillonnage audio max. : 48 kHz	Taux d'échantillonnage audio max. : 8 kHz
Canal stéréo	Canal mono

> **Conseil :**
>
> Utilisez PulseAudio 13.99 ou version ultérieure sur RHEL 8.x.
>
> Utilisez PulseAudio 14.2 ou version ultérieure sur SUSE 15.3.

Redirection du contenu du navigateur

December 16, 2022

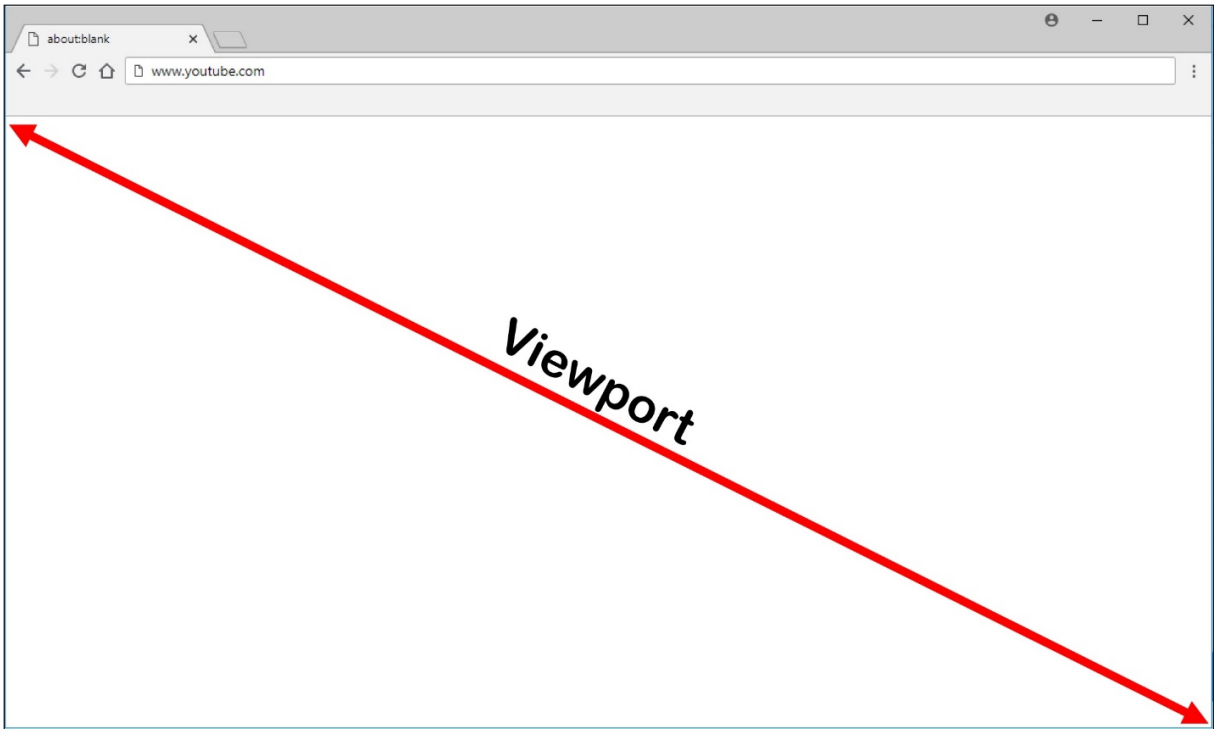
Vue d'ensemble

Le VDA Linux prend en charge la redirection du contenu du navigateur dans Google Chrome. La redirection du contenu du navigateur permet d'afficher les pages Web dans la liste verte du côté client. 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 les pages Web qui sont redirigées sur le client à l'aide d'une liste verte. Inversement, vous pouvez spécifier les pages Web qui ne sont pas redirigées sur le côté client à l'aide d'une liste rouge.

Ce moteur d'affichage Web en superposition est exécuté sur le client plutôt que sur le VDA et utilise l'UC, le GPU, la RAM et le réseau du client.

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 d'éléments tels que la barre d'adresse, la barre de favoris et la barre d'état. Ces éléments sont toujours en cours d'exécution dans le navigateur du VDA.



Configuration système requise

Client Windows :

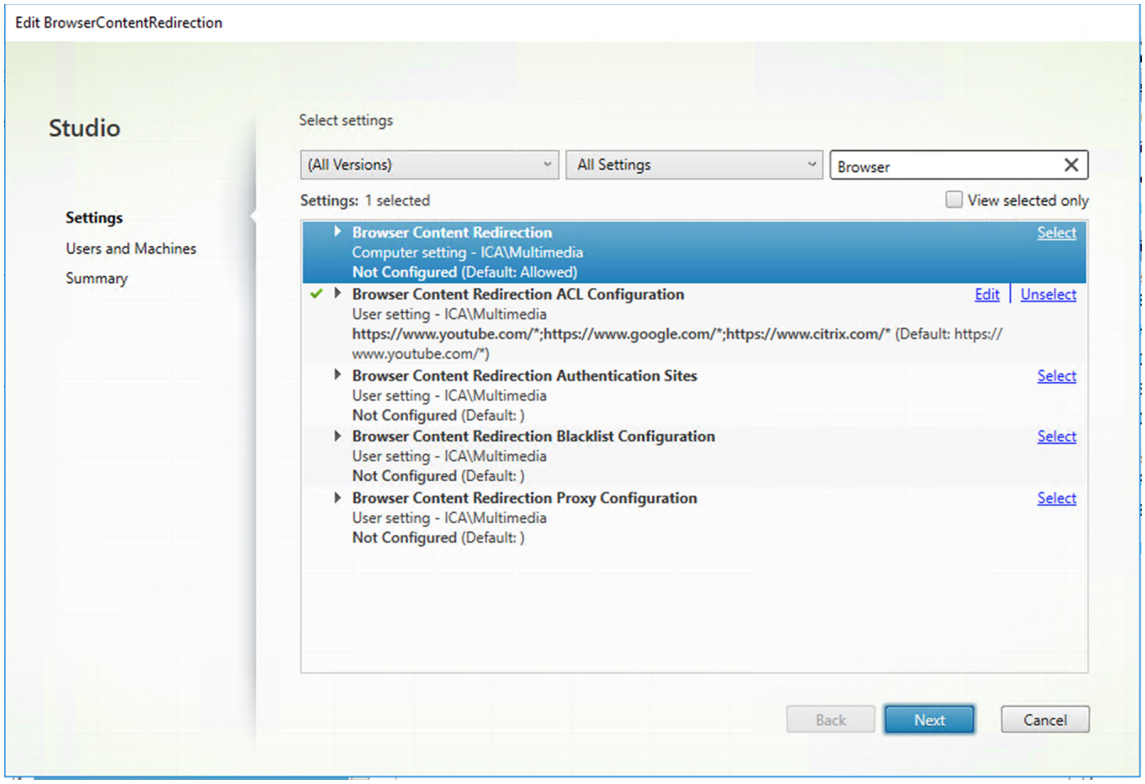
- Application Citrix Workspace 1809 pour Windows ou version ultérieure

Linux VDA :

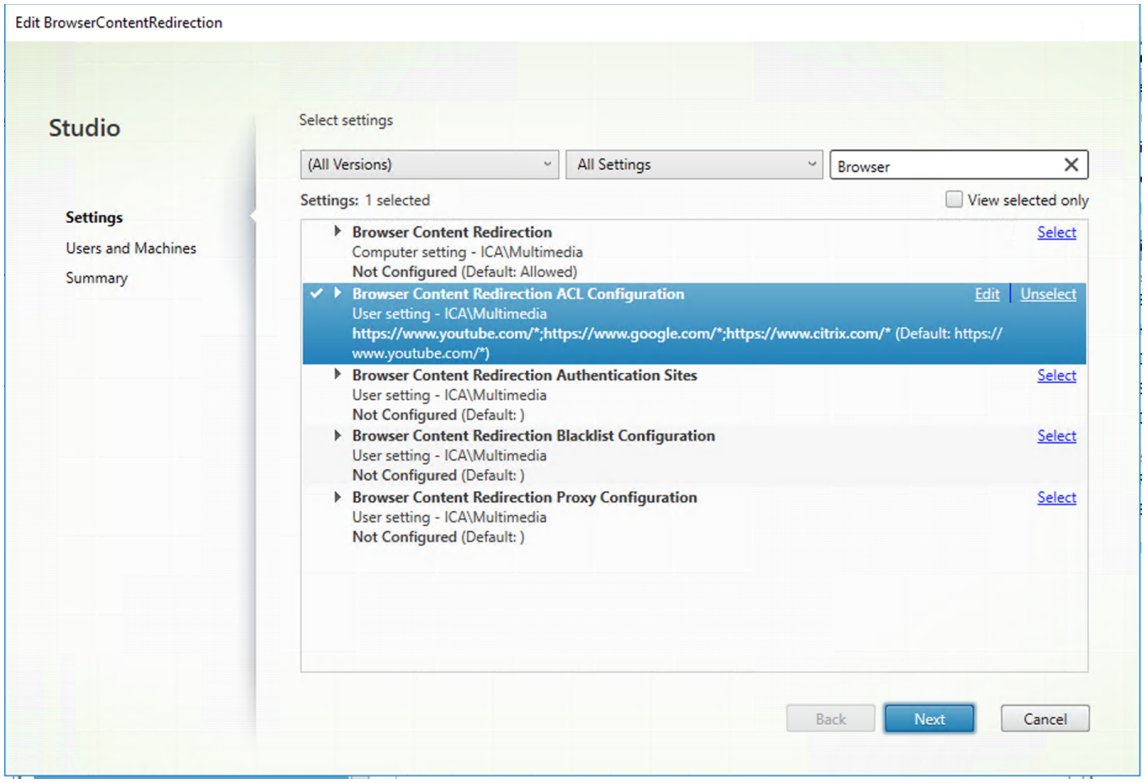
- Navigateur sur le VDA : Google Chrome v66 ou version ultérieure avec l'extension de redirection de contenu du navigateur Citrix ajoutée

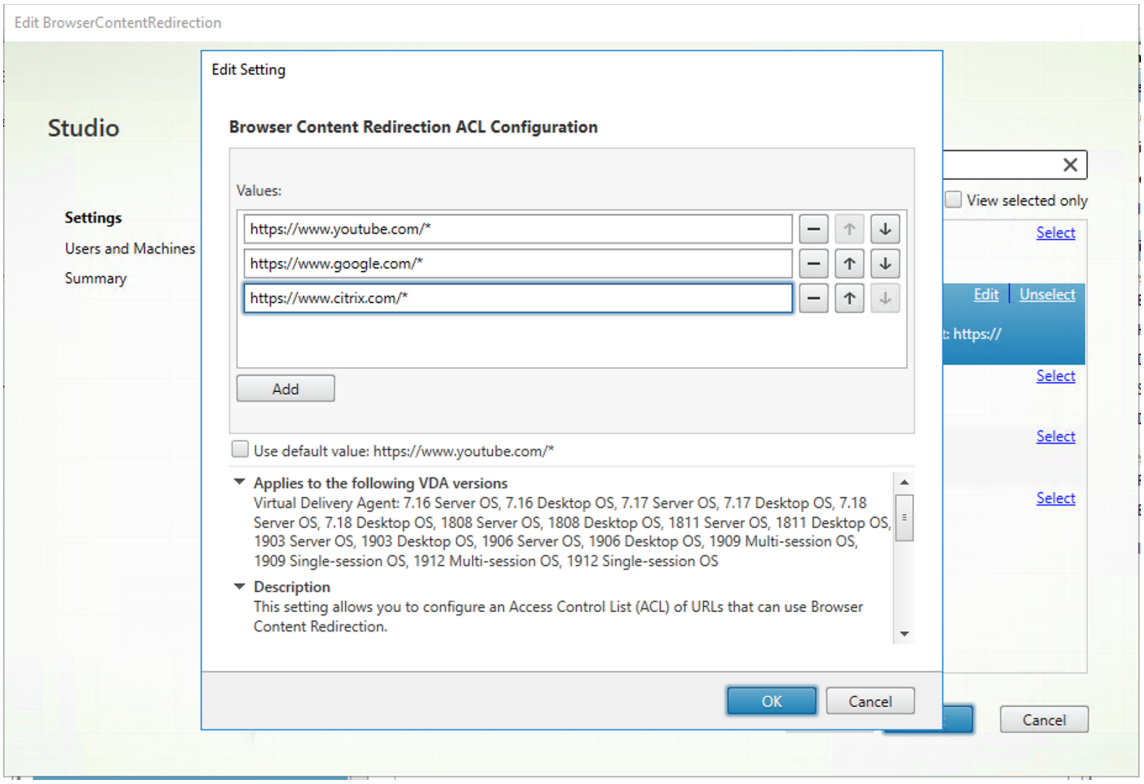
Configurer la redirection du contenu du navigateur

1. Dans Citrix Studio, configurez des stratégies pour spécifier une liste d'autorisation et une liste d'URL bloquées pour la redirection du contenu du navigateur. La redirection du contenu du navigateur est définie sur **Autorisé** par défaut.

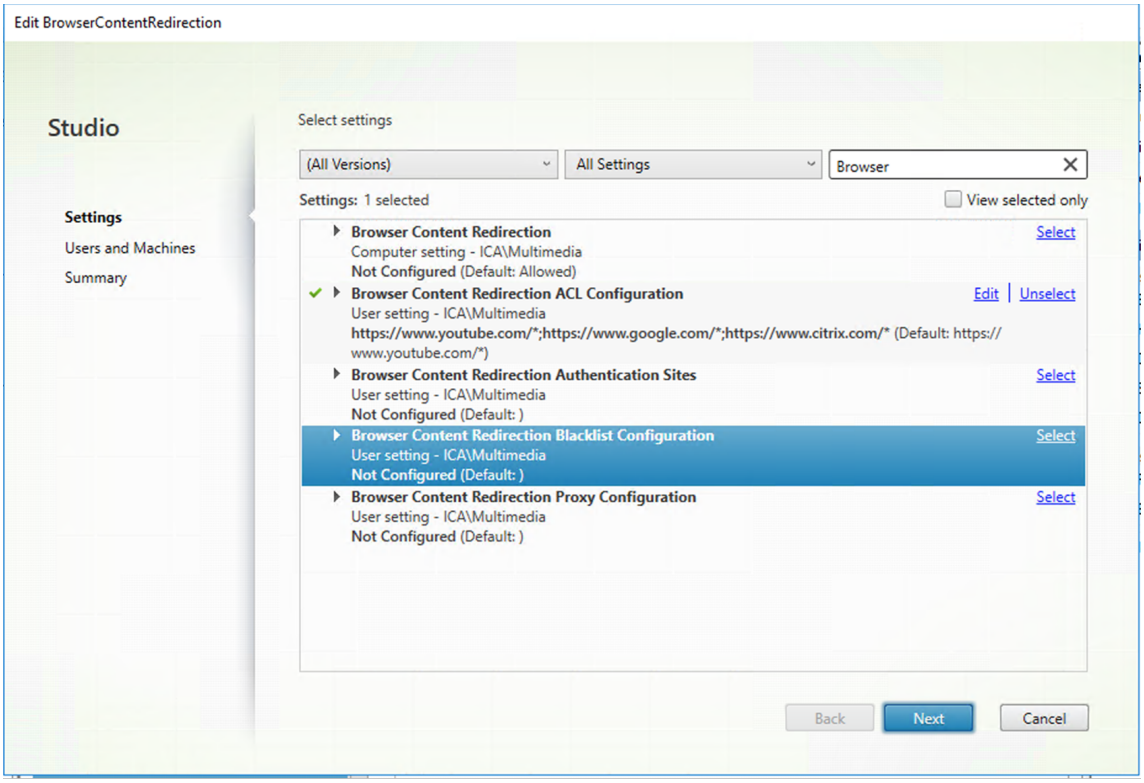


Le paramètre **Configuration de l'ACL de redirection du contenu de navigateur** spécifie une liste verte d'URL pouvant utiliser la redirection du contenu du navigateur.





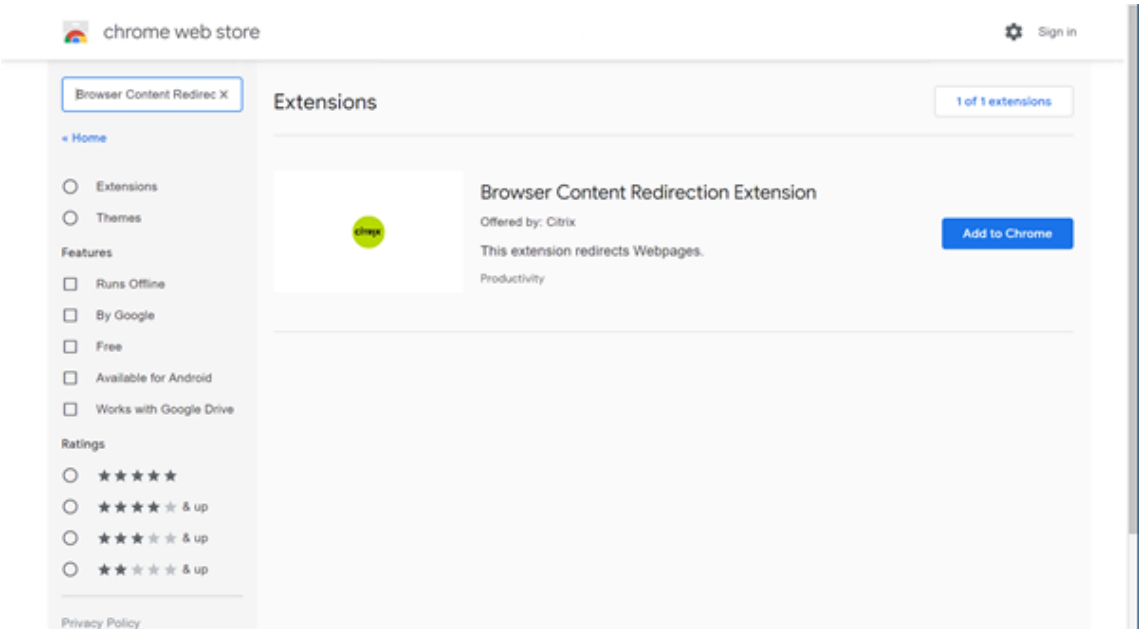
Le paramètre **Configuration d'une liste noire de redirection du contenu de navigateur** spécifie une liste rouge d'URL qui ne peuvent pas utiliser la redirection du contenu du navigateur.



> **Remarque:**
>
> le Linux VDA ne prend actuellement pas en charge le paramètre **Configuration du proxy de redirection du contenu de navigateur**.

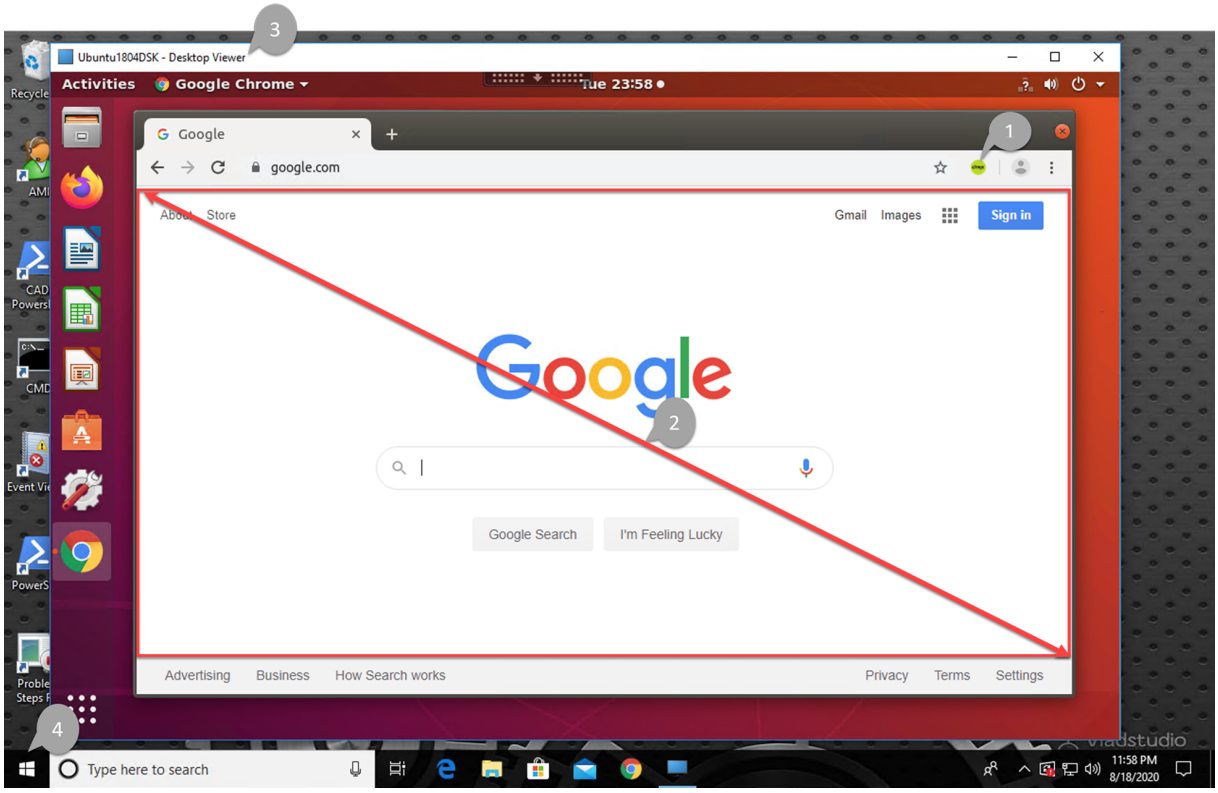
2. Cliquez sur **Ajouter à Chrome** sur le VDA pour ajouter l'extension de redirection de contenu du navigateur Citrix à partir du Chrome Web Store. Cela permet au navigateur du VDA de détecter si une URL (en cours de navigation) figure sur une liste d'autorisation ou une liste de blocage.

   > **Important :**
   >
   > l'extension n'est pas requise sur le client. Ajoutez-la uniquement sur le VDA.
   >
   > 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.



Si une correspondance avec une URL est trouvée dans une liste verte (par exemple, `https://www.mycompany.com/`) mais pas dans une liste rouge, 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.

L'application Citrix Workspace reproduit ensuite de manière transparente le site Web dans la zone de contenu du navigateur de bureau virtuel.



1. Icône de l'extension de redirection de contenu du navigateur Citrix

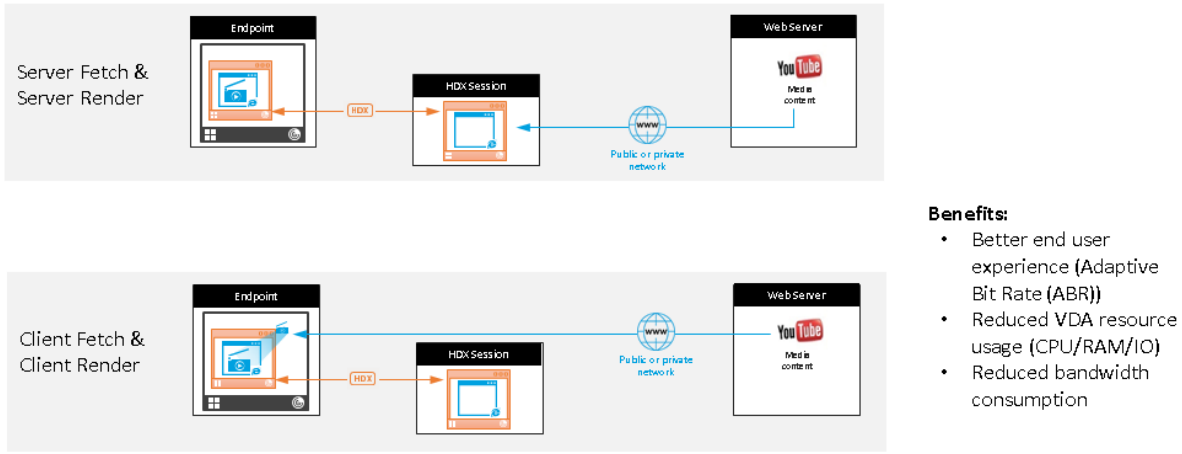
   La couleur de l'icône d'extension indique l'état de l'extension Chrome. Couleurs des différents états :

   - Vert : active et connectée
   - Gris : inactive sur l'onglet actuel
   - Rouge : interrompue/ne fonctionne pas

2. Affichage sur le client ou reproduit sur le bureau virtuel
3. Linux VDA
4. Client Windows

Scénarios de redirection

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. Ce scénario provoque une consommation élevée de CPU, de RAM et de bande passante sur le VDA.
- **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 Citrix Virtual Apps and Desktops.

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.

Compression vidéo pour Webcam HDX

March 27, 2023

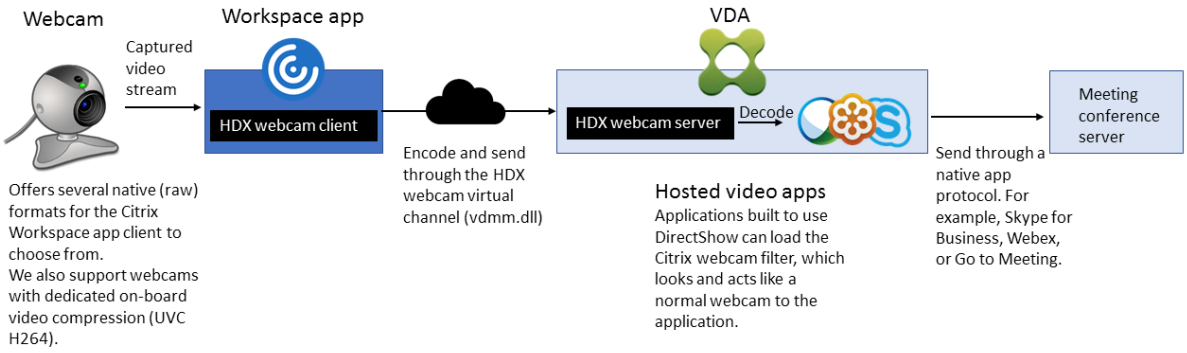
Vue d'ensemble

Les utilisateurs d'applications de visioconférence exécutées dans des sessions Linux VDA peuvent désormais utiliser leurs webcams avec la compression vidéo de webcam HDX. Par défaut, cette fonction

est activée. Nous vous conseillons de toujours utiliser la compression vidéo de webcam HDX si possible.

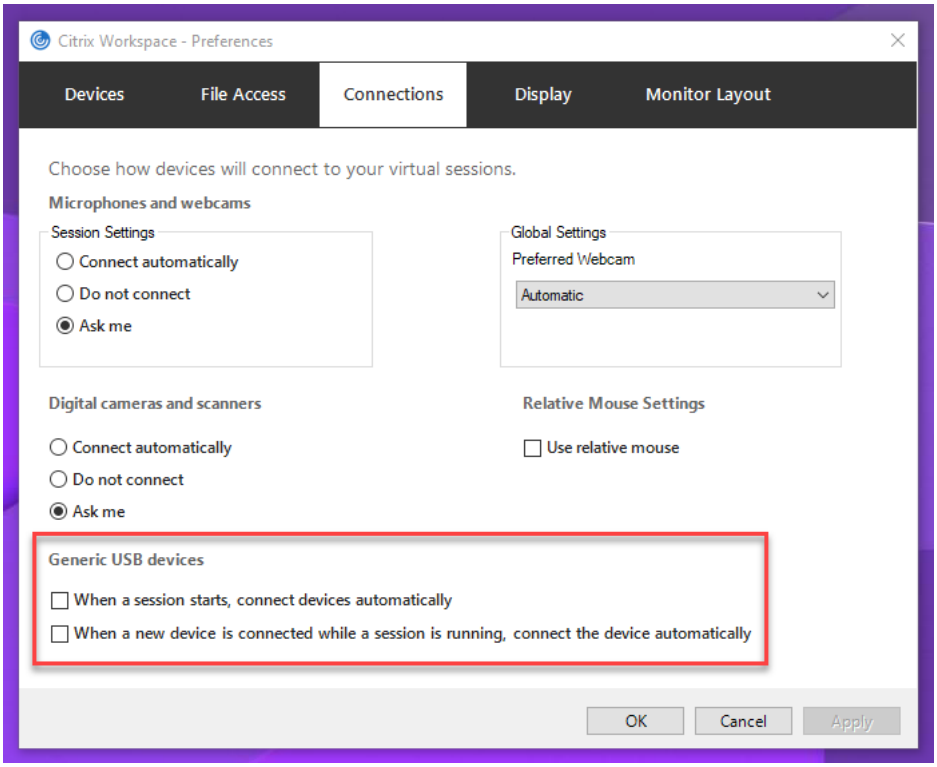
La compression vidéo de webcam HDX est également appelée mode webcam **optimisé**. Ce type de compression vidéo de webcam envoie la vidéo H.264 directement à l'application de visioconférence exécutée dans la session virtuelle. La compression vidéo de webcam HDX utilise la technologie d'infrastructure 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.



Remarque :

- La fonctionnalité n'est pas disponible pour les machines Azure car le module noyau **videodev** dont dépend la fonctionnalité est absent sur les machines Azure.
- Cette fonctionnalité ne prend en charge que les vidéos H.264 de votre client d'application Citrix Workspace.
- La résolution de la webcam prise en charge varie entre 48 x 32 et 1920 x 1080.
- Ne choisissez pas l'option **Périphériques USB génériques** dans la barre d'outils de votre application Citrix Workspace lorsque vous utilisez une webcam. Sinon, des problèmes inattendus peuvent survenir.



Application Citrix Workspace prise en charge

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 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.

Webcams entièrement testées

Différentes webcams offrent des fréquences d'images différentes et ont différents niveaux de luminosité et de contraste. Citrix utilise les webcams suivantes pour la validation initiale des fonctionnalités :

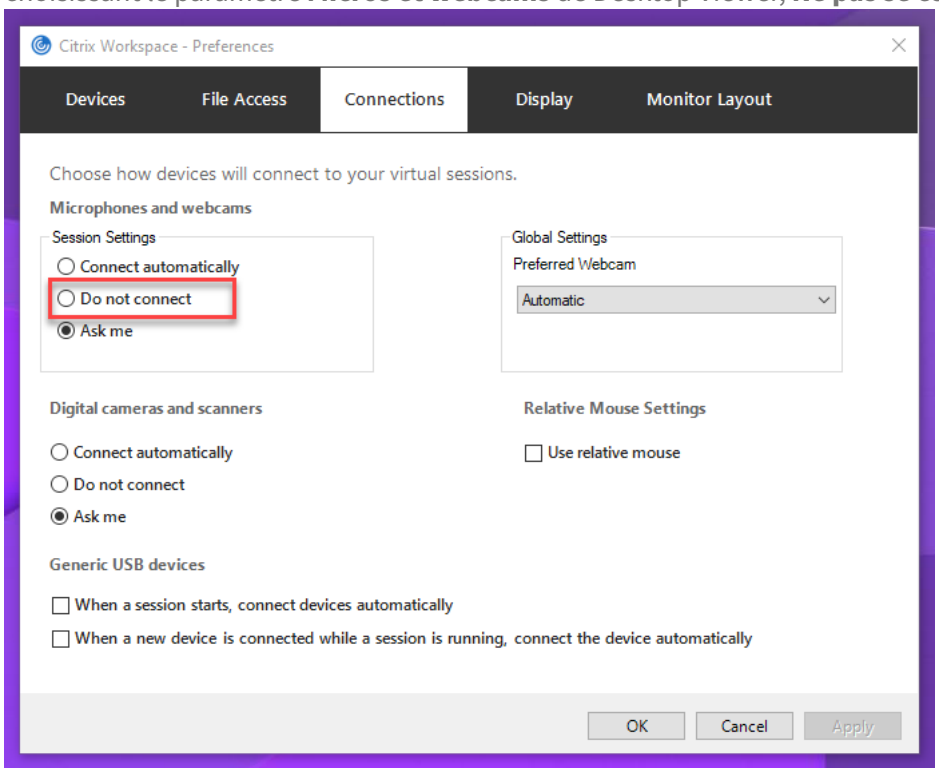
- Logitech HD Webcam C270
- Logitech Webcam C930e
- Microsoft-LifeCam-HD3000

Configuration

Par défaut, cette fonction est activée. Pour l'utiliser, effectuez la vérification et la configuration suivantes :

Conseil :

Les utilisateurs de l'application Citrix Workspace peuvent remplacer le paramètre par défaut en choisissant le paramètre **Micros et webcams** de Desktop Viewer, **Ne pas se connecter**.



1. Une fois l'installation du VDA terminée, vérifiez que votre VDA peut s'enregistrer auprès du Delivery Controller et que les sessions de bureau Linux publiées peuvent être lancées avec succès à l'aide des informations d'identification Windows.

2. Assurez-vous que votre VDA a accès à Internet, puis exécutez la commande `sudo /opt/Citrix/VDA/sbin/ctxwcamcfg.sh` pour terminer la configuration de votre webcam. Si votre VDA n'a pas accès à Internet, passez à l'étape 3.

   > **Remarque :**
   >
   > Une incompatibilité de noyau peut se produire entre `uname -r` et les en-têtes de noyau. Cette incompatibilité entraîne l'échec du script ctxwcamcfg.sh. Pour utiliser correctement la compression vidéo de webcam HDX, exécutez **sudo apt-get dist-upgrade**, redémarrez le VDA, puis réexécutez le script ctxwcamcfg.sh.

   Si votre VDA est déployé sur Debian, assurez-vous qu'il est exécuté sur la dernière version du noyau. Sinon, exécutez les commandes suivantes pour effectuer une mise à jour vers la dernière version du noyau :

   ```
   sudo apt-get update
   sudo apt-get dist-upgrade
   sudo reboot
   <!--NeedCopy-->
   ```

   Si votre VDA est déployé sur SUSE 15.3, SUSE 15.2 ou SUSE 12.5, exécutez les commandes suivantes pour effectuer la mise à jour vers la dernière version du noyau et redémarrer :

   ```
   zypper up kernel-default
   reboot
   <!--NeedCopy-->
   ```

   Le script ctxwcamcfg.sh permet d'effectuer les actions suivantes :

   a) Installez `kernel-devel` et DKMS (Dynamic Kernel Module Support) sur votre VDA.

      - `kernel-devel` est utilisé pour créer un module du noyau de la webcam virtuelle de la version correspondante.
      - DKMS est utilisé pour gérer dynamiquement le module du noyau de la webcam virtuelle.

      > **Remarque :**
      >
      > Lors de l'installation des programmes précédents sur RHEL et CentOS, le script `ctxwcamcfg.sh` installe et active les référentiels suivants sur votre VDA :
      >
      > - Packages supplémentaires pour Enterprise Linux (EPEL)
      > - RPM Fusion

   b) Téléchargez le code open source `v4l2loopback` depuis DKMS https://github.com/umlaeute/v4l2loopback et utilisez DKMS pour gérer `v4l2loopback`.
   `v4l2loopback` est un module de noyau qui permet de créer des périphériques de bouclage V4L2.

c) Exécutez la commande `sudo service ctxwcamsd restart`. Le service de webcam de Linux VDA, `ctxwcamsd`, redémarre et charge le module de noyau `v4l2loopback` pour la fonction de compression vidéo de webcam HDX.

3. Si votre VDA n'a pas accès à Internet, créez le module de noyau v4l2loopback sur une autre machine, puis copiez-le sur votre VDA.

   a) Préparez une machine disposant d'un accès Internet et disposant de la même version de noyau que votre VDA. La commande `uname -r` permet de trouver les versions de noyau.

   b) Sur la machine de build, exécutez la commande `sudo mkdir -p /var/xdl`.

   c) Copiez `/var/xdl/configure_*` depuis votre VDA vers la machine de build sous `/var/xdl/`.

   d) Sur la machine de build, exécutez la commande `sudo /opt/Citrix/VDA/sbin/ctxwcamcfg.sh` pour créer le module noyau. Si la commande s'exécute correctement, elle crée un fichier v4l2loopback.ko sous le chemin d'accès `/var/lib/dkms/v4l2loopback/1.81b8df79107d1fbf392fdcbaa051bd227a9c94c1/$(uname -r)/x86_64/module/`. Ignorez les erreurs qui peuvent se produire lorsque vous exécutez le script ctxwcamcfg.sh.

   e) Copiez v4l2loopback.ko depuis la machine de build sur votre VDA et placez-le sous `/opt/Citrix/VDA/lib64/`.

   f) Sur votre VDA, exécutez la commande `sudo service ctxwcamsd restart` pour redémarrer le service de webcam et chargez le module de noyau v4l2loopback.

VDA non joints à un domaine

January 10, 2023

Présentation de la configuration

Les VDA non joints à un domaine sont pris en charge pour Citrix DaaS uniquement. Pour créer des VDA non joints à un domaine dans Citrix DaaS, vous devez utiliser Machine Creation Services (MCS). Suivez les étapes suivantes :

1. Créez une image principale sur une VM modèle sur laquelle vous installez également le package VDA. Vous pouvez utiliser une seule image pour créer des VDA joints à un domaine et des VDA non joints à un domaine.

2. Utilisez l'image principale pour créer un catalogue de machines. Sélectionnez MCS comme méthode de déploiement de machine et sélectionnez **Non joint au domaine** comme identité pour les machines à créer dans le catalogue.

Pour plus d'informations, consultez la section Utiliser Machine Creation Services (MCS) pour créer des machines virtuelles Linux et Identités des machines.

Fonctionnalités disponibles pour les VDA non joints à un domaine

Créer des utilisateurs locaux avec des attributs spécifiés sur des VDA non joints à un domaine

Lorsque vous ouvrez une session hébergée sur un VDA non joint à un domaine, le VDA crée automatiquement un utilisateur local avec des attributs par défaut. Le VDA crée l'utilisateur local en fonction du nom d'utilisateur que vous avez utilisé pour vous connecter à l'application Citrix Workspace. Vous pouvez également spécifier des attributs utilisateur, notamment l'identifiant utilisateur (UID), l'ID de groupe (GID), le répertoire de base et le shell d'ouverture de session de l'utilisateur. Pour utiliser cette fonctionnalité, procédez comme suit :

1. Exécutez la commande suivante pour activer la fonctionnalité :

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent\LocalMappedAccount" -t "REG_DWORD" -v "
     CreateWithUidGid" -d "0x00000001" --force
2 <!--NeedCopy-->
```

2. Spécifiez les attributs suivants dans le script `/var/xdl/getuidgid.sh` situé sous le chemin d'installation du VDA :

Attribut	Requis ou facultatif	Description
`uid`	Requis	Un identificateur d'utilisateur (UID) est un numéro attribué par Linux à chaque utilisateur du système. Il détermine les ressources système auxquelles l'utilisateur peut accéder.
`gid`	Requis	Un identificateur de groupe (GID) est un nombre utilisé pour représenter un groupe spécifique.

Attribut	Requis ou facultatif	Description
homedir	Facultatif	Le répertoire de base Linux est un répertoire destiné à un utilisateur particulier.
shell	Facultatif	Un shell d'ouverture de session est un shell donné à un utilisateur lors de l'ouverture de session de son compte utilisateur.

Vous trouverez ci-dessous un exemple de script getuidgid.sh:

> **Remarque :**
>
> Assurez-vous que les attributs spécifiés dans le script sont valides.

```
#!/bin/bash

################################################################################

#
# Citrix Virtual Apps & Desktops For Linux Script: Get uid and gid for the user
#
# Copyright (c) Citrix Systems, Inc. All Rights Reserved.
#

export LC_ALL="en_US.UTF-8"

function get_uid_gid_for_user()
{

echo "uid:12345"
echo "gid:1003"
echo "homedir:/home/$1"
echo "shell:/bin/sh"
 }


get_uid_gid_for_user $1
<!--NeedCopy-->
```


Liste des stratégies prises en charge

December 16, 2022

Liste des stratégies prises en charge avec le Linux VDA

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Limiter le client du Presse-papiers à la taille de transfert de la session	LimitClipboardTransferC2H	boolean	HdxRedirectionPolicy	Désactivé (0)
Limiter la session du Presse-papiers à la taille de transfert du client	LimitClipboardTransferH2C	boolean	HdxRedirectionPolicy	Désactivé (0)

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Utilisation de l'heure locale du client	UseLocalTimeFromUserDevice	TrustedUserConfig	ICA\Control	Utiliser le fuseau horaire du serveur
Calcul des boucles ICA	IcaroundTripCalculation	TrustedUserConfig	ICA\Control	Activé (1)
Intervalle de calcul des boucles ICA	IcaroundTripCalculationInterval	TrustedUserConfig	ICA\Control	60
Calcul des boucles ICA pour les connexions inactives	IcaroundTripCalculationForIdleConnections	TrustedUserConfig	ICA\Control	Désactivé (0)

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Limite de bande passante globale de session	LimitOverallBandwidth	Utilisateur	ICA\Bande passante	0
Limite de bande passante de redirection audio	LimitAudioBandwidth	Utilisateur	ICA\Bande passante	0
Pourcentage de limite de bande passante de la redirection audio	LimitAudioBandwidthPercent	Utilisateur	ICA\Bande passante	0

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Limite de bande passante de redirection du périphérique USB client	LimitUSBBandwidth	Utilisateur	ICA\Bande passante	0
Pourcentage de bande passante de redirection du périphérique USB client	PercentageLimitUSBBandwidth	Utilisateur	ICA\Bande passante	0

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Limite de bande pas-sante de redi-rec-tion du Presse-papiers	LimitClipboardBandwidthValue	DWORD	ICA\Bande pas-sante	0
Pourcentage de la limite de la bande pas-sante de redi-rec-tion du Presse-papiers	LimitClipboardBandwidthPercent	DWORD	ICA\Bande pas-sante	0

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Limite de bande pas-sante de redi-rec-tion de fichier	LimitCdmBwUtilisateur	LongInt	ICA\Bande pas-sante	0
Pourcentage de limite de bande pas-sante de redi-rec-tion de fichier	LimitCdmBwPercent	LongInt	ICA\Bande pas-sante	0

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Limite de bande passante de redirection d'imprimante	LimitPrinterBandwidth	UInt32	ICA\Bandwidth	0
Pourcentage de limite de bande passante de redirection de l'imprimante	LimitPrinterBandwidthPercent	UInt32	ICA\Bandwidth	0
Connexions WebSockets	AcceptWebSocketConnections	UInt32	ICA\WebSockets	0

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Numéro de port WebSockets	WebSocketsPort	Entier	ICA\WebSockets	8008
Liste de serveurs d'origine approuvés WebSockets	WSTrustedOriginServerList	Chaîne	ICA\WebSockets	
Persistance ICA	CgpAllowed	Booléen	**Persistance ICA**	Ne pas envoyer de messages de persistance ICA (0)

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Délai d'expiration de persistance ICA	ICAKeepAliveTimeout	DWord	**Persistance ICA**	60 secondes
Numéro de port de l'écouteur ICA	IcaListenerPortNumber	DWord	ICA	1494
Transport adaptatif HDX	HDXoverUDP	DWord	ICA	Préféré (2)
Connexions de fiabilité de session	AcceptSessionReliability	DWord	ICA\Fiabilité de session	Autorisé (1)

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Niveau de transparence de l'interface durant la reconnexion	ReconnectionTransparency	DWORD	HDX\TeamsRedirection	80 %
Numéro de port de la fiabilité de session	SessionReliabilityPort	DWORD	HDX\Fiabilité	2598
Expiration de délai de la fiabilité de session	SessionReliabilityTimeout	DWORD	HDX\Fiabilité	180 s
Reconnexion automatique des clients	AllowAutoClientReconnect	DWORD	HDX\Reconnexion automatique des clients	Autorisé (1)

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Redirection audio cliente	AllowAudioRedirection	UInt32	Audio	Autorisé (1)
Redirection d'imprimante cliente	AllowPrinterRedirection	UInt32	Impression	Autorisé (1)
Créer automatiquement l'imprimante universelle PDF	AutoCreateUniversalPrinter	UInt32	Impression	Désactivé (0)

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Mappage et compatibilité du pilote d'imprimante	DriverMappingList	Utilisateur	Impression	"Microsoft XPS Document Writer *, Deny; Send to Microsoft OneNote *, Deny"
Redirection de Presse-papiers client	AllowClipboardRedir	Utilisateur	Presse-papiers	Autorisé (1)
Redirection de périphérique USB client	AllowUSBRedir	Utilisateur	USB	Interdit (0)

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut				
Règles de redirection des périphériques USB clients	USBDeviceRules	Utilisateur	USB	”	**Règles de redirection des périphériques USB clients**	USBDeviceRules	Utilisateur	USB	“\0”	”
Compression d’images en mouvement	MovingImageCompression	Utilisateur	Thinwire	Configuration (1)						
Compression couleur supplémentaire	ExtraColorCompression	Utilisateur	Thinwire	Désactivé (0)						
Taux de trame minimum cible	TargetedMinimumFrameRate	Utilisateur	Thinwire	10 fps						
Taux de trames cible	FramesPerSecond	Utilisateur	Thinwire	30 fps						

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Qualité visuelle	VisualQuality	Utilisateur	Thinwire	Moyenne (3)
Utiliser codec vidéo pour la compression	VideoCodec	Utilisateur	Thinwire	Utiliser au choix (3)
Utiliser le codage matériel pour le codec vidéo	UseHardwareEncodingForVideoCodec	Utilisateur	Thinwire	Préférer désactivé (1)
Autoriser la compression visuelle sans perte	AllowVisuallyLosslessCompression	Utilisateur	Thinwire	Désactivé (0)

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Optimiser pour la charge des graphiques 3D	OptimizeForGraphicsWorkload	EnableDisable	Thinwire	Désactivé (0)
Nombre de couleurs préféré pour les graphiques simples	PreferredColorDepth	UnsignedInt	Thinwire	24 bits par pixel (1)
Qualité audio	SoundQuality	Utilisateur	Audio	Élevée : audio à définition élevée (2)
Redirection du microphone client	AllowMicrophoneRedirection	EnableDisable	Audio	Autorisé (1)
Nombre maximum de sessions	MaximumNumberOfSessions	UnsignedInt	Gestion de la charge	250

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Tolérance d'ouvertures de session simultanées	ConcurrentLogonsTolerance	Ordinateur	Tolérance de la charge	2
Activer la mise à jour automatique des contrôleurs	EnableAutoUpdateOfControllers	Ordinateur	Paramètres Virtual Delivery Agent	Autorisé (1)
Mode de mise à jour de la sélection du Presse-papiers	ClipboardSelectionUpdateMode	Ordinateur	Presse-papiers	3

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Mode de mise à jour de la sélection principale	PrimarySelectionUpdateMode	Utilisateur	Presse-papiers	1
Qualité speex maximale	MaxSpeexQuality	Qualité	Audio	5
Connecter automatiquement les lecteurs clients	AutoConnectDrives	Lecteurs	Redirection de fichier/CDM	Activé (1)
Lecteurs optiques clients	AllowCdromDrives	Lecteurs	Redirection de fichier/CDM	Autorisé (1)
Lecteurs fixes clients	AllowFixedDrives	Lecteurs	Redirection de fichier/CDM	Autorisé (1)
Lecteurs de disquette clients	AllowFloppyDrives	Lecteurs	Redirection de fichier/CDM	Autorisé (1)

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Lecteurs réseau clients	AllowNetworkDrives	Utilisateur	Redirection de fichier/CDM	Autorisé (1)
Redirection de lecteur client	AllowDriveRedirection	Utilisateur	Redirection de fichier/CDM	Autorisé (1)
Accès en lecture unique sur le lecteur client	ReadOnlyMappedDrive	Utilisateur	Redirection de fichier/CDM	Désactivé (0)
Affichage de clavier automatique	AllowAutoKeyboard	Utilisateur	VDAPro	Désactivé (0)
Autoriser le transfert de fichiers entre le bureau et le client	AllowFileTransfer	Utilisateur	Transfert de fichiers	Autorisé

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Télécharger des fichiers depuis le bureau	AllowFileDownload	Utilisateur	Transfert de fichiers	Autorisé
Charger des fichiers sur le bureau	AllowFileUpload	Utilisateur	Transfert de fichiers	Autorisé
Horloge inactive de session	EnableSessionIdleTimer	Utilisateur	Horloges de session	Activé (1)
Intervalle d'horloge inactive de session	SessionIdleTimerInterval	Utilisateur	Horloges de session	1440 minutes
Horloge de session déconnectée	EnableSessionDisconnectTimer	Utilisateur	Horloges de session	Désactivé (0)

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Intervalle d'horloge de session déconnectée	SessionDisconnectedTimerInterval	Utilisateur ou machine	Fiabilité de session	1440 minutes

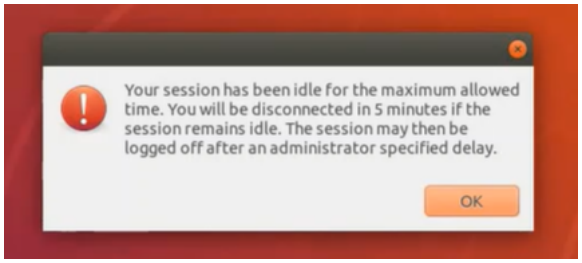
> **Remarque :**
>
> Seul le Virtual Delivery Agent (VDA) pour Windows prend en charge l'audio via UDP (User Datagram Protocol). Le VDA Linux ne prend pas en charge cette fonctionnalité. Pour de plus amples informations, consultez la section Transport en temps réel audio via UDP (User Datagram Protocol).

Vous pouvez utiliser les paramètres de stratégie Citrix suivants pour configurer des horloges de connexion de session dans Citrix Studio :

- **Horloge inactive de session** : détermine s'il faut appliquer un délai pour les sessions inactives.
- **Intervalle d'horloge inactive de session** : définit un délai pour les sessions inactives. Si l'option **Horloge inactive de session** est **Activé** et qu'une session active n'a pas reçu d'entrée utilisateur pendant la durée définie, la session se déconnecte.
- **Horloge de session déconnectée** : détermine s'il faut appliquer un délai pour les sessions déconnectées.
- **Intervalle d'horloge de session déconnectée** : définit un intervalle avant la déconnexion d'une session déconnectée.

Lorsque vous mettez à jour l'un de ces paramètres de stratégie, vous devez vous assurer qu'ils sont cohérents sur votre déploiement.

Un message d'avertissement s'affiche lorsque votre délai pour les sessions inactives expire. Pour obtenir un exemple, consultez la capture d'écran suivante. Lorsque vous sélectionnez **OK**, le message d'avertissement se ferme mais ne permet pas maintenir votre session active. Pour maintenir votre session active, fournissez une entrée utilisateur pour réinitialiser l'horloge inactive.



Les stratégies suivantes peuvent être configurées dans Citrix Studio 7.12 et versions ultérieures.

- MaxSpeexQuality

  Valeur (entier) : [0-10]

  Valeur par défaut : 5

  Détails :

  La redirection audio encode les données audio avec le codec Speex lorsque la qualité audio est moyenne voire faible (voir la stratégie Qualité audio). Speex est un codec avec perte, ce qui signifie qu'il atteint de meilleurs taux de compression au détriment de la fidélité du signal de la parole. Contrairement à d'autres codecs dédiés à la parole, il est possible de contrôler le compromis entre qualité et débit. Le processus de codage Speex est contrôlé la plupart du temps par un paramètre de qualité compris entre 0 et 10. Plus la qualité est élevée, plus le débit est élevé.

  La qualité Speex maximale est utilisée pour choisir la meilleure qualité Speex de codage des données audio en fonction de la qualité audio et de la limite de bande passante (voir la stratégie Limite de bande passante de la redirection audio). Si la qualité audio est moyenne, l'encodeur est en mode de bande étendue, ce qui implique une fréquence d'échantillonnage plus élevée. Si la qualité audio est faible, l'encodeur est en mode de bande étroite, ce qui implique une fréquence d'échantillonnage plus faible. La même qualité Speex dispose de différents débits pour chaque mode. La meilleure qualité Speex est atteinte lorsque la valeur la plus élevée respecte les conditions suivantes :

  - Elle est égale ou inférieure à la qualité Speex maximale
  - Son débit est égal ou inférieur à la limite de bande passante

  Paramètres connexes : Qualité audio, Limite de bande passante de la redirection audio

- PrimarySelectionUpdateMode

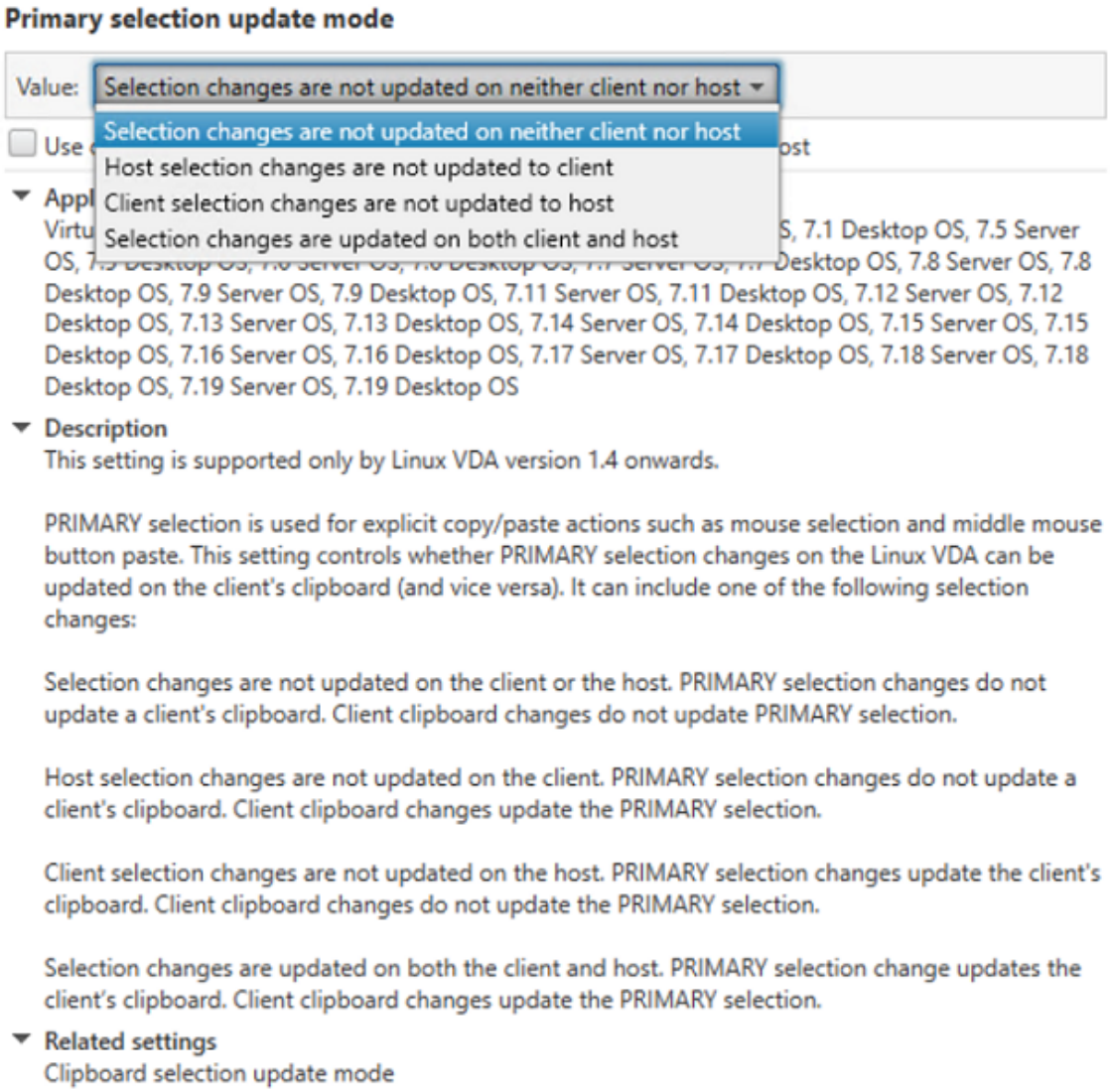
  Valeur (enum) : [0, 1, 2, 3]

  Valeur par défaut : 3

  Détails :

La sélection primaire est utilisée lorsque vous sélectionnez des données et les collez en appuyant sur le bouton central de la souris.

Cette stratégie contrôle si les modifications apportées à la sélection primaire sur le Linux VDA et le client peuvent actualiser le presse-papiers sur l'un sur l'autre. Il existe quatre options de valeur :



- **Les modifications apportées à la sélection ne sont mises à jour ni sur le client ni sur l'hôte**
  Les modifications apportées à la sélection primaire sur le Linux VDA ne mettent pas à jour le presse-papiers sur le client. Les modifications apportées à la sélection primaire sur le client ne mettent pas à jour le presse-papiers sur le Linux VDA.
- **Les modifications apportées à la sélection de l'hôte ne sont pas mises à jour sur le client**

Les modifications apportées à la sélection primaire sur le Linux VDA ne mettent pas à jour le presse-papiers sur le client. Les modifications apportées à la sélection primaire sur le client mettent à jour le presse-papiers sur le Linux VDA.

- **Les modifications apportées à la sélection du client ne sont mises à jour sur l'hôte**
  Les modifications apportées à la sélection primaire sur le Linux VDA mettent à jour le presse-papiers sur le client. Les modifications apportées à la sélection primaire sur le client ne mettent pas à jour le presse-papiers sur le Linux VDA.
- **Les modifications apportées à la sélection sont mises à jour sur le client et l'hôte**
  Les modifications apportées à la sélection primaire sur le Linux VDA mettent à jour le presse-papiers sur le client. Les modifications apportées à la sélection primaire sur le client mettent à jour le presse-papiers sur le Linux VDA. Cette option est la valeur par défaut.

Paramètres connexes : Mode de mise à jour de la sélection du presse-papiers

- ClipboardSelectionUpdateMode

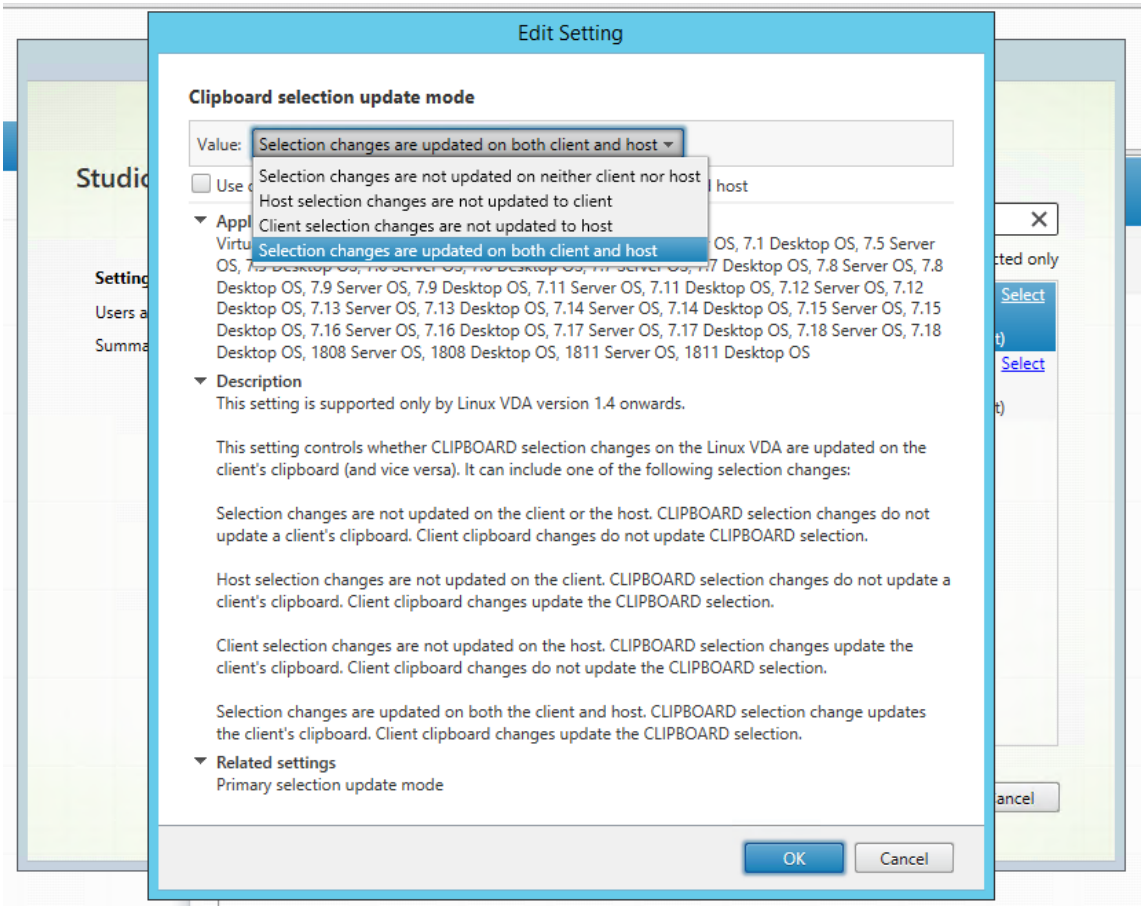
  Valeur (enum) : [0, 1, 2, 3]

  Valeur par défaut : 3

  Détails :

  La sélection du presse-papiers est utilisée lorsque vous sélectionnez des données et que vous demandez explicitement qu'elles soient « copiées » dans le presse-papiers, par exemple en sélectionnant « Copier » dans le menu contextuel. La sélection du presse-papiers est principalement utilisée dans le cadre des opérations de presse-papiers de Microsoft Windows alors que la sélection primaire est unique à Linux.

  Cette stratégie contrôle si les modifications apportées à la sélection du presse-papiers sur le Linux VDA et le client peuvent actualiser le presse-papiers sur l'un et l'autre. Il existe quatre options de valeur :



- **Les modifications apportées à la sélection ne sont mises à jour ni sur le client ni sur l'hôte**

  Les modifications apportées à la sélection du presse-papiers sur le Linux VDA ne mettent pas à jour le presse-papiers sur le client. Les modifications apportées à la sélection du presse-papiers sur le client ne mettent pas à jour le presse-papiers sur le Linux VDA.

- **Les modifications apportées à la sélection de l'hôte ne sont pas mises à jour sur le client**

  Les modifications apportées à la sélection du presse-papiers sur le Linux VDA ne mettent pas à jour le presse-papiers sur le client. Les modifications apportées à la sélection du presse-papiers sur le client mettent à jour le presse-papiers sur le Linux VDA.

- **Les modifications apportées à la sélection du client ne sont pas mises à jour sur l'hôte**

  Les modifications apportées à la sélection du presse-papiers sur le Linux VDA mettent à jour le presse-papiers sur le client. Les modifications apportées à la sélection du presse-papiers sur le client ne mettent pas à jour le presse-papiers sur le Linux VDA.

- **Les modifications apportées à la sélection sont mises à jour sur le client et l'hôte**

  Les modifications apportées à la sélection du presse-papiers sur le Linux VDA mettent à

jour le presse-papiers sur le client. Les modifications apportées à la sélection du presse-papiers sur le client mettent à jour le presse-papiers sur le Linux VDA. Cette option est la valeur par défaut.

Paramètres connexes : Mode de mise à jour de la sélection primaire

> **Remarque :**
>
> Le Linux VDA prend en charge à la fois la sélection presse-papiers et la sélection primaire. Pour contrôler les comportements de copier-coller entre le Linux VDA et le client, nous vous recommandons de définir la même valeur pour le mode de mise à jour de la sélection presse-papiers et le mode de mise à jour de la sélection primaire.

Impression

December 16, 2022

Cette section contient les rubriques suivantes :

- Meilleures pratiques d'impression
- Impression PDF

Meilleures pratiques d'impression

December 16, 2022

Cet article contient des informations sur les meilleures pratiques de l'impression.

Installation

Linux VDA requiert les filtres **cups** et **foomatic**. Les filtres sont installés lorsque vous installez le VDA. Vous pouvez également installer les filtres manuellement en fonction de la distribution. Par exemple :

Sur RHEL 7 :

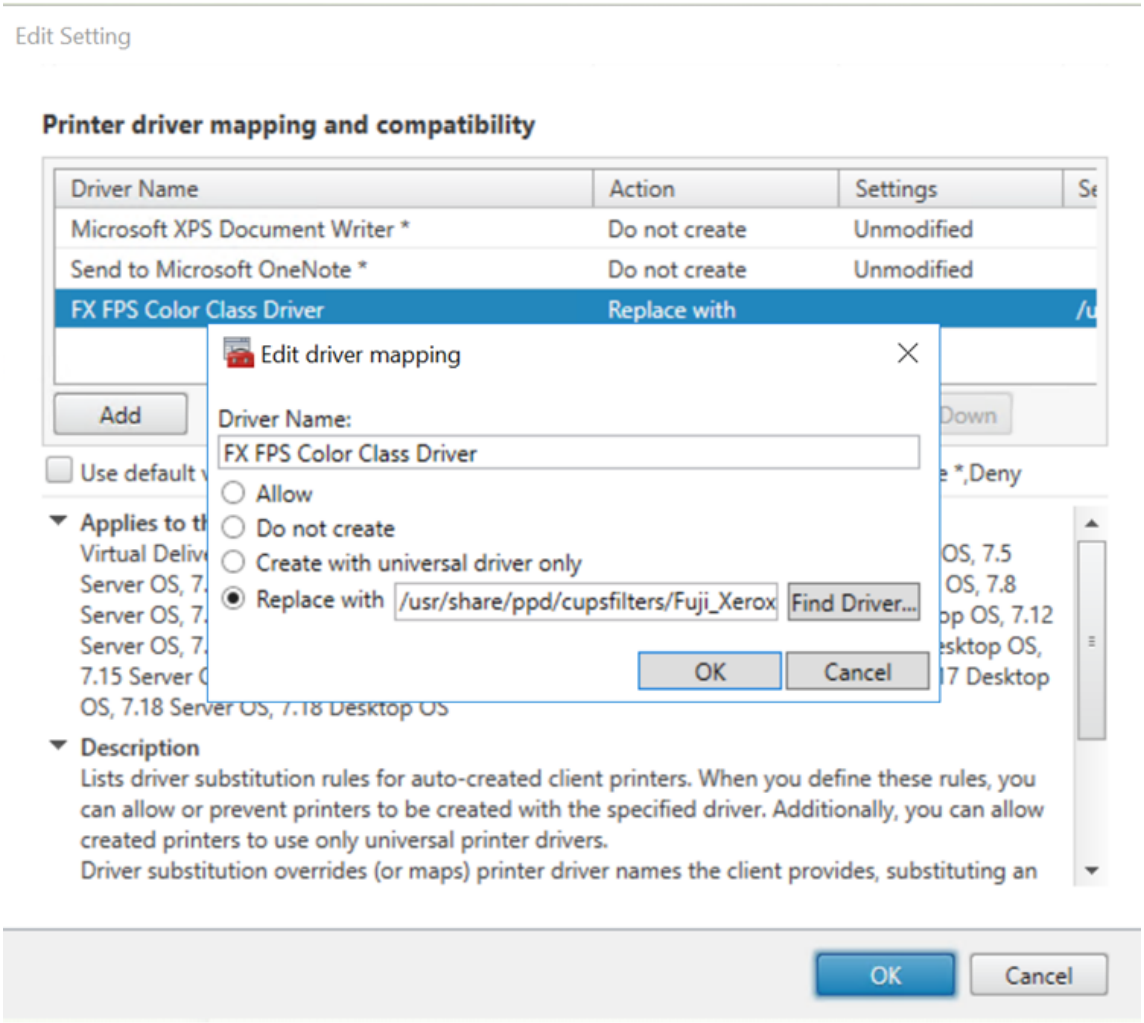
```
sudo yum –y install cups

sudo yum -y install foomatic-filters
<!--NeedCopy-->
```


Configuration

Il existe trois types de pilote d'imprimante universel fournis par Citrix (postscript, pcl5 et pcl6). Toutefois, le pilote d'imprimante universel peut ne pas être compatible avec votre imprimante cliente. Dans ce cas, la seule option dans les versions précédentes était de modifier le fichier de configuration ~/.CtxlpProfile$CLIENT_NAME. À partir de la version 1906, vous pouvez choisir de configurer la stratégie **Mappage et compatibilité du pilote d'imprimante** dans Citrix Studio.

Pour configurer la stratégie **Mappage et compatibilité du pilote d'imprimante** dans Citrix Studio, procédez comme suit :

1. Sélectionnez la stratégie **Mappage et compatibilité du pilote d'imprimante**.
2. Cliquez sur **Ajouter**.
3. Dans le champ **Nom du pilote**, spécifiez le nom du pilote de l'imprimante cliente. Si vous utilisez l'application Citrix Workspace pour Linux, spécifiez plutôt le nom de l'imprimante.
4. Choisissez **Remplacer par** et entrez le chemin d'accès absolu du fichier du pilote sur le VDA.



> **Remarque :**
>
> - Seuls les fichiers de pilote PPD sont pris en charge.
> - Les autres options de la stratégie **Mappage et compatibilité du pilote d'imprimante** ne sont pas prises en charge. Seule l'option **Remplacer par** prend effet.

Utilisation

Vous pouvez imprimer à partir d'applications et de bureaux publiés. Seule l'imprimante par défaut côté client est mappée vers une session Linux VDA. Les noms d'imprimante doivent être différents pour les bureaux et les applications.

- Pour les bureaux publiés : `CitrixUniversalPrinter:$CLIENT_NAME:dsk$SESSION_ID`
- Pour les applications publiées : `CitrixUniversalPrinter:$CLIENT_NAME:app$SESSION_ID`

> **Remarque :**
>
> Si le même utilisateur ouvre un bureau publié et une application publiée, les deux imprimantes sont disponibles pour la session. L'impression vers une imprimante de bureau dans une session d'application publiée ou l'impression vers une imprimante d'application dans un bureau publié échoue.

Résolution des problèmes

Impossible d'imprimer

Lorsque l'impression ne fonctionne pas correctement, vérifiez le démon d'impression, **ctxlpmngt**et l'infrastructure CUPS.

Le démon d'impression, **ctxlpmngt**, est un processus par session et doit être en cours d'exécution pour la durée de la session. Exécutez la commande suivante pour vérifier que le démon d'impression est en cours d'exécution. Si le processus **ctxlpmngt** n'est pas exécuté, démarrez manuellement **ctxlpmngt** à partir d'une ligne de commande.

```
1 ps –ef | grep ctxlpmngt
2 <!--NeedCopy-->
```

Si l'impression ne fonctionne toujours pas, vérifiez l'infrastructure CUPS. Le service **ctxcups** est destiné à la gestion d'imprimantes et communique avec l'infrastructure Linux CUPS. Il s'agit d'un processus unique par machine qui peut être vérifié en exécutant la commande suivante :


```
service ctxcups status
<!--NeedCopy-->
```

Étapes supplémentaires pour la collecte de journaux CUPS

Pour collecter les journaux CUPS, exécutez les commandes suivantes pour configurer le fichier de service CUPS. Sinon, les journaux CUPS ne peuvent pas être enregistrés dans **hdx.log** :

```
sudo service cups stop

sudo vi /etc/systemd/system/printer.target.wants/cups.service

PrivateTmp=false

sudo service cups start

sudo systemctl daemon-reload
<!--NeedCopy-->
```

> **Remarque :**
>
> Cette configuration sert uniquement à collecter le journal d'impression complet lorsqu'un problème survient. En général, cette configuration n'est pas recommandée car cette opération enfreint la sécurité CUPS.

L'impression est illisible

Un pilote d'imprimante incompatible peut causer une impression illisible. Une configuration pilote par utilisateur est disponible et peut être configurée en modifiant le fichier de configuration **~/.CtxlpProfile$CLIENT_NAME** :

```
[DEFAULT_PRINTER]

printername=

model=

ppdpath=

drivertype=
<!--NeedCopy-->
```

> **Important :**
>
> le champ **printername** contient le nom de l'imprimante par défaut actuelle côté client. Il s'agit d'une valeur en lecture seule. Ne la modifiez pas.

> Les champs **ppdpath**, **model** et **drivertype** ne peuvent pas être définis en même temps car un seul est appliqué pour l'imprimante mappée.

- Si le pilote d'imprimante universel n'est pas compatible avec l'imprimante cliente, configurez le modèle du pilote d'imprimante natif avec l'option **model**=. Vous pouvez trouver le nom du modèle actuel de l'imprimante avec la commande **lpinfo** :

```
lpinfo  -m

...

xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

<!--NeedCopy-->
```

  Vous pouvez ensuite définir le modèle pour qu'il corresponde à l'imprimante :

```
model=xerox/ph3115.ppd.gz
<!--NeedCopy-->
```

- Si le pilote d'imprimante universel n'est pas compatible avec l'imprimante cliente, configurez le chemin de fichier PPD du pilote d'imprimante natif. La valeur de **ppdpath** est le chemin d'accès absolu du fichier du pilote d'imprimante natif.

  Par exemple, il existe un **pilote ppd** sous /home/tester/NATIVE_PRINTER_DRIVER.ppd :

```
ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
<!--NeedCopy-->
```

- Il existe trois types de pilote d'imprimante universel fournis par Citrix (postscript, pcl5 et pcl6). Vous pouvez configurer le type de pilote en fonction des propriétés de votre imprimante.

  Par exemple, si le pilote d'imprimante par défaut est de type PCL5, définissez **drivertype** sur :

```
drivertype=pcl5
<!--NeedCopy-->
```

La taille de sortie est définie sur zéro

Essayez différents types d'imprimantes. Essayez également avec une imprimante virtuelle comme CutePDF et PDFCreator pour savoir si ce problème est lié au pilote d'imprimante.

La tâche d'impression dépend du pilote de l'imprimante par défaut du client. Il est important d'identifier le type de pilote actif. Si l'imprimante cliente utilise un pilote PCL5 mais que le Linux VDA choisit un pilote Postscript, un problème peut survenir.

Si le type de pilote d'imprimante est correct, vous pouvez identifier le problème en suivant les étapes suivantes :

1. Connectez-vous à une session de bureau publiée.
2. Exécutez la commande **vi ~/.CtxlpProfile$CLIENT_NAME**.
3. Ajoutez le champ suivant pour enregistrer fichier de spouleur sur le Linux VDA :

```
deletespoolfile=no
<!--NeedCopy-->
```

4. Fermez, puis rouvrez la session pour charger les modifications apportées à la configuration.
5. Imprimez le document pour reproduire le problème. Après l'impression, un fichier de spouleur est enregistré sous **/var/spool/cups-ctx/$logon_user/$spool_file**.
6. Vérifiez si le fichier de spouleur est vide. Si la taille du fichier de spouleur est zéro, ceci indique un problème. Contactez le support Citrix (et fournissez le journal d'impression) pour une assistance supplémentaire.
7. Si la taille du fichier de spouleur n'est pas zéro, copiez le fichier sur le client. Le contenu du fichier de spouleur dépend du type de pilote de l'imprimante par défaut du client. Si le pilote (natif) de l'imprimante mappée est postscript, le fichier de spouleur peut être ouvert directement dans le système d'exploitation Linux. Vérifiez si le contenu est correct.

   Si le fichier de spouleur est PCL ou si le système d'exploitation client est Windows, copiez le fichier de spouleur sur le client et imprimez-le à l'aide de l'imprimante côté client en utilisant un autre pilote d'imprimante.
8. Modifiez l'imprimante mappée pour utiliser un autre pilote d'imprimante. L'exemple suivant utilise l'imprimante client postscript :

   a) Connectez-vous à une session active et ouvrez un navigateur sur le bureau client.

   b) Ouvrez le portail de gestion de l'impression :

```
localhost:631
<!--NeedCopy-->
```

   c) Sélectionnez l'imprimante mappée **CitrixUniversalPrinter:$ClientName:app/dsk$SESSION_ID** et **Modify Printer**. Cette opération requiert des privilèges d'administrateur.

   d) Conservez la connexion cups-ctx, puis cliquez sur Continue pour modifier le pilote d'imprimante.

   e) Dans les champs **Make** et **Model**, choisissez un pilote d'imprimante autre que le pilote UPD Citrix. Par exemple, si l'imprimante virtuelle CUPS-PDF est installée, sélectionnez le pilote Generic CUPS-PDF Printer. Enregistrez la modification.

f) Si ce processus réussit, configurez le chemin d'accès au fichier PPD du pilote dans **.Ctxlp-Profile$CLIENT_NAME** pour autoriser l'imprimante mappée à utiliser le nouveau pilote sélectionné.

Problèmes connus

Les problèmes suivants ont été identifiés lors de l'impression sur le Linux VDA :

Le pilote CTXPS n'est pas compatible avec certaines imprimantes PLC

Si l'impression présente des anomalies, définissez le pilote d'imprimante sur le pilote d'imprimante natif fourni par le fabricant.

Impression lente avec les documents volumineux

Lorsque vous imprimez un document volumineux sur une imprimante cliente locale, le document est transféré sur une connexion serveur. Si la connexion est lente, le transfert risque de durer longtemps.

Notifications d'imprimante et de travaux d'impression d'autres sessions

Le concept de session de Linux n'est pas le même que celui du système d'exploitation Windows. Par conséquent, tous les utilisateurs reçoivent les notifications de l'ensemble du système. Vous pouvez désactiver ces notifications en modifiant le fichier de configuration CUPS : **/etc/cups/cupsd.conf**.

Recherchez le nom de stratégie configuré dans le fichier.

```
DefaultPolicy default
```

Si le nom de la stratégie est *default*, ajoutez les lignes suivantes dans le bloc XML de la stratégie par défaut :

```
<Policy default>

     # Job/subscription privacy...

     JobPrivateAccess default

     JobPrivateValues default

     SubscriptionPrivateAccess default

     SubscriptionPrivateValues default

```



```
13       ... ...
14
15       <Limit Create-Printer-Subscription>
16
17            Require user @OWNER
18
19            Order deny,allow
20
21       </Limit>
22
23       <Limit All>
24
25            Order deny,allow
26
27       </Limit>
28
29  </Policy>
30  <!--NeedCopy-->
```

Impression PDF

December 16, 2022

Si vous utilisez une version de l'application Citrix Workspace qui prend en charge l'impression PDF, vous pouvez imprimer des PDF convertis depuis les sessions Linux VDA. Les tâches d'impression de session sont envoyées à la machine locale sur laquelle l'application Citrix Workspace est installée. Sur la machine locale, vous pouvez ouvrir les fichiers PDF en utilisant la visionneuse PDF de votre choix et les imprimer sur l'imprimante de votre choix.

Le Linux VDA prend en charge l'impression PDF sur les versions suivantes de l'application Citrix Workspace :

- Citrix Receiver pour HTML5 versions 2.4 à 2.6.9, application Citrix Workspace 1808 pour HTML5 et versions ultérieures
- Citrix Receiver pour Chrome versions 2.4 à 2.6.9, application Citrix Workspace 1808 pour Chrome et versions ultérieures
- Application Citrix Workspace 1905 pour Windows et versions ultérieures

Configuration

En plus d'utiliser l'une des versions de l'application Citrix Workspace prenant en charge l'impression PDF, vous devez également activer les stratégies suivantes dans Citrix Studio :

- **Redirection d'imprimante cliente** (activée par défaut)

- **Créer automatiquement l'imprimante universelle PDF** (désactivée par défaut)

Lorsque ces stratégies sont activées, un aperçu d'impression s'affiche sur la machine locale, ce qui vous permet de sélectionner une imprimante lorsque vous cliquez sur **Imprimer** dans votre session. Consultez la documentation de l'application Citrix Workspace pour plus d'informations sur la configuration d'imprimantes par défaut.

Remote PC Access

December 16, 2022

Vue d'ensemble

Remote PC Access est une extension de Citrix Virtual Apps and Desktops. Il permet aux entreprises de permettre aux employés d'accéder facilement à leurs ordinateurs de bureau physiques à distance de manière sécurisée. 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 utilise les composants Citrix Virtual Apps and Desktops qui fournissent des bureaux virtuels et des applications. 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. Cette uniformité offre une expérience administrative cohérente et unifiée. Les utilisateurs bénéficient d'une meilleure expérience utilisateur lorsque Citrix HDX est utilisé pour fournir leurs sessions de bureau à distance.

Pour de plus amples informations, consultez Remote PC Access dans la documentation de Citrix Virtual Apps and Desktops.

Considérations

Ces considérations sont spécifiques au VDA Linux :

- Utilisez le VDA Linux sur des machines physiques uniquement en mode non-3D. En raison de limitations sur le pilote de NVIDIA, l'écran local du PC ne peut pas être éteint lorsque le mode HDX 3D est activé. L'affichage de cet écran représente un risque de sécurité potentiel.
- Utilisez des catalogues de machines de type OS mono-session pour les machines Linux physiques.

- L'attribution automatique d'utilisateurs n'est pas disponible pour les machines Linux. Avec l'attribution automatique d'utilisateurs, les utilisateurs sont automatiquement affectés à leurs machines lorsqu'ils ouvrent une session locale sur les PC. Cette ouverture de session se produit sans intervention de l'administrateur. L'application Citrix Workspace sur le client permet aux utilisateurs d'accéder aux applications et données sur le PC de bureau dans la session de bureau Remote PC Access.
- Si les utilisateurs sont déjà connectés localement à leur PC, les tentatives de lancement des PC à partir de StoreFront échouent.
- Les options d'économie d'énergie ne sont pas disponibles pour les machines Linux.

Configuration

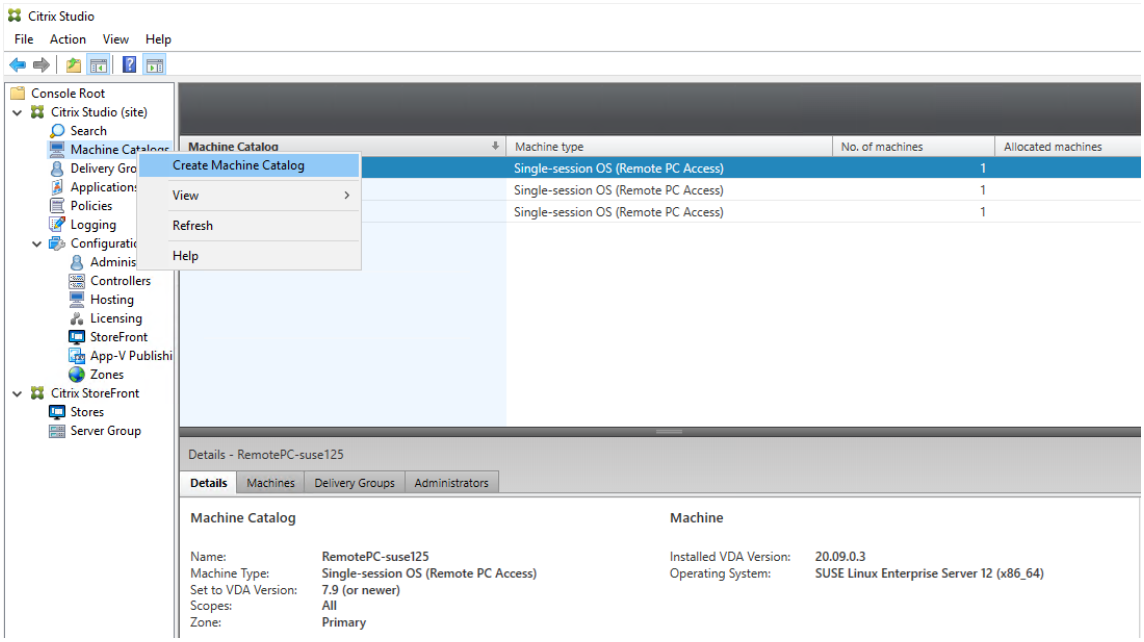
Pour fournir des sessions PC Linux, installez le Linux VDA sur les PC cibles, créez un catalogue de machines du type **Remote PC Access** et créez un groupe de mise à disposition pour rendre les PC du catalogue de machines disponibles pour les utilisateurs qui en demandent l'accès. La section suivante détaille la procédure :

Étape 1: installer le Linux VDA sur les PC cibles

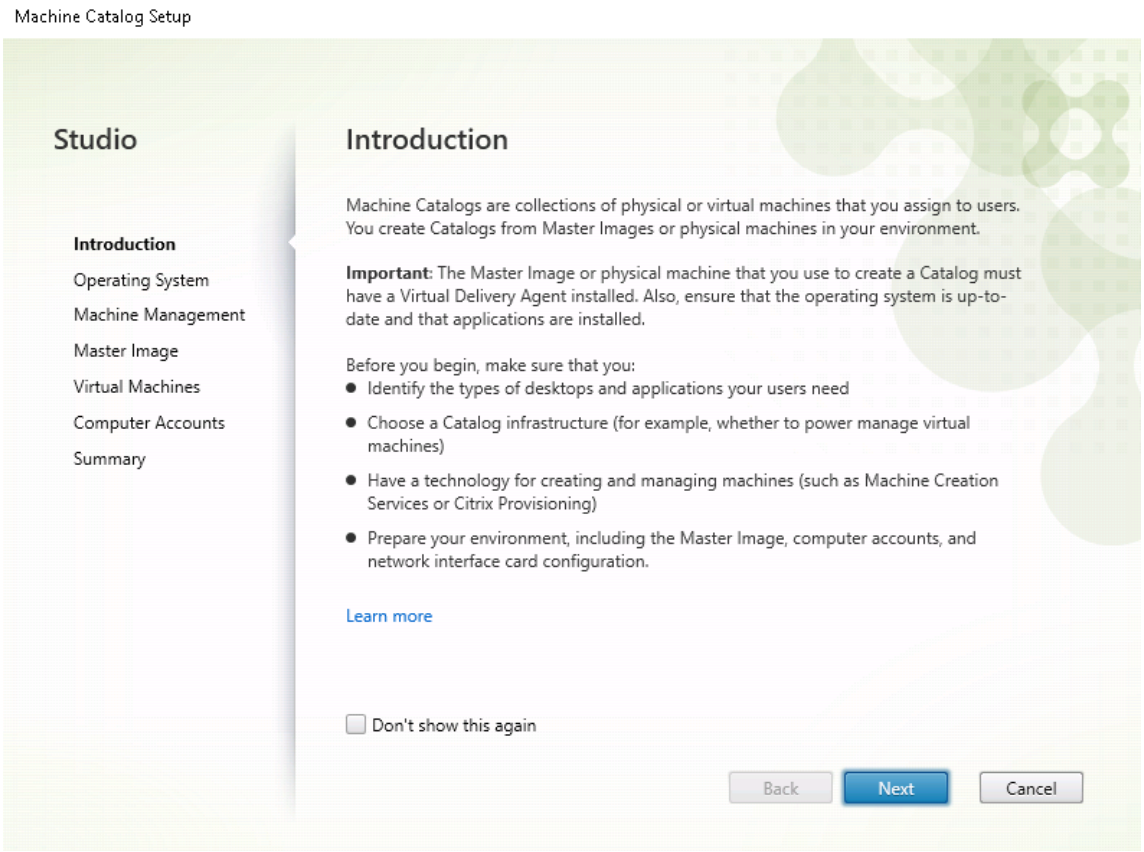
Nous vous recommandons d'utiliser Easy Install pour installer le Linux VDA. Pendant l'installation, définissez la valeur de la variable `CTX_XDL_VDI_MODE` sur `Y`.

Étape 2 : créer un catalogue de machines du type Remote PC Access

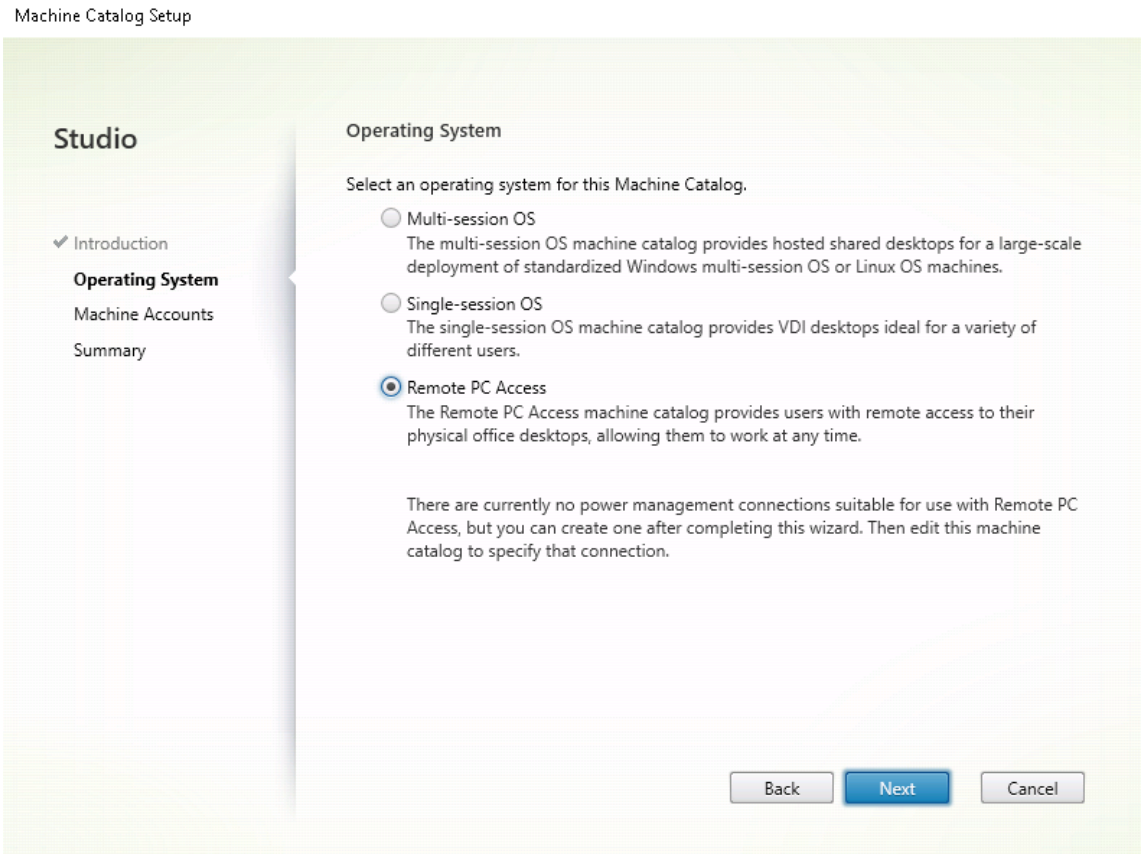
1. Dans Citrix Studio, cliquez avec le bouton droit sur **Catalogues de machines** et sélectionnez **Créer un catalogue de machines** dans le menu contextuel.



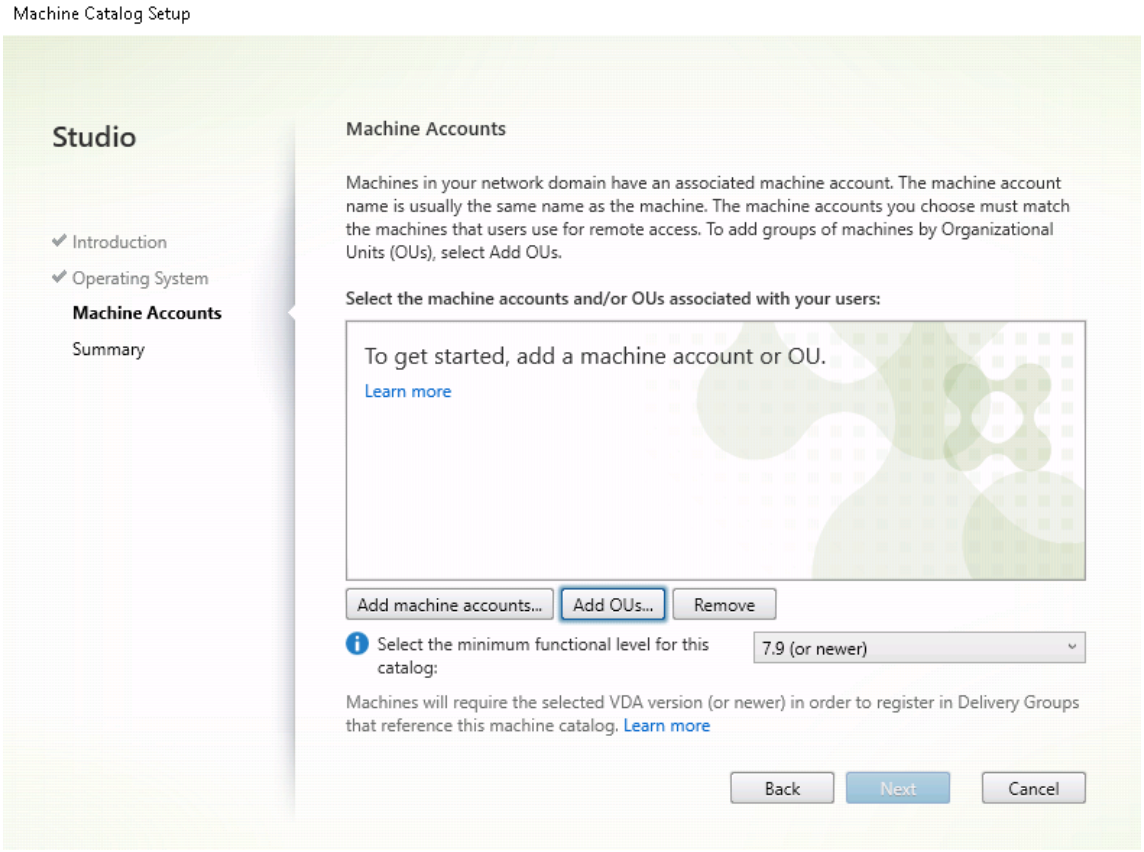
2. Cliquez sur **Suivant** sur la page **Introduction**.



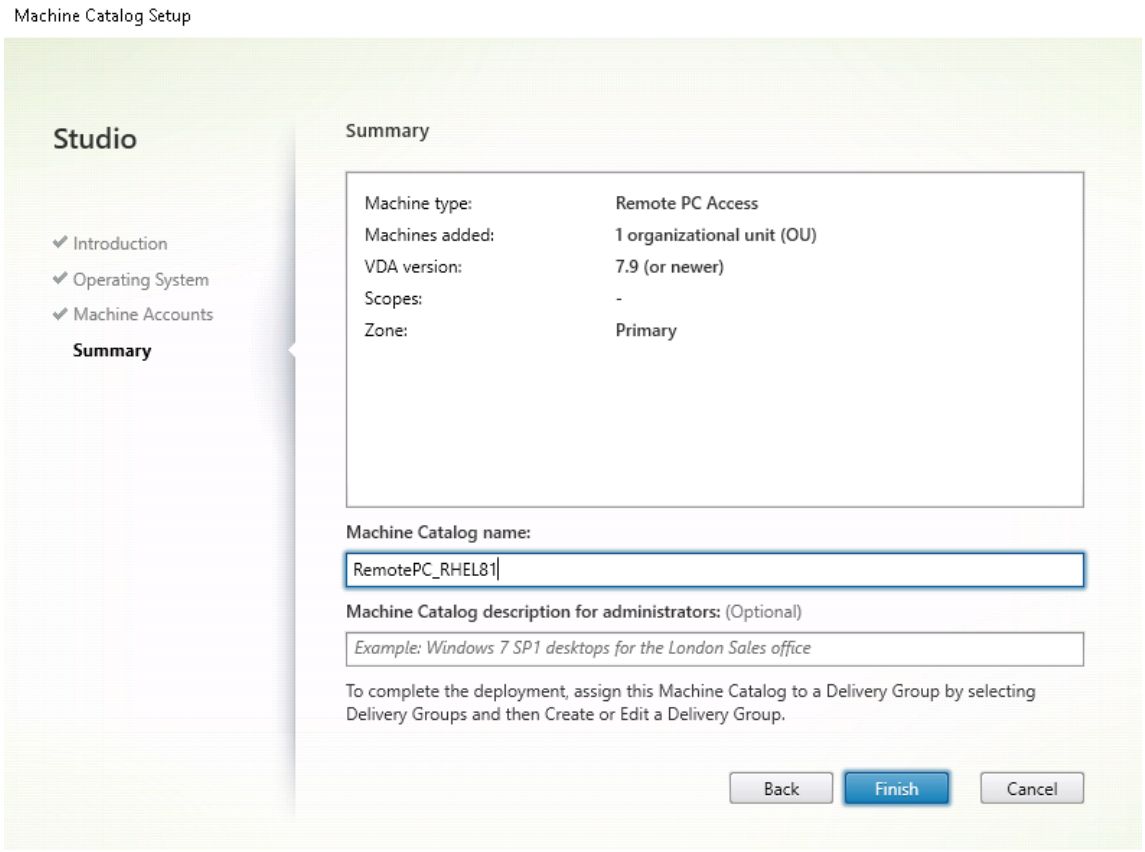
3. Sélectionnez **Remote PC Access** sur la page **Système d'exploitation**.



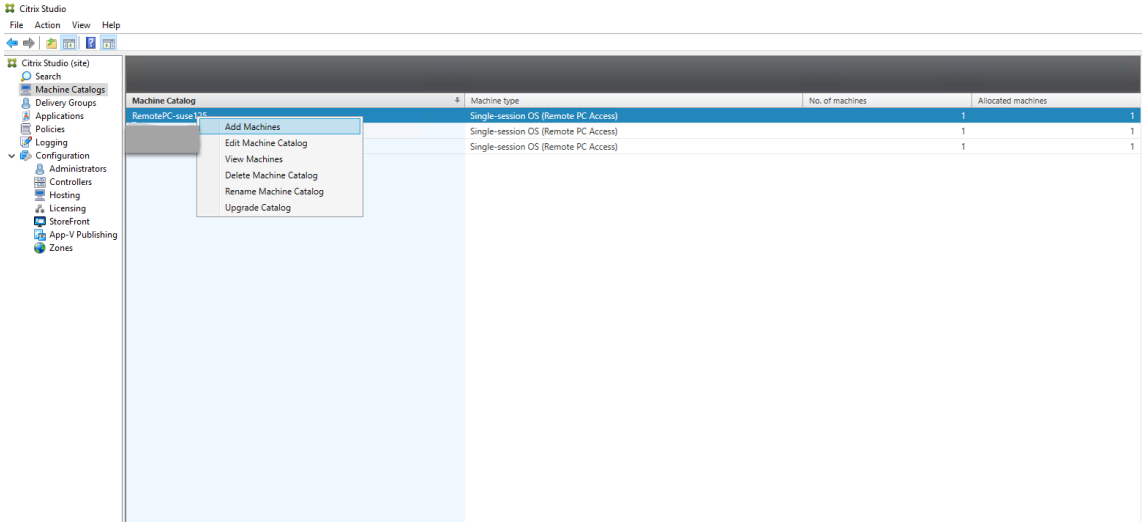
4. Cliquez sur **Ajouter des unités d'organisation** pour sélectionner des unités d'organisation contenant les ordinateurs cibles, ou cliquez sur **Ajouter des comptes de machines** pour ajouter des machines individuelles au catalogue de machines.



5. Nommez le catalogue de machines.

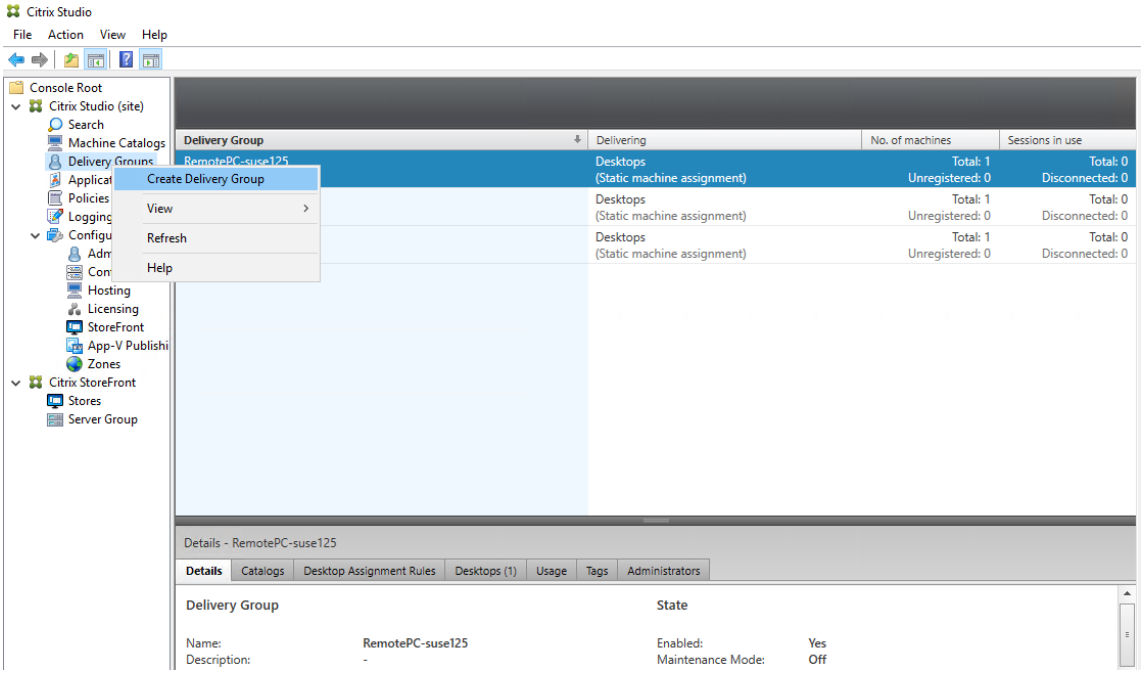


6. (Facultatif) Cliquez avec le bouton droit sur le catalogue de machines pour effectuer des opérations pertinentes.

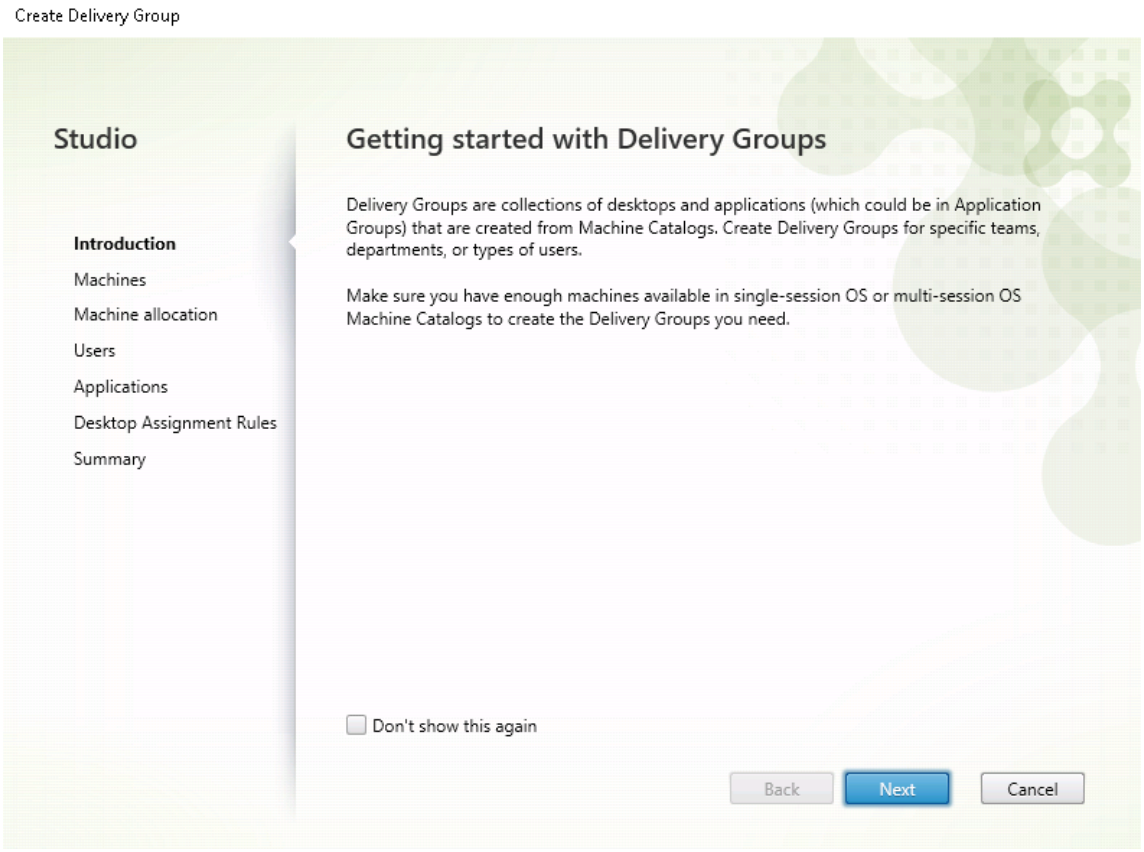


Étape 3 : créer un groupe de mise à disposition pour rendre les PC du catalogue de machines disponibles auprès des utilisateurs qui demandent l'accès

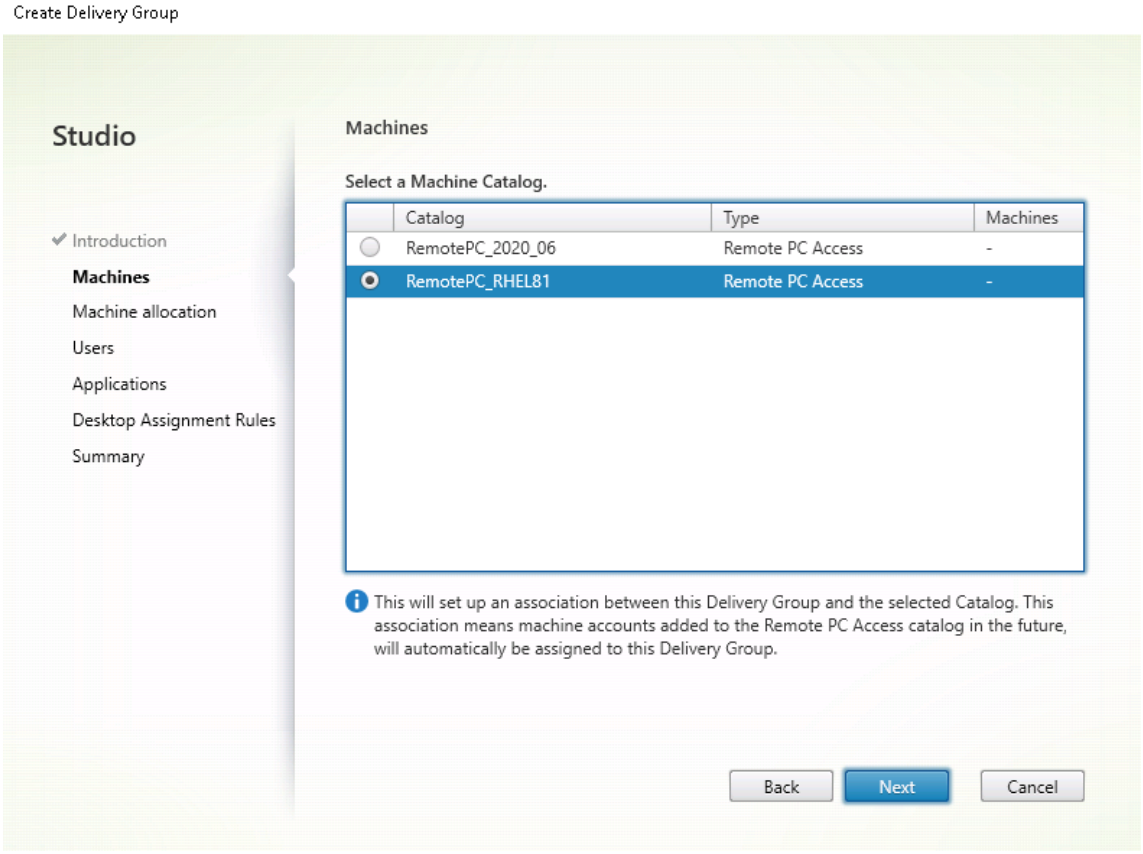
1. Dans Citrix Studio, cliquez avec le bouton droit sur **Groupes de mise à disposition** et sélectionnez **Créer un groupe de mise à disposition** dans le menu contextuel.



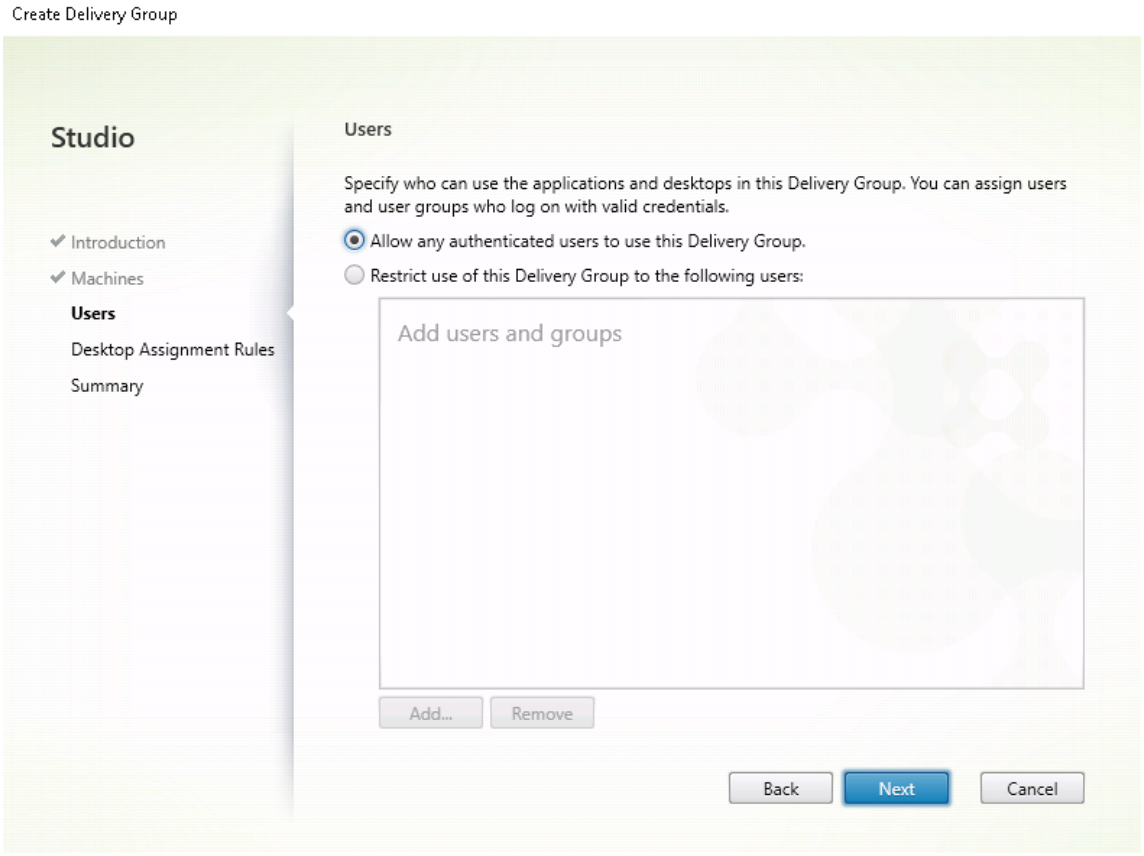
2. Cliquez sur **Suivant** sur la page **Présentation des groupes de mise à disposition**.



3. Sélectionnez le catalogue de machines créé à l'étape 2 pour l'associer au groupe de mise à disposition.



4. Ajoutez des utilisateurs qui peuvent accéder aux PC dans le catalogue de machines. Les utilisateurs que vous ajoutez peuvent utiliser l'application Citrix Workspace sur une machine cliente pour accéder aux PC à distance.



Wake on LAN

Remote PC Access prend en charge Wake on LAN, qui donne aux utilisateurs la possibilité d'activer des ordinateurs physiques à distance. Cette fonctionnalité permet aux utilisateurs de garder leur PC de bureau éteint lorsqu'il n'est pas en cours d'utilisation, et d'économiser de l'énergie. Elle offre également un accès distant quand une machine a été éteinte par inadvertance.

Avec la fonction Wake on LAN, les paquets magiques sont envoyés directement à partir du VDA exécuté sur le PC vers le sous-réseau dans lequel réside le PC selon les instructions du Delivery Controller. Cela permet à la fonction d'opérer sans dépendances sur des composants d'infrastructure supplémentaires ou des solutions tierces pour la mise à disposition de paquets magiques.

La fonction Wake on LAN diffère de la fonction Wake on LAN d'ancienne génération basée sur SCCM. Pour plus d'informations sur la fonction Wake on LAN basée sur SCCM, consultez Fonction Wake on LAN intégrée à SCCM.

Configuration système requise

Vous trouverez ci-dessous la configuration système requise pour l'utilisation de la fonction Wake on LAN :

- Plan de contrôle :
  - Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service)
  - Citrix Virtual Apps and Desktops 2012 ou version ultérieure
- PC physiques :
  - VDA 2012 ou version ultérieure
  - Wake on LAN activé dans BIOS et sur la carte d'interface réseau

Configurer Wake on LAN

Actuellement, la configuration de la fonction Wake on LAN intégrée n'est prise en charge qu'avec PowerShell.

Pour configurer Wake on LAN :

1. Créez le catalogue de machines Remote PC Access si vous n'en avez pas déjà.
2. Créez la connexion hôte Wake on LAN si vous n'en avez pas déjà.

   > **Remarque :**
   >
   > Pour utiliser la fonction Wake on LAN, si vous disposez d'une connexion hôte du type « Microsoft Configuration Manager Wake on LAN », créez une connexion hôte.

3. Récupérez l'identifiant unique de la connexion hôte Wake on LAN.
4. Associez la connexion hôte Wake on LAN à un catalogue de machines.

   Pour créer la connexion hôte Wake on LAN :

```
# Load Citrix SnapIns
Add-PSSnapIn -Name "\*citrix\*"

# Provide the name of the Wake on LAN host connection
[string]$connectionName = "Remote PC Access Wake on LAN"

# Create the hypervisor connection
$hypHc = New-Item -Path xdhyp:\Connections `
            -Name $connectionName `
            -HypervisorAddress "N/A" `
            -UserName "woluser" `
            -Password "wolpwd" `
            -ConnectionType Custom `
```



```
            -PluginId VdaWOLMachineManagerFactory `
            -CustomProperties "<CustomProperties></
               CustomProperties>" `
            -Persist

$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
   $hypHc.HypervisorConnectionUid

# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{

    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -
       HypHypervisorConnectionUid $hypHc.HypervisorConnectionUid
 }

<!--NeedCopy-->
```

Lorsque la connexion hôte est prête, exécutez les commandes suivantes pour récupérer l'identifiant unique de la connexion hôte :

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>
   "
$hypUid = $bhc.Uid
<!--NeedCopy-->
```

Après avoir récupéré l'identifiant unique de la connexion, exécutez les commandes suivantes pour associer la connexion au catalogue de machines Remote PC Access :

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
   RemotePCHypervisorConnectionUid $hypUid
<!--NeedCopy-->
```

5. Activez Wake on LAN dans BIOS et sur la carte d'interface réseau sur chaque machine virtuelle du catalogue de machines.

   Remarque : la méthode d'activation de Wake on LAN varie selon les configurations de machine.

   - Pour activer Wake on LAN dans BIOS :
     a) Entrez le BIOS et activez la fonction Wake on LAN.
        La méthode d'accès au BIOS dépend du fabricant de votre carte mère et du fournisseur BIOS sélectionné par le fabricant.
     b) Enregistrez vos paramètres et redémarrez la machine.
   - Pour activer Wake on LAN sur la carte d'interface réseau :
     a) Exécutez la commande `sudo ethtool <NIC>` pour vérifier si votre carte d'interface réseau prend en charge les paquets magiques.
        `<NIC>` est le nom de l'appareil de votre carte d'interface réseau, par exemple, `eth0`.

La commande `sudo ethtool <NIC>` fournit une sortie sur les capacités de votre carte d'interface réseau :

- Si la sortie contient une ligne similaire à `Supports Wake-on: <letters>` où `<letters>` contient la lettre `g`, votre carte d'interface réseau prend en charge la méthode de paquet magique Wake on LAN.
- Si la sortie contient une ligne similaire à `Wake-on: <letters>` où `<letters>` contient la lettre `g` et ne contient pas la lettre `d`, la méthode de paquet magique LAN est activée. Toutefois, si la chaîne `<letters>` contient la lettre `d`, elle indique que la fonction Wake on LAN est désactivée. Dans ce cas, activez Wake on LAN en exécutant la commande `sudo ethtool -s <NIC> wol g`.

b) Sur la plupart des distributions, la commande `sudo ethtool -s <NIC> wol g` est requise après chaque démarrage. Pour définir cette option de manière persistante, procédez comme suit en fonction de vos distributions :

Ubuntu :

Ajoutez la ligne `up ethtool -s <NIC> wol g` au fichier de configuration de l'interface `/etc/network/interfaces`. Par exemple :

```
# ifupdown has been replaced by netplan(5) on this system.
   See
# /etc/netplan for current configuration.
# To re-enable ifupdown on this system, you can run:
# sudo apt install ifupdown
auto eth0
iface eth0 inet static
           address 10.0.0.1
           netmask 255.255.240.0
           gateway 10.0.0.1
           up ethtool -s eth0 wol g
<!--NeedCopy-->
```

RHEL/SUSE :

Ajoutez le paramètre suivant `ETHTOOL_OPTS` au fichier de configuration de l'interface `/etc/sysconfig/network-scripts/ifcfg-<NIC>` :

```
ETHTOOL_OPTS="-s ${
 DEVICE }
  wol g"
<!--NeedCopy-->
```

Considérations relatives à la conception

Lorsque vous envisagez d'utiliser Wake on LAN avec Remote PC Access, tenez compte des points suivants :

- Plusieurs catalogues de machines peuvent utiliser la même connexion hôte Wake on LAN.

- Pour qu'un PC réveille un autre PC, les deux PC doivent se trouver dans le même sous-réseau et utiliser la même connexion hôte Wake on LAN, qu'ils soient dans les mêmes catalogues de machines ou non.
- Les connexions hôtes sont affectées à des zones spécifiques. Si votre déploiement contient plusieurs zones, vous avez besoin d'une connexion hôte Wake on LAN dans chaque zone. Il en va de même pour les catalogues de machines.
- Les paquets magiques sont diffusés à l'aide de l'adresse de diffusion globale 255.255.255.255. Assurez-vous que l'adresse n'est pas bloquée.
- Il doit y avoir au moins un PC allumé dans le sous-réseau - pour chaque connexion Wake on LAN - pour pouvoir réveiller les machines de ce sous-réseau.

Considérations opérationnelles

Les considérations suivantes sont à prendre en compte lors de l'utilisation de la fonctionnalité Wake on LAN :

- Le VDA doit s'enregistrer au moins une fois avant que le PC puisse être réveillé à l'aide de la fonction Wake on LAN intégrée.
- La fonction Wake on LAN ne peut être utilisée que pour réveiller les PC. Elle ne prend pas en charge d'autres actions d'alimentation, telles que le redémarrage ou l'arrêt.
- Une fois la connexion Wake on LAN créée, elle est visible dans Studio. Toutefois, la modification de ses propriétés dans Studio n'est pas prise en charge.
- Les paquets magiques sont envoyés de l'une des deux manières suivantes :
  - Lorsqu'un utilisateur tente de lancer une session sur son PC et que le VDA n'est pas enregistré
  - Lorsqu'un administrateur envoie manuellement une commande de mise sous tension à partir de Studio ou PowerShell
- Comme le Delivery Controller ne connaît pas l'état d'alimentation d'un PC, Studio affiche **Non pris en charge** sous l'état d'alimentation. Le Delivery Controller utilise donc l'état d'enregistrement du VDA pour déterminer si un PC est allumé ou éteint.

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.

La

December 16, 2022

Cette section contient les rubriques suivantes :

- Transport adaptatif
- Ouvrir une session à l'aide d'un répertoire de base temporaire
- Publier des applications
- Fiabilité de session
- Rendezvous V1
- Rendezvous V2
- Sécuriser les sessions utilisateur en utilisant TLS
- Sécuriser les sessions utilisateur en utilisant DTLS

Transport adaptatif

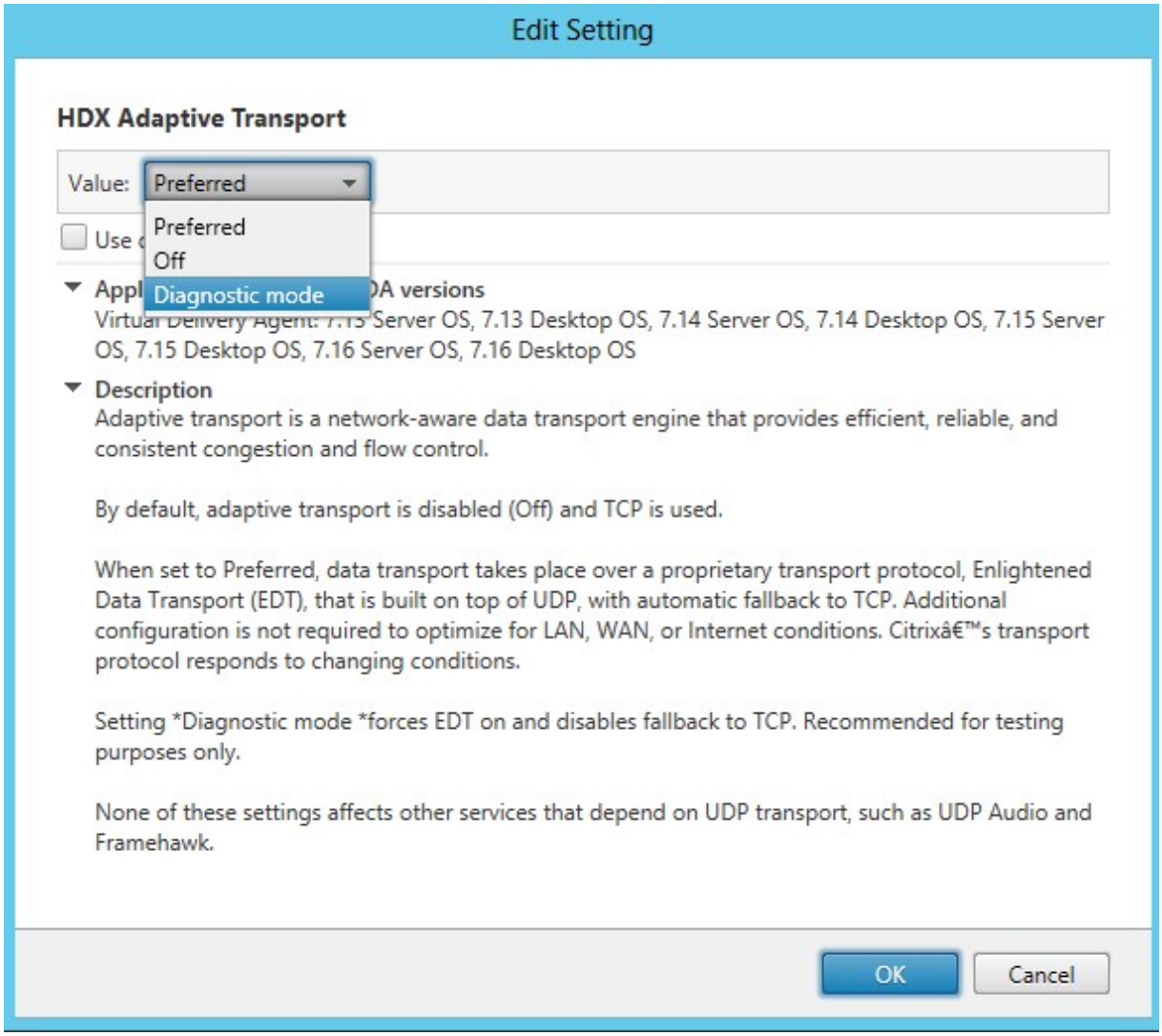
December 16, 2022

Le transport adaptatif est un mécanisme de transport de données pour Citrix Virtual Apps and Desktops. Plus rapide et plus évolutif, il améliore l'interactivité avec les applications et il est plus adapté aux connexions WAN et Internet longue distance difficiles. Pour plus d'informations sur le transport adaptatif, consultez la section Transport adaptatif.

Activer le transport adaptatif

Dans Citrix Studio, vérifiez que la stratégie **HDX Adaptive Transport** est définie sur le mode **Préféré** ou **Diagnostic**. Le paramètre **Préféré** est sélectionné par défaut.

- **Préféré** : le transport adaptatif via EDT (Enlightened Data Transport) est utilisé autant que possible, avec retour vers TCP.
- **Mode Diagnostic** : EDT est activé de force et le retour vers TCP est désactivé.



Désactiver le transport adaptatif

Pour désactiver le transport adaptatif, définissez la stratégie **HDX Adaptive Transport** sur **Off** dans Citrix Studio.

Vérifier si le transport adaptatif est activé

Exécutez la commande suivante pour vérifier si les écouteurs UDP sont en cours d'exécution.

```
netstat -an | grep "1494|2598"
<!--NeedCopy-->
```

Dans des circonstances normales, la sortie est similaire à ce qui suit.

```
udp        0      0 0.0.0.0:2598            0.0.0.0:*
```



```
2
3 udp        0      0 :::1494                 :::*
4 <!--NeedCopy-->
```

Découverte MTU EDT

EDT détermine 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.

Configuration minimale requise :

- Linux VDA 2012
- Application Citrix Workspace 1911 pour Windows
- Citrix ADC :
  - 13.0.52.24
  - 12.1.56.22
- La fiabilité de session doit être activée

Si vous utilisez des plates-formes clientes ou des versions qui ne prennent pas en charge cette fonctionnalité, vous pouvez configurer une MTU EDT personnalisée adaptée à votre environnement. Pour obtenir davantage d'informations, veuillez consulter l'article CTX231821 du centre de connaissances.

> **Avertissement :**
>
> La modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'**Éditeur du Registre**. Vous assumez l'ensemble des risques liés à l'utilisation de l'**Éditeur du Registre**. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Activer ou désactiver la découverte MTU EDT sur le VDA

La découverte MTU EDT est désactivée par défaut.

- Pour activer la découverte MTU EDT, définissez la clé de registre `MtuDiscovery` à l'aide de la commande suivante, redémarrez le VDA et attendez que le VDA s'enregistre :

  ```
  /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet
  \Control\Terminal Server\Wds\icawd"-t "REG_DWORD"-v "MtuDiscovery
  "-d "0x00000001"--force
  ```

- Pour désactiver la découverte MTU EDT, supprimez la valeur de registre `MtuDiscovery`.

Contrôler la découverte MTU EDT sur le client

Vous pouvez contrôler la découverte MTU EDT de manière sélective sur le client en ajoutant le paramètre `MtuDiscovery` dans le fichier ICA. Pour désactiver la fonctionnalité, définissez les éléments suivants dans la section `Application` :

```
MtuDiscovery=Off
```

Pour réactiver la fonctionnalité, supprimez le paramètre `MtuDiscovery` du fichier ICA.

> **Important :**
>
> Pour que ce paramètre de fichier ICA fonctionne, activez la découverte MTU EDT sur le VDA. Si la découverte MTU EDT n'est pas activée sur le VDA, le paramètre de fichier ICA n'a aucun effet.

Arrière-plans et messages de bannière personnalisés sur les écrans d'ouverture de session

December 16, 2022

Vous pouvez utiliser les commandes suivantes pour ajouter un arrière-plan ou un message de bannière personnalisé aux écrans d'**ouverture de session**. Pour ajouter à la fois un arrière-plan et un message de bannière aux écrans d'**ouverture de session**, vous pouvez intégrer le message de la bannière dans l'image d'arrière-plan.

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v
      "LogonDisplayString" -d "<text of custom logon banner message>" --
     force
2 <!--NeedCopy-->
```

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v
      "BackgroundImagePath" -d "<path to your custom logon screen
     background image>" --force
2 <!--NeedCopy-->
```

Pour utiliser la fonctionnalité sur SUSE 15.3, installez `imlib2` à partir de http://download.opensuse.org/distribution/leap/15.3/repo/oss/.

> **Conseil :**
>
> Si vous ajoutez un message de bannière personnalisé à l'aide de LogonDisplayString, l'arrière-plan de l'écran d'ouverture de session est bleu par défaut.

Environnements de bureau personnalisés par utilisateurs de session

December 16, 2022

Vous pouvez spécifier un environnement de bureau pour les utilisateurs de session à l'aide de la variable **CTX_XDL_DESKTOP_ENVIRONMENT**. À partir de la version 2209, les utilisateurs de session peuvent personnaliser leurs propres environnements de bureau. Pour activer cette fonctionnalité, vous devez installer au préalable des environnements de bureau sur le VDA.

Le tableau suivant présente une matrice des distributions Linux et des environnements de bureau qui prennent en charge les environnements de bureau personnalisés par utilisateurs de session.

Distribution Linux	Bureau pris en charge
Debian11.3	MATE, GNOME, GNOME-Classic, KDE
RHEL 8.6, RHEL 8.4	MATE, GNOME, GNOME-Classic
RHEL 7.9	MATE, GNOME, GNOME-Classic, KDE
Rocky Linux 8.6	MATE, GNOME, GNOME-Classic, KDE
SUSE 15.3	MATE, GNOME, GNOME-Classic
Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04	MATE, GNOME, GNOME-Classic, KDE

Commandes de commutation de bureau

Pour passer à un environnement de bureau cible, exécutez la commande correspondante dans la session :

Si l'environnement de bureau cible est	Exécutez la commande
GNOME	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh GNOME`
GNOME Classic	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh GNOME-CLASSIC`
MATE	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh MATE`
KDE	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh KDE`

Astuces pour KDE

- Magnus peut se charger au démarrage dans KDE. Pour contourner ce problème, vous pouvez supprimer le package Magnus en exécutant `sudo apt remove magnus`.
- Pour désactiver les avertissements QT qui apparaissent au démarrage de KDE, modifiez `/usr/share/qt5/qtlogging.ini` en tant qu'utilisateur racine en ajoutant les entrées suivantes :

```
qt.qpa.xcb.xcberror.error=false
qt.qpa.xcb.warning=false
qt.qpa.xcb.error=false
<!--NeedCopy-->
```

- Le déverrouillage de l'écran peut échouer pour KDE. Pour contourner ce problème, nous vous recommandons de désactiver la fonction de verrouillage automatique de votre bureau.

Ouvrir une session à l'aide d'un répertoire de base temporaire

December 16, 2022

Vous pouvez spécifier un répertoire de base temporaire dans les cas où le point de montage sur le Linux VDA échoue. Lorsqu'un répertoire de base temporaire est spécifié, une invite s'affiche lors de l'ouverture de session lorsque le point de montage échoue. Les données utilisateur sont ensuite stockées dans le répertoire de base temporaire.

Le tableau suivant décrit les clés de registre qui vous aident à définir les paramètres de votre répertoire de base.

Clé de registre	Description	Commande
`LogNoHome`	Contrôle si les utilisateurs peuvent ouvrir des sessions sans répertoire de base. La valeur par défaut est 1, ce qui signifie « activé ». Si la valeur est définie sur 0, les ouvertures de session sans répertoire de base sont désactivées.	`create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD"-v "LogNoHome"-d "0x00000001"--force`

Clé de registre	Description	Commande
HomeMountPoint	Définit un point de montage local sur le Linux VDA. Par exemple, si /mnt/home est le point de montage, le répertoire de base d'un utilisateur est /mnt/home/domain/<user_name>. Assurez-vous que le point de montage est le même que le répertoire de base de l'utilisateur dans votre environnement.	create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_SZ"-v "HomeMountPoint"-d "<A directory where the NFS share is to be mounted>"--force
TempHomeDirectoryPath	Définit un répertoire de base temporaire sur le Linux VDA en cas d'échec du point de montage. La valeur par défaut est /tmp. La clé de registre dépend de HomeMountPoint. Ce paramètre ne prend effet que lorsque le système détecte que le point de montage n'est pas disponible. Un répertoire de base temporaire pour un utilisateur est /tmp/domain/user_id.	create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_SZ"-v "TempHomeDirectoryPath"-d "</tmp by default>"--force
RemoveHomeOnLogoff	Contrôle si les répertoires de base temporaires doivent être supprimés lors de la fermeture de session des utilisateurs. 1 signifie « activé », 0 « désactivé ».	create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD"-v "RemoveHomeOnLogoff"-d "0x00000000"--force

Publier des applications

December 16, 2022

Avec la version 7.13 de Linux VDA, Citrix a ajouté la fonctionnalité d'applications transparentes à toutes les plates-formes Linux prises en charge. Aucune procédure d'installation spécifique n'est requise pour utiliser cette fonctionnalité.

> **Conseil :**
>
> Citrix a ajouté la prise en charge des applications publiées non transparentes et du partage de session dans la version 1.4 du Linux VDA.

Publier des applications à l'aide de Citrix Studio

Vous pouvez publier des applications installées sur un Linux VDA lorsque vous créez un groupe de mise à disposition ou ajoutez des applications à un groupe de mise à disposition. Ce processus est similaire à la publication d'applications installées sur un VDA Windows. Pour de plus amples informations, consultez la documentation de Citrix Virtual Apps and Desktops (en fonction de la version de Citrix Virtual Apps and Desktops utilisée).

> **Remarque :**
>
> - Lors de la configuration de groupes de mise à disposition, vous devez vous assurer que le type de mise à disposition est défini sur **Bureaux et applications** ou **Applications**.
> - La publication d'applications est prise en charge avec la version 1.4 de Linux VDA et les versions supérieures. Toutefois, le Linux VDA ne prend pas en charge la mise à disposition de bureaux et d'applications sur la même machine. Pour résoudre ce problème, nous vous recommandons de créer des groupes de mise à disposition distincts pour la mise à disposition d'applications et de bureaux.
> - Pour utiliser les applications transparentes, ne désactivez pas le mode transparent sur StoreFront. Le mode transparent est activé par défaut. Si vous l'avez déjà désactivé en définissant « TWIMode=Off », supprimez ce paramètre au lieu de le modifier sur « TWIMode=On ». Sinon, il est possible que vous ne puissiez pas lancer de bureau publié.

Limitation

L'agent Linux VDA ne prend pas en charge le lancement de plusieurs instances simultanées d'une même application par un seul utilisateur.

Dans une session d'application, seuls les raccourcis spécifiques à l'application fonctionnent comme prévu.

Problèmes connus

Les problèmes connus suivants sont identifiés lors de la publication d'applications :

- Les fenêtres non rectangulaires ne sont pas prises en charge. Les coins d'une fenêtre peuvent afficher l'arrière-plan du côté serveur.
- L'aperçu du contenu d'une fenêtre à partir d'une application publiée n'est pas pris en charge.
- Lorsque vous exécutez plusieurs applications LibreOffice, seule celle lancée en premier s'affiche sur Citrix Studio, car ces applications partagent le processus.
- Il est possible que les applications publiées basées sur Qt5, telles que « Dolphin », n'affichent pas d'icônes. Pour remédier à ce problème, reportez-vous à l'article https://wiki.archlinux.org/title/Qt.

Rendezvous V1

December 16, 2022

Lors de l'utilisation du service Citrix Gateway, le protocole Rendezvous permet au trafic de contourner les Citrix Cloud Connector et de 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 de session HDX.

Rendezvous V1 permet au trafic de session HDX de contourner les Cloud Connector, mais il nécessite toujours que les Cloud Connector proxysent tout le trafic de contrôle pour l'enregistrement de VDA et la négociation des sessions.

Exigences

- Accès à l'environnement à l'aide du service Citrix Workspace et Citrix Gateway.
- Plan de contrôle : Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service).
- VDA Linux version 2112 ou ultérieure.
  - La version 2112 est la version minimale requise pour les proxys HTTP non transparents.
  - La version 2204 est la version minimale requise pour les proxys transparents et SOCKS5.

- 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 mettre en liste blanche tous les sous-domaines de cette manière, utilisez plutôt `https://*.c.nssvc.net` et `https://*.g.nssvc.net`. Pour plus d'informations, reportez-vous à la section Exigences en termes de connexion Internet de la documentation Citrix Cloud (sous Virtual Apps and Desktop service) et à l'article du centre de connaissances CTX270584.
- Les Cloud Connector doivent obtenir les noms de domaine complets des VDA lors de la négociation d'une session. Pour atteindre cet objectif, activez la résolution DNS pour le site : à l'aide du SDK Citrix DaaS Remote PowerShell, exécutez la commande `Set-BrokerSite -DnsResolutionEnabled $true`. Pour plus d'informations sur le SDK Citrix DaaS Remote PowerShell, reportez-vous à la section SDK et API.

Configuration du proxy

Le VDA prend en charge les connexions Rendezvous via des proxys HTTP et SOCKS5.

Considérations relatives au proxy

Prenez les points suivants en considération lors de l'utilisation de proxy avec Rendezvous :

- Les proxys HTTP non transparents et les proxys 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. Lorsque vous vous connectez au serveur proxy, le schéma d'authentification Negotiate sélectionne automatiquement le protocole Kerberos. Kerberos est le seul schéma pris en charge par le Linux VDA.

  > **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 nom principal de service, l'authentification échoue.

- 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

Le proxy HTTP transparent est pris en charge pour Rendezvous. 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 pour que le VDA sache quel proxy utiliser. Par exemple :

- Adresse proxy : `http://<URL or IP>:<port>` ou `socks5://<URL or IP>:<port>`

Validation de Rendezvous

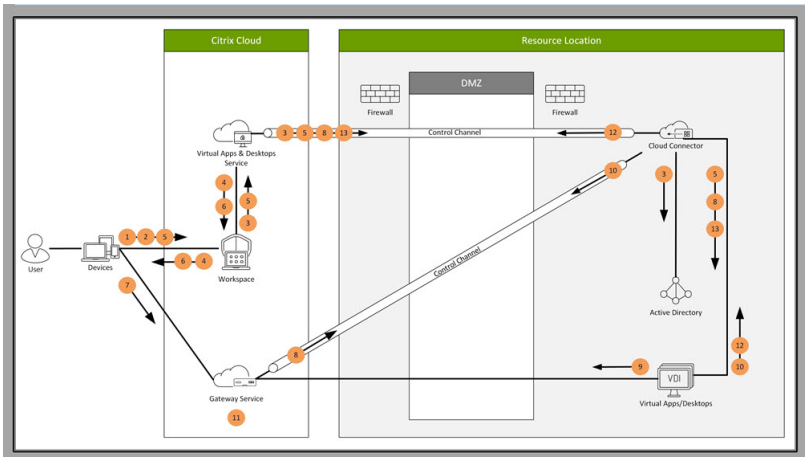
Si vous remplissez toutes les conditions requises, procédez comme suit pour confirmer si Rendezvous est utilisé :

1. Lancez un terminal sur le VDA.
2. Exécutez `/opt/Citrix/VDA/bin/ctxquery -f iP`.
3. Les protocoles de transport utilisés indiqueront le type de connexion :
    - TCP Rendezvous: TCP - TLS - CGP - ICA
    - EDT Rendezvous : UDP - DTLS - CGP - ICA
    - Proxy via Cloud Connector : TCP - PROXY - SSL - CGP - ICA ou UDP - PROXY - DTLS - CGP - ICA

> **Conseil :**
>
> Si vous activez Rendezvous et que le VDA ne parvient pas à atteindre directement le service Citrix Gateway, le VDA revient au proxy de la session HDX via le Cloud Connector.

Fonctionnement de Rendezvous

Ce diagramme donne une vue d'ensemble du flux de connexion Rendezvous.



Suivez les étapes pour comprendre le flux.

1. Accédez à Citrix Workspace.
2. Entrez les informations d'identification dans Citrix Workspace.
3. Si vous utilisez un Active Directory local, Citrix DaaS authentifie les informations d'identification avec Active Directory à l'aide du canal Cloud Connector.
4. Citrix Workspace affiche les ressources énumérées depuis Citrix DaaS.
5. Sélectionnez des ressources dans Citrix Workspace. Citrix DaaS envoie un message au VDA pour préparer une session entrante.
6. Citrix Workspace envoie un fichier ICA au point de terminaison qui contient un ticket STA généré par Citrix Cloud.
7. Le point de terminaison se connecte au service Citrix Gateway, fournit le ticket pour se connecter au VDA et Citrix Cloud valide le ticket.
8. Le service Citrix Gateway envoie des informations de connexion au Cloud Connector. Le Cloud Connector détermine si la connexion est une connexion Rendezvous et envoie les informations au VDA.
9. Le VDA établit une connexion directe au service Citrix Gateway.
10. Si une connexion directe entre le VDA et le service Citrix Gateway n'est pas possible, le VDA effectue via proxy sa connexion au Cloud Connector.
11. Le service Citrix Gateway établit une connexion entre le point de terminaison et le VDA.
12. Le VDA vérifie sa licence avec Citrix DaaS via Cloud Connector.
13. Citrix DaaS envoie des stratégies de session au VDA via Cloud Connector. Ces stratégies sont appliquées.

Rendezvous V2

December 16, 2022

Lors de l'utilisation du service Citrix Gateway, le protocole Rendezvous permet au trafic de contourner les Citrix Cloud Connector et de 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 de session HDX.

Rendezvous V1 permet au trafic de session HDX de contourner les Cloud Connector, mais il nécessite toujours que les Cloud Connector proxysent tout le trafic de contrôle pour l'enregistrement de VDA et la négociation des sessions.

Les machines jointes à un domaine AD standard et les machines n'appartenant pas à un domaine sont prises en charge pour l'utilisation de Rendezvous V2 avec des Linux VDA mono-session et multi-session. Avec les machines n'appartenant pas à un domaine, Rendezvous V2 permet à la fois au trafic HDX et au trafic de contrôle de contourner les Cloud Connector.

Exigences

Les conditions requises pour utiliser Rendezvous V2 sont les suivantes :

- Accès à l'environnement à l'aide du service Citrix Gateway et Citrix Workspace.
- Plan de contrôle : Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service).
- VDA version 2201 ou ultérieure.
  - La version 2204 est la version minimale requise pour les proxys HTTP et SOCKS5.
- 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 mettre en liste blanche tous les sous-domaines de cette manière, utilisez plutôt `https://*.c.nssvc.net` et `https://*.g.nssvc.net`. Pour plus d'informations, reportez-vous à la section Exigences en termes de connexion Internet de la documentation Citrix Cloud (sous Virtual Apps and Desktop service) et à l'article du centre de connaissances CTX270584.
- Les VDA doivent pouvoir se connecter aux adresses mentionnées précédemment :
  - Sur TCP 443, pour TCP Rendezvous.
  - Sur UDP 443, pour EDT Rendezvous.

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.
- Pour configurer un proxy pour contrôler le trafic, modifiez le registre comme suit :

```
1  /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
       VirtualDesktopAgent" -t "REG_SZ" -v "ProxySettings" -d "http
       ://<URL or IP>:<port>" --force
2  <!--NeedCopy-->
```

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.
- Pour configurer un proxy pour le trafic HDX, utilisez le paramètre de la 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.
- Les proxies HTTP prennent en charge l'authentification basée sur une machine à l'aide de Negotiate et des protocoles d'authentification Kerberos. Lorsque vous vous connectez au serveur proxy, le schéma d'authentification Negotiate sélectionne automatiquement le protocole Kerberos. Kerberos est le seul schéma pris en charge par le Linux VDA.

  > **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 nom principal de service, l'authentification échoue.

- 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

Le proxy HTTP transparent est pris en charge pour Rendezvous. Si vous utilisez un proxy transparent dans votre réseau, aucune configuration supplémentaire n'est requise sur le VDA.

Comment configurer Rendezvous V2

Voici les étapes à suivre pour configurer Rendezvous dans votre environnement :

1. Assurez-vous que toutes les exigences sont respectées.
2. Une fois le VDA installé, exécutez la commande suivante pour définir la clé de registre requise :

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent" -t "REG_DWORD" -v "GctRegistration" -d "0
     x00000001" --force
2 <!--NeedCopy-->
```

3. Redémarrez la machine VDA.
4. Créez une stratégie Citrix ou modifiez une stratégie existante :
   - Définissez le paramètre Protocole Rendezvous sur **Autorisé**.
   - Assurez-vous que les filtres de stratégie Citrix sont correctement définis. La stratégie s'applique aux machines pour lesquelles Rendezvous doit être activé.
   - Assurez-vous que la stratégie Citrix a la bonne priorité afin de ne pas en remplacer une autre.

Validation de Rendezvous

Pour vérifier si une session utilise le protocole Rendezvous, exécutez la commande `/opt/Citrix/VDA/bin/ctxquery -f iP` dans le terminal.

Les protocoles de transport utilisés indiquent le type de connexion :

- TCP Rendezvous: TCP - TLS - CGP - ICA
- EDT Rendezvous : UDP - DTLS - CGP - ICA
- Proxy via Cloud Connector : TCP - PROXY - SSL - CGP - ICA ou UDP - PROXY - DTLS - CGP - ICA

Si Rendezvous V2 est utilisé, la version du protocole affiche 2.0.

> **Conseil :**
>
> Si vous activez Rendezvous et que le VDA ne parvient pas à atteindre directement le service Citrix Gateway, le VDA revient au proxy de la session HDX via le Cloud Connector.

Sécuriser les sessions utilisateur en utilisant DTLS

December 16, 2022

Le cryptage DTLS est une fonctionnalité entièrement prise en charge à partir de la version 7.18. Par défaut, cette fonction est activée sur le Linux VDA. Pour plus d'informations, consultez la section Transport Layer Security.

Activer le chiffrement DTLS

Vérifier que le transport adaptatif est activé

Dans Citrix Studio, vérifiez que la stratégie **HDX Adaptive Transport** est définie sur le mode **Préféré** ou **Diagnostic**.

Activer le chiffrement SSL sur l'agent Linux VDA

Sur Linux VDA, utilisez l'outil **enable_vdassl.sh** dans **/opt/Citrix/VDA/sbin** pour activer (ou désactiver) le chiffrement SSL. Pour plus d'informations sur les options disponibles dans l'outil, exécutez la commande `/opt/Citrix/VDA/sbin/enable_vdassl.sh -h`.

> **Remarque :**
>
> Le Linux VDA prend actuellement en charge DTLS 1.0 et DTLS 1.2. DTLS 1.2 nécessite Citrix Receiver pour Windows 4.12 ou l'application Citrix Workspace 1808 pour Windows ou version ultérieure. Si votre client prend en charge uniquement DTLS 1.0 (par exemple, Citrix Receiver pour Windows 4.11), définissez **SSLMinVersion** to **TLS_1.0** et **SSLCipherSuite** sur **COM** ou **ALL** à l'aide de l'outil **enable_vdassl.sh**.

Sécuriser les sessions utilisateur en utilisant TLS

December 16, 2022

À compter de la version 7.16, l'agent Linux VDA prend en charge le chiffrement TLS pour des sessions utilisateur sécurisées. Le chiffrement TLS est désactivé par défaut.

Activer le chiffrement TLS

Pour activer le chiffrement TLS pour des sessions utilisateur sécurisées, installez des certificats et activez le chiffrement TLS sur le Linux VDA et le Delivery Controller (le Controller).

Installer des certificats sur le Linux VDA

Obtenez des certificats de serveur au format PEM et des certificats racine au format CRT. Un certificat de serveur contient les sections suivantes :

- Certificat
- Clé privée non chiffrée
- Certificats intermédiaires (facultatif)

Exemple de certificat de serveur


```
-----BEGIN CERTIFICATE-----
MIIDTTCCAragAwIBAgIJALluncpiqGXCMA0GCSqGSIb3DQEBBQUAMGcxCzAJBgNV
BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU
MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0
MB4XDTA4MDkzMDEwNTk1M1oXDTI4MDkyNTEwNTk1M1owgYoxCzAJBgNVBAYTAlVL
MRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEUMBIGA1UE
ChMLQ2l0cml4IFRlc3QxGzAZBgNVBAsTElNlcnZlciBDZXJ0aWZpY2F0ZTEgMB4G
A1UEAxMXY2EwMDEtc2MwMDEuY2l0cml0ZS5uZXQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALCTTOdxcivbI0LOF66xgO5gkNeIGKVP+37pSKV8B66lWCVzr6p9
t72Fa+9oCcf2x/ue274NXFcg4fqGRDsrEwl3YxM6COyBf7L6psrsCDNnBPlq8TJH
4xoPIXUeaW4MVk/3PVyfhHKs4fz8yy1I4VDnXVHhw+OFQ2Bq3NhwsRhnAgMBAAGj
gdwwgdkwCQYDVR0TBAIwADAdBgNVHQ4EFgQUrLidzYot+CUXSh9xMfp1M+/O8yOw
gZkGA1UdIwSBkTCBjoAU85kN1EPJOcVhcOss1slseDQwGsKha6RpMGcxCzAJBgNV
BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU
MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0
ggkAy8nC8dcB32EwEQYJYIZIAYb4QgEBBAQDAgVgMA0GCSqGSIb3DQEBBQUAA4GB
AD5axBYHwIxJCJzNt2zdXnbp2O0yUTowElBwQe/9cGaP6CpjoxJ7FJa2/8IpaT68
Vel8u1SEYY1GKCGCw93pc7sPKqb8pGBRI5/dygb+geFk1Q7KyVbuOIjOtr3pkxAe
b6CFJtNLudHUrwF6lOrB72zbyz3PiIx+HEwt1jOj8z4K
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQCwk0zncXIr2yNC9BeusYDuYJDXiBilT/t+6UilfAeupVglc6+q
fbe9hWvvaAnH9sf7ntu+DVxXIOH6hkQ7KxMNd2MTOgjsgX+y+qbK7AgzZwT9avEy
R+MaDyFlHmluDFZP9z1cn4RyrOH8/MstSOFQ511R4cPtBUNgatzYcLEYZwIDAQAB
AoGBAKwBgZu/bkl8edgB8YPyU7diiBX89IOs4b/aPjM+JDmjxb8N96RsPO24p9Ea
FtUc9+iL8mEroLUbSicCXjsJFc+cxg9vVaNa6EEkkBj735oCUERqSxOYb/lAdck/
FXzU0tqytUe/KHgcSgjtjrSeqLJqMm+yxzBAatVRTTzGdwAhAkEA3l1kRZjIN5uz
Enmi2RTI3ngBhBP/S3GEbvJfKsD5n2Ri9O+OoEPxclvvp5ne8QOzUpshbjFEPbOC
ykZ6UassFwJBAMtI5yPnV9ewPzJoaNjZIJcMtNXDchSlxXiJiyzv+Qmr8RuQz9Pv
fIenmTrfZ+Wo4DaKg+8ar2OvOnKFOHFAmDECQQDEWRlH6cE3WyCfN1u942M9XkhR
GvSpR7+b///vL6Nwwv3CwPV9n8DTpL+wuDkJZ9nCvRteil9MlaMTYjs3alNvAkEA
qy5JzZcbBnrYzMbVO32jju7ZPISnhTGO1xDjzMSLLpTGpNLN34b0k3sTclr8L42E
uQjtTqRm+wdsrVF3lFazkQJANudmsUVv3gZKhMGaV2hzIdXIfHyOIYv+3leZhQY6
h5eEmxSZS5OTvyNGt2e6m2ZgaZmjTagH59TCBHvR5nof2g==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDGTCCAoKgAwIBAgIJAMvJwvHXAd9hMA0GCSqGSIb3DQEBBQUAMGcxCzAJBgNV
BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU
MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0
MB4XDTA4MDkzMDEwNDExMVoXDTI4MDkyNTEwNDExMVowZzELMAkGA1UEBhMCVUsx
EjAQBgNVBAgTCUNhbWJyaWRnZTESMBAGA1UEBxMJQ2FtYm9lcmSlMRQwEgYDVQQK
EwtDaXRyaXggVGVzdDEaMBgGA1UEAxMRY2EwMDEuY2l0cml0ZS5uZXQwgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAKVZmF7Uj7uOnvO3Qwdfi0nr3QkNH2DXpWrZ
Zh8cI9Vv+UFRUiC6oB7izLtBMFn3fOUP7i2CfkHN3ZGJ17p89pdyjket1MslVeJw
acOqrYvD+fNNSvJjunTbaCywVtALjmFSfMHeZJXVSckrpEhnk0nkMS16tcrya/K/
osSlzvI3AgMBAAGjgcwwgckwDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQU85kN1EPJ
OcVhcOss1slseDQwGsIwgZkGA1UdIwSBkTCBjoAU85kN1EPJOcVhcOss1slseDQw
GsKha6RpMGcxCzAJBgNVBAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNV
BAcTCUNhbWJvdXJuZTEUMBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNh
MDAxLmNpdHJpdGUubmV0ggkAy8nC8dcB32EwDQYJKoZIhvcNAQEFBQADgYEAIZ4Z
gXLLXf12RNqh/awtSbd41Ugv8BIKAsg5zhNAiTiXbzz8Cl3ec53Fb6nigMWc5Tli
UNCLXwnxRUiD4O0tESLX9ACUNH3I94yxOgujkSOSBni21jjZTvfBB32Rmr5DByJg
UmKORn/hdqMlcqpe5wO6as6+HN4WUOi+hEtUMME=
-----END CERTIFICATE-----
```


Activer le chiffrement TLS

Activer le chiffrement TLS sur le Linux VDA Sur le Linux VDA, utilisez le script `enable_vdassl.sh` du répertoire **/opt/Citrix/VDA/Sbin** pour activer (ou désactiver) le chiffrement TLS. Pour plus d'informations sur les options disponibles dans le script, exécutez la commande `/opt/Citrix/VDA/sbin/enable_vdassl.sh -help`.

```
root@lxu1804:~# /opt/Citrix/VDA/sbin/enable_vdassl.sh
===Enable/Disable SSL on Linux VDA===
To enable SSL, a certificate file must be specified, otherwise the local certificate file under
/etc/xdl/.sslkeystore/ is used, If the local certificate file does not exist, the command
fails. You can specify the SSL port number, version and cipher suite, otherwise, their default
values are used!

Usage: enable_vdassl.sh -Disable
       Disable Linux VDA SSL.

Usage: enable_vdassl.sh -Enable [-Certificate <CERT-FILE>] [-SSLPort <SSL-PORT-NUMBER>]
       [-SSLMinVersion <SSL-MIN-VERSION>] [-SSLCipherSuite <SSL-CIPHER-SUITE>]
       Enable Linux VDA SSL.

Options:
       -Certificate <CERT-FILE>
       Specify a certificate file, where <CERT-FILE> must include the full file path. Only one format
       is currently supported, that is PEM.

       -RootCertificate <ROOT-CERT-FILE>
       Specify a root certificate file, where <ROOT-CERT-FILE> must include the full file path, The root certificate will be put in the local keystore(under /etc/xdl/.sslkeystore/cacerts).

       -SSLPort <SSL-PORT-NUMBER>
       Specify an SSL port number. Unless otherwise specified, the default port 443 used.

       -SSLMinVersion <TLS_1.0|TLS_1.1|TLS_1.2|TLS_1.3>
       Specify SSL version. Unless otherwise specified, the default value TLS_1.2 is used.

       -SSLCipherSuite <GOV|COM|ALL>
       Specify an SSL Cipher suite. Unless otherwise specified, the default value GOV is used.

Examples:
       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem"
       Enable Linux VDA SSL using Certificate cert001.pem.

       enable-vdassl.sh -Enable -RootCertificate "/home/rootCR.cer"
       Enable Linux VDA SSL using Root Certificate rootCR.cer with local certificate(under /etc/xdl/.sslkeystore).

       enable-vdassl.sh -Enable -SSLPort 445
       Enable Linux VDA SSL on port 445 using local certificate(under /etc/xdl/.sslkeystore).

       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445
       Enable Linux VDA SSL using Certificate cert001.pem on port 445, with default SSLMinVersion and SSLCipherSuite.

       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445 -SSLMinVersion "TLS_1.2"
       Enable Linux VDA SSL using Certificate cert001.pem on port 445 with SSLMinVersion TLS_1.2 and default SSLCipherSuite..

       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445 -SSLMinVersion "TLS_1.2" -SSLCipherSuite "GOV"
       Enable Linux VDA SSL using Certificate cert001.pem on port 445 with SSLMinVersion TLS_1.2 and SSLCipherSuite GOV.
```

Conseil : un certificat de serveur doit être installé sur chaque serveur Linux VDA et des certificats racine doivent être installés sur chaque serveur et client Linux VDA.

Activer le chiffrement TLS sur le Controller

> **Remarque :**
>
> Vous pouvez activer le chiffrement TLS uniquement pour les groupes de mise à disposition entiers. Vous ne pouvez pas activer le chiffrement TLS pour des applications spécifiques.

Dans une fenêtre PowerShell sur le Controller, exécutez les commandes suivantes dans l'ordre pour activer le chiffrement TLS pour le groupe de mise à disposition cible.

1. `Add-PSSnapin citrix.*`
2. `Get-BrokerAccessPolicyRule –DesktopGroupName 'GROUPNAME'| Set-BrokerAccessPolicyRule –HdxSslEnabled $true`

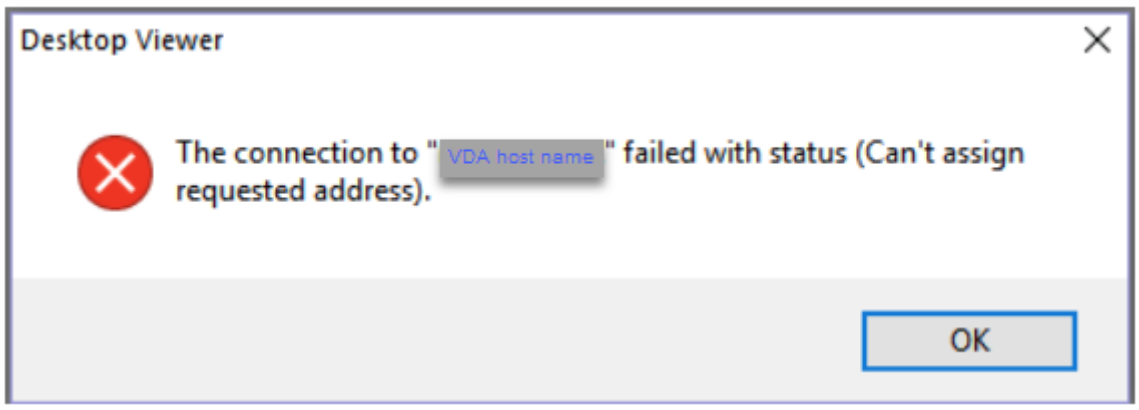
> **Remarque :**
>
> Pour vous assurer que seuls les noms de domaine complets VDA sont contenus dans un fichier de session ICA, vous pouvez également exécuter la commande `Set-BrokerSite –DnsResolutionEnabled $true`. La commande active la résolution DNS. Si vous désactivez la résolution DNS, un fichier de session ICA divulgue les adresses IP du VDA et fournit des noms de domaine complets uniquement pour les éléments liés à TLS tels que `SSLProxyHost` et `UDPDTLSPort`.

Pour désactiver le chiffrement TLS sur le Controller, exécutez les commandes suivantes dans l'ordre :

1. `Add-PSSnapin citrix.*`
2. `Get-BrokerAccessPolicyRule –DesktopGroupName 'GROUPNAME'| Set-BrokerAccessPolicyRule –HdxSslEnabled $false`
3. `Set-BrokerSite –DnsResolutionEnabled $false`

Résolution des problèmes

Le message d'erreur « Can't assign requested address » (Impossible d'attribuer l'adresse demandée) peut s'afficher dans l'application Citrix Workspace pour Windows lorsque vous tentez d'accéder à une session de bureau publié :



Pour résoudre ce problème, ajoutez une entrée au fichier **hosts**, comme :

```
<IP address of the Linux VDA>      <FQDN of the Linux VDA>
```

Sur les machines Windows, le fichier **hosts** est généralement situé dans `C:\Windows\System32\drivers\etc\hosts`.

Fiabilité de session

December 16, 2022

Citrix introduit la fonction de fiabilité de session sur toutes les plates-formes Linux prises en charge. L'option de fiabilité de session est activée par défaut.

La fiabilité de session reconnecte les sessions ICA en toute transparence pour toutes les interruptions réseau. Pour de plus amples informations sur la fiabilité de session, consultez la section Reconnexion automatique des clients et fiabilité de session.

Remarque : les données transmises via une connexion de fiabilité de session sont en texte brut par défaut. Pour des raisons de sécurité, nous vous recommandons d'activer le cryptage TLS. Pour de plus amples informations sur le cryptage TLS, consultez la section Sécuriser les sessions utilisateur en utilisant TLS.

Configuration

Paramètres de stratégie dans Citrix Studio

Vous pouvez définir les stratégies suivantes pour la fiabilité de session dans Citrix Studio :

- Connexions de fiabilité de session
- Expiration de délai de la fiabilité de session
- Numéro de port de la fiabilité de session
- Niveau de transparence de l'interface durant la reconnexion

Pour obtenir des informations supplémentaires, reportez-vous à Paramètres de stratégie Fiabilité de session et Paramètres de stratégie Reconnexion automatique des clients.

Remarque : après avoir défini la stratégie **Connexions de fiabilité de session** ou **Numéro de port de la fiabilité de session**, redémarrez le service VDA et le service HDX, dans cet ordre, pour que vos paramètres soient pris en compte.

Paramètres sur le Linux VDA

- **Activer/désactiver l'écouteur TCP de fiabilité de session**

Par défaut, l'écouteur TCP de fiabilité de session est activé et écoute sur le port 2598. Pour désactiver l'écouteur, exécutez la commande suivante.


```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
     CurrentControlSet\Control\Citrix\WinStations\cgp"   -v  "
     fEnableWinStation" -d "0x00000000"
2 <!--NeedCopy-->
```

Remarque : redémarrez le service HDX pour que vos paramètres soient pris en compte. La désactivation de l'écouteur TCP ne désactive pas la fiabilité de session. La fiabilité de session est toujours disponible au travers d'autres écouteurs (par exemple, SSL) si la fonctionnalité est activée via la stratégie **Connexions de fiabilité de session**.

- **Numéro de port de la fiabilité de session**

Vous pouvez également définir le numéro de port de fiabilité de session à l'aide de la commande suivante (qui utilise le numéro de port 2599 à titre d'exemple).

```
1 /opt/Citrix/VDA/bin/ctxreg update -k  "HKEY_LOCAL_MACHINE\SYSTEM\
     CurrentControlSet\Control\Citrix\WinStations\cgp"   -v  "PortNumber"
      -d  "2599"
2 <!--NeedCopy-->
```

Remarque : vous devez redémarrer le service HDX pour que ce paramètre soit pris en compte. Si le numéro de port a été défini via le paramètre de stratégie dans **Citrix Studio**, votre paramètre sur le Linux VDA est ignoré. Assurez-vous que le pare-feu sur le VDA est configuré pour ne pas interdire le trafic réseau via le port défini.

- **Intervalle de persistance serveur vers client**

Les messages de persistance sont envoyés entre le Linux VDA et le client lorsqu'il n'y a aucune activité dans la session (par exemple, aucun mouvement de souris, aucune mise à jour d'écran). Les messages de persistance sont utilisés pour détecter si le client est toujours réactif. S'il n'y a pas de réponse du client, la session est suspendue jusqu'à ce que le client se reconnecte. Ce paramètre spécifie le nombre de secondes entre les messages de persistance successifs. Ce paramètre n'est pas configuré par défaut. Pour le configurer, exécutez la commande suivante (qui utilise 10 secondes à titre d'exemple).

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\
     Citrix\XTEConfig"  -t "REG_DWORD"  -v  "CgpServerToClientKeepAlive"
      -d  "10"  --force
```

- **Intervalle de persistance client vers serveur**

Ce paramètre spécifie le nombre de secondes entre les messages de persistance successifs envoyés depuis le client ICA vers le Linux VDA. Ce paramètre n'est pas configuré par défaut. Pour le configurer, exécutez la commande suivante (qui utilise 10 secondes à titre d'exemple).


```
/opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\
    Citrix\XTEConfig"  -t "REG_DWORD"  -v  "CgpClientToServerKeepAlive"
     -d  "10"  --force
<!--NeedCopy-->
```

Résolution des problèmes

Impossible de lancer des sessions après avoir activé la fiabilité de session via le paramètre de stratégie.

Pour contourner ce problème, procédez comme suit :

1. Assurez-vous que le service VDA et le service HDX sont redémarrés, dans cet ordre, après avoir activé la fiabilité de session via le paramètre de stratégie dans Citrix Studio.
2. Sur le VDA, utilisez la commande suivante pour vérifier que l'écouteur TCP de fiabilité de session est en cours d'exécution (utilise le port 2598 à titre d'exemple).

   ```
   netstat -an | grep 2598
   <!--NeedCopy-->
   ```

   S'il n'y a pas d'écouteur TCP sur le port de fiabilité de session, activez l'écouteur en exécutant la commande suivante.

   ```
   /opt/Citrix/VDA/bin/ctxreg update -k  "HKEY_LOCAL_MACHINE\SYSTEM\
       CurrentControlSet\Control\Citrix\WinStations\cgp"   -v  "
       fEnableWinStation" -d "0x00000001"
   <!--NeedCopy-->
   ```

Redirection USB

December 16, 2022

Les périphériques USB sont partagés entre l'application Citrix Workspace et le bureau Linux VDA. Lorsqu'un périphérique USB a été redirigé sur le bureau, vous pouvez utiliser le périphérique USB comme s'il était connecté localement.

> **Conseil :**
>
> Nous vous recommandons d'utiliser la redirection USB lorsque la latence réseau est inférieure à 100 millisecondes. N'utilisez pas la redirection USB lorsque la latence réseau est supérieure à 200 millisecondes.

La redirection USB contient trois domaines de fonctionnalité :

- Open Source Project Implementation (VHCI)
- Service VHCI
- Service USB

Open-source VHCI :

Cette partie de la fonctionnalité de redirection USB développe un système de partage de périphérique USB général sur un réseau IP. Elle comprend un pilote noyau Linux et des bibliothèques en mode utilisateur, ce qui vous permet de communiquer avec le pilote noyau pour obtenir toutes les données USB. Dans la mise en œuvre du Linux VDA, Citrix réutilise le pilote noyau de VHCI. Toutefois tous les transferts de données USB entre le Linux VDA et l'application Citrix Workspace sont encapsulés dans le protocole ICA de Citrix.

Service VHCI :

Le service VHCI est un service open source fourni par Citrix pour communiquer avec le module noyau VHCI. Ce service fonctionne en tant que passerelle entre VHCI et le service USB Citrix.

Service USB :

Le service USB agit comme un module Citrix qui gère tous les transferts de données et de virtualisation sur le périphérique USB.

Fonctionnement de la redirection USB

En général, si un périphérique USB n'est pas redirigé correctement vers Linux VDA, un ou plusieurs nœuds de périphérique sont créés dans le chemin d'accès system/dev. Parfois, cependant, le périphérique redirigé ne peut pas être utilisé par une session Linux VDA active. Les périphériques USB s'appuient sur les pilotes pour fonctionner correctement et certains périphériques nécessitent des pilotes spéciaux. Si les pilotes ne sont pas fournis, les périphériques USB redirigés sont inaccessibles à la session Linux VDA active. Pour assurer la connectivité du périphérique USB, installez les pilotes et configurez le système correctement.

Le Linux VDA prend en charge une liste de périphériques USB qui peuvent être redirigés vers et depuis le client.

Périphériques USB pris en charge

Les périphériques suivants ont été testés pour prendre en charge cette version de Linux VDA. D'autres périphériques peuvent être utilisés, avec des résultats imprévisibles :

> **Remarque :**
>
> le VDA Linux ne prend en charge que les protocoles USB 2.0.

Périphérique de stockage de masse USB	VID:PID	Système de fichiers
Netac Technology Co., Ltd	0dd8:173c	FAT32
Kingston Datatraveler 101 II	0951:1625	FAT32
Kingston Datatraveler GT101 G2	1567:8902	FAT32
SanDisk SDCZ80 flash drive	0781:5580	FAT32
WD HDD	1058:10B8	FAT32

Souris 3D USB	VID:PID
3DConnexion SpaceMouse Pro	046d: c62b

Scanner USB	VID:PID
Epson Perfection V330 photo	04B8: 0142

Configurer la redirection USB

Une stratégie Citrix détermine si la redirection de périphérique USB est activée ou désactivée. Le type de périphérique peut également être spécifié à l'aide d'une stratégie Delivery Controller. Lors de la configuration de la redirection USB pour les Linux VDA, configurez les stratégies et règles suivantes :

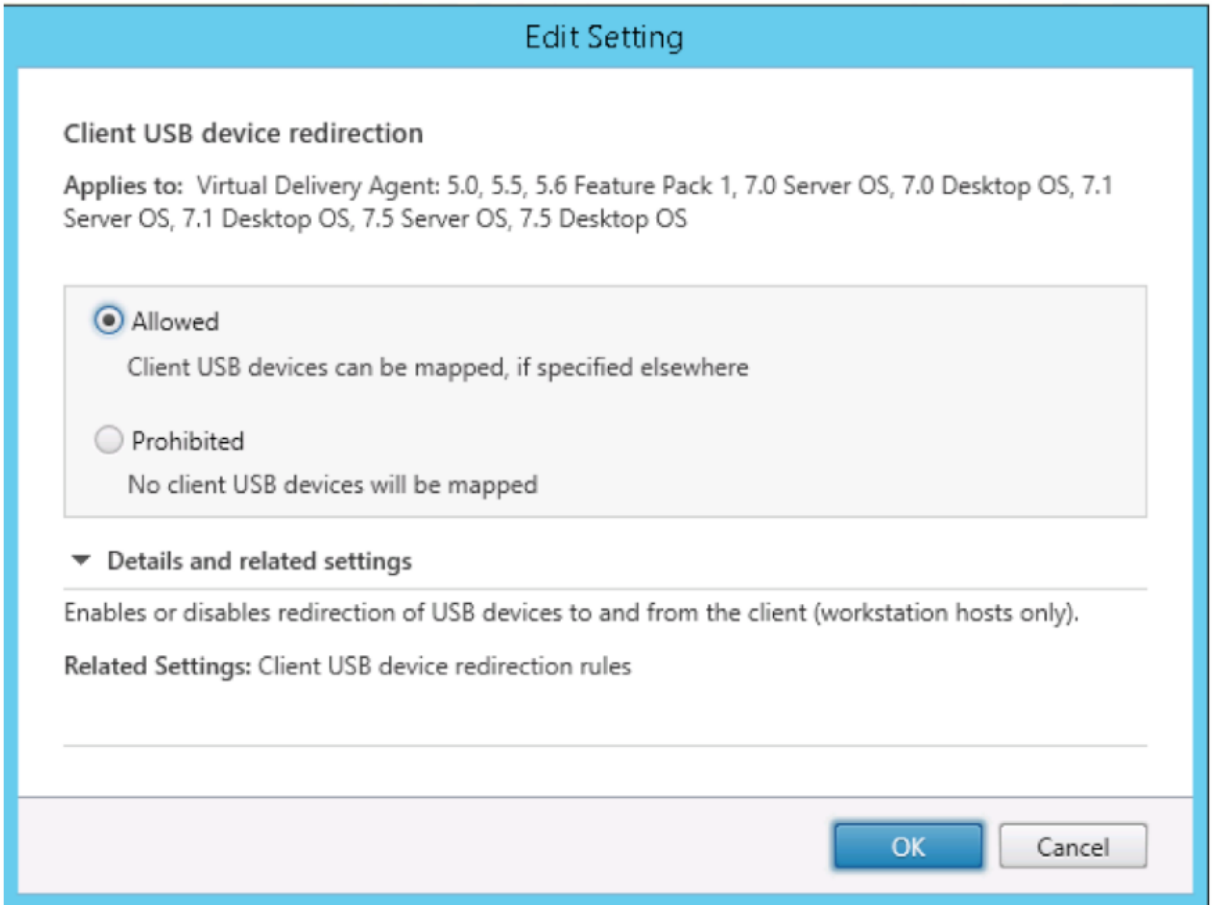
- Stratégie de redirection de périphérique USB client
- Règles de redirection des périphériques USB clients

Activer la redirection USB

Dans Citrix Studio, activez (ou désactivez) la redirection de périphérique USB vers et depuis le client (hôtes de station de travail uniquement).

Dans la boîte de dialogue **Modifier le paramètre** :

1. Sélectionnez **Autorisé**.
2. Cliquez sur **OK**.

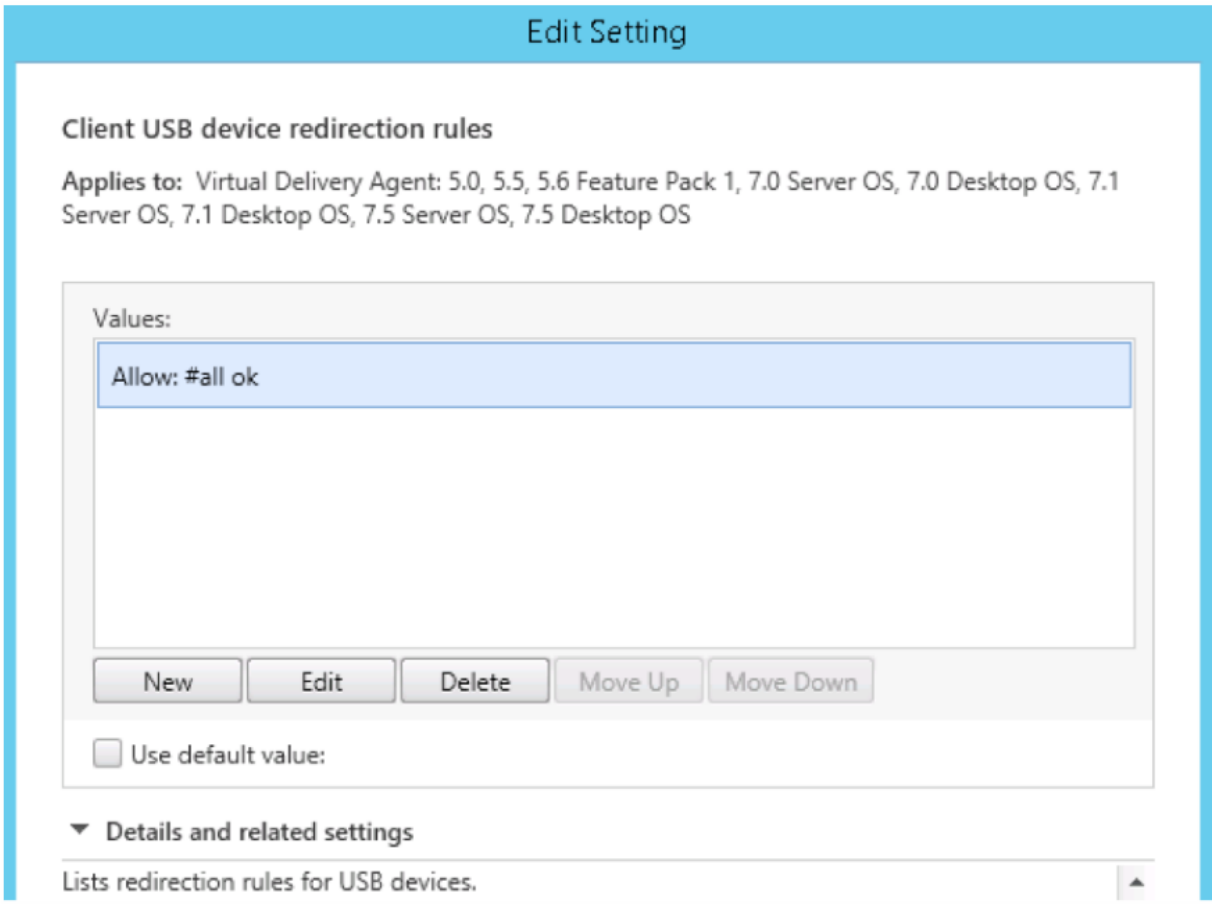


Définir des règles de redirection USB

Après activation de la stratégie de redirection USB, définissez les règles de redirection à l'aide de Citrix Studio en spécifiant les périphériques qui sont autorisés (ou interdits) sur le Linux VDA.

Dans la boîte de dialogue Règles de redirection de périphérique USB client :

1. Cliquez sur **Nouveau** pour ajouter une règle de redirection, ou cliquez sur **Modifier** pour vérifier une règle existante.
2. Après avoir créé (ou modifié) une règle, cliquez sur **OK**.



Pour de plus amples informations sur la configuration de la redirection USB générique, reportez-vous au Guide de configuration de la redirection USB générique Citrix.

Créer le module noyau VHCI

La redirection USB dépend des modules du noyau VHCI (`usb-vhci-hcd.ko` et `usb-vhci-iocif.ko`). Ces modules font partie de la distribution de Linux VDA (inclus dans le package RPM). Ils sont compilés selon les noyaux de distribution Linux officiels et sont indiqués dans le tableau suivant :

Distribution Linux prise en charge	Version du noyau
Amazon Linux 2	4.14.281-212
Debian 11.3	5.10.0-12
RHEL 8.x, Rocky Linux 8	4.18.0-372
RHEL 7.9, CentOS 7.9	3.10.0-1160
SUSE 15	5.3.18

Distribution Linux prise en charge	Version du noyau
Ubuntu 22.04	5.15.0-37
Ubuntu 20.04	5.4.0-117
Ubuntu 18.04	4.15.0-184

> **Important :**
>
> Si le noyau de votre machine n'est pas compatible avec le pilote créé pour les Linux VDA, le service USB peut ne pas parvenir à démarrer. Dans ce cas, vous pouvez utiliser la fonctionnalité de redirection USB uniquement si vous créez vos propres modules noyau VHCI.

Vérifier que votre noyau est cohérent avec les modules créés par Citrix

Sur la ligne de commande, exécutez la commande suivante pour vérifier si le noyau est cohérent :

```
insmod /opt/Citrix/VDA/lib64/usb-vhci-hcd.ko
<!--NeedCopy-->
```

Si la commande s'exécute correctement, le module noyau a été chargé avec succès et la version est cohérente avec celle installée par Citrix.

Si la commande s'exécute avec des erreurs, le noyau n'est pas cohérent avec le module Citrix et doit être recréé.

Recréer le module noyau VHCI

Si votre module noyau n'est pas cohérent avec la version Citrix, procédez comme suit :

1. Téléchargez le code source LVDA depuis le site de téléchargement de Citrix. Sélectionnez le fichier de la section « **Linux Virtual Delivery Agent (sources)** ».
2. Extrayez le fichier **citrix-linux-vda-sources.zip**. Accédez à **linux-vda-sources/vhci-hcd-1.15.zip** et extrayez les fichiers sources VHCI à l'aide de la commande `unzip vhci-hcd-1.15.zip`.
3. Assurez-vous que le package Linux VDA est installé, puis exécutez l'une des commandes suivantes :
   - `sudo bash ctxusbcfg.sh dkms`

     Cette commande vous permet d'utiliser le programme DKMS (Dynamic Kernel Module Support) pour gérer les modules du noyau VHCI. DKMS n'est pas disponible pour SUSE.

> **Remarque :**
>
> la commande `sudo bash ctxusbcfg.sh dkms` installe les programmes `kernel-devel` et `DKMS` sur votre VDA. Lors de l'installation des programmes sur RHEL et CentOS, la commande installe et active le référentiel Extra Packages for Enterprise Linux (EPEL) sur votre VDA.
>
> DKMS peut ne pas créer les modules du noyau VHCI (`usb-vhci-hcd.ko` et `usb-vhci-iocif.ko`) lorsque vous effectuez une mise à niveau majeure du noyau, par exemple, de la version 4.x.y à la version 5.x.y. Si DKMS échoue, exécutez `sudo bash ctxusbcfg.sh dkms` à nouveau.

- `sudo bash ctxusbcfg.sh build`

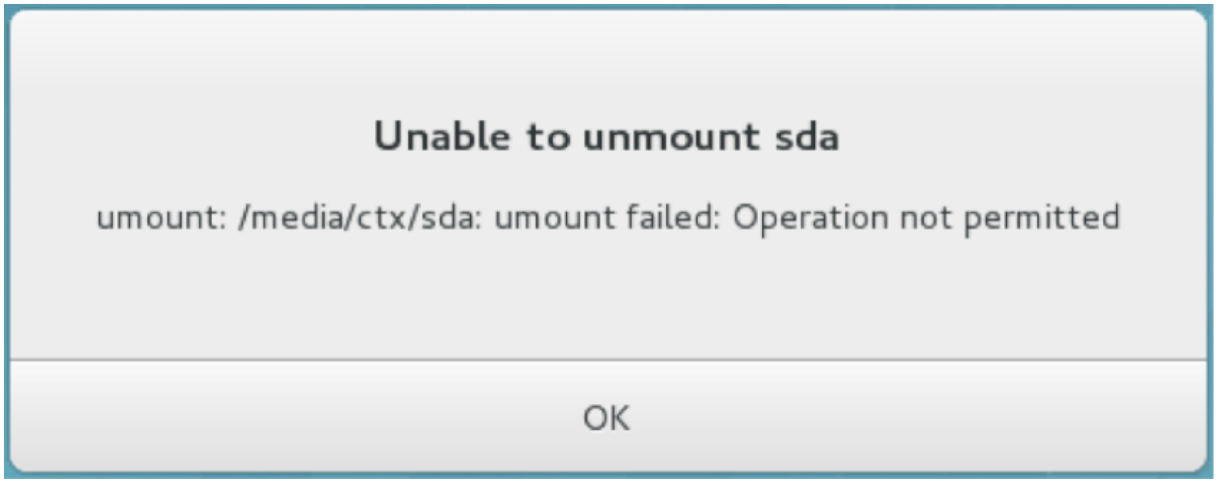
  Cette commande crée et installe les modules du noyau VHCI sans l'option DKMS.

Résolution des problèmes de redirection USB

Utilisez les informations de cette section pour résoudre les problèmes que vous pourriez rencontrer lors de l'utilisation du Linux VDA.

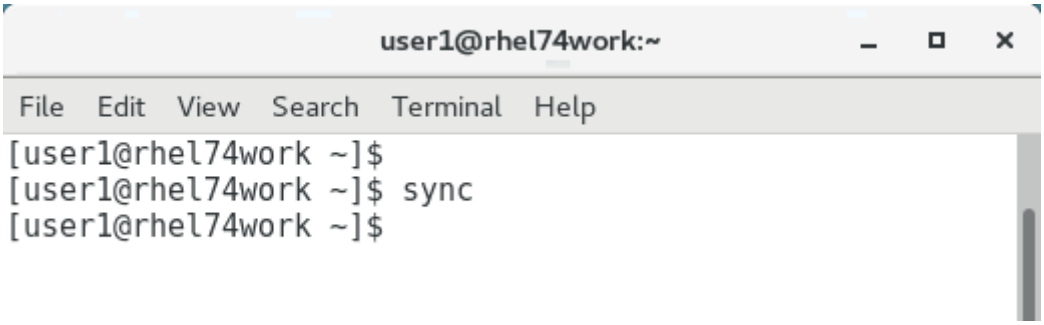
Impossible de démonter le disque USB redirigé

Le Linux VDA gère tous les disques USB redirigés à partir de l'application Citrix Workspace sous privilèges d'administrateur afin de garantir que seul le propriétaire peut accéder au périphérique redirigé. Par conséquent, vous ne pouvez pas démonter le périphérique sans privilèges d'administrateur.



Le fichier est perdu lorsque vous arrêtez la redirection d'un disque USB

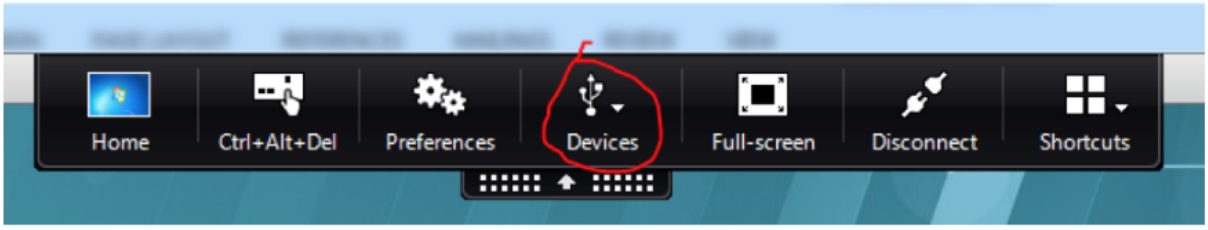
Si vous arrêtez de rediriger un disque USB immédiatement à l'aide de la barre d'outils de l'application Citrix Workspace, les fichiers que vous avez modifiés ou créés sur le disque peuvent être perdus. Ce problème se produit car, lors de l'écriture de données dans un système de fichiers, le système monte le cache mémoire dans le système de fichiers. Les données ne sont pas écrites sur le disque lui-même. Si vous arrêtez la redirection à l'aide de la barre d'outils de l'application Citrix Workspace, les données n'ont pas le temps d'être purgées vers le disque, ce qui entraîne une perte de données. Pour résoudre ce problème, utilisez la commande de synchronisation dans un terminal pour purger les données vers le disque avant d'arrêter la redirection USB.



Aucun périphérique dans la barre d'outils de l'application Citrix Workspace

Dans certains cas, vous ne pouvez pas voir les périphériques figurant sur la barre d'outils de l'application Citrix Workspace, ce qui indique qu'aucune redirection USB n'est en cours. Si vous rencontrez ce problème, vérifiez les points suivants :

- La stratégie est configurée pour permettre la redirection USB.
- Le module du noyau est compatible avec votre noyau



Affichage des périphériques USB dans la barre d'outils de l'application Citrix Workspace, mais avec la mention *Limité par une stratégie*, ce qui entraîne l'échec de la redirection

Lorsque le problème se produit, procédez comme suit :

- Configurez la stratégie du Linux VDA pour activer la redirection.

- Vérifiez si des restrictions de stratégie supplémentaires sont configurées dans le registre de l'application Citrix Workspace. Vérifiez **DeviceRules** dans le chemin d'accès du registre pour vous assurer que ce paramètre n'interdit pas l'accès au périphérique :

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB

Pour de plus amples informations
, consultez l'article du centre de connaissances Comment configurer la redirection automatique des périphériques USB.

Un périphérique USB est redirigé correctement, mais je ne peux pas l'utiliser dans ma session

Généralement, seuls les périphériques USB pris en charge peuvent être redirigés. D'autres périphériques peuvent également être redirigés vers une session VDA Linux active. Un nœud appartenant à l'utilisateur est créé dans le chemin d'accès **/dev** système. Toutefois, ce sont les pilotes et la configuration qui déterminent si l'utilisateur peut utiliser le périphérique. Si un périphérique vous appartenant (branché) n'est pas accessible, ajoutez-le à une stratégie sans restriction.

> **Remarque :**
>
> Pour les lecteurs USB, le Linux VDA configure et monte le disque. L'utilisateur (et seul l'utilisateur qui l'a installé) peut accéder au disque sans aucune configuration supplémentaire. Cela peut ne pas être possible avec les périphériques qui ne se trouvent pas dans la liste des périphériques pris en charge.

SDK Virtual Channel (expérimental)

December 16, 2022

Avec le kit SDK du canal virtuel, vous pouvez écrire des applications côté serveur pour les exécuter sur le VDA. Pour plus d'informations, consultez la documentation de Citrix Virtual Channel SDK pour Linux VDA.

Le SDK du canal virtuel Citrix pour Linux VDA peut être téléchargé depuis la page de téléchargement de Citrix Virtual Apps and Desktops. Développez la version appropriée de Citrix Virtual Apps and Desktops et cliquez sur **Composants** pour sélectionner le téléchargement du package Linux VDA.