



# Linux Virtual Delivery Agent 2311

## Contents

<b>Linux Virtual Delivery Agent 2311</b>	<b>6</b>
<b>Nouveautés</b>	<b>6</b>
<b>Problèmes résolus</b>	<b>10</b>
<b>Problèmes connus</b>	<b>11</b>
<b>Avis de tiers</b>	<b>14</b>
<b>Fin de prise en charge</b>	<b>15</b>
<b>Configuration système requise</b>	<b>16</b>
<b>Présentation de l'installation</b>	<b>21</b>
<b>Préparer l'installation</b>	<b>22</b>
<b>Créer des VDA joints à un domaine à l'aide d'Easy Install</b>	<b>23</b>
<b>Créer des VDA Linux non joints à un domaine à l'aide de MCS</b>	<b>48</b>
<b>Créer un Linux VDA non joint à un domaine à l'aide d'Easy Install (Technical Preview)</b>	<b>62</b>
<b>Créer des VDA Linux à l'aide de Machine Creation Services (MCS)</b>	<b>74</b>
<b>Créer des VDA Linux à l'aide de Citrix Provisioning</b>	<b>99</b>
<b>Créer des Linux VDA dans Citrix DaaS Standard pour Azure</b>	<b>100</b>
<b>Installer le Linux VDA manuellement</b>	<b>105</b>
<b>Installer le Linux VDA manuellement pour Amazon Linux 2, CentOS, RHEL et Rocky Linux</b>	<b>105</b>
<b>Installer le Linux VDA manuellement sur SUSE</b>	<b>144</b>
<b>Installer le Linux VDA manuellement sur Ubuntu</b>	<b>173</b>
<b>Installer le Linux VDA manuellement sur Debian</b>	<b>206</b>
<b>Configurer</b>	<b>237</b>
<b>Administration</b>	<b>237</b>
<b>Programme de collecte de données Linux VDA</b>	<b>238</b>

<b>HDX Insight</b>	<b>241</b>
<b>Intégration avec Citrix Telemetry Service</b>	<b>243</b>
<b>Mise à jour automatique de Linux VDA via Azure</b>	<b>246</b>
<b>Mesures pour les sessions Linux et les machines virtuelles Linux</b>	<b>250</b>
<b>Collecte de journaux</b>	<b>254</b>
<b>Observation de session</b>	<b>260</b>
<b>Démon du service de surveillance</b>	<b>267</b>
<b>Dépannage</b>	<b>269</b>
<b>Autres</b>	<b>276</b>
<b>Prise en charge de l'application Citrix Workspace pour HTML5</b>	<b>277</b>
<b>Créer un environnement virtuel Python3</b>	<b>278</b>
<b>Intégrer NIS avec Active Directory</b>	<b>280</b>
<b>IPv6</b>	<b>285</b>
<b>LDAPS</b>	<b>287</b>
<b>Xauthority</b>	<b>292</b>
<b>Authentification</b>	<b>294</b>
<b>Authentification avec Azure Active Directory</b>	<b>295</b>
<b>Authentification Single Sign-On double-hop</b>	<b>299</b>
<b>Service d'authentification fédérée</b>	<b>302</b>
<b>FIDO2 (version Technical Preview)</b>	<b>311</b>
<b>Pas d'authentification unique</b>	<b>313</b>
<b>Cartes à puce</b>	<b>314</b>
<b>Accès des utilisateurs non authentifiés (anonymes)</b>	<b>325</b>
<b>Fichier</b>	<b>327</b>

<b>Copier-coller de fichiers</b>	<b>327</b>
<b>Transfert de fichiers</b>	<b>329</b>
<b>Graphiques</b>	<b>332</b>
<b>Mise à l'échelle DPI automatique</b>	<b>333</b>
<b>Affichage de l'état de la batterie client</b>	<b>334</b>
<b>Configuration et réglage précis des graphiques</b>	<b>336</b>
<b>Partage d'écran HDX</b>	<b>348</b>
<b>Prise en charge multi-moniteurs</b>	<b>356</b>
<b>GPU non virtualisés</b>	<b>363</b>
<b>Filigrane de session</b>	<b>365</b>
<b>Accélération du GPU partagé sur un VDA Linux multi-session</b>	<b>371</b>
<b>Barre d'état système</b>	<b>373</b>
<b>Affichage progressif Thinwire</b>	<b>378</b>
<b>Redirection de contenu générale</b>	<b>381</b>
<b>Mappage des lecteurs clients</b>	<b>381</b>
<b>Redirection de périphérique USB</b>	<b>382</b>
<b>Redirection du Presse-papiers</b>	<b>391</b>
<b>Clavier</b>	<b>393</b>
<b>Éditeur IME</b>	<b>394</b>
<b>Synchronisation de l'interface utilisateur de l'éditeur IME client</b>	<b>395</b>
<b>Synchronisation dynamique de la disposition du clavier</b>	<b>399</b>
<b>Clavier logiciel</b>	<b>403</b>
<b>Prise en charge des entrées en plusieurs langues</b>	<b>406</b>
<b>Multimédia</b>	<b>408</b>

<b>Fonctionnalités audio</b>	<b>408</b>
<b>Redirection de contenu du navigateur</b>	<b>411</b>
<b>Compression vidéo pour Webcam HDX</b>	<b>421</b>
<b>VDA Linux non joints à un domaine</b>	<b>426</b>
<b>Liste des stratégies prises en charge</b>	<b>429</b>
<b>Impression</b>	<b>459</b>
<b>Meilleures pratiques d'impression</b>	<b>459</b>
<b>Impression PDF</b>	<b>466</b>
<b>Remote PC Access</b>	<b>467</b>
<b>Session</b>	<b>481</b>
<b>Transport adaptatif</b>	<b>482</b>
<b>Débit adaptatif HDX</b>	<b>485</b>
<b>Arrière-plans et messages de bannière personnalisés sur les écrans d'ouverture de session</b>	<b>486</b>
<b>Environnements de bureau personnalisés par utilisateurs de session</b>	<b>490</b>
<b>Ouvrir une session à l'aide d'un répertoire de base temporaire</b>	<b>491</b>
<b>Publier des applications</b>	<b>493</b>
<b>Rendezvous V1</b>	<b>496</b>
<b>Rendezvous V2</b>	<b>500</b>
<b>Secure HDX (Technical Preview)</b>	<b>505</b>
<b>Sécuriser les sessions utilisateur en utilisant DTLS</b>	<b>506</b>
<b>Sécuriser les sessions utilisateur en utilisant TLS</b>	<b>507</b>
<b>Fiabilité de session</b>	<b>511</b>
<b>Enregistrement de session (version Technical Preview)</b>	<b>513</b>
<b>SDK du canal virtuel (version Technical Preview)</b>	<b>515</b>

<b>Wayland (version Technical Preview)</b>	<b>516</b>
<b>Recommandations</b>	<b>517</b>
<b>Créer des Linux VDA sur Google Cloud Platform (GCP) à l'aide de Machine Creation Services (MCS)</b>	<b>517</b>

## Linux Virtual Delivery Agent 2311

August 20, 2024

### Important :

La stratégie de cycle de vie du produit des versions Current Releases (CR) et Long Term Service Releases (LTSR) est décrite dans [Étapes du cycle de vie](#).

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

August 20, 2024

### Nouveautés de la version 2311

#### Prise en charge de SUSE 15.5 et de Debian 11.7

Le Linux VDA prend désormais en charge SUSE 15.5 et Debian 11.7. Pour plus d'informations, consultez la section [Configuration système requise](#).

#### Débit adaptatif HDX

Le Linux VDA prend désormais en charge le débit adaptatif HDX. Cette fonctionnalité permet d'ajuster intelligemment le débit maximal des sessions ICA en ajustant les buffers de sortie, ce qui améliore l'expérience utilisateur. Pour plus d'informations, consultez l'article sur le [débit adaptatif HDX](#).

#### Prise en charge du codec AOMedia Video 1 (AV1)

Cette version introduit le nouveau codec, AV1, qui vous permet de recevoir des images de meilleure qualité avec la même utilisation de la bande passante et des images par seconde plus élevées sur des bandes passantes plus faibles. Le codec AV1 utilise une bande passante par image inférieure à celle

de H.264 ou H.265. Pour plus d'informations, consultez la section [Configuration et réglage précis des graphiques](#).

**Conseil :**

Pour utiliser HDX 3D Pro avec une unité de traitement graphique NVIDIA, vous devez installer une version du pilote graphique NVIDIA qui prend en charge la version 8 du SDK NVIDIA Capture. Pour plus d'informations, consultez la [documentation du SDK NVIDIA Capture](#).

### **État des graphiques disponible dans la barre d'état système**

Les utilisateurs de session peuvent désormais consulter l'état des graphiques en cliquant sur l'icône de la barre d'état système dans leurs sessions.

Pour plus d'informations, consultez la section [Barre d'état système](#).

### **Prise en charge de plusieurs périphériques audio (version Technical Preview)**

Cette version introduit une fonctionnalité de redirection audio. Cette fonctionnalité permet de rediriger vers la session Linux VDA distante plusieurs périphériques audio sur la machine cliente sur laquelle l'application Citrix Workspace est installée.

Lorsque cette fonctionnalité est activée :

- Tous les périphériques audio locaux de la machine cliente sont affichés au cours d'une session. Au lieu d'indiquer CitrixAudioSink (sortie audio) ou CitrixAudioSource (entrée audio), les périphériques audio sont affichés avec leur nom d'appareil respectif. Vous pouvez sélectionner un périphérique audio dans une application dans une session ou utiliser le périphérique audio par défaut pendant une session qui est également le périphérique audio par défaut de la machine cliente. Si nécessaire, vous pouvez modifier le périphérique audio par défaut à partir des paramètres système de l'ordinateur client. Une fois le périphérique audio par défaut de la machine cliente mis à jour, le nouveau périphérique apparaît comme périphérique audio par défaut dans la session.
- Les sessions sont mises à jour de manière dynamique lorsque vous branchez ou supprimez des périphériques audio.

Pour plus d'informations, consultez la section [Prise en charge de plusieurs périphériques audio](#).

### **Inscription basée sur un jeton (Technical Preview)**

Vous pouvez désormais inscrire des VDA non joints à un domaine dans un catalogue de machines et les authentifier auprès du plan de contrôle Citrix Cloud à l'aide d'un fichier de jeton.

L'inscription basée sur un jeton convient parfaitement aux cas d'utilisation où vous préparez vous-même des machines (physiques ou virtuelles) à l'aide d'une technologie autre que Citrix Provisioning. Elle offre les avantages suivants :

- Élimine le besoin d'installer et de gérer des Cloud Connector.
- Supprime la dépendance à AD pour l'authentification des utilisateurs et des machines, en activant l'authentification pour les machines non jointes à un domaine.

Pour plus d'informations, reportez-vous à la section [Créer un Linux VDA non joint à un domaine à l'aide d'Easy Install \(Technical Preview\)](#).

### Améliorations apportées à Easy Install

Nous avons remanié et simplifié la fonctionnalité Easy Install pour améliorer votre expérience. Vous pouvez désormais :

- Créer des VDA non joints à un domaine à l'aide d'**Easy Install**. Cette fonctionnalité est disponible dans la Tech Preview. Pour plus d'informations, reportez-vous à la section [Créer un Linux VDA non joint à un domaine à l'aide d'Easy Install \(Technical Preview\)](#).
- Exécuter le script Easy Install (ctxinstall.sh) via tous les modules ou des modules spécifiques. Pour obtenir des instructions sur l'exécution modulaire, exécutez **ctxinstall.sh -h** pour consulter des informations d'aide contenant des exemples. Pour plus d'informations sur ctxinstall.sh, consultez la section [ctxinstall.sh](#) de l'article [Créer des VDA joints à un domaine à l'aide d'Easy Install](#).
- Mieux comprendre le fichier ctxinstall.conf.tmpl dans lequel les variables sont regroupées en fonction des cas d'utilisation.

### Programme de collecte de données Linux VDA

Désormais, vous participez automatiquement au programme de collecte de données après avoir installé le Linux VDA. Le programme de collecte de données collecte des statistiques et des données d'utilisation et les envoie à Citrix Analytics pour améliorer la qualité et les performances des produits Citrix. Pour désactiver le programme et afficher plus de détails, consultez la section [Programme de collecte de données Linux VDA](#).

### Nouvelles mesures disponibles pour les sessions Linux

Cette version ajoute deux nouvelles mesures pour les sessions Linux dans Citrix Director et Monitor :

- **Latence ICA**

La latence ICA est en fait la latence du réseau. Cette mesure indique si le réseau est lent.

- **Stratégies**

Toutes les stratégies appliquées à la session en cours sont affichées dans l'onglet Stratégies de la vue **Détails de la session**.

Pour plus d'informations, consultez l'article [Métriques de la machine virtuelle Linux et des sessions Linux](#).

### **Contrôle de congestion EDT amélioré désormais disponible pour tous**

Nous avons ajouté un nouvel algorithme de contrôle de congestion pour optimiser le protocole EDT (Enlightened Data Transport). Cette implémentation permet à EDT d'atteindre un débit plus élevé et de réduire la latence pour une expérience utilisateur améliorée. Cette fonctionnalité est activée par défaut. Pour plus d'informations, consultez la section [Transport adaptatif](#).

### **Rendezvous V2 par défaut**

Le protocole Rendezvous est désactivé par défaut. Lorsque le protocole Rendezvous est activé, Rendezvous V2 est appliqué à la place de V1.

### **Découverte MTU EDT désormais activée par défaut sur le VDA**

La découverte MTU permet à EDT de déterminer automatiquement l'unité de transmission maximale (MTU) lors de l'établissement d'une session. Cela empêche la fragmentation des paquets EDT, qui pourrait entraîner une dégradation des performances ou l'échec de l'établissement d'une session. Pour plus d'informations, consultez la section [Transport adaptatif](#).

### **Secure HDX (Technical Preview)**

Vous pouvez crypter les sessions ICA de bout en bout entre l'application Citrix Workspace (client) et le VDA (hôte de session).

La fonctionnalité de cryptage de bout en bout (E2EE) n'autorise aucun élément réseau intermédiaire, y compris Citrix Gateway, à déchiffrer le trafic ICA. Le cryptage de bout en bout améliore la sécurité de votre environnement et est facile à configurer et à gérer. Pour plus d'informations, consultez [Secure HDX \(version Technical Preview\)](#).

## 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 2308 CR, consultez l'article [Historique des nouveautés](#).

## Problèmes résolus

August 20, 2024

Les problèmes suivants ont été résolus depuis Linux Virtual Delivery Agent 2311 :

- Lorsque vous accédez à une session de bureau virtuel à l'aide d'une machine cliente dépourvue de batterie, l'état de la batterie du client peut apparaître de manière inattendue dans la session. Le problème se produit lorsque vous utilisez l'un des clients suivants pour accéder à la même session que celle que vous avez précédemment ouverte à l'aide d'un appareil client équipé d'une batterie :
  - Application Citrix Workspace pour Mac
  - Application Citrix Workspace pour Linux

[LNXVDA-15406]

- Lorsque vous mettez à jour le VDA Linux vers la version 2308 et que vous réexécutez `ctxinstall.sh`, votre dossier de base est modifié. Le problème se produit lorsque vous définissez le nom de domaine Kerberos en majuscules et que vous utilisez SSSD comme méthode de jonction de domaine. Pour résoudre le problème, apportez les modifications suivantes au fichier `ctxinstall.sh` :
  - Dans la fonction de script `get_realm`, remplacez `realm=$(tr '[:upper:]' '[:lower:]' <<<"${ CTX_EASYINSTALL_REALM } ")` par `realm="${ CTX_EASYINSTALL_REALM } "` et remplacez `realm=$(tr '[:upper:]' '[:lower:]' <<<"$val")` par `realm="$val"`.
  - Dans la fonction de script `get_netbios_domain`, remplacez `workgroup=$(tr '[:upper:]' '[:lower:]' <<<"$CTX_EASYINSTALL_NETBIOS_DOMAIN")` par `workgroup="$CTX_EASYINSTALL_NETBIOS_DOMAIN"`.

[CVADHELP-23303]

- Lorsque HDX 3D Pro est activé, les sessions sur les écrans étendus sont masquées et seul le moniteur principal affiche correctement les sessions. Pour résoudre le problème, ouvrez un terminal sur le VDA et exécutez les commandes suivantes selon vos besoins :
  - Pour deux écrans, exécutez :

```
1 #sed -i "/UseEDID/a \ \ Option "ConnectedMonitor" "DFP, DFP""  
    /etc/X11/ctx-nvidia-2.conf
```

- Pour trois écrans, exécutez :

```
1 #sed -i "/UseEDID/a \ \ Option "ConnectedMonitor" "DFP, DFP,  
    DFP"" /etc/X11/ctx-nvidia-3.conf
```

- Pour quatre écrans, exécutez :

```
1 #sed -i "/UseEDID/a \ \ Option "ConnectedMonitor" "DFP, DFP,  
    DFP, DFP"" /etc/X11/ctx-nvidia-4.conf
```

[LNXVDA-15259]

- Les sessions Linux VDA peuvent ne plus répondre lorsque vous arrêtez de les utiliser pendant un certain temps. [CVADHELP-21344]
- Les VDA Linux provisionnés par Machine Creation Services (MCS) peuvent ne pas s'enregistrer auprès de Citrix Cloud. [CVADHELP-23600]
- L'enregistrement du VDA peut échouer lorsque le nombre de connexions simultanées est déjà établi. [CVADHELP-23789]
- Lorsque vous connectez le périphérique USB et que vous le sélectionnez, au lieu de le rediriger vers la machine Ubuntu, il se peut qu'il soit répertorié dans l'onglet **Périphériques** de la barre d'outils de l'application Citrix Workspace. [CVADHELP-23798]
- Lorsque vous faites glisser une application publiée, une partie de la fenêtre de l'application peut afficher des images d'arrière-plan. [CVADHELP-23824]

## Problèmes connus

August 20, 2024

Les problèmes suivants ont été identifiés dans cette version :

- Si vous ne spécifiez pas la variable CTX\_XDL\_DESKTOP\_ENVIRONMENT, il n'est pas possible de savoir quel bureau sera utilisé lors du processus suivant. Par conséquent, les variables d'environnement liées au bureau ne sont pas configurées et les applications ou plug-ins qui dépendent de ces variables peuvent ne pas fonctionner comme prévu. [LNXVDA-16212]
- En raison d'un problème lié à GNOME, le Linux VDA ne fonctionne pas comme prévu après la mise à niveau de **samba-winbind** vers la version 4.18.6 sur RHEL 8.X, Rocky Linux 8.x, RHEL 9.x

et Rocky Linux 9.x. Pour plus d'informations, consultez <https://issues.redhat.com/browse/HEL-17122>.

- Les échecs de lancement de session se produisent lorsque le nombre maximum de connexions défini dans PostgreSQL est insuffisant pour gérer des sessions simultanées. Pour résoudre ce problème, augmentez le nombre maximum de connexions en modifiant le paramètre **max\_connections** dans le fichier **postgresql.conf**.
- L'enregistrement du VDA peut échouer en raison de l'exception LDAP suivante générée dans le fichier **/var/log/xdl/jproxy.log** :

```
1 javax.naming.NamingException: LDAP response read timed out,
   timeout used: 10000 ms.
```

Pour contourner le problème, procédez comme suit :

- Modifiez la valeur du délai d'expiration LDAP. Par exemple, modifiez la valeur du délai d'expiration LDAP à 60s à l'aide de la commande suivante :

```
1 ctxreg create -k "HKLM\Software\Citrix\GroupPolicy\Defaults"
   -t "REG_DWORD" -v "LDAPTimeout" -d "0x000EA60" --force
```

- Accélérez les requêtes LDAP en définissant une base de recherche. Vous pouvez définir une base de recherche à l'aide de la variable **CTX\_XDL\_SEARCH\_BASE** dans le fichier **ctxsetup.sh** ou à l'aide de la commande suivante :

```
1 ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent" -
   t "REG_SZ" -v "LDAPComputerSearchBase" -d "<specify a
   search base instead of the root of the domain to improve
   search performance>" --force
```

[CVADHELP-20895]

- Microsoft a publié les mises à jour cumulatives KB5019966 et KB5019964 pour Windows 10 en novembre 2022. Les mises à jour introduisent des échecs lors de la jonction et de l'enregistrement de domaines. Pour contourner ce problème, consultez l'article [CTX474888](#) du centre de connaissances.
- Le type de cryptage **RC4\_HMAC\_MD5** étant autorisé pour Kerberos, le Linux VDA peut ne pas s'enregistrer auprès du Contrôleur 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 l'entrée suivante 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]
- 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 :

```
1 klist -li 0x3e4 purge
```

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

August 20, 2024

## [Linux Virtual Delivery Agent version 2311 \(PDF\)](#)

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

August 21, 2024

Les annonces de cet article visent à vous avertir à l'avance des plates-formes, des produits Citrix et des fonctionnalités qui vont disparaître pour que vous puissiez prendre les décisions appropriées. Citrix surveille l'utilisation des clients et leurs commentaires pour déterminer quand les retirer. Les annonces peuvent être modifiées dans les versions ultérieures et peuvent ne pas contenir chaque fonctionnalité amenée à disparaître.

Pour obtenir des informations sur la prise en charge du cycle de vie d'un produit, consultez l'article [Politique relative au cycle de vie du support produit Citrix](#).

## 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	Supprimé dans
Prise en charge de SUSE 15.4	2308	2311
Prise en charge de Rocky Linux 9.1, Rocky Linux 8.7	2305	2308
Prise en charge de RHEL 9.1, RHEL 8.7	2305	2308
Prise en charge de RHEL 8.4	2303	2308
Prise en charge de Ubuntu 18.04	2212	2305
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

<b>Élément</b>	<b>Abandon annoncé</b>	<b>Supprimé dans</b>
Prise en charge de RHEL 8.2	2206	2209
Prise en charge de RHEL 8.1, RHEL 8.3	2203	2206
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

August 20, 2024

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, versions Xorg et environnements de bureau pris en charge**

Pour une matrice des distributions Linux, des versions Xorg et des environnements de bureau 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	GNOME, GNOME Classic, MATE
Debian 11.7/11.3	1.20	GNOME, GNOME Classic, KDE, MATE
RHEL 9.2/9.0	1.20	GNOME
RHEL 8.8/8.6	1.20	GNOME, GNOME Classic, MATE
RHEL 7.9, CentOS 7.9	1.20	GNOME, GNOME Classic, KDE, MATE
Rocky Linux 9.2/9.0	1.20	GNOME
Rocky Linux 8.8/8.6	1.20	GNOME, GNOME Classic, KDE, MATE
SUSE 15.5	1.20	GNOME, GNOME Classic, MATE
Ubuntu 22.04	1.21	GNOME, GNOME Classic, KDE, MATE
Ubuntu 20.04	1.20	GNOME, GNOME Classic, KDE, MATE

---

**Remarque :**

- 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](#).
- Au moins un bureau doit être installé. Vous pouvez spécifier via le script `ctxinstall.sh` ou `ctxsetup.sh` l'environnement de bureau GNOME, GNOME Classic ou MATE à utiliser dans les sessions.
- Selon la [documentation de Red Hat Enterprise Linux](#), GNOME est le seul environnement de bureau disponible dans RHEL 9.
- N'utilisez pas `HWE kernel` ou `HWE Xorg` sur Ubuntu.
- 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](#).

## Configuration requise pour .NET

Vous devez installer le runtime .NET 6.0 sur toutes les distributions Linux prises en charge avant d'installer le Linux VDA.

## Environnements de virtualisation et plates-formes hôte pris en charge

- Serveurs bare metal
- Amazon Web Services (AWS)
- XenServer (anciennement 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.

À partir de la version 2203, vous pouvez héberger le Linux VDA sur Microsoft Azure, AWS et GCP pour Citrix Virtual Apps and Desktops ainsi que Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). Pour ajouter ces connexions hôtes au cloud public à votre déploiement Citrix

Virtual Apps and Desktops, vous avez besoin de la licence Citrix Universal Hybrid Multi-Cloud (HMC).

## 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 11.7/11.3	Oui	Oui	Oui	Oui	Oui
RHEL 9.2/9.0, Rocky Linux 9.2/9.0/8.8/8.6	Oui	Oui	Non	Non	Oui (Quest v4.1 et versions ultérieures)
RHEL 8.8/8.6	Oui	Oui	Oui	Oui	Oui (Quest v4.1 et versions ultérieures)
RHEL 7.9, CentOS 7.9	Oui	Oui	Oui	Oui	Oui (Quest v4.1 et versions ultérieures)
SUSE 15.5	Oui	Oui	Oui	Oui	Oui
Ubuntu 22.04/20.04	Oui	Oui	Oui	Oui	Oui (Quest v4.1 et versions ultérieures)

## Considérations sur le dimensionnement et la scalabilité des Cloud Connector

Lorsque vous connectez des VDA Linux au plan de contrôle à l'aide de composants Citrix Cloud Connector, tenez compte des points suivants sur la base des tests internes de Citrix :

- Chaque composant Citrix Cloud Connector (4 processeurs virtuels, 10 Go de mémoire) peut prendre en charge 3 000 Linux VDA.

- Pour bénéficier d'une haute disponibilité, déployez deux composants Cloud Connector et un maximum de 3 000 VDA Linux dans chaque [emplacement de ressources](#).

## 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 :

- XenServer (anciennement 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 le Linux VDA, HDX 3D Pro prend en charge les types de GPU suivants :

**GPU NVIDIA** 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 15. Pour plus d'informations, accédez à la page [NVIDIA Virtual GPU Software Supported GPUs](#).

**GPU non virtualisés** Dans la documentation du Linux VDA, les GPU non virtualisés font référence à :

- GPU utilisés dans les scénarios Remote PC Access
- GPU transmis par un hyperviseur

**GPU NVIDIA compatibles avec le SDK NVIDIA Capture pour Linux** Pour les GPU NVIDIA qui prennent en charge le [SDK NVIDIA Capture pour Linux](#), activez HDX 3D Pro en définissant **CTX\_XDL\_HDX\_3D\_PRO** sur **Y** lors de l'installation du Linux VDA. Aucune configuration supplémentaire n'est requise. L'accélération matérielle est activée par défaut après l'activation de HDX 3D Pro.

**Conseil :**

Pour utiliser HDX 3D Pro avec une unité de traitement graphique NVIDIA, vous devez installer une version du pilote graphique NVIDIA qui prend en charge la version 8 du SDK NVIDIA Capture. Pour plus d'informations, consultez la [documentation du SDK NVIDIA Capture](#).

## Présentation de l'installation

August 20, 2024

Cette section vous guide tout au long des procédures suivantes :

- [Préparer l'installation](#)
- [Créer des VDA joints à un domaine à l'aide d'Easy Install](#)
- [Créer des VDA Linux non joints à un domaine à l'aide de MCS](#)
- [Créer un Linux VDA non joint à un domaine à l'aide d'Easy Install \(Technical Preview\)](#)
- [Créer des VDA Linux à l'aide de MCS](#)
- [Créer des VDA Linux à l'aide de Citrix Provisioning](#)
- [Créer des Linux VDA dans Citrix DaaS Standard pour Azure](#)
- [Installer le Linux VDA manuellement](#)
  - [Installer le Linux VDA manuellement pour Amazon Linux 2, CentOS, RHEL et Rocky Linux](#)
  - [Installer le Linux VDA manuellement sur SUSE](#)
  - [Installer le Linux VDA manuellement sur Ubuntu](#)
  - [Installer le Linux VDA manuellement sur Debian](#)

## Préparer l'installation

August 21, 2024

Cet article explique comment choisir une méthode d'installation adaptée à votre situation particulière et vous oriente vers le guide d'installation correspondant. Pour plus d'informations sur la planification des déploiements de Citrix Virtual Apps and Desktops et de Citrix DaaS, consultez les sections [Préparation à l'installation](#) et [Premiers pas : planifier et créer un déploiement](#) respectivement.

Avant de commencer à installer le VDA, tenez compte des points suivants :

- Vérifiez que votre déploiement cible est officiellement pris en charge en vérifiant [la configuration système requise de Linux VDA](#).
- Décidez si vous souhaitez connecter vos VDA à un domaine ou non.
- Choisissez un lien approprié dans le tableau suivant en fonction de votre méthode de provisioning et de votre décision de jonction de domaine :

	Script d'installation facile	Machine Creation Services (MCS)	Citrix Provisioning	Purement manuelle	Remarque
Jonction à un domaine	<a href="#">Créer des VDA joints à un domaine à l'aide d'Easy Install</a>	<a href="#">Créer des VDA Linux à l'aide de Machine Creation Services (MCS)</a>	<a href="#">Créer des VDA Linux à l'aide de Citrix Provisioning</a>	<a href="#">Installer le Linux VDA manuellement</a>	S/O
Non joint au domaine	<a href="#">Créer un Linux VDA non joint à un domaine à l'aide d'Easy Install (Technical Preview)</a>	<a href="#">Créer des VDA Linux non joints à un domaine à l'aide de MCS</a>	Non pris en charge	Non pris en charge	DaaS uniquement

**Remarque :**

- MCS n'est PAS pris en charge pour les cas d'utilisation de Remote PC Access.
- Pour le provisioning en masse, vous pouvez utiliser MCS, Citrix Provisioning ou une automatisation tierce à votre guise. Pour l'automatisation tierce, vous avez la possibilité d'intégrer le script d'installation facile (recommandé) ou d'automatiser les étapes d'installation purement manuelle dans votre script.
- Pour obtenir une preuve de concept (POC) rapide sur une seule machine virtuelle, nous vous recommandons d'utiliser Easy Install.
- Vous pouvez également exécuter le script d'installation facile (ctxinstall.sh -s) pour mettre à jour rapidement vos variables d'environnement telles que CTX\_XDL\_DDC\_LIST et CTX\_XDL\_LDAP\_LIST.

## Créer des VDA joints à un domaine à l'aide d'Easy Install

August 21, 2024

**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 non joints à un domaine, vous pouvez utiliser Machine Creation Services (MCS) et Easy Install. Pour plus d'informations, consultez [Créer des VDA Linux non joints à un domaine à l'aide de MCS](#) et [Créer un Linux VDA non joint à un domaine à l'aide d'Easy Install \(Technical Preview\)](#).
- Pour en savoir plus sur les fonctionnalités disponibles pour les VDA non joints à un domaine, consultez la section [VDA non joints 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
- Méthode d'intégration d'Active Directory (AD) : actuellement, Easy Install prend en charge Winbind, SSSD, Centrify, PBIS et Quest. Easy install prend en charge Quest uniquement pour RHEL et Rocky Linux.
- Nom d'utilisateur : nom de l'utilisateur qui joint la machine au domaine
- Mot de passe : mot de passe de l'utilisateur qui joint la machine au domaine
- Unité d'organisation (UO) Facultatif.

**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.
- Pour des raisons de sécurité, Easy Install n'enregistre pas le mot de passe permettant de joindre le domaine. Chaque fois que vous exécutez le script Easy Install (ctxinstall.sh) en mode interactif, vous devez saisir manuellement le mot de passe pour joindre le domaine. En mode silencieux, vous devez définir le mot de passe permettant de joindre le domaine dans **/Citrix/VDA/sbin/ctxinstall.conf** ou exporter le mot de passe. Nous vous recommandons de ne pas utiliser le compte administrateur pour rejoindre un domaine. Déléguez plutôt les autorisations pour joindre un domaine à un utilisateur Active Directory autre que le compte administrateur. Pour ce faire, déléguez le contrôle sur le contrôleur de domaine à l'aide de l'**Assistant Délégation de contrôle**.

## 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 XenServer (anciennement Citrix Hypervisor)

Lorsque la fonctionnalité de synchronisation de l'heure de XenServer est activée, vous rencontrez des problèmes avec NTP et XenServer au sein de chaque machine virtuelle Linux paravirtualisée. 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 XenServer VM Tools installé, vous pouvez vérifier si la fonctionnalité de synchronisation de l'heure de XenServer est présente et activée à partir de la VM Linux :

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
```

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 désactivée, désactivez-la en entrant 1 dans le fichier :

```
1 sudo echo 1 > /proc/sys/xen/independent_wallclock
```

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 :

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
```

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 XenServer (anciennement 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

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>.

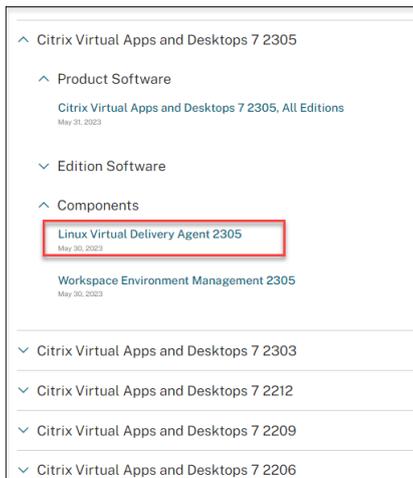
Après avoir installé .NET Runtime 6.0, exécutez la commande **which dotnet** pour trouver votre chemin d'exécution.

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.

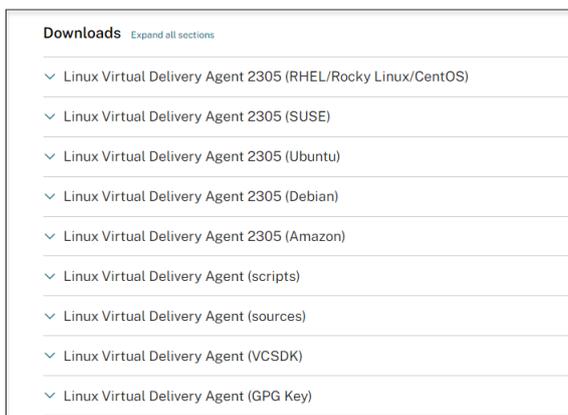
### Étape 4 : télécharger le package Linux VDA

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. Développez **Components** pour trouver le Linux VDA. Par exemple :

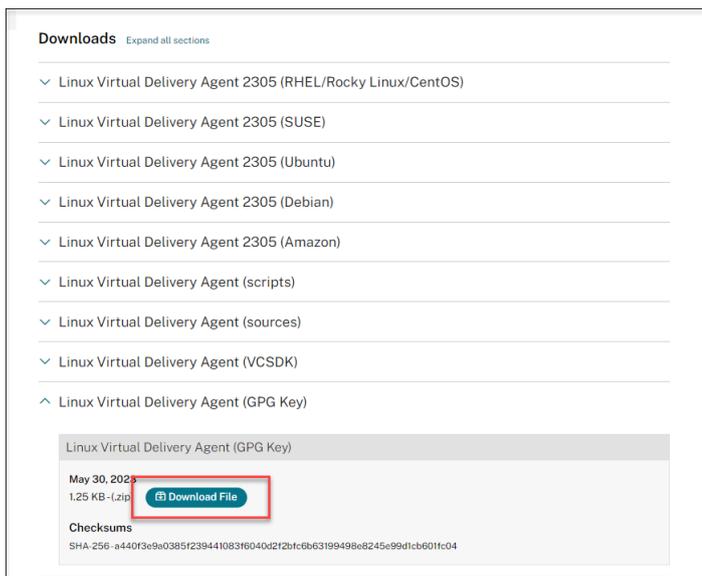


4. Cliquez sur le lien Linux VDA pour accéder aux téléchargements de Linux VDA.



5. Téléchargez le package Linux VDA correspondant à votre distribution Linux.

6. Téléchargez la clé publique GPG que vous pouvez utiliser pour vérifier l'intégrité du package Linux VDA. Par exemple :



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

- Pour un package RPM, exécutez les commandes suivantes pour importer la clé publique dans la base de données RPM et vérifier l'intégrité du package :

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

- Pour un package DEB, exécutez les commandes suivantes pour importer la clé publique dans la base de données DEB et vérifier l'intégrité du package :

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

### Étape 5 : installer le package VDA Linux

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

Pour les distributions Amazon Linux 2, CentOS, RHEL et Rocky Linux :

#### 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 de la page <https://docs.fedoraproject.org/en-US/epel/>.
- Avant d'installer le Linux VDA sur RHEL 9.2/9.0 et Rocky Linux 9.2/9.0, mettez à jour le package **libsepol** vers la version 3.4 ou ultérieure.

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

**Remarque :**

Après avoir installé le Linux VDA sur RHEL 8.x/9.x et Rocky Linux 8.x/9.x hébergés sur GCP, la connexion Ethernet peut être perdue et le Linux VDA peut être inaccessible après le redémarrage d'une machine virtuelle. Pour contourner ce problème, définissez un mot de passe racine lorsque vous vous connectez à la VM pour la première fois et assurez-vous que vous pouvez vous connecter à la VM en tant qu'utilisateur racine. Exécutez ensuite les commandes suivantes dans la console après avoir redémarré la VM :

```
1 nmcli dev connect eth0
2 systemctl restart NetworkManager
```

Pour les distributions Ubuntu/Debian :

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

**Remarque :**

- Pour installer les dépendances nécessaires pour une distribution Debian 11, ajoutez la ligne `deb http://deb.debian.org/debian/ bullseye main` au fichier `/etc/apt/sources.list`.
- Pour Ubuntu 20.04 sur GCP, désactivez RDNS. Pour ce faire, ajoutez la ligne `rdns = false` sous `[libdefaults]` dans `/etc/krb5.conf`.

Pour les distributions SUSE :

1. Pour SUSE 15.5 sur AWS, Azure et GCP, assurez-vous que :
  - Vous utilisez **libstdc++6** version 12 ou ultérieure.
  - Le paramètre **Default\_WM** dans `/etc/sysconfig/windowmanager` est défini sur « **gnome** ».
2. Exécutez la commande suivante pour installer le Linux VDA :

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

## 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 :

- [XenServer](#)
- [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 : spécifier la base de données à utiliser

Vous pouvez également basculer entre SQLite et PostgreSQL après avoir installé le package Linux VDA. Pour ce faire, procédez comme suit :

### Remarque :

- Nous vous recommandons d'utiliser SQLite pour le mode VDI uniquement et d'utiliser PostgreSQL pour un modèle de mise à disposition de bureaux partagés hébergés.
- Pour Easy Install et MCS, vous pouvez spécifier SQLite ou PostgreSQL sans avoir à les installer manuellement. Sauf indication contraire dans **/etc/xdl/db.conf**, le Linux VDA utilise PostgreSQL par défaut.
- Vous pouvez également utiliser **/etc/xdl/db.conf** pour configurer le numéro de port de PostgreSQL.

1. Modifiez **/etc/xdl/db.conf** pour spécifier la base de données à utiliser.
2. Exécutez **sudo /opt/Citrix/VDA/sbin/ctxinstall.sh** ou **/opt/Citrix/VDA/bin/easyinstall**.

## Étape 8 : terminez l'installation en exécutant Easy Install pour configurer l'environnement et le VDA

Après l'installation du package Linux VDA, configurez l'environnement d'exécution à l'aide du script `ctxinstall.sh` ou de l'interface utilisateur.

### 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**.

## **ctxinstall.sh**

Le script Easy Install `ctxinstall.sh` permet d'effectuer certaines préconfigurations et de configurer le VDA exécutant des variables d'environnement.

- Seul un accès racine peut exécuter ce script.
- Easy Install utilise le fichier de configuration `"/opt/Citrix/VDA/sbin/ctxinstall.conf"` pour définir, enregistrer et synchroniser les valeurs de toutes les variables d'environnement utilisées. Nous vous recommandons de lire attentivement le modèle (`ctxinstall.conf.tpl`), puis de personnaliser votre propre fichier `"ctxinstall.conf"`. Lorsque vous créez le fichier de configuration pour la première fois, utilisez l'une des méthodes suivantes :
  - Copiez le fichier de modèle `/opt/Citrix/VDA/sbin/ctxinstall.conf.tpl` et enregistrez-le sous `/opt/Citrix/VDA/sbin/ctxinstall.conf`.
  - Exécutez `ctxinstall.sh`. Chaque fois que vous exécutez `ctxinstall.sh`, votre entrée est enregistrée dans `/opt/Citrix/VDA/sbin/ctxinstall.conf`.
- Easy Install permet un fonctionnement modulaire. Les modules incluent la pré-vérification, l'installation, la configuration de domaine, la configuration et la vérification.
- Les détails de débogage de ce script se trouvent dans le fichier `"/var/log/xdl/ctxinstall.log"`.

Pour plus d'informations, utilisez la commande d'aide **ctxinstall.sh -h**.

### **Remarque :**

- Respectez le principe du moindre privilège et assurez-vous que seul l'utilisateur racine peut lire **/opt/Citrix/VDA/sbin/ctxinstall.conf** ; en effet, le mot de passe permettant de joindre domaine peut être défini dans le fichier.
- La désinstallation du Linux VDA supprime les fichiers situés sous **/opt/Citrix/VDA**. Nous vous recommandons de sauvegarder **/opt/Citrix/VDA/sbin/ctxinstall.conf** avant de désinstaller le VDA.

Vous pouvez exécuter `ctxinstall.sh` en mode interactif ou en mode silencieux. Avant d'exécuter le script, définissez les variables d'environnement suivantes :

- **CTX\_XDL\_NON\_DOMAIN\_JOINED='Y|N'** : indique s'il faut associer la machine à un domaine . La valeur par défaut est "n". Pour les scénarios liés à un domaine, définissez la valeur sur "n".

- **CTX\_XDL\_AD\_INTEGRATION='winbind|sssd|centrify|pbis|quest'** : 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.
- **CTX\_XDL\_DDC\_LIST='<list-ddc-fqdns>'** : 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\_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\_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 VDA doit être configuré pour le mode Bureaux VDI (session unique), c'est-à-dire, CTX\_XDL\_VDI\_MODE='y'.
- **CTX\_XDL\_START\_SERVICE='y|n'** : indique si les services Linux VDA sont lancés une fois la configuration de Linux VDA terminée.
- **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 Virtual Desktop 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\_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 par défaut configuré sur le VDA est utilisé.
- **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 d'accès par défaut est **'/usr/bin'**.
- **CTX\_XDL\_VDA\_PORT=port-number** : le Linux VDA communique avec les Delivery Controller via un port TCP/IP.
- **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. Pour accélérer les requêtes LDAP dans une forêt Active directory, 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\_SUPPORT\_DDC\_AS\_CNAME=y|n** : le Linux VDA prend en charge la spécification d'un nom de composant Delivery Controller à l'aide d'un enregistrement DNS CNAME.
- **CTX\_EASYINSTALL\_DNS='<ip-address-of-dns>'** : adresse IP du DNS.
- **CTX\_EASYINSTALL\_HOSTNAME=host-name** : nom d'hôte du serveur Linux VDA.
- **CTX\_EASYINSTALL\_NTPS=address-of-ntps** : adresse IP ou nom de chaîne du serveur NTP.
- **CTX\_EASYINSTALL\_REALM=realm-name** : nom de la zone Kerberos.
- **CTX\_EASYINSTALL\_FQDN=ad-fqdn-name**
- **CTX\_EASYINSTALL\_USERNAME=domain-user-name** : nom de l'utilisateur qui joint la machine au domaine.
- **CTX\_EASYINSTALL\_PASSWORD=password** : mot de passe de l'utilisateur qui joint la machine au domaine.

**Remarque :**

Nous vous recommandons de ne pas utiliser le compte administrateur pour rejoindre un domaine. Déléguez plutôt les autorisations pour joindre un domaine à un utilisateur Active Directory autre que le compte administrateur. Pour ce faire, déléguez le contrôle sur le contrôleur de domaine à l'aide de l'**Assistant Délégation de contrôle**.

Les quatre variables suivantes sont facultatives. Même si elles ne sont pas définies, ctxinstall.sh ne s'interrompra pas en mode silencieux et vous ne serez pas invité à saisir des informations utilisateur en mode interactif. Vous pouvez les définir uniquement en exportant leurs valeurs ou en modifiant **/Citrix/VDA/sbin/cxinstall.conf**.

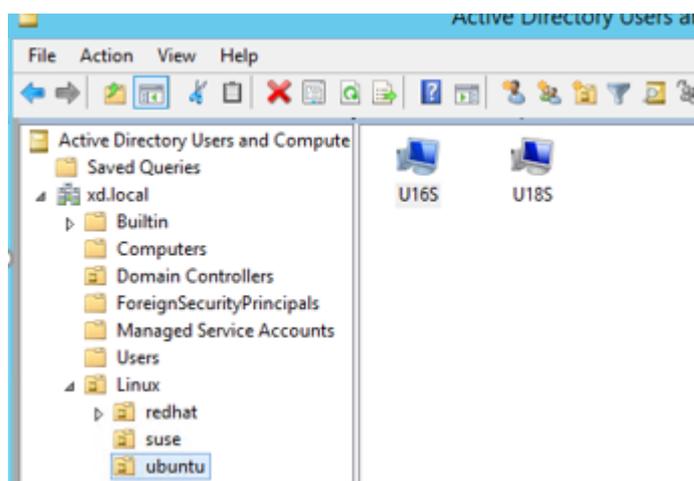
- **CTX\_EASYINSTALL\_NETBIOS\_DOMAIN=netbios-domain-name** : le nom de domaine NetBIOS est généralement le premier composant du nom de domaine DNS séparé par un point (.). Vous pouvez également personnaliser un autre nom de domaine NetBIOS. Cette variable est facultative.

- **CTX\_EASYINSTALL\_OU=ou-value** : les valeurs de l'unité d'organisation varient en fonction des différentes méthodes d'intégration AD. Pour obtenir un exemple de valeurs d'unité d'organisation, consultez le tableau de la section Considérations de cet article. Cette variable est facultative.
- **CTX\_EASYINSTALL\_CENTRIFY\_LOCAL\_PATH=centrify-local-path** : grâce à Easy Install, vous pouvez télécharger le package Centrify depuis Internet. Toutefois, si Centrify est déjà installé, vous pouvez récupérer le package Centrify à partir d'un répertoire local défini par cette variable. Cette variable est facultative.
- **CTX\_EASYINSTALL\_PBIS\_LOCAL\_PATH=pbis-local-path** : grâce à Easy Install, vous pouvez télécharger le package PBIS depuis Internet. Toutefois, si PBIS est déjà installé, vous pouvez récupérer le package PBIS depuis un répertoire local défini par cette variable. Cette variable est facultative.

## Considérations

- Le nom de domaine NetBIOS est généralement le premier composant du nom de domaine DNS séparé par un point (.). Pour personnaliser un nom de domaine NetBIOS différent dans votre environnement, définissez la variable d'environnement **CTX\_EASYINSTALL\_NETBIOS\_DOMAIN** dans **/opt/Citrix/VDA/sbin/ctxinstall.conf**.
- 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. Définissez la variable d'environnement **CTX\_EASYINSTALL\_OU** dans **/opt/Citrix/VDA/sbin/ctxinstall.conf**.

Les valeurs de l'unité d'organisation varient en fonction des différentes méthodes AD. Le tableau suivant présente les exemples de noms d'unité organisationnelle figurant dans

la capture d'écran précédente. Vous pouvez utiliser n'importe quel autre nom d'unité organisationnelle au sein de votre organisation.

OS	Winbind	SSSD	Centrify	PBIS
Amazon Linux 2	"Linux/ amazon"	"Linux/ amazon"	"XD.LOCAL/ Linux/amazon "	"Linux/ amazon"
Debian	"Linux/ debian"	"Linux/ debian"	"XD.LOCAL/ Linux/debian "	"Linux/ debian"
RHEL 9.2/9.0, Rocky Linux 9.2/9.0	"OU=redhat, OU=Linux"	"OU=redhat, OU=Linux"	S/O	S/O
RHEL 8.x	"OU=redhat, OU=Linux"	"OU=redhat, OU=Linux"	"XD.LOCAL/ Linux/redhat "	"Linux/ redhat"
Rocky Linux 8.x	"OU=redhat, OU=Linux"	"OU=redhat, OU=Linux"	S/O	S/O
RHEL 7	"Linux/ redhat"	"Linux/ redhat"	"XD.LOCAL/ Linux/redhat "	"Linux/ redhat"
SUSE	"Linux/suse"	"Linux/suse"	"XD.LOCAL/ Linux/suse"	"Linux/suse"
Ubuntu	"Linux/ ubuntu"	"Linux/ ubuntu"	"XD.LOCAL/ Linux/ubuntu "	"Linux/ ubuntu"

- Centrify ne prend pas en charge la configuration DNS **IPv6** pures. Au moins un serveur DNS utilisant **IPv4** doit être spécifié dans le fichier `/etc/resolv.conf` pour que **adclient** puisse trouver les services AD appropriés.

**Journal :**

```

1  ADSITE      : Check that this machine's subnet is in a site known by
   AD         : Failed
2           : This machine's subnet is not known by AD.
3           : We guess you should be in the site Site1.
```

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**.
- 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.
    - Centrifý 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.

- 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**

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

- **Pour le bureau GNOME Classic**

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

- Si vous choisissez Centrify comme méthode pour rejoindre un domaine, le script `ctxinstall.sh` exige le package Centrify. `ctxinstall.sh` peut obtenir le package Centrify de plusieurs manières :

- Easy Install permet de télécharger le package Centrify depuis Internet automatiquement. Les adresses URL pour chaque distribution sont les suivantes :

Amazon Linux 2/RHEL: `wget https://downloads.centrify.com/products/server-suite/2022/component-update-1/delinea-server-suite-2022-rhel6-x86_64.tgz`

CentOS : `wget https://downloads.centrify.com/products/server-suite/2022/component-update-1/delinea-server-suite-2022-rhel6-x86_64.tgz`

SUSE : `wget https://downloads.centrify.com/products/server-suite/2022/component-update-1/delinea-server-suite-2022-suse12-x86_64.tgz`

Ubuntu/Debian : `wget https://downloads.centrify.com/products/server-suite/2022/component-update-1/delinea-server-suite-2022-deb9-x86_64.tgz`

- Vous pouvez récupérer le package Centrify depuis un répertoire local si Centrify est déjà installé. Pour désigner le répertoire du package Centrify, définissez `CTX_EASYINSTALL_CENTRIFY_LOCAL` dans `/opt/Citrix/VDA/sbin/ctxinstall.conf`. Par exemple :

```
1  ls -ls /home/mydir
2      9548 -r-xr-xr-x. 1 root root 9776688 May 13 2016
      adcheck-rhel4-x86_64
3      4140 -r--r--r--. 1 root root 4236714 Apr 21 2016
      centrfyda-3.3.1-rhel4-x86_64.rpm
4      33492 -r--r--r--. 1 root root 34292673 May 13 2016
      centrfydc-5.3.1-rhel4-x86_64.rpm
5      4 -rw-rw-r--. 1 root root 1168 Dec 1 2015
      centrfydc-install.cfg
6      756 -r--r--r--. 1 root root 770991 May 13 2016
      centrfydc-ldaproxy-5.3.1-rhel4-x86_64.rpm
7      268 -r--r--r--. 1 root root 271296 May 13 2016
      centrfydc-nis-5.3.1-rhel4-x86_64.rpm
8      1888 -r--r--r--. 1 root root 1930084 Apr 12 2016
      centrfydc-openssh-7.2p2-5.3.1-rhel4-x86_64.rpm
9      124 -rw-rw-r--. 1 root root 124543 Apr 19 2016
      centrfy-suite.cfg
10     0 lrwxrwxrwx. 1 root root 10 Jul 9 2012 install-
      express.sh -> install.sh
```

11	332 -r-xr-xr--. 1 root root	338292	Apr 10	2016	install
	.sh				
12	12 -r--r--r--. 1 root root	11166	Apr 9	2015	release-
	notes-agent-rhel4-x86_64.txt				
13	4 -r--r--r--. 1 root root	3732	Aug 24	2015	release-
	notes-da-rhel4-x86_64.txt				
14	4 -r--r--r--. 1 root root	2749	Apr 7	2015	release-
	notes-nis-rhel4-x86_64.txt				
15	12 -r--r--r--. 1 root root	9133	Mar 21	2016	release-
	notes-openssh-rhel4-x86_64.txt				

- Si vous choisissez PBIS comme méthode pour rejoindre un domaine, le script `ctxinstall.sh` exige le package PBIS. `ctxinstall.sh` peut obtenir le package PBIS de plusieurs manières :

- 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 15.5 : `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 :

```
pbisDownloadPath_RHEL="https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh"
pbisDownloadPath_Ubuntu="https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh"
```

- Vous pouvez récupérer le package PBIS depuis un répertoire local si PBIS est déjà installé. Pour désigner le répertoire du package PBIS, définissez la variable d'environnement **CTX\_EASYINSTALL\_PBIS\_LOCAL\_PATH** dans `/opt/Citrix/VDA/sbin/ctxinstall.conf`.

**Mode interactif** Pour exécuter le script `ctxinstall.sh` en mode interactif, exécutez la commande `sudo /opt/Citrix/VDA/sbin/ctxinstall.sh` sans l'option **-S**. Entrez la valeur de variable appropriée à chaque invite dans l'interface de ligne de commande. Si une variable est déjà définie, `ctxinstall.sh` demande une confirmation au cas où vous souhaiteriez la modifier.

**Mode silencieux** En mode silencieux, vous devez définir les variables précédentes à l'aide de `/opt/Citrix/VDA/sbin/ctxinstall.conf` ou de la commande `export`. Exécutez ensuite `ctxinstall.sh -S` (notez que la lettre **S** est ici en **majuscules**). Si toutes les variables requises ne sont pas définies ou si certaines valeurs ne sont pas valides, `ctxinstall.sh` interrompt l'exécution, sauf s'il existe des valeurs par défaut.

La valeur exportée pour chaque variable remplace la valeur dans **/Citrix/VDA/sbin/ctxinstall.conf**, sauf si elle n'est pas définie. Toutes les valeurs mises à jour sont enregistrées dans **/Citrix/VDA/sbin/ctxinstall.conf**, à l'exception du mot de passe permettant de joindre le domaine. Ainsi, en mode silencieux, vous devez définir le mot de passe permettant de joindre le domaine dans **/Citrix/VDA/sbin/ctxinstall.conf** ou exporter le mot de passe.

```

1 export CTX_XDL_NON_DOMAIN_JOINED='n'
2 export CTX_XDL_AD_INTEGRATION=winbind|centrify|sssd|pbis|quest
3 export CTX_XDL_DDC_LIST='<list-ddc-fqdns>'
4 export CTX_XDL_VDI_MODE='y|n'
5 export CTX_XDL_HDX_3D_PRO='y|n'
6 export CTX_XDL_START_SERVICE='y|n'
7 export CTX_XDL_REGISTER_SERVICE='y|n'
8 export CTX_XDL_ADD_FIREWALL_RULES='y|n'
9 export CTX_XDL_DESKTOP_ENVIRONMENT= gnome|gnome-classic|mate|'<none>'
10 export CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime>'
11 export CTX_XDL_VDA_PORT='<port-number>'
12 export CTX_XDL_SITE_NAME='<dns-site-name>' | '<none>'
13 export CTX_XDL_LDAP_LIST='<list-ldap-servers>' | '<none>'
14 export CTX_XDL_SEARCH_BASE='<search-base-set>' | '<none>'
15 export CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n'
16 export CTX_EASYINSTALL_DNS='<ip-address-of-dns>'
17 export CTX_EASYINSTALL_HOSTNAME='<host-name>'
18 export CTX_EASYINSTALL_NTPTS='<address-of-ntps>'
19 export CTX_EASYINSTALL_REALM='<realm-name>'
20 export CTX_EASYINSTALL_FQDN='<ad-fqdn-name>'
21 export CTX_EASYINSTALL_USERNAME='<domain-user-name>'
22 export CTX_EASYINSTALL_PASSWORD='<password>'
23 export CTX_EASYINSTALL_NETBIOS_DOMAIN='<netbios-domain>'
24 export CTX_EASYINSTALL_OU='<organization-unit>'
25 sudo -E /opt/Citrix/VDA/sbin/ctxinstall.sh -S

```

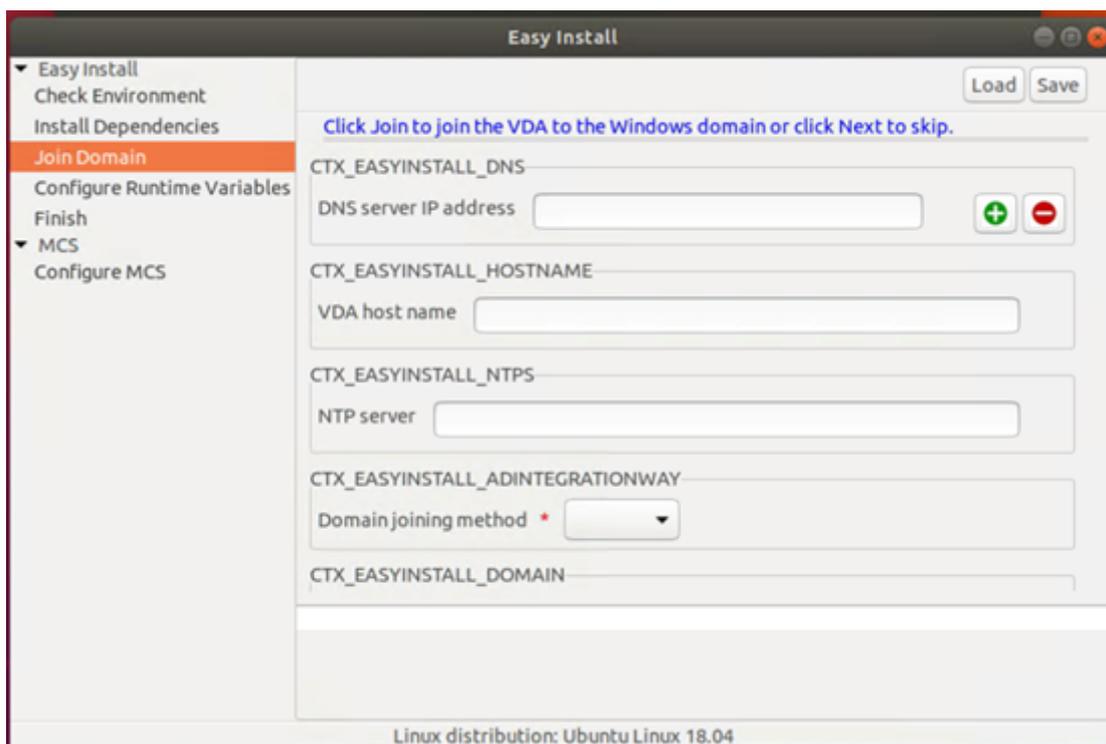
Lors de l'exécution de la commande `sudo`, entrez l'option **-E** pour transmettre les variables d'environnement au nouveau shell créé. Nous vous recommandons de créer un fichier de script shell à partir des commandes précédentes avec **#!/bin/bash** en tant que première ligne.

Vous pouvez également spécifier toutes les variables à l'aide d'une seule commande.

Pour configurer les variables d'environnement d'exécution du VDA (celles commençant par **CTX\_XDL\_**), vous pouvez exécuter **ctxinstall.sh -s** (notez que la lettre **s** est ici en **minuscules**).

## GUI

Vous pouvez utiliser Easy Install via l'interface graphique. 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

#### Conseil :

Cliquez sur **Enregistrer** pour enregistrer les paramètres des variables dans un fichier local sous le chemin que vous spécifiez. Cliquez sur **Charger** pour charger les paramètres des variables à partir d'un fichier que vous spécifiez. Pour plus d'informations sur la configuration des variables MCS, consultez [Étape 3 : préparer une image principale](#).

## 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

### Démarrer Linux VDA :

Pour démarrer les services Linux VDA :

```
1 sudo systemctl start ctxhdx.service
2
3 sudo systemctl start ctxvda.service
```

### Arrêter Linux VDA :

Pour arrêter les services Linux VDA :

```
1 sudo systemctl stop ctxvda.service
2
3 sudo systemctl stop ctxhdx.service
```

#### Remarque :

Avant d'arrêter les services **ctxvda** et **ctxhdx**, exécutez la commande **systemctl stop ctxmonitord** 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 systemctl stop ctxvda.service
2
3 sudo systemctl restart ctxhdx.service
4
5 sudo systemctl start ctxvda.service
```

### Vérifier l'état de Linux VDA :

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

```
1 sudo systemctl status ctxvda.service
2
3 sudo systemctl status ctxhdx.service
```

## Étape 11 : créer des catalogues de machines

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 vous 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 des groupes de mise à disposition

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 2311](#).

## Étape 13 : mettre à niveau le Linux VDA (facultatif)

Le Linux VDA prend en charge les mises à niveau depuis la version la plus récente. Par exemple, vous pouvez mettre à niveau le Linux VDA de 2308 à 2311 et de 1912 LTSR à 2203 LTSR.

### Pour RHEL 7 et CentOS 7 :

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

### Pour RHEL 8 et Rocky Linux 8 :

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

### Pour RHEL 9.2/9.0 et Rocky Linux 9.2/9.0 :

#### Remarque :

Avant de mettre à niveau le Linux VDA sur RHEL 9.2/9.0 et Rocky Linux 9.2/9.0, mettez à jour le package **libsepol** vers la version 3.4 ou ultérieure.

```
1 sudo rpm -U XenDesktopVDA-<version>.el9x.x86_64.rpm
```

### Pour SUSE :

```
1 sudo rpm -U XenDesktopVDA-<version>.sle15_x.x86_64.rpm
```

### Pour Ubuntu 20.04 :

```
1 sudo dpkg -i xendesktopvda_<version>.ubuntu20.04_amd64.deb
```

### Pour Ubuntu 22.04 :

```
1 sudo dpkg -i xendesktopvda_<version>.ubuntu22.04_amd64.deb
```

## Dépannage

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 :

```

1 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)'.
2 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))
3 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')
4 Check the following:- The system clock is in sync between this machine
  and the delivery controller.
5 - The Active Directory provider (e.g. winbind daemon) service is
  running and correctly configured.
6 - Kerberos is correctly configured on this machine.
7 If the problem persists, please refer to Citrix Knowledge Base article
  CTX117248 for further information.
8 Error Details:
9 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'.
10 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.
11 Ensure that the system clock is in sync between this machine and the
  delivery controller.
12 Verify the NTP daemon is running on this machine and is correctly
  configured.
13 2016-11-04 02:11:52.364 [ERROR] - Could not register with any
  controllers. Waiting to try again in 120000 ms. Multi-forest - false
14 2016-11-04 02:11:52.365 [INFO ] - The Citrix Desktop Service failed to
  register with any controllers in the last 470 minutes.

```

/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`:

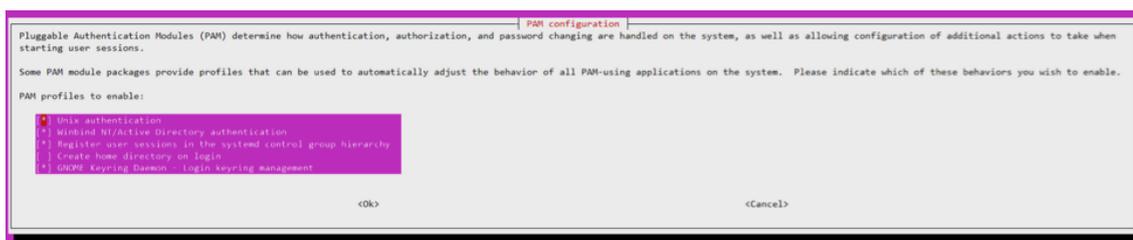
```
1 2016-11-02 13:21:19.015 <P22492:S1> citrix-ctxlogin: StartUserSession:
   failed to change to directory(/home/CITRIXLAB/ctxadmin) errno(2)
2
3 2016-11-02 13:21:19.017 <P22227> citrix-ctxhdx: logSessionEvent:
   Session started for user ctxadmin.
4
5 2016-11-02 13:21:19.023 <P22492:S1> citrix-ctxlogin: ChildPipeCallback:
   Login Process died: normal.
6
7 2016-11-02 13:21:59.217 <P22449:S1> citrix-ctxgfx: main: Exiting
   normally.
```

#### 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) :

```
1 Oct 27 04:17:16 CentOS7 citrix-ctxhdx[8978]: Session started for user
  CITRIXLAB\ctxadmin.
2
3 Oct 27 04:17:18 CentOS7 kernel: traps: gnome-session[19146] trap int3
  ip:7f89b3bde8d3 sp:7fff8c3409d0 error:0
4
5 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...
6
7 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)
8
9 Oct 27 04:17:18 CentOS7 gnome-session: aborting...
10
11 Oct 27 04:17:18 CentOS7 citrix-ctxgfx[18981]: Exiting normally.
12
13 Oct 27 04:17:18 CentOS7 citrix-ctxhdx[8978]: Session stopped for user
  CITRIXLAB\ctxadmin.
```

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

```
1 Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] pid.c:
  Stale PID file, overwriting.
2
3 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.
4
5 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.
6
7 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.
8
9 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.]
10
11 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

```

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/xdl/ctxinstall.log:

```

1 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
2
3 Jan 25 23:30:31 yz-rhel72-1 python[3945]: SELinux is preventing /usr/
      sbin/sshd from setattr access on the directory /root.
4
5 ***** Plugin catchall_boolean (89.3 confidence) suggests
      *****
6
7 If you want to allow polyinstantiation to enabled
8
9 Then you must tell SELinux about this by enabling the '
      polyinstantiation_enabled' boolean.
10
11 You can read 'None' man page for more details.
12
13 Do
14
15     setsebool -P polyinstantiation_enabled 1
16
17 ***** Plugin catchall (11.6 confidence) suggests
      *****
18

```

```
19 If you believe that sshd should be allowed setattr access on the root
    directory by default.
20
21 Then you should report this as a bug.
22
23 You can generate a local policy module to allow this access.
24
25     Do
26
27     allow this access for now by executing:
28
29     # grep sshd /var/log/audit/audit.log | audit2allow -M mypol
30
31 # semodule -i mypol.pp
```

Pour résoudre ce problème :

1. Désactivez SELinux en apportant la modification suivante à /etc/selinux/config.  
SELINUX=disabled
2. Redémarrez le VDA.

## Créer des VDA Linux non joints à un domaine à l'aide de MCS

August 20, 2024

Cet article explique comment utiliser Machine Creation Services (MCS) pour créer des VDA Linux non joints à un domaine dans Citrix DaaS.

### Important :

- Les VDA non joints à un domaine sont pris en charge pour Citrix DaaS.
  - Votre plan de contrôle doit être déployé via Citrix DaaS.
  - Vous pouvez déployer des VDA non joints à un domaine dans un cloud public ou un centre de données sur site. Les VDA non joints à un domaine sont gérés par le plan de contrôle dans Citrix DaaS.
  - Pour créer des VDA non joints à un domaine, les clients utilisant Citrix Gateway Service doivent s'assurer que [Rendezvous V2](#) est activé. Les composants Cloud Connector ne sont nécessaires que si vous envisagez de provisionner des machines sur des hyperviseurs locaux ou si vous souhaitez utiliser Active Directory comme fournisseur d'identité dans Workspace.
- Pour créer des VDA non joints à un domaine, vous pouvez utiliser MCS et Easy Install. Pour plus d'informations, consultez [Créer des VDA Linux non joints à un domaine à l'aide de MCS](#)

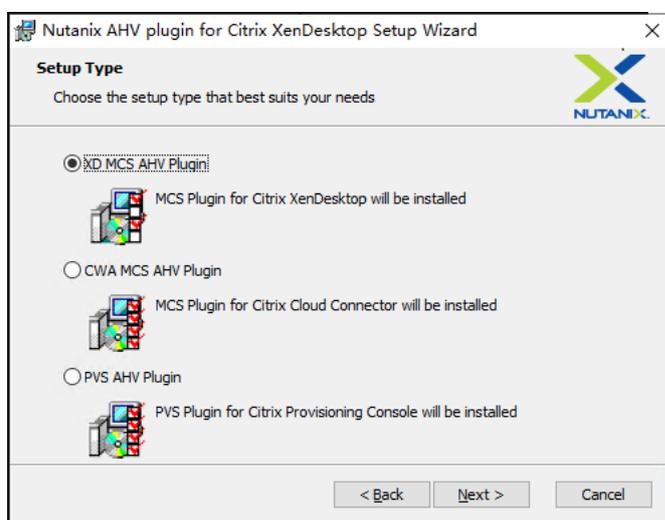
- et [Créer un Linux VDA non joint à un domaine à l'aide d'Easy Install \(Technical Preview\)](#).
- MCS ne prend pas en charge les serveurs bare metal.
- Les fonctionnalités suivantes sont disponibles pour les VDA Linux non joints à un domaine :
  - [Créer des utilisateurs locaux avec des attributs spécifiés sur des VDA non joints à un domaine](#)
  - [Pas d'authentification unique](#)
  - [Authentification avec Azure Active Directory](#)
  - [Rendezvous V2](#)

### **(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 hôte

Les hôtes sont des hyperviseurs ou des services cloud utilisés dans vos emplacements de ressources. Cette étape vous permet de spécifier les informations que DaaS utilise pour communiquer avec les machines virtuelles d'un hôte. Les informations détaillées incluent l'emplacement des ressources, le type d'hôte, les informations d'identification d'accès, la méthode de stockage à utiliser et les réseaux que les machines virtuelles de l'hôte peuvent utiliser.

#### Important :

Les ressources hôte (stockage et réseau) dans votre emplacement de ressources doivent être disponibles avant de créer une connexion.

1. Connectez-vous à Citrix Cloud.
2. Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS**.
3. Dans **Gérer > Configuration complète**, sélectionnez **Hébergement** dans le panneau de gauche.
4. Sélectionnez **Ajouter une connexion et des ressources** dans le volet Actions.
5. L'assistant vous guide à travers les pages suivantes. Le contenu de la page dépend du type de connexion sélectionné. Après avoir complété chaque page, sélectionnez **Suivant** jusqu'à la page **Résumé**.

## Étape 2a : Connexion

Sur la page **Connexion** :

- Pour créer une connexion, sélectionnez **Créer une nouvelle connexion**. Pour créer une connexion basée sur la même configuration d'hôte qu'une connexion existante, sélectionnez **Utiliser une connexion existante**, puis choisissez la connexion appropriée
- Sélectionnez une zone dans le champ **Nom de la zone**. Les options correspondent à tous les emplacements de ressources que vous avez configurés.
- Sélectionnez un hyperviseur ou un service cloud dans le champ **Type de connexion**. Les options disponibles sont des hyperviseurs et des services cloud dont les plug-ins sont correctement installés dans la zone.  
Vous pouvez également utiliser la commande PowerShell `Get-HypHypervisorPlugin -ZoneUid` pour obtenir la liste des plug-ins d'hyperviseur disponibles avec la zone sélectionnée.
- Entrez un nom pour la connexion. Ce nom apparaît dans l'écran **Gérer**.
- Choisissez l'outil utilisé pour créer des machines virtuelles : Machine Creation Services ou Citrix Provisioning.

Les informations sur la page **Connexion** diffèrent en fonction de l'hôte (type de connexion) que vous utilisez. Par exemple, lorsque vous utilisez Azure Resource Manager, vous pouvez utiliser un principal

de service existant ou en créer un.

## Étape 2b : Gestion du stockage

The screenshot shows a dialog box titled "Add Connection and Resources" with a close button (X) in the top right corner. On the left side, there is a vertical list of steps: 1. Connection (checked), 2. Storage Management (current step), 3. Storage Selection, 4. Network, and 5. Summary. The main area is titled "Storage Management" and contains the following text: "Configure virtual machine storage resources for this connection." Below this, there is a "Select a cluster:" label followed by a text input field and a "Browse" button. Underneath, it says "Select an optimization method for available site storage." and lists three radio button options: "Use storage shared by hypervisors" (selected), "Optimize temporary data on available local storage" (unchecked), and "Use storage local to the hypervisor" (unchecked). At the bottom of the dialog, there are three buttons: "Back", "Next", and "Cancel".

Pour de plus amples informations sur les types et méthodes de gestion du stockage, consultez la section [Stockage hôte](#).

Si vous configurez une connexion à un hôte Hyper-V ou VMware, sélectionnez un nom de cluster. D'autres types de connexion ne nécessitent pas de nom de cluster.

Sélectionnez une méthode de gestion du stockage : stockage partagé par les hyperviseurs ou stockage local sur l'hyperviseur.

- Si vous choisissez le stockage partagé par les hyperviseurs, indiquez si vous souhaitez conserver les données temporaires sur l'espace de stockage local disponible. (Vous pouvez spécifier des tailles de stockage temporaire autres que les valeurs par défaut dans les catalogues de machines qui utilisent cette connexion.) **Exception** : lors de l'utilisation de volumes de stockage en cluster (CSV), Microsoft System Center Virtual Machine Manager n'autorise pas les disques de mise en cache des données temporaires sur le stockage local. Les tentatives de configuration de cette gestion du stockage dans la console **Gérer** échoue.

Si vous utilisez un espace de stockage partagé dans un pool Citrix Hypervisor, indiquez si vous

souhaitez utiliser IntelliCache pour réduire la charge sur le périphérique de stockage partagé. Voir [Environnements de virtualisation Citrix Hypervisor](#).

## Étape 2c : Sélection du stockage

**Add Connection and Resources** [X]

Connection  
 Storage Management  
 **Storage Selection**  
 Network  
 Summary

**Storage Selection**

When using local storage, you must select the type of data to store on each local storage device; machine operating system data, temporary data, and if not storing personal user data remotely, personal user data. At least one device must be selected for each data type.

Select data storage locations:

Name ↓	OS	Temporary
Library1 on [redacted]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Local storage on [redacted]	<input type="checkbox"/>	<input type="checkbox"/>
System32 on [redacted]	<input type="checkbox"/>	<input type="checkbox"/>
Users on [redacted]	<input type="checkbox"/>	<input type="checkbox"/>

Pour de plus amples informations sur la sélection du stockage, consultez la section [Stockage hôte](#).

Sélectionnez au moins un périphérique de stockage hôte pour chaque type de données disponible. La méthode de gestion du stockage que vous avez sélectionnée sur la page précédente affecte les types de données disponibles sur cette page. Vous devez sélectionner au moins un périphérique de stockage pour chaque type de données pris en charge avant de pouvoir passer à la page suivante de l'assistant.

La partie inférieure de la page **Sélection du stockage** contient d'autres options de configuration si vous avez choisi le stockage partagé par les hyperviseurs et activé **Optimiser les données temporaires sur le stockage local disponible**. Vous pouvez sélectionner les périphériques de stockage locaux (dans le même pool d'hyperviseurs) à utiliser pour les données temporaires.

Le nombre de périphériques de stockage actuellement sélectionnés est affiché (dans le diagramme, « 1 périphérique de stockage sélectionné »). Lorsque vous placez le curseur sur cette entrée, les noms des périphériques sélectionnés s'affichent (sauf si aucun périphérique n'est configuré).

1. Sélectionnez **Sélectionner** pour modifier les périphériques de stockage à utiliser.
2. Dans la boîte de dialogue **Sélectionner un stockage**, activez ou désactivez les cases de périphérique de stockage, puis sélectionnez **OK**.

### Étape 2d : Région

(N'apparaît que pour certains types d'hôtes.) La sélection de la région indique où les machines virtuelles seront déployées. Dans l'idéal, choisissez une région proche de l'endroit où les utilisateurs accèdent à leurs applications.

### Étape 2e : Réseau

Entrez un nom pour les ressources. Ce nom apparaît dans la console **Gérer** pour identifier la combinaison stockage et réseau associée à la connexion.

Sélectionnez un ou plusieurs réseaux que les machines virtuelles utilisent.

Certains types de connexions (telles que Azure Resource Manager) dressent également la liste des sous-réseaux que les machines virtuelles utilisent. Sélectionnez un ou plusieurs sous-réseaux.

### Étape 2f : Résumé

Vérifiez vos sélections ; si vous souhaitez apporter des modifications, revenez sur les pages précédentes de l'assistant. Lorsque vous avez terminé votre évaluation, sélectionnez **Terminer**.

**Rappel :** si vous stockez les données temporaires localement, vous pouvez configurer des valeurs autres que les valeurs par défaut pour le stockage des données temporaires lorsque vous créez le catalogue contenant les machines utilisant cette connexion.

#### Remarque :

Une étendue n'est pas affichée pour les administrateurs avec accès complet. Pour plus d'informations, consultez [Administrateurs, rôles et étendues](#).

Pour plus d'informations, consultez la section [Créer et gérer des connexions](#).

## Étape 3 : préparer une image principale

#### Conseil :

Vous pouvez utiliser une seule image pour créer des VDA joints à un domaine et des VDA non joints à un domaine.

### (Pour XenServer (anciennement Citrix Hypervisor) uniquement) Étape 3a : Installer le composant XenServer VM Tools

Installez le composant XenServer 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. Téléchargez le fichier des outils de machine virtuelle XenServer pour Linux depuis la [page de téléchargement de XenServer](#) ou la [page de téléchargement de Citrix Hypervisor](#) en fonction de la version de l'hyperviseur utilisée.
  2. Copiez le fichier `LinuxGuestTools-xxx.tar.gz` sur votre machine virtuelle Linux ou sur un lecteur partagé auquel la machine virtuelle Linux peut accéder.
  3. Extrayez le contenu du fichier tar : `tar -xzf LinuxGuestTools-xxx.tar.gz`
  4. Exécutez la commande suivante pour installer le package `xe-guest-utilities` en fonction de votre distribution Linux.

**Pour RHEL/CentOS/Rocky Linux/SUSE :**

```
1 sudo rpm -i <extract-directory>/xe-guest-utilities_{
2   package-version }
3   _x86.64.rpm
```

**Pour Ubuntu/Debian :**

```
1 sudo dpkg -i <extract-directory>/xe-guest-utilities_{
2   package-version }
3   _amd64.deb
```

**Pour SUSE :**

```
1 sudo rpm -i /mnt/Linux/xe-guest-utilities_{
2   package-version }
3   _all.rpm
```

5. Vérifiez l'état de la virtualisation de la VM modèle dans l'onglet **General** de XenCenter. Si le composant XenServer VM Tools est correctement installé, l'état de la virtualisation est défini sur **Optimized**.

### Étape 3b : 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 :**

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

**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 de la page <https://docs.fedoraproject.org/en-US/epel/>.

- Après avoir installé le Linux VDA sur RHEL 8.x/9.x et Rocky Linux 8.x/9.x hébergés sur GCP, la connexion Ethernet peut être perdue et le Linux VDA peut être inaccessible après le redémarrage d'une machine virtuelle. Pour contourner le problème, exécutez les commandes suivantes avant de redémarrer la machine virtuelle :

```
1 nmcli dev connect eth0
2 systemctl restart NetworkManager
```

**Pour Ubuntu/Debian :**

```
1 sudo dpkg -i <PATH>/<Linux VDA DEB>
2
3 apt-get install -f
```

**Pour SUSE :**

```
1 sudo zypper -i install <PATH>/<Linux VDA RPM>
```

**Étape 3c : activer les référentiels pour installer le package tdb-tools (pour RHEL 7 uniquement)**

**Pour un serveur RHEL 7 :**

```
1 subscription-manager repos --enable=rhel-7-server-optional-rpms
```

**Pour un poste de travail RHEL 7 :**

```
1 subscription-manager repos --enable=rhel-7-workstation-optional-rpms
```

**Étape 3d : (Pour SUSE uniquement) 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** :

```
1 sudo zypper install gcc
2 sudo zypper install make
```

2. Téléchargez le package ntfs-3g.

3. Décompressez le package ntfs-3g :

```
1 sudo tar -xvzf ntfs-3g_ntfsprogs-<package version>.tgz
```

4. Entrez le chemin d'accès au package ntfs-3g :

```
1 sudo cd ntfs-3g_ntfsprogs-<package version>
```

5. Installez ntfs-3g :

```
1 ./configure
2 make
3 make install
```

**Étape 3e : (Pour Ubuntu uniquement) Modifier le fichier /etc/network/interfaces**

Ajoutez la ligne `source /etc/network/interfaces.d/*` au fichier `/etc/network/interfaces`.

**Conseil :**

Le fichier `/etc/network/interfaces` n'est peut-être pas disponible sur votre machine Ubuntu. Si le fichier n'existe pas, vous devez d'abord installer les packages `net-tools` et `ifupdown`.

**Étape 3f : (Pour Ubuntu uniquement) Pointer /etc/resolv.conf**

Pointez `/etc/resolv.conf` sur `/run/systemd/resolve/resolv.conf` au lieu de le pointer sur `/run/systemd/resolve/stub-resolv.conf` :

```
1 unlink /etc/resolv.conf
2
3 ln -s /run/systemd/resolve/resolv.conf /etc/resolv.conf
```

### Étape 3g : spécifier la base de données à utiliser

Vous pouvez également basculer entre SQLite et PostgreSQL après avoir installé le package Linux VDA. Pour ce faire, procédez comme suit :

#### Remarque :

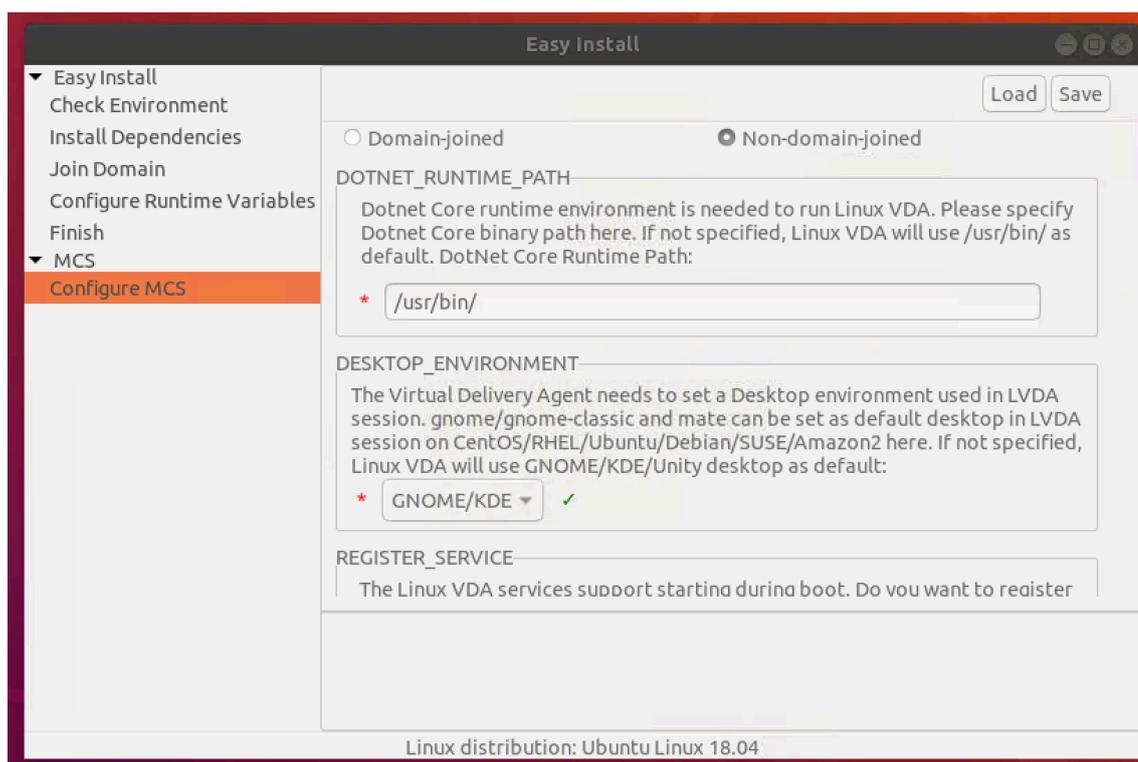
- Nous vous recommandons d'utiliser SQLite pour le mode VDI uniquement et d'utiliser PostgreSQL pour un modèle de mise à disposition de bureaux partagés hébergés.
- Pour Easy Install et MCS, vous pouvez spécifier SQLite ou PostgreSQL sans avoir à les installer manuellement. Sauf indication contraire dans `/etc/xdl/db.conf`, le Linux VDA utilise PostgreSQL par défaut.
- Vous pouvez également utiliser `/etc/xdl/db.conf` pour configurer le numéro de port de PostgreSQL.

1. Exécutez `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omettez cette étape s'il s'agit d'une nouvelle installation.
2. Modifiez `/etc/xdl/db.conf` avant de lancer `deploymcs.sh`.

### Étape 3h : configurer les variables MCS

Il existe deux manières de configurer les variables MCS :

- Modifiez le fichier `/etc/xdl/mcs/mcs.conf`.
- Utilisez l'interface graphique Easy Install. Pour ouvrir l'interface utilisateur graphique Easy Install, exécutez la commande `/opt/Citrix/VDA/bin/easyinstall` dans l'environnement de bureau de votre Linux VDA.

**Conseil :**

Cliquez sur **Enregistrer** pour enregistrer les paramètres des variables dans un fichier local sous le chemin que vous spécifiez. Cliquez sur **Charger** pour charger les paramètres des variables à partir d'un fichier que vous spécifiez.

Les variables MCS suivantes peuvent être configurées pour des scénarios de non-appartenance à un domaine. Vous pouvez utiliser les valeurs des variables par défaut ou personnaliser les variables selon vos besoins (facultatif) :

```
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
```

**Étape 3i : -crire ou mettre à jour les valeurs de registre pour MCS (facultatif)**

Sur la machine modèle, ajoutez des lignes de commande au fichier `/etc/xdm/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.

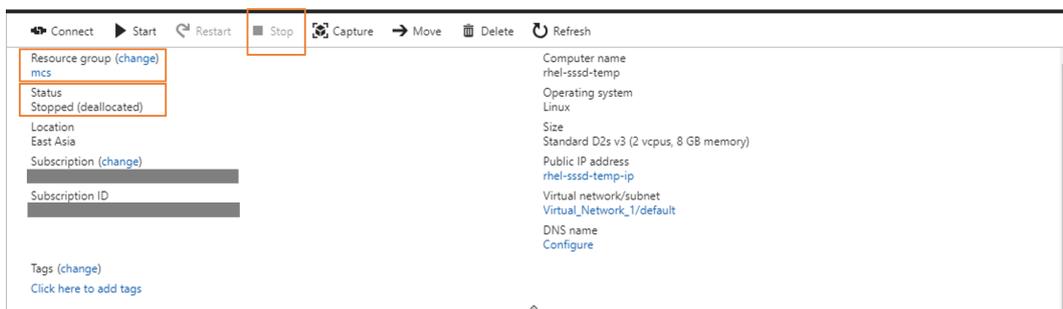
Par exemple, vous pouvez ajouter les lignes de commande suivantes au fichier `/etc/xdl/mcs/mcs_local_setting.reg` pour écrire ou modifier une valeur de registre respectivement :

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard\ClipboardSelection" -t "REG_DWORD" -v "Flags" -d "0x00000003" --force
```

```
1 update -k "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard\ClipboardSelection" -v "Flags" -d "0x00000003"
```

### Étape 3j : créer une image principale

1. Si vous configurez des variables MCS en modifiant `/etc/xdl/mcs/mcs.conf`, exécutez `/opt/Citrix/VDA/sbin/deploymcs.sh`. Si vous configurez des variables MCS à l'aide de l'interface graphique, cliquez sur **Déployer**. Une fois que vous avez cliqué sur **Déployer** dans l'interface graphique, les variables que vous définissez dans l'interface utilisateur remplacent les variables que vous avez définies dans le fichier `/etc/xdl/mcs/mcs.conf`.
2. Créez et nommez un instantané de votre image principale en fonction du cloud public que vous utilisez.
  - **(Pour XenServer (anciennement 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)**. Mémoirisez 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 indique **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 renomez un instantané, redémarrez l'assistant **Créer un catalogue** pour afficher une liste actualisée.

## Étape 4 : créer un catalogue de machines

1. Connectez-vous à [Citrix Cloud](#).
2. Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS**.
3. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines**.
4. L'assistant vous guide dans le processus de création du catalogue de machines.

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. Sélectionnez MCS comme méthode de déploiement de machine et sélectionnez **Non joint au domaine** comme identité pour les machines à créer dans le catalogue.

Effectuez d'autres tâches de configuration si nécessaire. Pour de plus amples informations, consultez l'article [Créer des catalogues de machines](#).

**Remarque :**

Si le processus de création de votre catalogue de machines sur le composant Delivery Controller prend beaucoup de temps, accédez à Nutanix Prism et mettez sous tension manuellement la machine dont le nom est précédé du préfixe **Préparation**. Cette approche permet de poursuivre le processus de création.

## 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](#).

## Créer un Linux VDA non joint à un domaine à l'aide d'Easy Install (Technical Preview)

August 20, 2024

Cet article explique comment utiliser Easy Install pour créer un Linux VDA non joint à un domaine dans Citrix DaaS.

**Important :**

- Les VDA non joints à un domaine sont pris en charge pour Citrix DaaS.
  - Votre plan de contrôle doit être déployé via Citrix DaaS.
  - Vous pouvez déployer des VDA non joints à un domaine dans un cloud public ou un centre de données sur site. Les VDA non joints à un domaine sont gérés par le plan de contrôle dans Citrix DaaS.
  - Pour créer des VDA non joints à un domaine, les clients utilisant Citrix Gateway Service doivent s'assurer que [Rendezvous V2](#) est activé. Les composants Cloud Connector ne sont nécessaires que si vous envisagez de provisionner des machines sur des hyperviseurs locaux ou si vous souhaitez utiliser Active Directory comme fournisseur d'identité dans Workspace.
- Pour créer des VDA non joints à un domaine, vous pouvez également utiliser MCS. Pour plus d'informations, consultez la section [Créer des VDA Linux non joints à un domaine à l'aide de MCS](#).
  - MCS ne prend pas en charge les serveurs bare metal.

- Les fonctionnalités suivantes sont disponibles pour les VDA Linux non joints à un domaine :
  - [Créer des utilisateurs locaux avec des attributs spécifiés sur des VDA non joints à un domaine](#)
  - [Pas d'authentification unique](#)
  - [Authentification avec Azure Active Directory](#)
  - [Rendezvous V2](#)

## Étape 1 : Créer un catalogue de machines

Créez un catalogue de machines vide ne contenant aucune machine. Par exemple, utilisez Citrix Remote PowerShell SDK et exécutez la commande suivante pour créer le catalogue de machines vide **Your-Catalog-name** prenant en charge les machines avec système d'exploitation mono-session.

```
1 New-BrokerCatalog -AllocationType 'Static' -Description 'Your
  description' -MinimumFunctionalLevel 'L7_20' -Name 'Your-catalog-
  name' -SessionSupport 'SingleSession' -PersistUserChanges 'OnLocal'
  -ProvisioningType 'Manual' -MachinesArePhysical $true
```

Conservez un enregistrement de l'UUID du catalogue créé. L'UUID est nécessaire lorsque vous créez un jeton d'inscription ultérieurement.

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.
- Ne mélangez pas des machines jointes et non jointes à un domaine dans le même catalogue de machines.
- Les catalogues de machines Remote PC Access sont pris en charge pour les machines jointes à un domaine uniquement et ne sont pas pris en charge pour les machines non jointes à un domaine.

**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.

**Étape 2 : créer un jeton d'inscription VDA**

Pour créer un VDA non joint à un domaine à l'aide d'Easy Install, vous avez besoin d'un fichier de jeton pour inscrire le VDA dans un catalogue de machines et l'authentifier auprès du plan de contrôle Citrix Cloud. Le Linux VDA ne prend pas en charge l'utilisation d'un fichier de jetons pour l'inscription à un catalogue de machines à alimentation gérée.

Pour créer un jeton d'inscription, envoyez un message HTTP POST à l'URL semblable au message suivant : `[DdcServerAddress]/citrix/orchestration/api/techpreview/{customerid} /{ siteid } /enrollments`.

```
1 POST https://[DdcServerAddress]/citrix/orchestration/api/techpreview/[
  customerid]/[siteid]/enrollments HTTP/1.1
2 Accept: application/json
3 Content-Type: application/json; charset=utf-8
4 Authorization: Bearer <bearer-token>
5
6 {
7
8   "TokenName": "string",
9   "IssuedToUser": "string",
10  "ExpirationDate": "2023-10-13T08:00:25.796Z",
11  "NotValidBeforeDate": "2023-10-13T08:00:25.796Z",
12  "NumMachinesAllowed": number,
13  "CatalogId": "string"
14 }
```

Dans le message HTTP POST, définissez **CatalogId** sur l'UUID du catalogue de machines que vous avez créé précédemment et définissez **[DdcServerAddress]** sur l'une des valeurs suivantes si nécessaire :

- Commercial [https://\[customerid\].xendesktop.net](https://[customerid].xendesktop.net)
- Japon [https://\[customerid\].apps.citrixworkspacesapi.jp](https://[customerid].apps.citrixworkspacesapi.jp)
- Gouvernement [https://\[customerid\].xendesktop.us](https://[customerid].xendesktop.us)

### Étape 3 : installer .NET Runtime 6.0

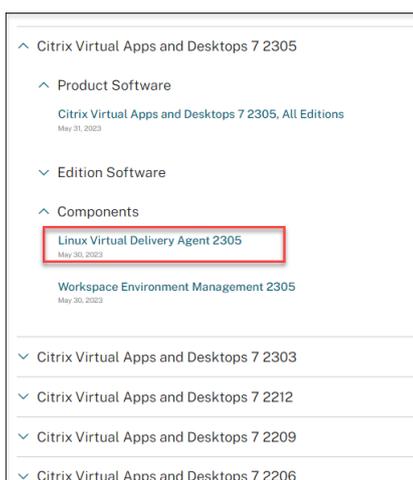
Avant d'installer Linux VDA, installez .NET Runtime 6.0 conformément aux instructions de l'article <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers>.

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

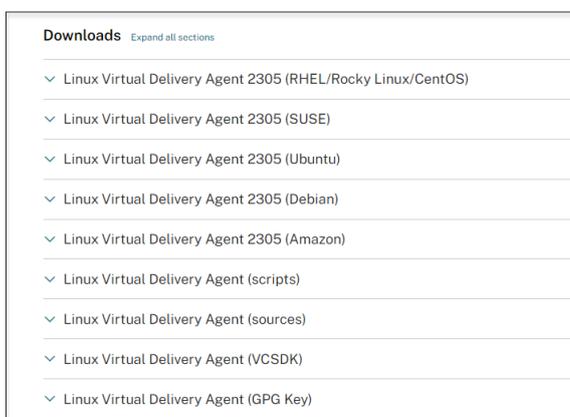
En fonction de la sortie de la commande, définissez le chemin binaire de .NET Runtime. Par exemple, si la sortie de la commande est /aa/bb/dotnet, utilisez /aa/bb comme chemin binaire .NET.

### 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. Développez **Components** pour trouver le Linux VDA. Par exemple :

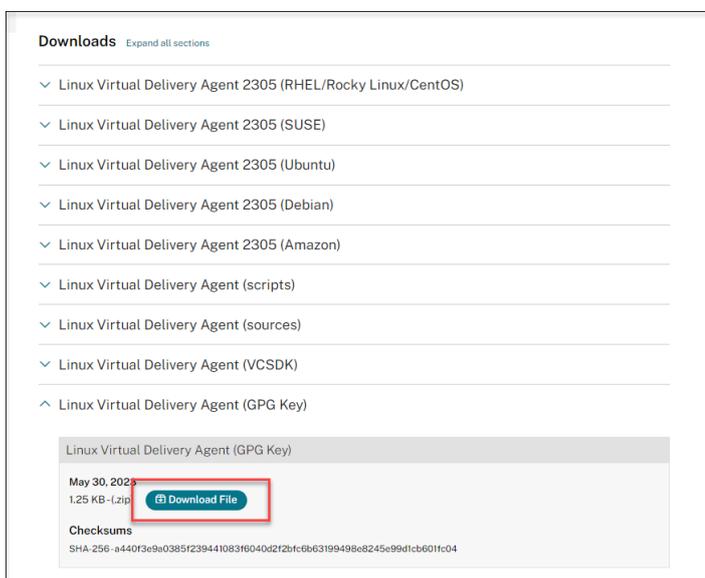


4. Cliquez sur le lien Linux VDA pour accéder aux téléchargements de Linux VDA.



5. Téléchargez le package Linux VDA correspondant à votre distribution Linux.

6. Téléchargez la clé publique GPG que vous pouvez utiliser pour vérifier l'intégrité du package Linux VDA. Par exemple :



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

- Pour un package RPM, exécutez les commandes suivantes pour importer la clé publique dans la base de données RPM et vérifier l'intégrité du package :

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

- Pour un package DEB, exécutez les commandes suivantes pour importer la clé publique dans la base de données DEB et vérifier l'intégrité du package :

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

## Étape 5 : installer le package VDA Linux

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

Pour les distributions Amazon Linux 2, CentOS, RHEL et Rocky Linux :

### 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 de la page <https://docs.fedoraproject.org/en-US/epel/>.
- Avant d'installer le Linux VDA sur RHEL 9.2/9.0 et Rocky Linux 9.2/9.0, mettez à jour le pack-

age **libsepol** vers la version 3.4 ou ultérieure.

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

**Remarque :**

Après avoir installé le Linux VDA sur RHEL 8.x/9.x et Rocky Linux 8.x/9.x hébergés sur GCP, la connexion Ethernet peut être perdue et le Linux VDA peut être inaccessible après le redémarrage d'une machine virtuelle. Pour contourner ce problème, définissez un mot de passe racine lorsque vous vous connectez à la VM pour la première fois et assurez-vous que vous pouvez vous connecter à la VM en tant qu'utilisateur racine. Exécutez ensuite les commandes suivantes dans la console après avoir redémarré la VM :

```
1 nmcli dev connect eth0
2 systemctl restart NetworkManager
```

Pour les distributions Ubuntu/Debian :

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

**Remarque :**

- Pour installer les dépendances nécessaires pour une distribution Debian 11, ajoutez la ligne `deb http://deb.debian.org/debian/ bullseye main` au fichier `/etc/apt/sources.list`.
- Pour Ubuntu 20.04 sur GCP, désactivez RDNS. Pour ce faire, ajoutez la ligne `rdns = false` sous `[libdefaults]` dans `/etc/krb5.conf`.

Pour les distributions SUSE :

1. Pour SUSE 15.5 sur AWS, Azure et GCP, assurez-vous que :
  - Vous utilisez **libstdc++6** version 12 ou ultérieure.
  - Le paramètre **Default\_WM** dans `/etc/sysconfig/windowmanager` est défini sur « **gnome** ».
2. Exécutez la commande suivante pour installer le Linux VDA :

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

## Étape 6 : installer les pilotes NVIDIA GRID

Pour activer HDX 3D Pro, vous devez installer les pilotes NVIDIA GRID sur votre hyperviseur et sur la machine 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 : spécifier la base de données à utiliser

Vous pouvez spécifier le système SQLite ou PostgreSQL à utiliser en modifiant **/etc/xdl/db.conf** après avoir installé le package Linux VDA.

Pour ce faire, modifiez **/etc/xdl/db.conf** avant d'exécuter **sudo /opt/Citrix/VDA/sbin/ctxinstall.sh** ou **/opt/Citrix/VDA/bin/easyinstall**.

### Remarque :

- Nous vous recommandons d'utiliser SQLite uniquement pour le mode VDI.
- Pour Easy Install et MCS, vous pouvez spécifier SQLite ou PostgreSQL sans avoir à les installer manuellement. Sauf indication contraire dans **/etc/xdl/db.conf**, le Linux VDA utilise PostgreSQL par défaut.
- Vous pouvez également utiliser **/etc/xdl/db.conf** pour configurer le numéro de port de PostgreSQL.

## Étape 8 : terminez l'installation en exécutant Easy Install pour configurer l'environnement et le VDA

Après l'installation du package Linux VDA, configurez l'environnement d'exécution à l'aide du script `ctxinstall.sh`.

### 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**.

## **ctxinstall.sh**

Le script Easy Install `ctxinstall.sh` permet d'effectuer certaines préconfigurations et de configurer le VDA exécutant des variables d'environnement.

- Seul un accès racine peut exécuter ce script.
- Easy Install utilise le fichier de configuration `"/opt/Citrix/VDA/sbin/ctxinstall.conf"` pour définir, enregistrer et synchroniser les valeurs de toutes les variables d'environnement utilisées. Nous vous recommandons de lire attentivement le modèle (`ctxinstall.conf.tpl`), puis de personnaliser votre propre fichier `"/opt/Citrix/VDA/sbin/ctxinstall.conf"`. Lorsque vous créez le fichier de configuration pour la première fois, utilisez l'une des méthodes suivantes :
  - Copiez le fichier de modèle `"/opt/Citrix/VDA/sbin/ctxinstall.conf.tpl"` et enregistrez-le sous `"/opt/Citrix/VDA/sbin/ctxinstall.conf"`.
  - Exécutez `ctxinstall.sh`. Chaque fois que vous exécutez `ctxinstall.sh`, votre entrée est enregistrée dans `"/opt/Citrix/VDA/sbin/ctxinstall.conf"`.
- Easy Install permet un fonctionnement modulaire. Les modules incluent la pré-vérification, l'installation, la configuration de domaine, la configuration et la vérification.
- Les détails de débogage de ce script se trouvent dans le fichier `"/var/log/xdl/ctxinstall.log"`.

Pour plus d'informations, utilisez la commande d'aide **ctxinstall.sh -h**.

### **Remarque :**

- Respectez le principe du moindre privilège et assurez-vous que seul l'utilisateur racine peut lire `"/opt/Citrix/VDA/sbin/ctxinstall.conf"` ; en effet, le mot de passe permettant de joindre domaine peut être défini dans le fichier.
- La désinstallation du Linux VDA supprime les fichiers situés sous `"/opt/Citrix/VDA"`. Nous vous recommandons de sauvegarder `"/opt/Citrix/VDA/sbin/ctxinstall.conf"` avant de désinstaller le VDA.

Vous pouvez exécuter `ctxinstall.sh` en mode interactif ou en mode silencieux. Avant d'exécuter le script, définissez les variables d'environnement suivantes :

- **\*\*CTX\_XDL\_NON\_DOMAIN\_JOINED='y|n'\*\*** : indique s'il faut associer la machine à un domaine. La valeur par défaut est "n". Pour les scénarios de non-appartenance à un domaine, définissez la variable sur « y ».

- **CTX\_XDL\_NDJ\_ENROLLMENT\_TOKEN\_FILE=<path-to-token-file-on-vda-machine>** : pour créer un VDA non joint à un domaine en utilisant Easy Install, vous avez besoin d'un fichier de jeton pour inscrire le VDA dans un catalogue de machines du Delivery Controller. Enregistrez le jeton dans un fichier avec des droits d'accès minimaux sous un chemin approprié.
- **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\_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 VDA doit être configuré pour le mode Bureaux VDI (session unique), c'est-à-dire, CTX\_XDL\_VDI\_MODE='y'.
- **CTX\_XDL\_START\_SERVICE='y|n'** : indique si les services Linux VDA sont lancés une fois la configuration de Linux VDA terminée.
- **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 Virtual Desktop 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\_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 par défaut configuré sur le VDA est utilisé.
- **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 d'accès par défaut est '/usr/bin'.
- **CTX\_XDL\_VDA\_PORT=<port-number>** : le Linux VDA communique avec les Delivery Controller via un port TCP/IP.

## Considérations

- 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**

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

**- Pour le bureau GNOME Classic**

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

**Mode interactif** Pour exécuter le script **ctxinstall.sh** en mode interactif, exécutez la commande **sudo /opt/Citrix/VDA/sbin/ctxinstall.sh** sans l'option **-S**. Entrez la valeur de variable appropriée à chaque invite dans l'interface de ligne de commande. Si une variable est déjà définie, **ctxinstall.sh** demande une confirmation au cas où vous souhaiteriez la modifier.

**Mode silencieux** En mode silencieux, vous devez définir les variables précédentes à l'aide de **/opt/Citrix/VDA/sbin/ctxinstall.conf** ou de la commande **export**. Exécutez ensuite **ctxinstall.sh -S** (notez que la lettre **S** est ici en **majuscules**). Si toutes les variables requises ne sont pas définies ou si certaines valeurs ne sont pas valides, **ctxinstall.sh** interrompt l'exécution, sauf s'il existe des valeurs par défaut.

Si vous le définissez, la valeur exportée pour chaque variable remplace la valeur de **/Citrix/VDA/sbin/ctxinstall.conf**. Toutes les valeurs mises à jour sont enregistrées dans **/Citrix/VDA/sbin/ctxinstall.conf**.

```
1 export CTX_XDL_NON_DOMAIN_JOINED='y'
2 export CTX_XDL_NDJ_ENROLLMENT_TOKEN_FILE='<token-file-path>'
```

```
3 export CTX_XDL_VDI_MODE='y|n'
4 export CTX_XDL_START_SERVICE='y|n'
5 export CTX_XDL_REGISTER_SERVICE='y|n'
6 export CTX_XDL_ADD_FIREWALL_RULES='y|n'
7 export CTX_XDL_HDX_3D_PRO='y|n'
8 export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<
  none>'
9 export CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime>'
10 export CTX_XDL_VDA_PORT='<port-number>'
11 sudo -E /opt/Citrix/VDA/sbin/ctxinstall.sh -S
```

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 toutes les variables à l'aide d'une seule commande.

Pour configurer les variables d'environnement d'exécution du VDA (celles commençant par **CTX\_XDL\_**), vous pouvez exécuter **ctxinstall.sh -s** (notez que la lettre **s** est ici en **minuscules**).

## 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

### Démarrer Linux VDA :

Pour démarrer les services Linux VDA :

```
1 sudo systemctl start ctxhdx.service
2
3 sudo systemctl start ctxvda.service
```

### Arrêter Linux VDA :

Pour arrêter les services Linux VDA :

```
1 sudo systemctl stop ctxvda.service
2
3 sudo systemctl stop ctxhdx.service
```

#### Remarque :

Avant d'arrêter les services **ctxvda** et **ctxhdx**, exécutez la commande **systemctl stop ctxmonitord** 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 systemctl stop ctxvda.service
2
3 sudo systemctl restart ctxhdx.service
4
5 sudo systemctl start ctxvda.service
```

### **Vérifier l'état de Linux VDA :**

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

```
1 sudo systemctl status ctxvda.service
2
3 sudo systemctl status ctxhdx.service
```

## **Étape 11 : créer des groupes de mise à disposition**

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 2311](#).

## Créer des VDA Linux à l'aide de Machine Creation Services (MCS)

August 20, 2024

Vous pouvez créer des VDA joints à un domaine et non joints à un domaine à l'aide de MCS.

### Important :

À compter de la version 2212, les modifications importantes suivantes sont apportées :

- La variable **AD\_INTEGRATION** du fichier `/etc/xdl/mcs/mcs.conf` ou de l'interface graphique Easy Install n'a plus de valeur par défaut. Vous devez définir une valeur selon vos besoins. Pour plus d'informations, consultez la section [Étape 3h : configurer les variables MCS](#) dans cet article.
- La valeur valide de l'entrée **UPDATE\_MACHINE\_PW** dans `/etc/xdl/mcs/mcs.conf` n'est plus définie sur **on** ou **off**, mais sur **Y** ou **N**. Pour plus d'informations, consultez [Automatiser les mises à jour du mot de passe du compte de machine](#) dans cet article.

### Distributions prises en charge

	Winbind	SSSD	Centrify	PBIS
Debian 11.7/11.3	Oui	Oui	Non	Oui
RHEL 9.2/9.0	Oui	Oui	Non	Non
RHEL 8.8/8.6	Oui	Oui	Oui	Oui
Rocky Linux 9.2/9.0	Oui	Oui	Non	Non
Rocky Linux 8.8/8.6	Oui	Oui	Non	Non
RHEL 7.9, CentOS 7.9	Oui	Oui	Oui	Oui
SUSE 15.5	Oui	Oui	Non	Oui
Ubuntu 22.04, Ubuntu 20.04	Oui	Oui	Non	Oui

### Remarque :

Pour utiliser un VDA RHEL 8.x/9.x ou Rocky Linux 8.x/9.x en cours d'exécution connecté au domaine à l'aide de SSSD comme machine virtuelle modèle pour MCS, assurez-vous que les exi-

gences suivantes sont remplies :

- Le VDA est installé manuellement, et non via Easy Install. Easy Install utilise **Adcli** pour RHEL 8.x/9.x et Rocky Linux 8.x/9.x ; la combinaison de SSSD et **Adcli** n'est pas prise en charge par MCS.
- Un serveur Samba est configuré pour utiliser SSSD pour l'authentification AD. Pour plus d'informations, consultez l'article de Red Hat en accédant à <https://access.redhat.com/solutions/3802321>.

## Hyperviseurs pris en charge

- AWS
- XenServer (anciennement 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

- À partir de la version 2203, vous pouvez héberger le Linux VDA sur Microsoft Azure, AWS et GCP pour Citrix Virtual Apps and Desktops ainsi que Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). Pour ajouter ces connexions hôtes au cloud public à votre déploiement Citrix Virtual Apps and Desktops, vous avez besoin de la licence Citrix Universal Hybrid Multi-Cloud (HMC).
- 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 7/8	5.8.0
SUSE	5.7.1

---

---

Distribution Linux	Version de Centrifify
Debian, Ubuntu	5.6.1

---

L'utilisation d'autres versions de Centrifify peut provoquer des erreurs. N'utilisez pas Centrifify pour joindre un modèle de machine à un domaine.

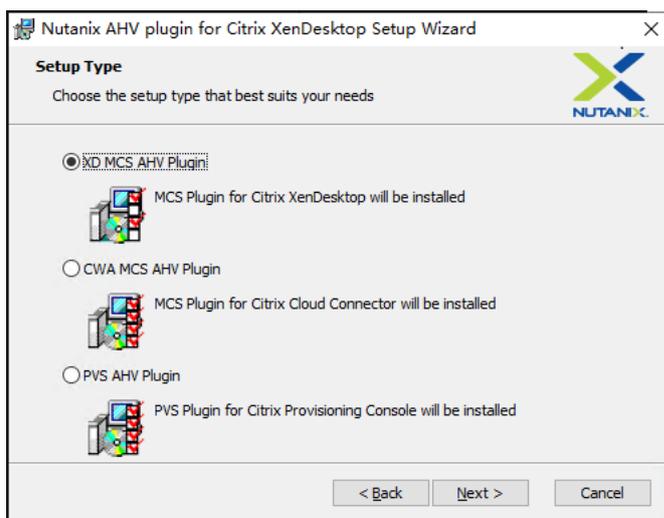
- Si vous utilisez PBIS ou Centrifify pour joindre des machines créées avec MCS à des domaines Windows, effectuez les tâches suivantes :
  - Sur la machine modèle, configurez le chemin de téléchargement du package PBIS ou Centrifify dans le fichier `/etc/xdm/mcs/mcs.conf` ou installez directement le package PBIS ou Centrifify.
  - 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 hôte

Cette section fournit des exemples sur la création d'une connexion hôte à Azure, AWS, XenServer (anciennement Citrix Hypervisor), GCP, Nutanix AHV et VMware vSphere.

**Remarque :**

Pour les Delivery Controller locaux, choisissez **Configuration > Hébergement > Ajouter une connexion et des ressources** dans la configuration locale Citrix Studio pour créer une connexion hôte. 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 hôte.

Pour plus d'informations, consultez [Créer et gérer des connexions et des ressources](#) dans la documentation Citrix Virtual Apps and Desktops et [Créer et gérer des connexions](#) dans la documentation Citrix DaaS.

- [Créer une connexion hôte à Azure dans Citrix Studio](#)
- [Créer une connexion hôte à AWS dans Citrix Studio](#)
- [Créer une connexion hôte à XenServer dans Citrix Studio](#)
- [Créer une connexion hôte à GCP dans Citrix Studio](#)
- [Créer une connexion hôte à Nutanix dans Citrix Studio](#)
- [Créer une connexion hôte vers VMware dans Citrix Studio](#)

### **Créer une connexion hôte à Azure 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 créer une connexion hôte. 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 hôte.
2. Dans l'assistant **Ajouter une connexion et des ressources**, sélectionnez Microsoft Azure comme type de connexion.
3. Sélectionnez le type de connexion Microsoft Azure.
4. L'assistant vous guide à travers les pages. Le contenu de la page dépend du type de connexion sélectionné. Après avoir complété chaque page, sélectionnez **Suivant** jusqu'à la page **Résumé**. Pour plus d'informations, consultez **Étape 2 : créer une connexion hôte** dans l'article [Créer des VDA Linux non joints à un domaine à l'aide de MCS](#).

### **Créer une connexion hôte à AWS 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 créer une connexion hôte. 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 hôte.

2. Dans l'assistant **Ajouter une connexion et des ressources**, sélectionnez **Amazon EC2** comme type de connexion.

Par exemple, dans la configuration locale Citrix Studio :

The screenshot shows the 'Add Connection and Resources' wizard in Citrix Studio. The left sidebar has 'Connection' selected. The main area is titled 'Connection' and has two radio buttons: 'Use an existing Connection' (with a dropdown menu showing 'awsec2') and 'Create a new Connection' (which is selected). Under 'Create a new Connection', there is a 'Connection type' dropdown menu set to 'Amazon EC2'. Below this, a note says 'Your cloud administrator should provide the following information.' There are three input fields: 'Import keys file:' with a 'Browse...' button and a note 'Use a file to automatically enter API key and Secret key.', 'API key:', and 'Secret key:'. Below these is a link 'Learn about user permissions'. At the bottom, there is a 'Connection name:' field with the example text 'Example: MyConnection'. At the very bottom of the wizard are three buttons: 'Back', 'Next', and 'Cancel'.

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.
4. L’assistant vous guide à travers les pages. Le contenu de la page dépend du type de connexion sélectionné. Après avoir complété chaque page, sélectionnez **Suivant** jusqu’à la page **Résumé**.

### Créer une connexion hôte à XenServer 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 créer une connexion hôte. 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 hôte.

2. Dans l'assistant **Ajouter une connexion et des ressources**, sélectionnez XenServer (anciennement Citrix Hypervisor) dans le champ **Type de connexion**.
3. Tapez l'adresse de connexion (l'URL XenServer) et les informations d'identification.
4. Entrez un nom pour la connexion.

**Créer une connexion hôte 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 hôte à GCP.

1. Pour les Delivery Controller locaux, choisissez **Configuration > Hébergement > Ajouter une connexion et des ressources** dans la configuration locale Citrix Studio pour créer une connexion hôte. 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 hôte.
2. Dans l'assistant **Ajouter une connexion et des ressources**, sélectionnez **Google Cloud Platform** comme type de connexion.

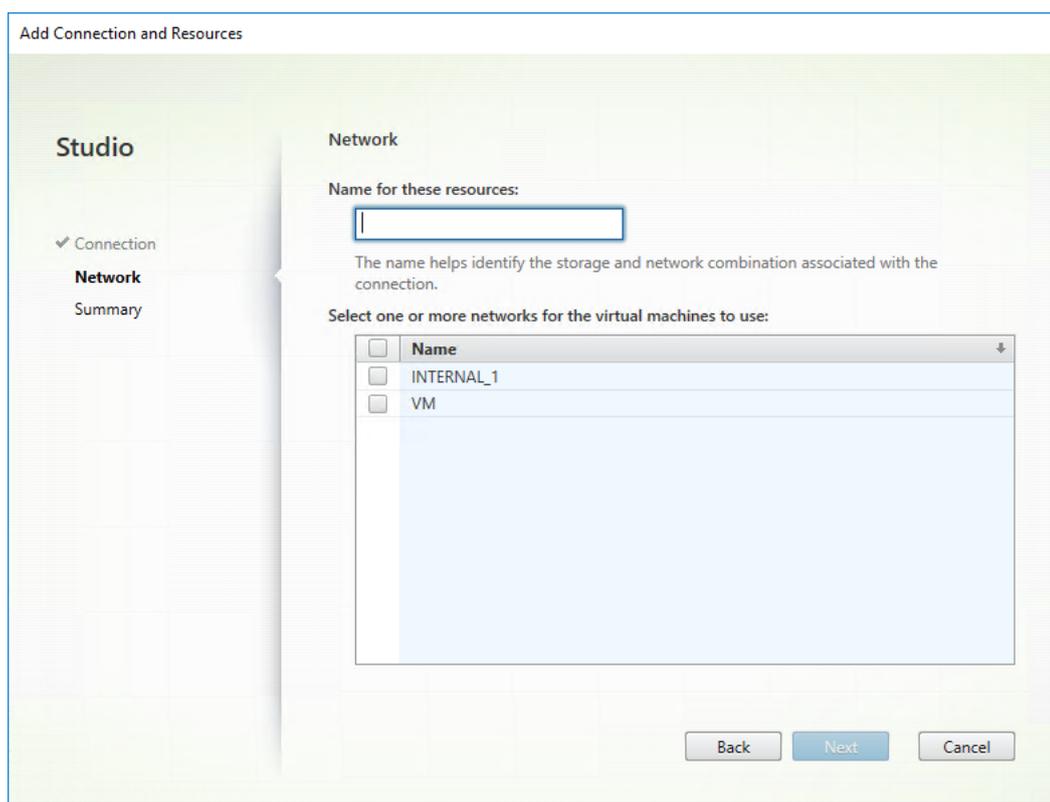
Par exemple, dans la console Studio Web sur Citrix Cloud :

3. Importez la clé de compte de service de votre compte GCP et saisissez votre nom de connexion.
4. L'assistant vous guide à travers les pages. Le contenu de la page dépend du type de connexion sélectionné. Après avoir complété chaque page, sélectionnez **Suivant** jusqu'à la page **Résumé**. Pour plus d'informations, consultez **Étape 2 : créer une connexion hôte** dans l'article [Créer des VDA Linux non joints à un domaine à l'aide de MCS](#).

### Créer une connexion hôte à Nutanix dans Citrix Studio

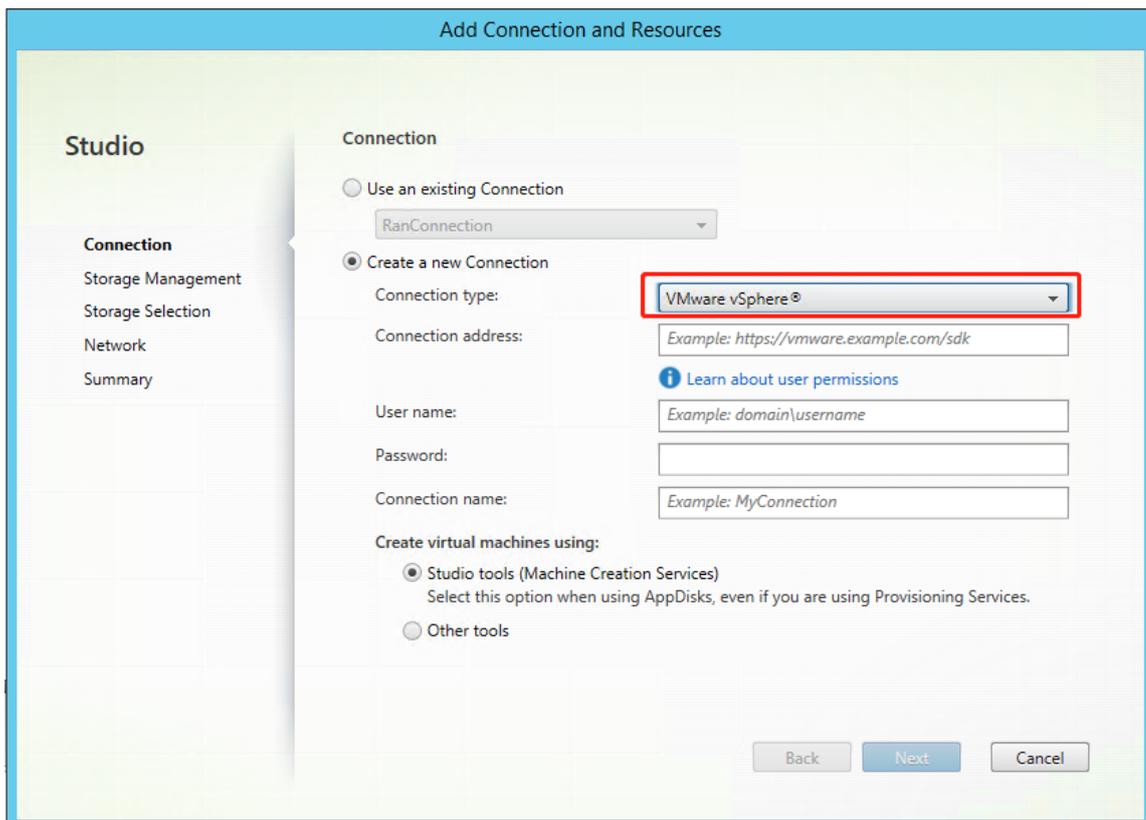
1. Pour les Delivery Controller locaux, choisissez **Configuration > Hébergement > Ajouter une connexion et des ressources** dans la configuration locale Citrix Studio pour créer une connexion hôte. Pour les Delivery Controller cloud, choisissez **Gérer > Hébergement > Ajouter une connexion et des ressources** dans la console Studio Web sur Citrix Cloud pour créer une connexion hôte.
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.

Par exemple, dans la configuration locale Citrix Studio :

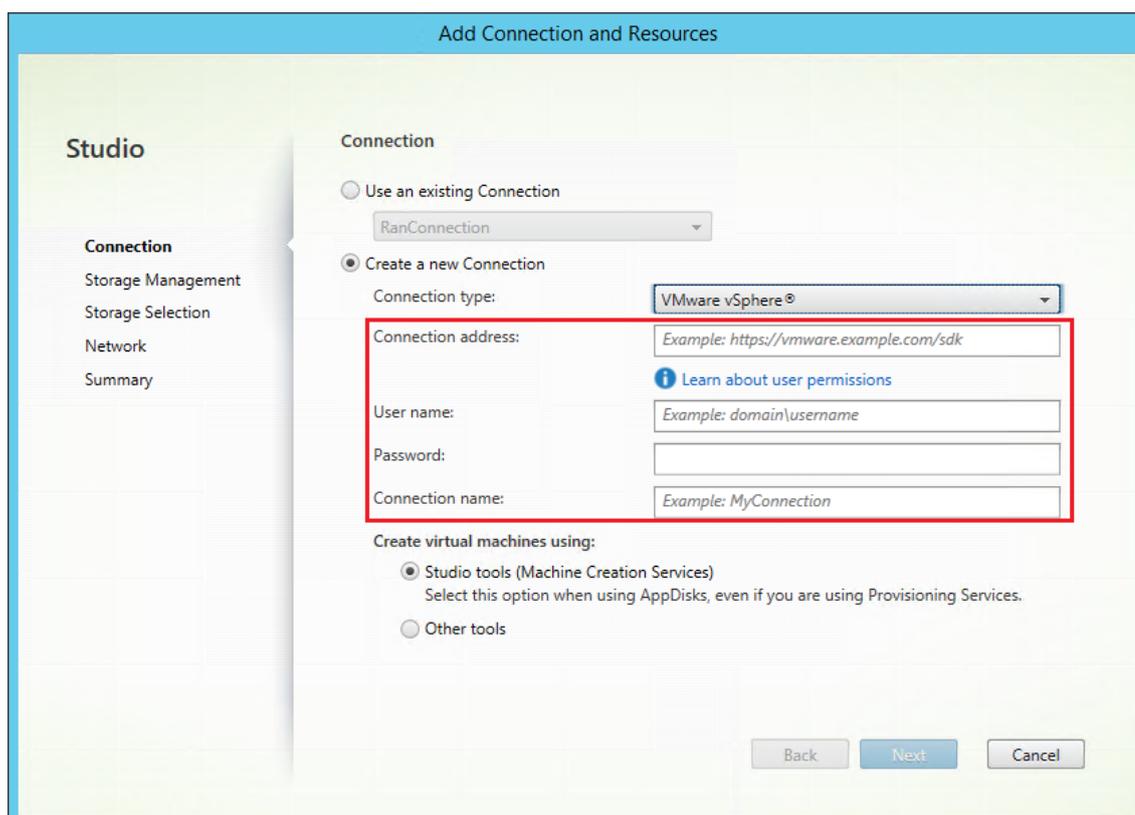


### Créer une connexion hôte vers VMware dans Citrix Studio

1. Installez vCenter Server dans l'environnement vSphere. Pour plus d'informations, consultez la section [VMware vSphere](#).
2. Pour les Delivery Controller locaux, choisissez **Configuration > Hébergement > Ajouter une connexion et des ressources** dans la configuration locale Citrix Studio pour créer une connexion hôte. 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 hôte.
3. Sélectionnez le type de connexion VMware vSphere.  
Par exemple, dans la configuration locale Citrix Studio :



4. Saisissez l'adresse de connexion (l'adresse URL du serveur vCenter) de votre compte VMware, vos informations d'identification et votre nom de connexion.



### Étape 3 : préparer une image principale

**(Pour XenServer uniquement) Étape 3a : Installer le composant XenServer VM Tools** Installez le composant XenServer 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. Téléchargez le fichier des outils de machine virtuelle XenServer pour Linux depuis la [page de téléchargement de XenServer](#) ou la [page de téléchargement de Citrix Hypervisor](#) en fonction de la version de l'hyperviseur utilisée.
  2. Copiez le fichier `LinuxGuestTools-xxx.tar.gz` sur votre machine virtuelle Linux ou sur un lecteur partagé auquel la machine virtuelle Linux peut accéder.
  3. Extrayez le contenu du fichier tar : `tar -xzf LinuxGuestTools-xxx.tar.gz`

4. Exécutez la commande suivante pour installer le package `xe-guest-utilities` en fonction de votre distribution Linux.

**Pour RHEL/CentOS/Rocky Linux/SUSE :**

```
1 sudo rpm -i <extract-directory>/xe-guest-utilities_{
2   package-version }
3   _x86_64.rpm
```

**Pour Ubuntu/Debian :**

```
1 sudo dpkg -i <extract-directory>/xe-guest-utilities_{
2   package-version }
3   _amd64.deb
```

**Pour SUSE :**

```
1 sudo rpm -i /mnt/Linux/xe-guest-utilities_{
2   package-version }
3   _all.rpm
```

5. Vérifiez l'état de la virtualisation de la VM modèle dans l'onglet **General** de XenCenter. Si le composant XenServer VM Tools est correctement installé, l'état de la virtualisation est défini sur **Optimized**.

**Étape 3b : vérifier les configurations pour SUSE 15.5 sur AWS, Azure et GCP** Pour SUSE 15.5 sur AWS, Azure et GCP, assurez-vous que :

- Vous utilisez **libstdc++6** version 12 ou ultérieure.
- Le paramètre **Default\_WM** dans `/etc/sysconfig/windowmanager` est défini sur « **gnome** ».

**Étape 3c : désactiver RDNS pour Ubuntu 20.04 sur GCP** Sur la VM modèle, ajoutez la ligne `rdns = false` sous `[libdefaults]` dans `/etc/krb5.conf`.

**Étape 3d : 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. Pour utiliser un VDA RHEL 8.x/9.x ou Rocky Linux 8.x/9.x en cours d'exécution connecté au domaine à l'aide de SSSD comme machine virtuelle modèle, assurez-vous que les exigences suivantes sont remplies :
  - The VDA is installed manually and not by using easy install. Easy install uses **Adcli** for RHEL 8.x/9.x and Rocky Linux 8.x/9.x and the combination of SSSD and **Adcli** is not supported by MCS.

- A Samba server is configured to use SSSD for AD authentication. For more information, see the Red Hat article at <https://access.redhat.com/solutions/3802321>.
- 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 :

##### 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 de la page <https://docs.fedoraproject.org/en-US/epel/>.
- Avant d'installer le Linux VDA sur RHEL 9.2/9.0 et Rocky Linux 9.2/9.0, mettez à jour le package **libsepol** vers la version 3.4 ou ultérieure.

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

#### Pour Ubuntu/Debian :

```
1 sudo dpkg -i <PATH>/<Linux VDA DEB>
2
3 apt-get install -f
```

#### Pour SUSE :

```
1 sudo zypper -i install <PATH>/<Linux VDA RPM>
```

### Étape 3e : activer les référentiels pour installer le package tdb-tools (pour RHEL 7 uniquement)

#### Pour un serveur RHEL 7 :

```
1 subscription-manager repos --enable=rhel-7-server-optional-rpms
```

#### Pour un poste de travail RHEL 7 :

```
1 subscription-manager repos --enable=rhel-7-workstation-optional-rpms
```

**Étape 3f : (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 :

```
1 sudo zypper install gcc
2 sudo zypper install make
```

2. Téléchargez le package ntfs-3g.

3. Décompressez le package ntfs-3g :

```
1 sudo tar -xvzf ntfs-3g_ntfsprogs-<package version>.tgz
```

4. Entrez le chemin d'accès au package ntfs-3g :

```
1 sudo cd ntfs-3g_ntfsprogs-<package version>
```

5. Installez ntfs-3g :

```
1 ./configure
2 make
3 make install
```

**Étape 3g : spécifier la base de données à utiliser** Vous pouvez également basculer entre SQLite et PostgreSQL après avoir installé le package Linux VDA. Pour ce faire, procédez comme suit :

**Remarque :**

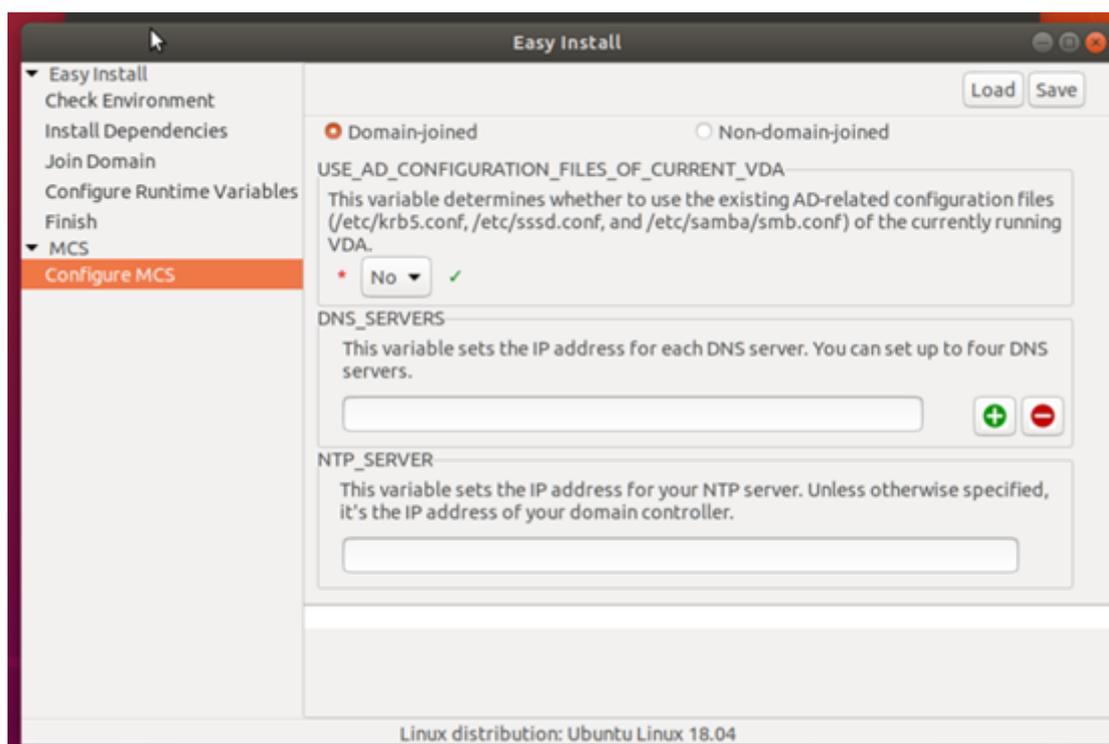
- Nous vous recommandons d'utiliser SQLite pour le mode VDI uniquement et d'utiliser PostgreSQL pour un modèle de mise à disposition de bureaux partagés hébergés.
- Pour Easy Install et MCS, vous pouvez spécifier SQLite ou PostgreSQL sans avoir à les installer manuellement. Sauf indication contraire dans **/etc/xdl/db.conf**, le Linux VDA utilise PostgreSQL par défaut.
- Vous pouvez également utiliser **/etc/xdl/db.conf** pour configurer le numéro de port de PostgreSQL.

1. Exécutez `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omettez cette étape s'il s'agit d'une nouvelle installation.

2. Modifiez `/etc/xdl/db.conf` avant de lancer `deploymcs.sh`.

**Étape 3h : configurer les variables MCS** Il existe deux manières de configurer les variables MCS :

- Modifiez le fichier `/etc/xdl/mcs/mcs.conf`.
- Utilisez l'interface graphique Easy Install. Pour ouvrir l'interface utilisateur graphique Easy Install, exécutez la commande `/opt/Citrix/VDA/bin/easyinstall` dans l'environnement de bureau de votre Linux VDA.

**Conseil :**

Cliquez sur **Enregistrer** pour enregistrer les paramètres des variables dans un fichier local sous le chemin que vous spécifiez. Cliquez sur **Charger** pour charger les paramètres des variables à partir d'un fichier que vous spécifiez.

Les variables MCS suivantes peuvent être configurées pour des scénarios de non-appartenance à un domaine et d'appartenance à un domaine :

- **Pour les scénarios de non-appartenance à un domaine**

Vous pouvez utiliser les valeurs des variables par défaut ou personnaliser les variables selon vos besoins (facultatif) :

```
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**

- `Use_AD_Configuration_Files_Of_Current_VDA` : détermine s'il faut utiliser les fichiers de configuration liés à AD existants (/etc/krb5.conf, /etc/sss.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. Pour utiliser un VDA en cours d'exécution comme machine virtuelle modèle, définissez la valeur sur Y. Sinon, définissez-la sur N.

- `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 domaine 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
```

**Étape 3i : écrire ou mettre à jour les valeurs de registre pour MCS** 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 :

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels
\Clipboard\ClipboardSelection" -t "REG_DWORD" -v "Flags" -d "0
x00000003" --force
```

```
1 update -k "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels
\Clipboard\ClipboardSelection" -v "Flags" -d "0x00000003"
```

#### Remarque

Pour modifier les paramètres MCS, vous êtes autorisé à modifier des fichiers sous `/etc/xdl/ad_join` et `/etc/xdl/mcs/`, mais il est interdit de modifier des fichiers sous `/var/xdl/mcs/`.

### Étape 3j : créer une image principale

1. (Pour SSSD + RHEL 8.x/9.x ou Rocky Linux 8.x/9.x uniquement) Exécutez la commande `update -crypto-policies --set DEFAULT:AD-SUPPORT`, puis redémarrez la machine virtuelle modèle.
2. Si vous configurez des variables MCS en modifiant `/etc/xdl/mcs/mcs.conf`, exécutez `/opt/Citrix/VDA/sbin/deploymcs.sh`. Si vous configurez des variables MCS à l'aide de l'interface graphique, cliquez sur **Déployer**. Une fois que vous avez cliqué sur **Déployer** dans

l'interface graphique, les variables que vous définissez dans l'interface utilisateur remplacent les variables que vous avez définies dans le fichier `/etc/xdl/mcs/mcs.conf`.

3. (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/sss/sss.conf` sur toutes les VM créées.

Pour les utilisateurs Winbind, mettez à jour les modèles `/etc/xdl/ad_join/winbind_krb5.conf.tpl` et `/etc/xdl/ad_join/winbind_smb.conf.tpl`.

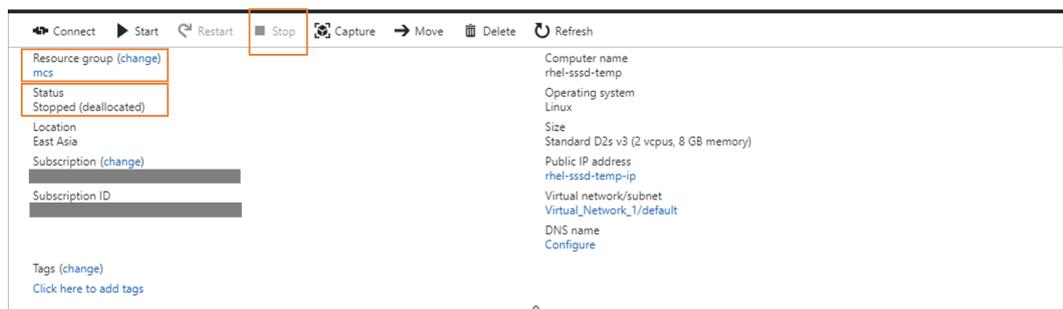
Pour les utilisateurs SSSD, mettez à jour les modèles `/etc/xdl/ad_join/sss.conf.tpl`, `/etc/xdl/ad_join/sss_krb5.conf.tpl` et `/etc/xdl/ad_join/sss_smb.conf.tpl`.

Pour les utilisateurs Centrify, mettez à jour les modèles `/etc/xdl/ad_join/centrify_krb5.conf.tpl` et `/etc/xdl/ad_join/centrify_smb.conf.tpl`.

#### 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`.

4. Créez et nommez un instantané de votre image principale en fonction du cloud public que vous utilisez.
  - **(Pour XenServer, 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.**

**Create Image**
✕

Instance ID ⓘ i-011f us-east-1-ami-011f00000000

Image name ⓘ

Image description ⓘ

No reboot ⓘ

**Instance Volumes**

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ	Encrypted ⓘ
Root	/dev/sda1	snap-02 <small>us-east-1-ami-011f00000000</small>	40	General Purpose SSD (gp2)	120 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Total size of EBS Volumes: 40 GiB  
When you create an EBS image, an EBS snapshot will also be created for each of the above volumes.

Cancel
Create 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.

### **(Pour GCP) Étape 3k : configurer la connexion Ethernet sur RHEL 8.x/9.x et Rocky Linux 8.x/9.x**

Après avoir installé le Linux VDA sur RHEL 8.x/9.x et Rocky Linux 8.x/9.x hébergés sur GCP, la connexion Ethernet peut être perdue et le Linux VDA peut être inaccessible après le redémarrage d'une machine virtuelle. Pour contourner ce problème, définissez un mot de passe racine lorsque vous vous connectez à la VM pour la première fois et assurez-vous que vous pouvez vous connecter à la VM en tant qu'utilisateur racine. Exécutez ensuite les commandes suivantes dans la console après avoir redémarré la VM :

```
1 nmcli dev connect eth0
2 systemctl restart NetworkManager
```

### **Étape 4 : créer un catalogue de machines**

Dans Citrix Studio ou Web Studio, créez un catalogue de machines et spécifiez le nombre de VM à créer dans le catalogue. Lorsque vous créez le catalogue de machines, choisissez votre image principale et tenez compte des points suivants :

- Sur la page **Conteneur** unique à Nutanix, sélectionnez le conteneur que vous avez spécifié précédemment pour la VM modèle.
- Lorsque vous créez un catalogue contenant des machines avec **OS mono-session**, la page **Expérience de bureau** s'affiche et vous permet de déterminer ce qui se passe chaque fois qu'un utilisateur ouvre une session.

The screenshot shows a 'Machine Catalog Setup' window with a sidebar on the left and a main content area on the right. The sidebar contains a list of steps from 1 to 16, with '4 Desktop Experience' highlighted. The main content area is titled 'Desktop Experience' and contains two sections of radio button options. The first section asks 'Which desktop experience do you want users to have?' with two options: 'I want users to connect to a new (random) desktop each time they log on.' (selected) and 'I want users to connect to the same (static) desktop each time they log on.' The second section asks 'Do you want to save any changes that the user makes to the desktop?' with two options: 'Yes, create a dedicated virtual machine and save changes on the local disk.' (selected) and 'No, discard all changes and clear virtual desktops when the user logs off.' At the bottom of the window are three buttons: 'Back', 'Next', and 'Cancel'.

Sur la page **Expérience de bureau**, sélectionnez l'une des options suivantes :

- Les utilisateurs se connectent à un nouveau bureau (aléatoire) chaque fois qu'ils ouvrent une session
- Les utilisateurs se connectent au même bureau (statique) chaque fois qu'ils ouvrent une session.

Si vous choisissez la première option, les modifications apportées par les utilisateurs au bureau seront annulées (non persistantes).

Si vous choisissez la deuxième option et que vous utilisez MCS pour provisionner les machines, vous pouvez configurer la manière dont les modifications apportées par l'utilisateur au bureau doivent être gérées :

- Enregistrer les modifications apportées par l'utilisateur au bureau sur un disque local (persistantes).
  - Supprimer toutes les modifications et effacer le bureau virtuel à la fermeture de session (non-persistantes). Sélectionnez cette option si vous utilisez la couche de personnalisation de l'utilisateur.
- Lors de la mise à jour de l'image principale d'un catalogue MCS contenant des machines persistantes, toutes les nouvelles machines ajoutées au catalogue utilisent l'image mise à jour. Les machines préexistantes continuent d'utiliser l'image principale d'origine.

Pour plus d'informations, consultez la section Création d'un catalogue de machines dans la documentation de [Citrix Virtual Apps and Desktops](#) et la documentation de [Citrix DaaS](#).

**Remarque :**

Dans les environnements Nutanix, 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.

## 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 Création de groupes de mise à disposition dans la documentation de [Citrix Virtual Apps and Desktops](#) et la documentation de [Citrix DaaS](#).

**Remarque :**

Les machines virtuelles que vous créez à l'aide de MCS peuvent ne pas être enregistrées auprès de Citrix Cloud Connector et leur état peut apparaître comme **Non enregistré**. Le problème se produit lorsque vous hébergez les machines virtuelles sur Azure et que vous rejoignez le domaine AD avec Samba Winbind. Pour contourner le problème, procédez comme suit :

1. Accédez à la console ADSI Edit, sélectionnez une machine virtuelle non enregistrée et mod-

- ifiez l'attribut **msDS-SupportedEncryptionTypes** de son compte de machine.
- Redémarrez les services **ctxjproxy** et **ctxvda** sur la machine virtuelle. Si l'état de la machine virtuelle passe à **Enregistré**, passez aux étapes 3 à 5.
  - Ouvrez le fichier **/var/xdl/mcs/ad\_join.sh** sur la machine virtuelle modèle.
  - Ajoutez la ligne **net ads entypes set \$NEW\_HOSTNAME\$ <Decimal value of encryption type attribute, for example, 28> -U \$NEW\_HOSTNAME\$ -P password** après les lignes suivantes dans le fichier **/var/xdl/mcs/ad\_join.sh** :

```
1 if [ "$AD_INTEGRATION" == "winbind" ]; then
2     join_domain_samba
3     restart_service winbind /usr/bin/systemctl
```

- Prenez un nouvel instantané et créez des machines virtuelles à l'aide du nouveau modèle.

## Utiliser MCS pour effectuer la mise à niveau de votre Linux VDA

Pour utiliser MCS pour la mise à niveau de votre Linux VDA, procédez comme suit :

- Vérifiez que vous avez installé .NET Runtime 6.0 avant de mettre à niveau votre Linux VDA vers la version actuelle.
- Mettez à niveau 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 :

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix\
   SelfUpdate" -t "REG_DWORD" -v "fEnabled" -d "0x00000001" -
   force
2
3 create -k "HKLM\System\CurrentControlSet\Control\Citrix\
   SelfUpdate" -t "REG_SZ" -v "ScheduledTime" -d "Immediately"
   - force
4
5 create -k "HKLM\System\CurrentControlSet\Control\Citrix\
   SelfUpdate" -t "REG_SZ" -v "Url" -d "<Your-Azure-Container-
   Url>" - force
6
7 create -k "HKLM\System\CurrentControlSet\Control\Citrix\
   SelfUpdate" -t "REG_SZ" -v "CaCertificate" -d "<Local-
   Certificate-Path-of-PortalAzureCom>" --force
```

### Pour RHEL 7 et CentOS 7 :

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

**Pour RHEL 8.x et Rocky Linux 8.x :**

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

**Pour RHEL 9.2/9.0 et Rocky Linux 9.2/9.0 :****Remarque :**

Avant de mettre à niveau le Linux VDA sur RHEL 9.2/9.0 et Rocky Linux 9.2/9.0, mettez à jour le package **libsepol** vers la version 3.4 ou ultérieure.

```
1 sudo rpm -U XenDesktopVDA-<version>.el9_x.x86_64.rpm
```

**Pour SUSE :**

```
1 sudo rpm -U XenDesktopVDA-<version>.sle15_x.x86_64.rpm
```

**Pour Ubuntu 20.04 :**

```
1 sudo dpkg -i xendesktopvda_<version>.ubuntu20.04_amd64.deb
```

**Pour Ubuntu 22.04 :**

```
1 sudo dpkg -i xendesktopvda_<version>.ubuntu22.04_amd64.deb
```

3. Modifiez `/etc/xdm/mcs/mcs.conf` et `/etc/xdm/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/xdm/mcs/mcs.conf` avant d'exécuter `/opt/Citrix/VDA/sbin/deploymcs.sh`.

```
UPDATE_MACHINE_PW="Y"
```

2. Après avoir exécuté `/opt/Citrix/VDA/sbin/deploymcs.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/jjproxy.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 9.2/9.0	Oui	Non	Non	Non
RHEL 8.x	Oui	Non	Non	Oui
Rocky Linux 9.2/9.0	Oui	Non	Non	Non
Rocky Linux 8.x	Oui	Non	Non	Non
RHEL 7, CentOS 7	Oui	Oui	Non	Oui
Ubuntu 22.04, Ubuntu 20.04	Oui	Non	Non	Non
Debian 11.7/11.3	Oui	Non	Non	Non
SUSE 15.5	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.

```
1 sudo cp root.pem /etc/pki/CA/certs/
```

2. Exécutez `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.

```
1 sudo cp root.pem /etc/pki/CA/certs/
```

3. Exécutez le script `/opt/Citrix/VDA/sbin/ctxfascfg.sh`.

## Créer des VDA Linux à l'aide de Citrix Provisioning

August 20, 2024

Vous pouvez créer des VDA joints à un domaine à l'aide de Citrix Provisioning.

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
- RHEL 9.2
- RHEL 9.0
- RHEL 8.8
- RHEL 8.6
- RHEL 7.9
- Rocky Linux 9.2
- Rocky Linux 9.0
- Rocky Linux 8.8
- Rocky Linux 8.6

**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.

## Créer des Linux VDA dans Citrix DaaS Standard pour Azure

August 20, 2024

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 9.2
- RHEL 9.0
- RHEL 8.8
- RHEL 8.6
- Rocky Linux 9.2
- Rocky Linux 9.0
- Rocky Linux 8.8
- Rocky Linux 8.6
- SUSE 15.5
- Ubuntu 22.04
- Ubuntu 20.04

## Étape 1 : préparer 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 :

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate"  
    -t "REG_DWORD" -v "fEnabled" -d "0x00000001" - force  
2  
3 create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate"  
    -t "REG_SZ" -v "ScheduledTime" -d "Immediately" - force  
4  
5 create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate"  
    -t "REG_SZ" -v "Url" -d "<Your-Azure-Container-Url>" - force  
6  
7 create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate"  
    -t "REG_SZ" -v "CaCertificate" -d "<Local-Certificate-Path-of-  
    PortalAzureCom>" --force
```

1. Dans Azure, créez une machine virtuelle Linux d'une distribution prise en charge.
2. Installez un environnement de bureau sur la machine virtuelle Linux si nécessaire.
3. 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>.
4. (Pour Ubuntu uniquement) Ajoutez la ligne `source /etc/network/interfaces.d/*` dans le fichier `/etc/network/interfaces`.
5. (Pour Ubuntu uniquement) Pointez `/etc/resolv.conf` sur `/run/systemd/resolve/resolv.conf` au lieu de `/run/systemd/resolve/stub-resolv.conf` :

```
1 unlink /etc/resolv.conf
2
3 ln -s /run/systemd/resolve/resolv.conf /etc/resolv.conf
```

6. Installez le package Linux VDA.

7. Spécifiez la base de données à utiliser.

À titre expérimental, vous pouvez utiliser SQLite en plus de PostgreSQL. Vous pouvez également basculer entre SQLite et PostgreSQL après avoir installé le package Linux VDA. Pour ce faire, procédez comme suit :

- a) Exécutez `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omettez cette étape s'il s'agit d'une nouvelle installation.
- b) Modifiez `/etc/xdm/db.conf` avant de lancer `deploymcs.sh`.

**Remarque :**

- Nous vous recommandons d'utiliser SQLite uniquement pour le mode VDI.
- Pour Easy Install et MCS, vous pouvez basculer entre SQLite et PostgreSQL sans avoir à les installer manuellement. Sauf indication contraire dans `/etc/xdm/db.conf`, le Linux VDA utilise PostgreSQL par défaut.
- Vous pouvez également l'utiliser `/etc/xdm/db.conf` pour configurer le numéro de port pour PostgreSQL.

8. Modifiez les variables MCS.

Il existe deux manières de configurer les variables MCS :

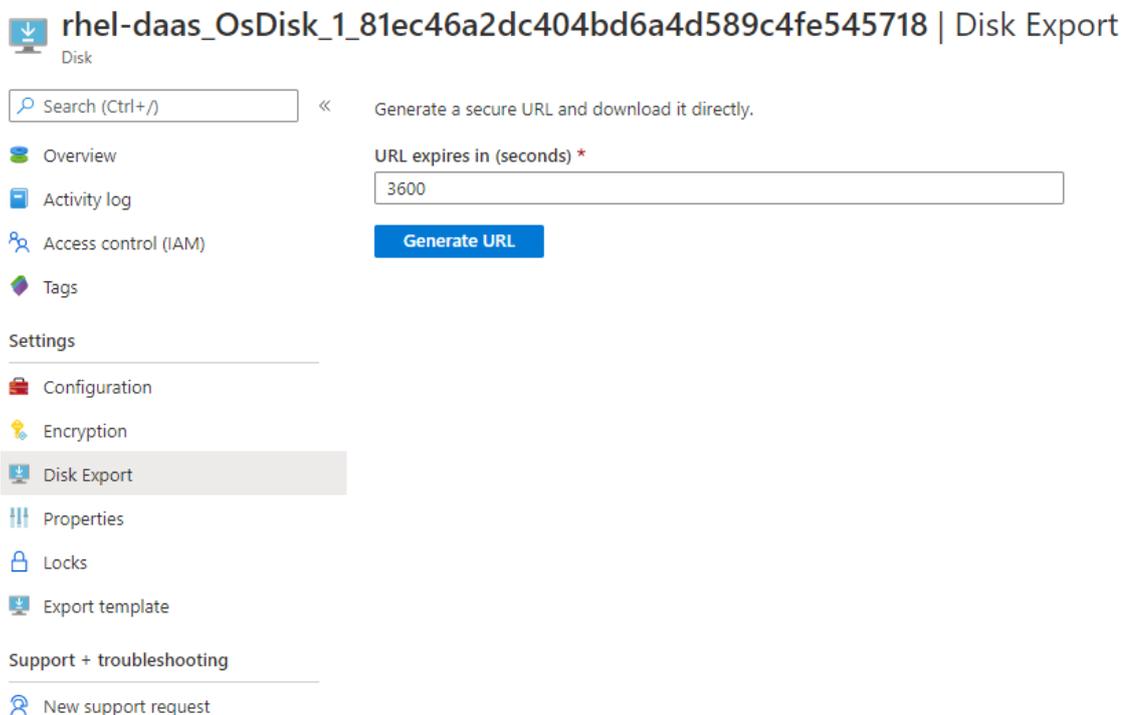
- Modifiez le fichier `/etc/xdm/mcs/mcs.conf`.
- Utilisez l'interface graphique Easy Install. Pour ouvrir l'interface utilisateur graphique Easy Install, exécutez la commande `/opt/Citrix/VDA/bin/easyinstall` dans l'environnement de bureau de votre Linux VDA.

**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`.

Si vous configurez des variables MCS en modifiant `/etc/xdm/mcs/mcs.conf`, exécutez `/opt/Citrix/VDA/sbin/deploymcs.sh`. Si vous configurez des variables MCS à l'aide de l'interface graphique, cliquez sur **Déployer**. Une fois que vous avez cliqué sur **Déployer** dans l'interface graphique, les variables que vous définissez dans l'interface utilisateur remplacent les variables que vous avez définies dans le fichier `/etc/xdm/mcs/mcs.conf`.

9. 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.



10. (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
```

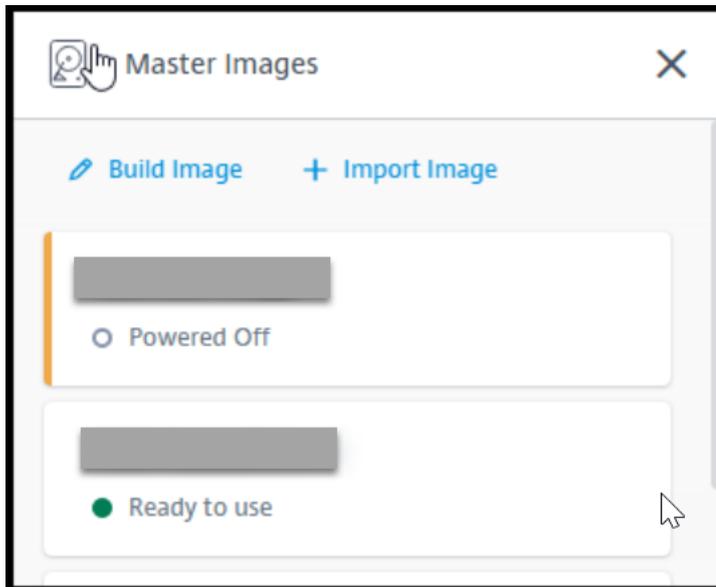
## Étape 2 : importer l'image principale à partir d'Azure

1. 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**.



2. Cliquez sur **Importer une image**.
3. Entrez l'URL SAS du fichier VHD que vous avez généré dans Azure. Sélectionnez **Linux** en tant que type d'image principale.

Import Image from Azure

Enter the Azure-generated URL for the Virtual Hard Disk [?](#)

[How do I find my Url?](#)

Master image type

- Windows  
 Linux

Name The New Master Image

E.g. "Windows 10 + My Apps"

4. Suivez les instructions de l'assistant pour procéder à l'importation de l'image principale.

### Étape 3 : créer 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.

## Installer le Linux VDA manuellement

August 20, 2024

Vous pouvez installer le Linux VDA manuellement sur les distributions Linux suivantes :

- [Amazon Linux 2, CentOS, RHEL et Rocky Linux](#)
- [SUSE](#)
- [Ubuntu](#)
- [Debian](#)

## Installer le Linux VDA manuellement pour Amazon Linux 2, CentOS, RHEL et Rocky Linux

August 21, 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 les informations de configuration et la machine Linux

#### 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 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
```

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 :

```
1 hostname -f
```

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 :

```
1 nslookup domain-controller-fqdn
2
3 ping domain-controller-fqdn
4
5 nslookup delivery-controller-fqdn
6
7 ping delivery-controller-fqdn
```

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 (VM) 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 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 :

```
1 server peer1-fqdn-or-ip-address iburst
2
3 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 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 :

```
1 sudo systemctl restart chronyd
```

### Étape 1g : installer PulseAudio (pour RHEL 9.2/9.0 et Rocky Linux 9.2/9.0 uniquement)

Exécutez la commande suivante pour installer **pulseaudio** :

```
1 sudo yum -y install pulseaudio --allowerasing
```

Ouvrez `/etc/pulse/client.conf` et ajoutez l'entrée suivante :

```
1 autospawn = yes
```

### Étape 1h : installer OpenJDK 11

Le Linux VDA nécessite la présence d'OpenJDK 11.

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

```
1 amazon-linux-extras install java-openjdk11
```

Vérifiez que la version est correcte :

```
1 sudo yum info java-11-openjdk
```

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

```
1 sudo yum -y update java-11-openjdk
```

### Étape 1i : installer et spécifier la base de données à utiliser

#### Remarque :

- Nous vous recommandons d'utiliser SQLite pour le mode VDI uniquement et d'utiliser PostgreSQL pour un modèle de mise à disposition de bureaux partagés hébergés.
- Pour Easy Install et MCS, vous pouvez spécifier SQLite ou PostgreSQL sans avoir à les installer manuellement. Sauf indication contraire dans `/etc/xdl/db.conf`, le Linux VDA utilise PostgreSQL par défaut.
- Pour les installations manuelles, vous devez installer SQLite, PostgreSQL ou les deux manuellement. Si vous installez SQLite et PostgreSQL, vous pouvez spécifier l'un d'entre eux à utiliser en modifiant `/etc/xdl/db.conf` après avoir installé le package Linux VDA.

Cette section explique la procédure d'installation de PostgreSQL et SQLite, et comment spécifier l'utilisation de l'un ou l'autre.

**Installer PostgreSQL** La machine Linux VDA requiert PostgreSQL :

- PostgreSQL 9 pour Amazon Linux 2, RHEL 7 et CentOS 7
- PostgreSQL 10 pour RHEL 8.x et Rocky Linux 8.x
- PostgreSQL 13 pour RHEL 9.2/9.0 et Rocky Linux 9.2/9.0

Exécutez les commandes suivantes pour installer PostgreSQL :

```
1 sudo yum -y install postgresql-server
2
3 sudo yum -y install postgresql-jdbc
```

Pour RHEL 8.x et RHEL 9.2/9.0, exécutez la commande suivante pour installer `libpq` pour PostgreSQL :

```
1 sudo yum -y install libpq
```

Exécutez la commande suivante pour initialiser la base de données. Cette opération crée les fichiers de base de données sous `/var/lib/pgsql/data`.

```
1 sudo postgresql-setup initdb
```

Exécutez les commandes suivantes pour démarrer PostgreSQL au démarrage de la machine ou immédiatement, respectivement :

```
1 sudo systemctl enable postgresql
2
3 sudo systemctl start postgresql
```

Vérifiez la version de PostgreSQL avec :

```
1 psql --version
```

(Pour RHEL 7 et Amazon Linux 2 uniquement) Vérifiez que le répertoire de données est défini à l'aide de l'utilitaire de ligne de commande `psql` :

```
1 sudo -u postgres psql -c 'show data_directory'
```

**Installer SQLite** Exécutez la commande suivante pour installer SQLite :

```
1 sudo yum -y install sqlite
```

**Spécifier la base de données à utiliser** Si vous installez SQLite et PostgreSQL, vous pouvez spécifier l'un d'entre eux à utiliser en modifiant `/etc/xdl/db.conf` après avoir installé le package Linux VDA.

1. Exécutez **/opt/Citrix/VDA/sbin/ctxcleanup.sh**. Omettez cette étape s'il s'agit d'une nouvelle installation.
2. Modifiez **/etc/xdl/db.conf** pour spécifier la base de données à utiliser.
3. Exécutez le fichier **ctxsetup.sh**.

**Remarque :**

Vous pouvez également utiliser **/etc/xdl/db.conf** pour configurer le numéro de port de PostgreSQL.

## Étape 2 : préparer l'hyperviseur

Certaines modifications sont requises pour l'exécution du Linux VDA en tant que VM 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 XenServer (anciennement Citrix Hypervisor)

Lorsque la fonctionnalité de synchronisation de l'heure de XenServer est activée, vous rencontrez des problèmes avec NTP et XenServer au sein de chaque machine virtuelle Linux paravirtualisée. 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 XenServer VM Tools installé, vous pouvez vérifier si la fonctionnalité de synchronisation de l'heure de XenServer est présente et activée à partir de la VM Linux :

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
```

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 désactivée, désactivez-la en entrant 1 dans le fichier :

```
1 sudo echo 1 > /proc/sys/xen/independent_wallclock
```

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 :

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
```

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 XenServer (anciennement 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 VM Linux au domaine Windows

Les méthodes suivantes sont disponibles 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

Pour RHEL 9.2/9.0 et Rocky Linux 9.2/9.0, exécutez les commandes suivantes pour éviter que **pam\_winbind** modifie la propriété du répertoire racine :

```
1 usermod -d /nonexistent nobody
```

Installez ou mettez à jour les packages requis :

Pour RHEL 9.2/9.0/8.x et Rocky Linux 9.2/9.0/8.x :

```
1 sudo yum -y install samba-winbind samba-winbind-clients krb5-workstation oddjob-mkhomedir realmd authselect
```

Pour Amazon Linux 2, CentOS 7 et RHEL 7 :

```
1 sudo yum -y install samba-winbind samba-winbind-clients krb5-workstation oddjob-mkhomedir realmd authconfig
```

**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 :

```
1 sudo /sbin/chkconfig winbind on
```

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

1. Exécutez la commande suivante.

Pour RHEL 9.2/9.0/8.x et Rocky Linux 9.2/9.0/8.x :

```
1 sudo authselect select winbind with-mkhomedir --force
```

Pour Amazon Linux 2, CentOS 7 et RHEL 7 :

```
1 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
```

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. (Pour RHEL 9.2/9.0/8.x et Rocky Linux 9.2/9.0/8.x 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 ajouter une VM Linux au domaine Windows, exécutez la commande suivante :

```
1 sudo realm join -U user --client-software=winbind REALM
```

**Conseil :**

Pour les VM Linux exécutées sur Amazon Linux 2, RHEL 7.9 et CentOS 7.9, vous pouvez également utiliser la commande suivante pour les ajouter au domaine Windows :

```
1 sudo net ads join REALM -U user
```

**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 :

```
1 sudo systemctl restart winbind
```

**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 }
```

Pour RHEL 9.2/9.0 et Rocky Linux 9.2/9.0, exécutez les commandes suivantes pour résoudre le problème SELinux avec Winbind :

```
1 ausearch -c 'winbindd' --raw | audit2allow -M my-winbindd -p /etc/
   selinux/targeted/policy/policy.*
2
3 semodule -X 300 -i my-winbindd.pp
```

**Vérifier l'appartenance à un domaine** Le composant Delivery Controller exige 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 si la machine est associée à un domaine :

```
1 sudo net ads testjoin
```

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

```
1 sudo net ads info
```

**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 :

```
1 sudo klist -ke
```

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 :

```
1 sudo kinit -k MACHINE$@REALM
```

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 inversée (\) 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 :

```
1 sudo klist
```

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

```
1 sudo net ads status
```

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

```
1 wbinfo --krb5auth=domain\username%password
```

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.

```
1 ssh localhost -l domain\username
2 id -u
```

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

```
1 klist
```

Quittez la session.

```
1 exit
```

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 :

```
1 reboot
```

**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.

```
1 sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-  
   interval 32400  
2  
3 sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-  
   auth false
```

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 :

```
1 sudo /opt/quest/bin/vastool configure pam
2
3 sudo /opt/quest/bin/vastool configure nss
```

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

```
1 sudo /opt/quest/bin/vastool -u user join domain-name
```

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.

Redémarrez la machine Linux une fois le domaine rejoint.

**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 :

```
1 sudo /opt/quest/bin/vastool info domain
```

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.

```
1 ssh localhost -l domain\username
2 id -u
```

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

```
1 ls /tmp/krb5cc_uid
```

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

```
1 /opt/quest/bin/vastool klist
```

Quittez la session.

```
1 exit
```

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

**Associer 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` :

```
1 su -
2 adjoin -w -V -u user domain-name
```

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 composant Delivery Controller exige 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 :

```
1 su -
2 adinfo
```

Vérifiez que la valeur `Joined to domain` est valide et que le mode CentrifyDC 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 :

```
1 adinfo --sysinfo all
2 adinfo -diag
```

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

```
1 adinfo --test
```

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.x/9.x et Rocky Linux 8.x/9.x. 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
```

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
```

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 :

```
--enablekrb5kdc dns --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.

```
1 sudo net ads join REALM -U user
```

**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 9.2/9.0/8.x et Rocky Linux 9.2/9.0/8.x) :**

Installez ou mettez à jour les packages requis :

```
1 sudo yum -y install samba-common samba-common-tools krb5-  
workstation authconfig oddjob-mkhomedir realmd oddjob  
authselect
```

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

```
1 sudo authselect select sssd with-mkhomedir --force
```

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.

```
1 sudo realm join REALM -U user
```

**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 9.2/9.0/8.x and Rocky Linux 9.2/9.0/8.x uniquement)

Ouvrez **/etc/sss/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 du fichier `sssd.conf` :

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

### **Activer SSSD Pour RHEL 9.2/9.0/8.x et Rocky Linux 9.2/9.0/8.x :**

Exécutez les commandes suivantes pour activer SSSD :

```
1 sudo systemctl restart sssd
2 sudo systemctl enable sssd.service
3 sudo chkconfig sssd on
```

### **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 :

```
1 authconfig --enablesssd --enablesssdauth --enablemkhomedir --update
2
3 sudo systemctl start sssd
4
5 sudo chkconfig sssd on
```

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

```
1 sudo klist -ke
```

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 :

```
1 sudo kinit -k MACHINE$@REALM
```

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 inversée (\*\*\\*\*) 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 :

```
1 sudo klist
```

**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 :

```
1 sudo getent passwd DOMAIN\username
```

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.

```
1 sudo ssh localhost -l DOMAIN\username
2
3 id -u
```

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

```
1 ls /tmp/krb5cc_{
2 uid }
```

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

```
1 klist
```

Passez à l'[étape 6 : installer le Linux VDA](#) après vérification de la jonction du domaine.

## PBIS

### Télécharger le package PBIS requis

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

**Rendre le script d'installation PBIS exécutable**

```
1 chmod +x pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

**Exécuter le script d'installation PBIS**

```
1 sh pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

**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 /opt/pbis/bin/domainjoin-cli join domain-name user
```

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 composant Delivery Controller exige 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 :

```
1 /opt/pbis/bin/domainjoin-cli query
```

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.

```
1 ssh localhost -l domain\user
2
3 id -u
```

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

```
1 ls /tmp/krb5cc_uid
```

Quittez la session.

```
1 exit
```

Passez à l'[étape 6 : installer le Linux VDA](#) après vérification de la jonction du domaine.

#### Étape 4 : installer .NET Runtime 6.0

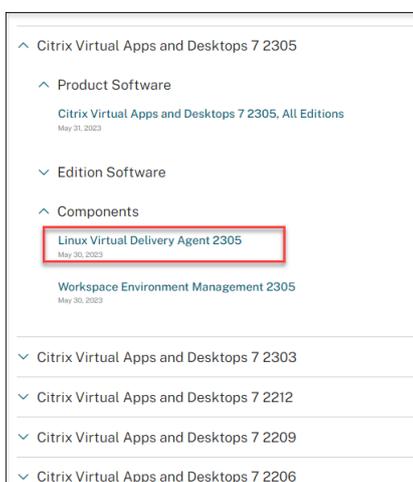
Avant d'installer Linux VDA, installez .NET Runtime 6.0 conformément aux instructions de l'article <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers>.

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

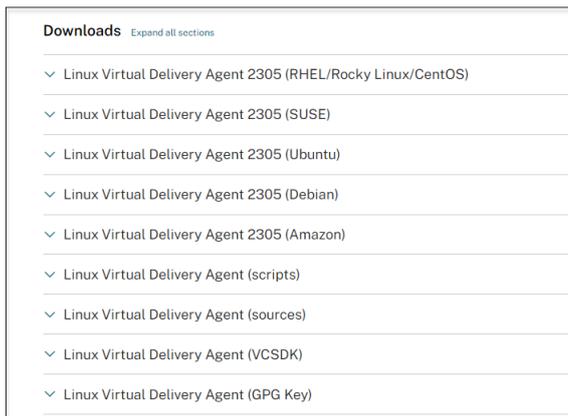
En fonction de la sortie de la commande, définissez le chemin binaire de .NET Runtime. Par exemple, si la sortie de la commande est /aa/bb/dotnet, utilisez /aa/bb comme chemin binaire .NET.

#### Étape 5 : télécharger le package Linux VDA

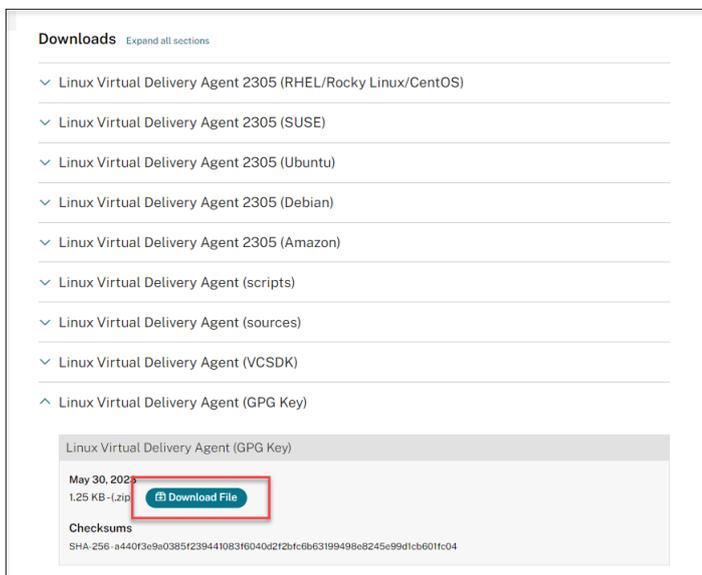
1. Accédez à la [page de téléchargement de Citrix Virtual Apps and Desktops](#).
2. Développez la version appropriée de Citrix Virtual Apps and Desktops.
3. Développez **Components** pour trouver le Linux VDA. Par exemple :



4. Cliquez sur le lien Linux VDA pour accéder aux téléchargements de Linux VDA.



5. Téléchargez le package Linux VDA correspondant à votre distribution Linux.
6. Téléchargez la clé publique GPG que vous pouvez utiliser pour vérifier l'intégrité du package Linux VDA. Par exemple :



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

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

### Étape 6 : installer le Linux VDA

Vous pouvez effectuer une nouvelle installation ou mettre à niveau une installation existante. Le Linux VDA prend en charge les mises à niveau depuis la version la plus récente. Par exemple, vous pouvez mettre à niveau le Linux VDA de 2308 à 2311 et de 1912 LTSR à 2203 LTSR.

## Étape 6a : 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 :

```
1 sudo systemctl stop ctxvda
2
3 sudo systemctl stop ctxhdx
```

#### Remarque :

Avant d'arrêter les services **ctxvda** et **ctxhdx**, exécutez la commande **systemctl stop ctxmonitord** 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 :

```
1 sudo rpm -e XenDesktopVDA
```

#### 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 CentOS, RHEL et Rocky Linux, 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 de la page <https://docs.fedoraproject.org/en-US/epel/>.
- Avant d'installer le Linux VDA sur RHEL 9.2/9.0 et Rocky Linux 9.2/9.0, mettez à jour le package **libsepol** vers la version 3.4 ou ultérieure.

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

#### Pour Amazon Linux 2 :

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

**Pour RHEL 9.2/9.0 et Rocky Linux 9.2/9.0 :**

```
1 sudo yum install -y XenDesktopVDA-<version>.el9.x.x86_64.rpm
```

**Pour RHEL 8.x et Rocky Linux 8.x :**

```
1 sudo yum install -y XenDesktopVDA-<version>.el8.x.x86_64.rpm
```

**Pour CentOS 7 et RHEL 7 :**

```
1 sudo yum install -y XenDesktopVDA-<version>.el7.x.x86_64.rpm
```

- 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 :**

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

**Pour RHEL 9.2/9.0 et Rocky Linux 9.2/9.0 :**

```
1 sudo rpm -i XenDesktopVDA-<version>.el9.x.x86_64.rpm
```

**Pour RHEL 8.x et Rocky Linux 8.x :**

```
1 sudo rpm -i XenDesktopVDA-<version>.el8.x.x86_64.rpm
```

**Pour CentOS 7 et RHEL 7 :**

```
1 sudo rpm -i XenDesktopVDA-<version>.el7.x.x86_64.rpm
```

**Liste des dépendances RPM pour RHEL 9.2/9.0 et Rocky Linux 9.2/9.0 :**

```
1 tzdata-java >= 2022
2
3 java-11-openjdk >= 11
4
5 icoutils >= 0.32
6
7 firewalld >= 0.6.3
8
9 policycoreutils-python >= 2.8.9
10
11 policycoreutils-python-utils >= 2.8
12
13 python3-policycoreutils >= 2.8
14
15 dbus >= 1.12.8
16
17 dbus-common >= 1.12.8
```

```
18
19  dbus-daemon >= 1.12.8
20
21  dbus-tools >= 1.12.8
22
23  dbus-x11 >= 1.12.8
24
25  xorg-x11-server-utils >= 7.7
26
27  xorg-x11-xinit >= 1.3.4
28
29  libXpm >= 3.5.12
30
31  libXrandr >= 1.5.1
32
33  libXtst >= 1.2.3
34
35  pam >= 1.3.1
36
37  util-linux >= 2.32.1
38
39  util-linux-user >= 2.32.1
40
41  xorg-x11-utils >= 7.5
42
43  bash >= 4.3
44
45  findutils >= 4.6
46
47  gawk >= 4.2
48
49  sed >= 4.5
50
51  cups >= 1.6.0
52
53  foomatic-filters >= 4.0.9
54
55  cups-filters >= 1.20.0
56
57  ghostscript >= 9.25
58
59  libxml2 >= 2.9
60
61  libmspack >= 0.7
62
63  krb5-workstation >= 1.13
64
65  ibus >= 1.5
66
67  nss-tools >= 3.44.0
68
69  gperftools-libs >= 2.4
70
```

```
71 cyrus-sasl-gssapi >= 2.1
72
73 python3 >= 3.6~
74
75 qt5-qtbase >= 5.5~
76
77 qt5-qtbase-gui >= 5.5~
78
79 qrencode-libs >= 3.4.4
80
81 imlib2 >= 1.4.9
```

**Liste des dépendances RPM pour RHEL 8.x et Rocky Linux 8.x :**

```
1 java-11-openjdk >= 11
2
3 icoutils >= 0.32
4
5 firewalld >= 0.6.3
6
7 policycoreutils-python >= 2.8.9
8
9 policycoreutils-python-utils >= 2.8
10
11 python3-policycoreutils >= 2.8
12
13 dbus >= 1.12.8
14
15 dbus-common >= 1.12.8
16
17 dbus-daemon >= 1.12.8
18
19 dbus-tools >= 1.12.8
20
21 dbus-x11 >= 1.12.8
22
23 xorg-x11-server-utils >= 7.7
24
25 xorg-x11-xinit >= 1.3.4
26
27 libXpm >= 3.5.12
28
29 libXrandr >= 1.5.1
30
31 libXtst >= 1.2.3
32
33 pam >= 1.3.1
34
35 util-linux >= 2.32.1
36
37 util-linux-user >= 2.32.1
38
39 xorg-x11-utils >= 7.5
```

```
40
41  bash >= 4.3
42
43  findutils >= 4.6
44
45  gawk >= 4.2
46
47  sed >= 4.5
48
49  cups >= 1.6.0
50
51  foomatic-filters >= 4.0.9
52
53  cups-filters >= 1.20.0
54
55  ghostscript >= 9.25
56
57  libxml2 >= 2.9
58
59  libmspack >= 0.7
60
61  krb5-workstation >= 1.13
62
63  ibus >= 1.5
64
65  nss-tools >= 3.44.0
66
67  gperftools-libs >= 2.4
68
69  cyrus-sasl-gssapi >= 2.1
70
71  python3 >= 3.6~
72
73  qt5-qtbase >= 5.5~
74
75  qt5-qtbase-gui >= 5.5~
76
77  qrencode-libs >= 3.4.4
78
79  imlib2 >= 1.4.9
```

**Liste des dépendances RPM pour CentOS 7 et RHEL 7 :**

```
1  java-11-openjdk >= 11
2
3  ImageMagick >= 6.7.8.9
4
5  firewalld >= 0.3.9
6
7  policycoreutils-python >= 2.0.83
8
9  dbus >= 1.6.12
10
```

```
11  dbus-x11 >= 1.6.12
12
13  xorg-x11-server-utils >= 7.7
14
15  xorg-x11-xinit >= 1.3.2
16
17  xorg-x11-server-Xorg >= 1.20.4
18
19  libXpm >= 3.5.10
20
21  libXrandr >= 1.4.1
22
23  libXtst >= 1.2.2
24
25  pam >= 1.1.8
26
27  util-linux >= 2.23.2
28
29  bash >= 4.2
30
31  findutils >= 4.5
32
33  gawk >= 4.0
34
35  sed >= 4.2
36
37  cups >= 1.6.0
38
39  foomatic-filters >= 4.0.9
40
41  libxml2 >= 2.9
42
43  libmspack >= 0.5
44
45  ibus >= 1.5
46
47  cyrus-sasl-gssapi >= 2.1
48
49  python3 >= 3.6~
50
51  gperftools-libs >= 2.4
52
53  nss-tools >= 3.44.0
54
55  qt5-qtbase >= 5.5~
56
57  qt5-qtbase >= 5.5~
58
59  imlib2 >= 1.4.5
```

**Liste des dépendances RPM pour Amazon Linux 2 :**

```
1  java-11-openjdk >= 11
```

```
2
3 ImageMagick >= 6.7.8.9
4
5 firewalld >= 0.3.9
6
7 polycoreutils-python >= 2.0.83
8
9 dbus >= 1.6.12
10
11 dbus-x11 >= 1.6.12
12
13 xorg-x11-server-utils >= 7.7
14
15 xorg-x11-xinit >= 1.3.2
16
17 xorg-x11-server-Xorg >= 1.20.4
18
19 libXpm >= 3.5.10
20
21 libXrandr >= 1.4.1
22
23 libXtst >= 1.2.2
24
25 pam >= 1.1.8
26
27 util-linux >= 2.23.2
28
29 bash >= 4.2
30
31 findutils >= 4.5
32
33 gawk >= 4.0
34
35 sed >= 4.2
36
37 cups >= 1.6.0
38
39 foomatic-filters >= 4.0.9
40
41 libxml2 >= 2.9
42
43 libmspack >= 0.5
44
45 ibus >= 1.5
46
47 cyrus-sasl-gssapi >= 2.1
48
49 gperftools-libs >= 2.4
50
51 nss-tools >= 3.44.0
52
53 qt5-qtbase >= 5.5~
54
```

```
55  qrencode-libs >= 3.4.1
56
57  imlib2 >= 1.4.5
```

**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-websocketify x11vnc`. Le but est d'installer `python-websocketify` et `x11vnc` manuellement pour utiliser la fonctionnalité d'observation de session. Pour en savoir plus, consultez la section [Observer des sessions](#).

**Étape 6b : mettre à niveau une installation existante (facultatif)**

Le Linux VDA prend en charge les mises à niveau depuis la version la plus récente. Par exemple, vous pouvez mettre à niveau le Linux VDA de 2308 à 2311 et de 1912 LTSR à 2203 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.
  - Avant de mettre à niveau le Linux VDA sur RHEL 9.2/9.0 et Rocky Linux 9.2/9.0, mettez à jour le package **libsepol** vers la version 3.4 ou ultérieure.
- Pour effectuer une mise à niveau de votre logiciel à l'aide de Yum :

**Pour Amazon Linux 2 :**

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

**Pour RHEL 9.2/9.0 et Rocky Linux 9.2/9.0 :**

```
1  sudo yum install -y XenDesktopVDA-<version>.el9_x.x86_64.rpm
```

**Pour RHEL 8.x et Rocky Linux 8.x :**

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

**Pour CentOS 7 et RHEL 7 :**

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

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

**Pour Amazon Linux 2 :**

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

**Pour RHEL 9.2/9.0 et Rocky Linux 9.2/9.0 :**

```
1 sudo rpm -U XenDesktopVDA-<version>.el9.x.x86_64.rpm
```

**Pour RHEL 8.x et Rocky Linux 8.x :**

```
1 sudo rpm -U XenDesktopVDA-<version>.el8.x.x86_64.rpm
```

**Pour CentOS 7 et RHEL 7 :**

```
1 sudo rpm -U XenDesktopVDA-<version>.el7.x.x86_64.rpm
```

**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 :

- [XenServer](#)
- [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 :

```
1 yum install gcc
2
3 yum install "kernel-devel-$(uname -r)"
4
5 systemctl set-default multi-user.target
```

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

### 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 sur 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**.

Après l'installation du package, vous devez configurer le VDA Linux 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 pré-configurées. Consultez l'aide sur le script avant de continuer :

```
1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
```

### Configuration avec invites

Exécutez une configuration manuelle avec questions :

```
1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

### 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\_NON\_DOMAIN\_JOINED='Y|N'** : indique s'il faut associer la machine à un domaine . La valeur par défaut est "n". Pour les scénarios liés à un domaine, définissez la valeur sur "n".
- **CTX\_XDL\_AD\_INTEGRATION='winbind|sssd|centrify|pbis|quest'** : 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.

- **CTX\_XDL\_DDC\_LIST=<list-ddc-fqdns>** : 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\_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\_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 VDA doit être configuré pour le mode Bureaux VDI (session unique), c'est-à-dire, CTX\_XDL\_VDI\_MODE='y'.
- **CTX\_XDL\_START\_SERVICE='y|n'** : indique si les services Linux VDA sont lancés une fois la configuration de Linux VDA terminée.
- **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 Virtual Desktop 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\_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 par défaut configuré sur le VDA est utilisé.

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**

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

– **Pour le bureau GNOME Classic**

```
1 GSESSION="$(type -p gnome-session)"
2 if [ -n "$GSESSION" ]; then
3 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\_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 service Broker Agent. Le chemin d'accès par défaut est `/usr/bin`.
- **CTX\_XDL\_VDA\_PORT=port-number** : le Linux VDA communique avec les composants Delivery Controller via un port TCP/IP.
- **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`. Pour accélérer les requêtes LDAP dans une forêt Active directory, 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\_SUPPORT\_DDC\_AS\_CNAME='y|n'** : le Linux VDA prend en charge la spécification d'un nom de composant Delivery Controller à l'aide d'un enregistrement DNS CNAME.

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

```

1 export CTX_XDL_NON_DOMAIN_JOINED='n'
2 export CTX_XDL_AD_INTEGRATION=winbind|centrify|sssd|pbis|quest
3 export CTX_XDL_DDC_LIST='<list-ddc-fqdns>'
4 export CTX_XDL_VDI_MODE='y|n'
5 export CTX_XDL_HDX_3D_PRO='y|n'
6 export CTX_XDL_START_SERVICE='y|n'
7 export CTX_XDL_REGISTER_SERVICE='y|n'
8 export CTX_XDL_ADD_FIREWALL_RULES='y|n'
9 export CTX_XDL_DESKTOP_ENVIRONMENT= gnome|gnome-classic|mate|'<none>'
10 export CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime>'
11 export CTX_XDL_VDA_PORT='<port-number>'
12 export CTX_XDL_SITE_NAME='<dns-site-name>'|'<none>'
13 export CTX_XDL_LDAP_LIST='<list-ldap-servers>'|'<none>'
14 export CTX_XDL_SEARCH_BASE='<search-base-set>'|'<none>'
15 export CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n'
16 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh --silent

```

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_NON_DOMAIN_JOINED='n' \
2 CTX_XDL_AD_INTEGRATION=winbind|centrify|sssd|pbis|quest \
3 CTX_XDL_DDC_LIST='<list-ddc-fqdns>' \
4 CTX_XDL_VDI_MODE='y|n' \
5 CTX_XDL_HDX_3D_PRO='y|n' \
6 CTX_XDL_START_SERVICE='y|n' \
7 CTX_XDL_REGISTER_SERVICE='y|n' \
8 CTX_XDL_ADD_FIREWALL_RULES='y|n' \
9 CTX_XDL_DESKTOP_ENVIRONMENT= gnome|gnome-classic|mate|'<none>' \
10 CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime>' \
11 CTX_XDL_VDA_PORT='<port-number>' \
12 CTX_XDL_SITE_NAME='<dns-site-name>'|'<none>' \
13 CTX_XDL_LDAP_LIST='<list-ldap-servers>'|'<none>' \
14 CTX_XDL_SEARCH_BASE='<search-base-set>'|'<none>' \
15 CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n' \
16 /opt/Citrix/VDA/sbin/ctxsetup.sh --silent

```

## 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
```

Pour supprimer les modifications de configuration :

```
1 sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
```

**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 :

```
1 sudo systemctl start ctxhdx
2
3 sudo systemctl start ctxvda
```

**Arrêter Linux VDA :**

Pour arrêter les services Linux VDA :

```
1 sudo systemctl stop ctxvda
2
3 sudo systemctl stop ctxhdx
```

**Remarque :**

Avant d'arrêter les services **ctxvda** et **ctxhdx**, exécutez la commande **systemctl stop ctxmoni-**

**tor** 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 systemctl stop ctxvda
2
3 sudo systemctl restart ctxhdx
4
5 sudo systemctl start ctxvda
```

### Vérifier l'état de Linux VDA :

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

```
1 sudo systemctl status ctxvda
2
3 sudo systemctl status ctxhdx
```

## Étape 11 : créer des catalogues de machines

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 des groupes de mise à disposition

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 2311](#).

## Installer le Linux VDA manuellement sur SUSE

August 21, 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 les informations de configuration et la machine Linux

### 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 :

```
1 su -  
2  
3 yast
```

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

```
1 su -  
2  
3 yast2 &
```

### 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 :

```
1 hostname
```

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 :

```
1 hostname -f
```

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 :

```
1 nslookup domain-controller-fqdn
2
3 ping domain-controller-fqdn
4
5 nslookup delivery-controller-fqdn
6
7 ping delivery-controller-fqdn
```

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 (VM) 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 15.5 :**

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
```

### Étape 1d : installer les packages dépendants de Linux VDA

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

- 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
```

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
```

### Installer et spécifier la base de données à utiliser

#### Remarque :

- Nous vous recommandons d'utiliser SQLite pour le mode VDI uniquement et d'utiliser PostgreSQL pour un modèle de mise à disposition de bureaux partagés hébergés.
- Pour Easy Install et MCS, vous pouvez spécifier SQLite ou PostgreSQL sans avoir à les installer manuellement. Sauf indication contraire dans **/etc/xdl/db.conf**, le Linux VDA utilise PostgreSQL par défaut.
- Pour les installations manuelles, vous devez installer SQLite, PostgreSQL ou les deux manuellement. Si vous installez SQLite et PostgreSQL, vous pouvez spécifier l'un d'entre eux à utiliser en modifiant **/etc/xdl/db.conf** après avoir installé le package Linux VDA.

Cette section explique la procédure d'installation de PostgreSQL et SQLite, et comment spécifier l'utilisation de l'un ou l'autre.

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

```
1 sudo zypper install postgresql-server
2
3 sudo zypper install postgresql-jdbc
```

Exécutez les commandes suivantes pour démarrer PostgreSQL au démarrage de la machine ou immédiatement, respectivement :

```
1 sudo systemctl enable postgresql
2
3 sudo systemctl restart postgresql
```

**Installer SQLite** Pour SUSE, exécutez la commande suivante pour installer SQLite :

```
1 sudo zypper install sqlite3
```

**Spécifier la base de données à utiliser** Si vous installez SQLite et PostgreSQL, vous pouvez spécifier l'un d'entre eux à utiliser en modifiant `/etc/xdl/db.conf` après avoir installé le package Linux VDA.

1. Exécutez `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omettez cette étape s'il s'agit d'une nouvelle installation.
2. Modifiez `/etc/xdl/db.conf` pour spécifier la base de données à utiliser.
3. Exécutez le fichier `ctxsetup.sh`.

**Remarque :**

Vous pouvez également utiliser `/etc/xdl/db.conf` pour configurer le numéro de port de PostgreSQL.

## Étape 2 : préparer l'hyperviseur

Certaines modifications sont requises pour l'exécution du Linux VDA en tant que VM 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 XenServer (anciennement Citrix Hypervisor)

Si la fonctionnalité de synchronisation de l'heure de XenServer est activée, vous rencontrez des problèmes avec NTP et XenServer au sein de chaque machine virtuelle Linux paravirtualisée. 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 XenServer VM Tools installé, vous pouvez vérifier si la fonctionnalité de synchronisation de l'heure de XenServer est présente et activée à partir de la VM Linux :

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
```

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 désactivée, désactivez-la en entrant **1** dans le fichier :

```
1 sudo echo 1 > /proc/sys/xen/independent_wallclock
```

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 :

```
1 reboot
```

Après le redémarrage, vérifiez que le paramètre est correct :

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
```

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 XenServer (anciennement 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 VM Linux au domaine Windows

Les méthodes suivantes sont disponibles pour ajouter des machines Linux au domaine Active Directory (AD) :

- [Samba Winbind](#)
- [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 Authentication** (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 :

```
1 su -
2 reboot
```

**Vérifier l'appartenance à un domaine** Le composant Delivery Controller exige 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 si la machine est associée à un domaine :

```
1 sudo net ads testjoin
```

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

```
1 sudo net ads info
```

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

```
1 sudo klist -ke
```

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 :

```
1 sudo kinit -k MACHINE$@REALM
```

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 inversée (\) 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 :

```
1 sudo klist
```

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

```
1 sudo net ads status
```

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

```
1 wbinfo --krb5auth=domain\username%password
```

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.

```
1 ssh localhost -l domain\username
2 id -u
```

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

```
1 ls /tmp/krb5cc_uid
```

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

```
1 klist
```

Quittez la session.

```
1 exit
```

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 :

```
1 sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-  
   interval 32400  
2  
3 sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-  
   auth false
```

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 :

```
1 sudo /opt/quest/bin/vastool configure pam  
2  
3 sudo /opt/quest/bin/vastool configure nss
```

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

```
1 sudo /opt/quest/bin/vastool -u user join domain-name
```

Le paramètre **user** 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.

Redémarrez la machine Linux une fois le domaine rejoint.

**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 :

```
1 sudo /opt/quest/bin/vastool info domain
```

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.

```
1 ssh localhost -l domain\username  
2 id -u
```

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

```
1 ls /tmp/krb5cc_uid
```

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

```
1 /opt/quest/bin/vastool klist
```

Quittez la session.

```
1 exit
```

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 l'agent Centrify DirectControl installé, associez la machine Linux au domaine Active Directory en exécutant la commande Centrify **adjoin** :

```
1 sudo adjoin -w -V -u user domain-name
```

Le paramètre **user** est un utilisateur de domaine Active Directory 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 composant Delivery Controller exige 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 :

```
1 sudo adinfo
```

Vérifiez que la valeur **Joined to domain** est valide et que le **mode CentrifyDC** 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 :

```
1 adinfo --sysinfo all
2
3 adinfo -diag
```

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

```
1 adinfo --test
```

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).

```
1 sudo systemctl stop nscd
2 sudo systemctl disable nscd
```

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

```
1 hostname
2 hostname -f
3 chronyc traking
```

3. Installez ou mettez à jour les packages requis :

```
1 sudo zypper install samba-client sssd-ad
```

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.

```
1 [libdefaults]
2
3     dns_canonicalize_hostname = false
4
5     rdns = false
6
7     default_realm = REALM
8
9     forwardable = true
10
11 [realms]
12
13     REALM = {
14
15
16         kdc = fqdn-of-domain-controller
17
```

```

18     default_domain = realm
19
20     admin_server = fqdn-of-domain-controller
21 }
22
23 [domain_realm]
24
25     .realm = REALM

```

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]** :

```

1 [global]
2     workgroup = domain
3
4     client signing = yes
5
6     client use spnego = yes
7
8     kerberos method = secrets and keytab
9
10    realm = REALM
11
12    security = ADS

```

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.

```

1 passwd: compat sss
2
3 group: compat sss

```

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

```

1 kinit administrator

```

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

```

1 net ads join osname="SUSE Linux Enterprise Server" osVersion=15 -U
  administrator

```

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

```
1 sudo zypper install sssd sssd-ad
```

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

```
1 sudo pam-config --add --sss
2 sudo pam-config --add --mkhomedir
```

## Configurer SSSD

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

```
1 [sss]
2     config_file_version = 2
3     services = nss,pam
4     domains = domain-dns-name
5
6 [domain/domain-dns-name]
7     id_provider = ad
8     auth_provider = ad
9     access_provider = ad
10    ad_domain = domain-dns-name
11    ad_server = fqdn-of-domain-controller
12    ldap_id_mapping = true
13    ldap_schema = ad
14
15 # Kerberos settings
16    krb5_ccachedir = /tmp
17    krb5_ccname_template = FILE:%d/krb5cc_%U
18
19 # Comment out if the users have the shell and home dir set on the
20    AD side
21
22    fallback_homedir = /home/%d/%u
23    default_shell = /bin/bash
24
25 # Uncomment and adjust if the default principal SHORTNAME$@REALM
26    is not available
27
28    ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
29
30    ad_gpo_access_control = permissive
```

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

### Remarque :

Le paramètre **ldap\_id\_mapping** est défini sur « true » pour que le démon SSSD mappe

les identifiants de sécurité Windows avec les identifiants utilisateur 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` :

```
1 sudo chmod 0600 /etc/sssd/sssd.conf
```

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

```
1 sudo systemctl enable sssd
2 sudo systemctl start sssd
```

### Vérifier l'appartenance à un domaine

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

```
1 sudo net ads testjoin
```

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

```
1 sudo net ads info
```

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

```
1 sudo klist -ke
```

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 :

```
1 sudo kinit -k MACHINE$@REALM
```

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 inversée (\*\*\\*\*) 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 :

```
1 sudo klist
```

**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.

```
1 ssh localhost -l domain\username
2
3 id -u
4
5 klist
6
7 exit
```

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
```

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
```

**Rendre le script d'installation PBIS exécutable** Par exemple :

```
1 chmod +x pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

**Exécuter le script d'installation PBIS** Par exemple :

```
1 sh pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

**Associer 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
```

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 :

```
1 /opt/pbis/bin/domainjoin-cli query
```

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.

```
1 ssh localhost -l domain\user
2
3 id -u
```

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

```
1 ls /tmp/krb5cc_uid
```

Quittez la session.

```
1 exit
```

Passez à l'[étape 6 : installer le Linux VDA](#) après vérification de la jonction du domaine.

## Étape 4 : installer .NET Runtime 6.0

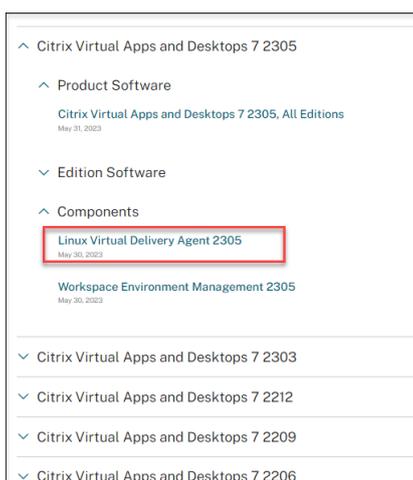
Avant d'installer Linux VDA, installez .NET Runtime 6.0 conformément aux instructions de l'article <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers>.

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

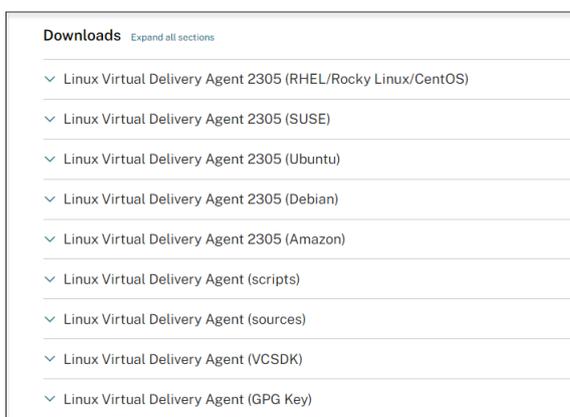
En fonction de la sortie de la commande, définissez le chemin binaire de .NET Runtime. Par exemple, si la sortie de la commande est /aa/bb/dotnet, utilisez /aa/bb comme chemin binaire .NET.

## 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. Développez **Components** pour trouver le Linux VDA. Par exemple :

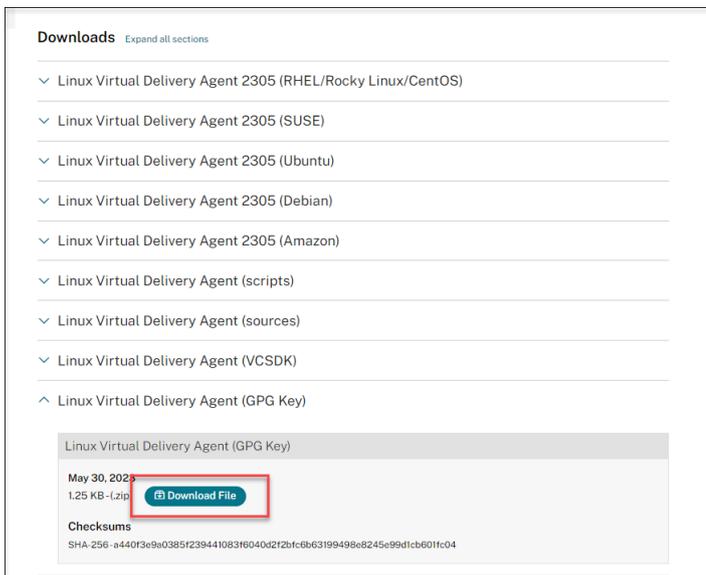


4. Cliquez sur le lien Linux VDA pour accéder aux téléchargements de Linux VDA.



5. Téléchargez le package Linux VDA correspondant à votre distribution Linux.

6. Téléchargez la clé publique GPG que vous pouvez utiliser pour vérifier l'intégrité du package Linux VDA. Par exemple :



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

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

## 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 :

```
1 sudo systemctl stop ctxvda
2
3 sudo systemctl stop ctxhdx
```

#### Remarque :

Avant d'arrêter les services **ctxvda** et **ctxhdx**, exécutez la commande **systemctl stop ctx-monitor** 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 :

```
1 sudo rpm -e XenDesktopVDA
```

**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 :

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

Installez le logiciel Linux VDA à l'aide du gestionnaire de package RPM :

```
1 sudo rpm -i XenDesktopVDA-<version>.sle15_x.x86_64.rpm
```

### Étape 6c : mettre à niveau le Linux VDA (facultatif)

Le Linux VDA prend en charge les mises à niveau depuis la version la plus récente. Par exemple, vous pouvez mettre à niveau le Linux VDA de 2308 à 2311 et de 1912 LTSR à 2203 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.

```
1 sudo rpm -U XenDesktopVDA-<version>.sle15_x.x86_64.rpm
```

### Liste des dépendances RPM pour SUSE 15 :

```
1 java-11-openjdk >= 11
2
3 ImageMagick >= 7.0
4
5 dbus-1 >= 1.12.2
6
7 dbus-1-x11 >= 1.12.2
8
9 xorg-x11 >= 7.6_1
10
```

```
11 libXpm4 >= 3.5.12
12
13 libXrandr2 >= 1.5.1
14
15 libXtst6 >= 1.2.3
16
17 pam >= 1.3.0
18
19 bash >= 4.4
20
21 findutils >= 4.6
22
23 gawk >= 4.2
24
25 sed >= 4.4
26
27 cups >= 2.2
28
29 cups-filters >= 1.25
30
31 libxml2-2 >= 2.9
32
33 libmspack0 >= 0.6
34
35 ibus >= 1.5
36
37 libtcmalloc4 >= 2.5
38
39 libcap-progs >= 2.26
40
41 mozilla-nss-tools >= 3.53.1
42
43 libpython3_6m1_0 >= 3.6~
44
45 libQt5Widgets5 >= 5.12
46
47 libqrencode4 >= 4.0.0
48
49 libImlib2-1 >= 1.4.10
```

**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 :

- [XenServer](#)
- [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

### 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 sur 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**.

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 pré-configurées. Consultez l'aide sur le script avant de continuer :

```
1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh - help
```

### Configuration avec invites

Exécutez une configuration manuelle avec questions :

```
1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

### 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\_NON\_DOMAIN\_JOINED='Y|N'** : indique s'il faut associer la machine à un domaine . La valeur par défaut est "n". Pour les scénarios liés à un domaine, définissez la valeur sur "n".
- **CTX\_XDL\_AD\_INTEGRATION='winbind|sssd|centrify|pbis|quest'** : 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.
- **CTX\_XDL\_DDC\_LIST='<list-ddc-fqdns>'** : 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\_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\_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 VDA doit être configuré pour le mode Bureaux VDI (session unique), c'est-à-dire, CTX\_XDL\_VDI\_MODE='y'.
- **CTX\_XDL\_START\_SERVICE='y|n'** : indique si les services Linux VDA sont lancés une fois la configuration de Linux VDA terminée.
- **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 Virtual Desktop 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\_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 par défaut configuré sur le VDA est utilisé.

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**

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

- **Pour le bureau GNOME Classic**

```
1 GSESSION="$$(type -p gnome-session)"
2 if [ -n "$GSESSION" ]; then
3     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\_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 service Broker Agent. Le chemin d'accès par défaut est `"/usr/bin"`.
- **CTX\_XDL\_VDA\_PORT=port-number** : le Linux VDA communique avec les composants Delivery Controller via un port TCP/IP.
- **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`. Pour accélérer les requêtes LDAP dans une forêt Active directory, 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\_SUPPORT\_DDC\_AS\_CNAME='y|n'** : le Linux VDA prend en charge la spécification d'un nom de composant Delivery Controller à l'aide d'un enregistrement DNS CNAME.

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

```

1 export CTX_XDL_NON_DOMAIN_JOINED='n'
2 export CTX_XDL_AD_INTEGRATION=winbind|centrify|sssd|pbis|quest
3 export CTX_XDL_DDC_LIST='<list-ddc-fqdns>'
4 export CTX_XDL_VDI_MODE='y|n'
5 export CTX_XDL_HDX_3D_PRO='y|n'
6 export CTX_XDL_START_SERVICE='y|n'
7 export CTX_XDL_REGISTER_SERVICE='y|n'
8 export CTX_XDL_ADD_FIREWALL_RULES='y|n'
9 export CTX_XDL_DESKTOP_ENVIRONMENT= gnome|gnome-classic|mate|'<none>'
10 export CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime>'
11 export CTX_XDL_VDA_PORT='<port-number>'
12 export CTX_XDL_SITE_NAME='<dns-site-name>'|'<none>'
13 export CTX_XDL_LDAP_LIST='<list-ldap-servers>'|'<none>'
14 export CTX_XDL_SEARCH_BASE='<search-base-set>'|'<none>'
15 export CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n'
16 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh --silent

```

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_NON_DOMAIN_JOINED='n' \
2 CTX_XDL_AD_INTEGRATION=winbind|centrify|sssd|pbis|quest \
3 CTX_XDL_DDC_LIST='<list-ddc-fqdns>' \
4 CTX_XDL_VDI_MODE='y|n' \
5 CTX_XDL_HDX_3D_PRO='y|n' \
6 CTX_XDL_START_SERVICE='y|n' \
7 CTX_XDL_REGISTER_SERVICE='y|n' \
8 CTX_XDL_ADD_FIREWALL_RULES='y|n' \
9 CTX_XDL_DESKTOP_ENVIRONMENT= gnome|gnome-classic|mate|'<none>' \
10 CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime>' \
11 CTX_XDL_VDA_PORT='<port-number>' \
12 CTX_XDL_SITE_NAME='<dns-site-name>'|'<none>' \
13 CTX_XDL_LDAP_LIST='<list-ldap-servers>'|'<none>' \
14 CTX_XDL_SEARCH_BASE='<search-base-set>'|'<none>' \
15 CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n' \
16 /opt/Citrix/VDA/sbin/ctxsetup.sh --silent

```

## 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 /usr/local/sbin/ctxcleanup.sh --help
```

Pour supprimer les modifications de configuration :

```
1 sudo /usr/local/sbin/ctxcleanup.sh
```

### 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 :

```
1 sudo systemctl start ctxhdx
2
3 sudo systemctl start ctxvda
```

### Arrêter Linux VDA :

Pour arrêter les services Linux VDA :

```
1 sudo systemctl stop ctxvda
2
3 sudo systemctl stop ctxhdx
```

#### Remarque :

Avant d'arrêter les services **ctxvda** et **ctxhdx**, exécutez la commande **systemctl stop ctxmonitord** 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 systemctl stop ctxvda
2
3 sudo systemctl restart ctxhdx
4
5 sudo systemctl start ctxvda
```

### Vérifier l'état de Linux VDA :

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

```
1 sudo systemctl status ctxvda
2
3 sudo systemctl status ctxhdx
```

## Étape 11 : créer des catalogues de machines

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 vous supprimez une machine puis que vous la rejoindez au domaine Active Directory, vous devez supprimer et rajouter la machine au catalogue de machines.

## Étape 12 : créer des groupes de mise à disposition

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 2311](#).

## Installer le Linux VDA manuellement sur Ubuntu

August 21, 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 les informations de configuration et la machine Linux

### 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 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
```

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
```

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 le fichier **/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 :

```
1 nslookup domain-controller-fqdn
2
3 ping domain-controller-fqdn
4
5 nslookup delivery-controller-fqdn
6
7 ping delivery-controller-fqdn
```

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 (VM) 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 :

```
1 apt-get install chrony
```

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 :

```
1 sudo systemctl restart chrony
```

### Étape 1h : installer OpenJDK 11

Le Linux VDA nécessite la présence d'OpenJDK 11.

Ubuntu 22.04 inclut OpenJDK 11.

Pour installer OpenJDK 11 sur Ubuntu 20.04, exécutez la commande suivante :

```
1 sudo apt-get install -y openjdk-11-jdk
```

### Étape 1i : installer et spécifier la base de données à utiliser

#### Remarque :

- Nous vous recommandons d'utiliser SQLite pour le mode VDI uniquement et d'utiliser PostgreSQL pour un modèle de mise à disposition de bureaux partagés hébergés.
- Pour Easy Install et MCS, vous pouvez spécifier SQLite ou PostgreSQL sans avoir à les installer manuellement. Sauf indication contraire dans **/etc/xdl/db.conf**, le Linux VDA utilise

PostgreSQL par défaut.

- Pour les installations manuelles, vous devez installer SQLite, PostgreSQL ou les deux manuellement. Si vous installez SQLite et PostgreSQL, vous pouvez spécifier l'un d'entre eux à utiliser en modifiant **/etc/xdl/db.conf** après avoir installé le package Linux VDA.

Cette section explique la procédure d'installation de PostgreSQL et SQLite, et comment spécifier l'utilisation de l'un ou l'autre.

**Installer PostgreSQL** Exécutez les commandes suivantes pour installer PostgreSQL :

```
1 sudo apt-get install -y postgresql
2
3 sudo apt-get install -y libpostgresql-jdbc-java
```

Exécutez les commandes suivantes pour démarrer PostgreSQL au démarrage de la machine ou immédiatement, respectivement :

```
1 sudo systemctl enable postgresql
2
3 sudo systemctl restart postgresql
```

**Installer SQLite** Pour Ubuntu, exécutez la commande suivante pour installer SQLite :

```
1 sudo apt-get install -y sqlite3
```

**Spécifier la base de données à utiliser** Si vous installez SQLite et PostgreSQL, vous pouvez spécifier l'un d'entre eux à utiliser en modifiant **/etc/xdl/db.conf** après avoir installé le package Linux VDA.

1. Exécutez **/opt/Citrix/VDA/sbin/ctxcleanup.sh**. Omettez cette étape s'il s'agit d'une nouvelle installation.
2. Modifiez **/etc/xdl/db.conf** pour spécifier la base de données à utiliser.
3. Exécutez le fichier **ctxsetup.sh**.

**Remarque :**

Vous pouvez également utiliser **/etc/xdl/db.conf** pour configurer le numéro de port de PostgreSQL.

### Étape 1j : installer Motif

```
1 sudo apt-get install -y libxm4
```

## Étape 1k : installer les autres packages

Pour Ubuntu 22.04 :

```
1 sudo apt-get install -y libsasl2-2
2 sudo apt-get install -y libsasl2-modules-gssapi-mit
3 sudo apt-get install -y libldap-2.5-0
4 sudo apt-get install -y krb5-user
5 sudo apt-get install -y libgtk2.0-0
```

Pour Ubuntu 20.04 :

```
1 sudo apt-get install -y libsasl2-2
2 sudo apt-get install -y libsasl2-modules-gssapi-mit
3 sudo apt-get install -y libldap-2.4-2
4 sudo apt-get install -y krb5-user
5 sudo apt-get install -y libgtk2.0-0
```

## Étape 2 : préparer l'hyperviseur

Certaines modifications sont requises pour l'exécution du Linux VDA en tant que VM 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 XenServer (anciennement Citrix Hypervisor)

Lorsque la fonctionnalité de synchronisation de l'heure de XenServer est activée, vous rencontrez des problèmes avec NTP et XenServer au sein de chaque machine virtuelle Linux paravirtualisée. 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 XenServer VM Tools installé, vous pouvez vérifier si la fonctionnalité de synchronisation de l'heure de XenServer est présente et activée à partir de la VM Linux :

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
```

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 désactivée, désactivez-la en entrant 1 dans le fichier :

```
1 sudo echo 1 > /proc/sys/xen/independent_wallclock
```

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 :

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
```

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 XenServer (anciennement Citrix Hypervisor), pour lesquels la synchronisation de l'heure de l'hôte 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 VM Linux au domaine Windows

Les méthodes suivantes sont disponibles pour ajouter des machines Linux au domaine Active Directory (AD) :

- [Samba Winbind](#)
- Service d'authentification Quest
- [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

```
1 sudo apt-get install winbind samba libnss-winbind libpam-winbind krb5-config krb5-locales krb5-user
```

**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 :

```
1 sudo systemctl enable winbind
```

**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
```

Dans ce contexte, le paramètre **domain-dns-name** est le nom de domaine DNS, tel que **exemple.com**. L'élément **REALM** est le nom du royaume Kerberos en majuscules, tel que **EXEMPLE.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` en exécutant la commande `vim /etc/samba/smb.conf`, puis définissez les paramètres suivants :

```
[global]
workgroup = WORKGROUP
security = ADS
realm = REALM
```

```
encrypt passwords = yes
idmap config *:range = 16777216-33554431
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
```

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
```

**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
```

#### 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 si la machine est associée à un domaine :

```
1 sudo net ads testjoin
```

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

```
1 sudo net ads info
```

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

```
1 sudo klist -ke
```

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 :

```
1 sudo kinit -k MACHINE$@REALM
```

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 inversée (\) 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 :

```
1 sudo klist
```

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

```
1 sudo net ads status
```

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

```
1 wbinfo --krb5auth=domain\username%password
```

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.

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

```
2
3 id -u
```

**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** :

```
1 ls /tmp/krb5cc_uid
```

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

```
1 klist
```

Quittez la session.

```
1 exit
```

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 :

```
1 reboot
```

**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 :

```
1 sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-  
   interval 32400  
2  
3 sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-  
   auth false
```

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 :

```
1 sudo /opt/quest/bin/vastool configure pam
2
3 sudo /opt/quest/bin/vastool configure nss
```

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

```
1 sudo /opt/quest/bin/vastool -u user join domain-name
```

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.

Redémarrez la machine Linux une fois le domaine rejoint.

**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 :

```
1 sudo /opt/quest/bin/vastool info domain
```

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.

```
1 ssh localhost -l domain\username
2
3 id -u
```

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

```
1 ls /tmp/krb5cc_uid
```

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

```
1 /opt/quest/bin/vastool klist
```

Quittez la session.

```
1 exit
```

Passez à l'[étape 6 : installer le Linux VDA](#) après vérification de la jonction du domaine.

## Centrify DirectControl

**Rejoindre un domaine Windows** Une fois l'agent Centrify DirectControl installé, associez la machine Linux au domaine Active Directory en exécutant la commande Centrify **adjoin** :

```
1 su -
2 adjoin -w -V -u user domain-name
```

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, Windows ou Linux, aient un objet ordinateur dans **Active Directory**. Pour vérifier qu'une machine Linux associée à Centrify se trouve sur le domaine :

```
1 su -
2
3 adinfo
```

Vérifiez que la valeur **Joined to domain** est valide et que le **mode CentrifyDC** 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 :

```
1 adinfo --sysinfo all
2
3 adinfo --diag
```

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

```
1 adinfo --test
```

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 :

```
1 sudo apt-get install krb5-user
```

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 royaume Kerberos en majuscules, tel que `EXEMPLE.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**.

```
1 sudo apt-get install adcli
```

2. Rejoignez le domaine avec **adcli**.

Supprimez l'ancien fichier keytab du système et rejoignez le domaine à l'aide de :

```
1 su -
2
3 rm -rf /etc/krb5.keytab
4
5 adcli join domain-dns-name -U user -H hostname-fqdn
```

**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.

- **Si vous utilisez Samba pour rejoindre le domaine, procédez comme suit :**

1. Installez le pack.

```
1 sudo apt-get install samba krb5-user
```

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.

```
1 sudo net ads join REALM -U user
```

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 :

```
1 sudo apt-get install sssd
```

Si les packages sont déjà installés, une mise à jour est recommandée :

```
1 sudo apt-get install --only-upgrade sssd
```

#### 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 démarer le démon SSSD. Pour certaines versions de SSSD, le fichier de configuration **/etc/sss/sss.conf** n'est pas installé par défaut et doit être créé manuellement. En tant qu'utilisateur racine, créez ou ouvrez **/etc/sss/sss.conf** et configurez les paramètres suivants :

```
[sss]
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`.

Dans ce contexte, le paramètre **domain-dns-name** est le nom de domaine DNS, tel que `exemple.com`. L'élément **REALM** est le nom du royaume Kerberos en majuscules, tel que `EXEMPLE.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
```

**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 :

```
1 sudo systemctl start sssd
2
3 sudo systemctl enable sssd
```

**Configuration de PAM** Exécutez la commande suivante et assurez-vous que les options **SSS authentication** et **Create home directory on login** sont sélectionnées :

```
1 sudo pam-auth-update
```

**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 VDA Linux, vérifiez que le fichier keytab système a été créé et contient des clés valides :

```
1 sudo klist -ke
```

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 :

```
1 sudo kinit -k MACHINE$@REALM
```

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 inversée (\) 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 :

```
1 sudo klist
```

**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.

```
1 ssh localhost -l domain\username
2
3 id -u
4
5 klist
6
7 exit
```

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
```

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

```
1 sudo wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

### Rendre le script d'installation PBIS exécutable

```
1 sudo chmod +x pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

### Exécuter le script d'installation PBIS

```
1 sudo sh pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

**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 /opt/pbis/bin/domainjoin-cli join domain-name user
```

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 :

```
1 /opt/pbis/bin/domainjoin-cli query
```

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.

```
1 sudo ssh localhost -l domain\user
2
3 id -u
```

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

```
1 ls /tmp/krb5cc_uid
```

Quittez la session.

```
1 exit
```

Passez à l'[étape 6 : installer le Linux VDA](#) après vérification de la jonction du domaine.

## Étape 4 : installer .NET Runtime 6.0

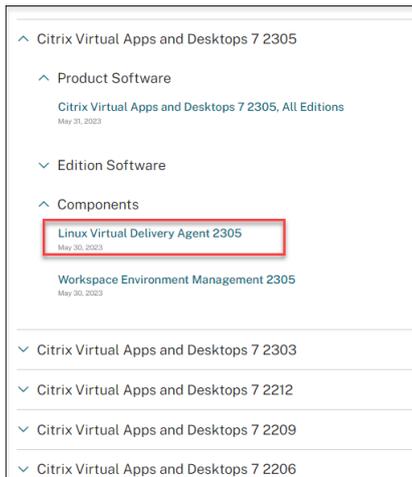
Avant d'installer Linux VDA, installez .NET Runtime 6.0 conformément aux instructions de l'article <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers>.

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

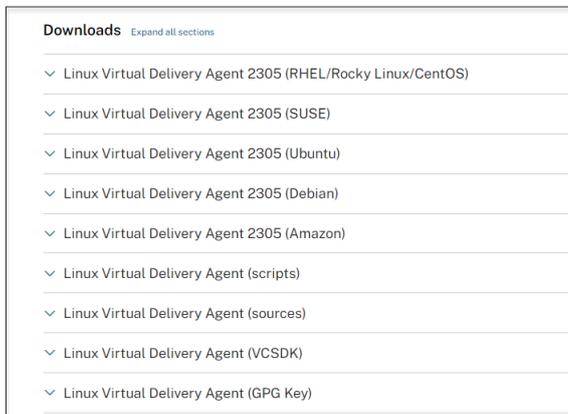
En fonction de la sortie de la commande, définissez le chemin binaire de .NET Runtime. Par exemple, si la sortie de la commande est /aa/bb/dotnet, utilisez /aa/bb comme chemin binaire .NET.

## 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. Développez **Components** pour trouver le Linux VDA. Par exemple :

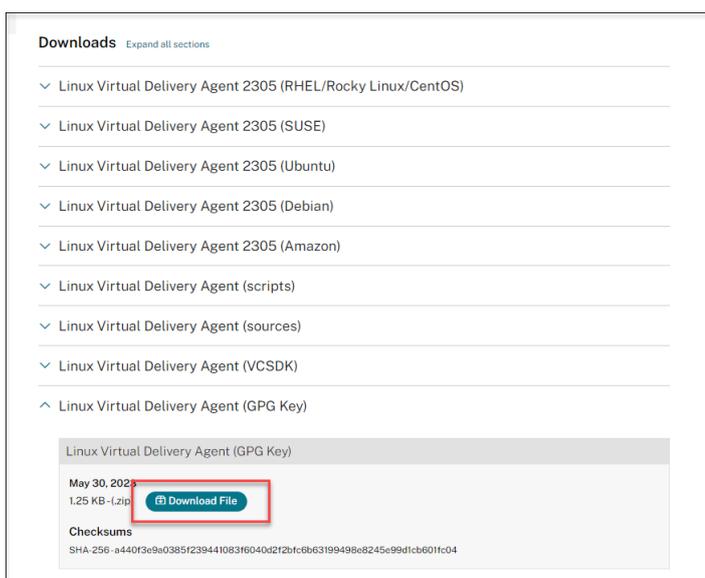


4. Cliquez sur le lien Linux VDA pour accéder aux téléchargements de Linux VDA.



5. Téléchargez le package Linux VDA correspondant à votre distribution Linux.

6. Téléchargez la clé publique GPG que vous pouvez utiliser pour vérifier l'intégrité du package Linux VDA. Par exemple :



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

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

## 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 :

```
1 sudo dpkg -i <PATH>/<Linux VDA DEB>
2 apt-get install -f
```

#### Remarque :

Pour Ubuntu 20.04 sur GCP, désactivez RDNS. Pour ce faire, ajoutez la ligne **rdns = false** sous **[libdefaults]** dans `/etc/krb5.conf`.

### Liste des dépendances Debian pour Ubuntu 22.04 :

```
1 openjdk-11-jdk >= 11
2
3 imagemagick >= 8:6.9.11
4
5 libgtkmm-3.0-1v5 >= 3.24.5
6
7 ufw >= 0.36
8
```

```
9  ubuntu-desktop >= 1.481
10
11  libxrandr2 >= 2:1.5.2
12
13  libxtst6 >= 2:1.2.3
14
15  libxm4 >= 2.3.8
16
17  util-linux >= 2.37
18
19  gtk3-nocsd >= 3
20
21  bash >= 5.1
22
23  findutils >= 4.8.0
24
25  sed >= 4.8
26
27  cups >= 2.4
28
29  libmspack0 >= 0.10
30
31  ibus >= 1.5
32
33  libgoogle-perftools4 >= 2.9~
34
35  libpython3.10 >= 3.10~
36
37  libsasl2-modules-gssapi-mit >= 2.1.~
38
39  libnss3-tools >= 2:3.68
40
41  libqt5widgets5 >= 5.15~
42
43  libqrencode4 >= 4.1.1
44
45  libimlib2 >= 1.7.4
```

**Liste des dépendances Debian pour Ubuntu 20.04 :**

```
1  openjdk-11-jdk >= 11
2
3  imagemagick >= 8:6.9.10
4
5  libgtkmm-3.0-1v5 >= 3.24.2
6
7  ufw >= 0.36
8
9  ubuntu-desktop >= 1.450
10
11  libxrandr2 >= 2:1.5.2
12
13  libxtst6 >= 2:1.2.3
```

```
14
15 libxm4 >= 2.3.8
16
17 util-linux >= 2.34
18
19 gtk3-nocsd >= 3
20
21 bash >= 5.0
22
23 findutils >= 4.7.0
24
25 sed >= 4.7
26
27 cups >= 2.3
28
29 libmspack0 >= 0.10
30
31 ibus >= 1.5
32
33 libgoogle-perftools4 >= 2.7~
34
35 libpython3.8 >= 3.8~
36
37 libsasl2-modules-gssapi-mit >= 2.1.~
38
39 libnss3-tools >= 2:3.49
40
41 libqt5widgets5 >= 5.7~
42
43 libqrencode4 >= 4.0.0
44
45 libimlib2 >= 1.6.1
```

**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)**

Le Linux VDA prend en charge les mises à niveau depuis la version la plus récente. Par exemple, vous pouvez mettre à niveau le Linux VDA de 2308 à 2311 et de 1912 LTSR à 2203 LTSR.

```
1 sudo dpkg -i <PATH>/<Linux VDA deb>
```

**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 :

- [XenServer](#)
- [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

### 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 sur 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**.

Après l'installation du package, vous devez configurer le VDA Linux 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 pré-configurées. Consultez l'aide sur le script avant de continuer :

```
1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
```

### Configuration avec invites

Exécutez une configuration manuelle avec questions :

```
1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

## 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\_NON\_DOMAIN\_JOINED='Y|N'** : indique s'il faut associer la machine à un domaine . La valeur par défaut est "n". Pour les scénarios liés à un domaine, définissez la valeur sur "n".
- **CTX\_XDL\_AD\_INTEGRATION='winbind|sssd|centrify|pbis|quest'** : 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.
- **CTX\_XDL\_DDC\_LIST='<list-ddc-fqdns>'** : 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\_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\_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 VDA doit être configuré pour le mode Bureaux VDI (session unique), c'est-à-dire, CTX\_XDL\_VDI\_MODE='y'.
- **CTX\_XDL\_START\_SERVICE='y|n'** : indique si les services Linux VDA sont lancés une fois la configuration de Linux VDA terminée.
- **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 Virtual Desktop 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\_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 par défaut configuré sur le VDA est utilisé.

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**

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

– **Pour le bureau GNOME Classic**

```
1 GSESSION="$(type -p gnome-session)"
2 if [ -n "$GSESSION" ]; then
3     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\_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 service Broker Agent. Le chemin d'accès par défaut est `/usr/bin`.
- **CTX\_XDL\_VDA\_PORT=port-number** : le Linux VDA communique avec les composants Delivery Controller via un port TCP/IP.
- **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. Pour accélérer les requêtes LDAP dans une forêt Active directory, 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\_SUPPORT\_DDC\_AS\_CNAME='y|n'** : le Linux VDA prend en charge la spécification d'un nom de composant Delivery Controller à l'aide d'un enregistrement DNS CNAME.

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

```

1 export CTX_XDL_NON_DOMAIN_JOINED='n'
2 export CTX_XDL_AD_INTEGRATION=winbind|centrify|sssd|pbis|quest
3 export CTX_XDL_DDC_LIST='<list-ddc-fqdns>'
4 export CTX_XDL_VDI_MODE='y|n'
5 export CTX_XDL_HDX_3D_PRO='y|n'
6 export CTX_XDL_START_SERVICE='y|n'
7 export CTX_XDL_REGISTER_SERVICE='y|n'
8 export CTX_XDL_ADD_FIREWALL_RULES='y|n'
9 export CTX_XDL_DESKTOP_ENVIRONMENT= gnome|gnome-classic|mate|'<none>'
10 export CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime>'
11 export CTX_XDL_VDA_PORT='<port-number>'
12 export CTX_XDL_SITE_NAME='<dns-site-name>'|'<none>'
13 export CTX_XDL_LDAP_LIST='<list-ldap-servers>'|'<none>'
14 export CTX_XDL_SEARCH_BASE='<search-base-set>'|'<none>'
15 export CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n'
16 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh --silent

```

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_NON_DOMAIN_JOINED='n' \
2 CTX_XDL_AD_INTEGRATION=winbind|centrify|sssd|pbis|quest \
3 CTX_XDL_DDC_LIST='<list-ddc-fqdns>' \
4 CTX_XDL_VDI_MODE='y|n' \
5 CTX_XDL_HDX_3D_PRO='y|n' \
6 CTX_XDL_START_SERVICE='y|n' \

```

```
7 CTX_XDL_REGISTER_SERVICE='y|n' \  
8 CTX_XDL_ADD_FIREWALL_RULES='y|n' \  
9 CTX_XDL_DESKTOP_ENVIRONMENT= gnome|gnome-classic|mate|'<none>' \  
10 CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime>' \  
11 CTX_XDL_VDA_PORT='<port-number>' \  
12 CTX_XDL_SITE_NAME='<dns-site-name>'|'<none>' \  
13 CTX_XDL_LDAP_LIST='<list-ldap-servers>'|'<none>' \  
14 CTX_XDL_SEARCH_BASE='<search-base-set>'|'<none>' \  
15 CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n' \  
16 /opt/Citrix/VDA/sbin/ctxsetup.sh --silent
```

## 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
```

Pour supprimer les modifications de configuration :

```
1 sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
```

### 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.config.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
```

Pour afficher des informations plus détaillées :

```
1 apt-cache show xendesktopvda
```

Pour désinstaller le logiciel Linux VDA :

```
1 dpkg -r xendesktopvda
```

**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 :

```
1 sudo systemctl start ctxhdx
2
3 sudo systemctl start ctxvda
```

**Arrêter Linux VDA :**

Pour arrêter les services Linux VDA :

```
1 sudo systemctl stop ctxvda
2
3 sudo systemctl stop ctxhdx
```

**Remarque :**

Avant d'arrêter les services `ctxvda` et `ctxhdx`, exécutez la commande `systemctl stop ctxmonitord` 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 systemctl stop ctxvda
2
3 sudo systemctl restart ctxhdx
4
5 sudo systemctl restart ctxvda
```

### Vérifier l'état de Linux VDA :

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

```
1 sudo systemctl status ctxvda
2
3 sudo systemctl status ctxhdx
```

## Étape 11 : créer des catalogues de machines

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 vous 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 des groupes de mise à disposition

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 2311](#).

## Installer le Linux VDA manuellement sur Debian

August 21, 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 les informations de configuration et la machine Linux

### Étape 1a : 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 1b : 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 1c : vérifier le nom d'hôte

Redémarrez l'ordinateur et vérifiez que le nom d'hôte est correctement configuré :

```
1 hostname
```

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
```

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

### Étape 1d : 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 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 :

```
1 nslookup domain-controller-fqdn
2
3 ping domain-controller-fqdn
4
5 nslookup delivery-controller-fqdn
6
7 ping delivery-controller-fqdn
```

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 (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 (VM) 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 :

```
1 apt-get install chrony
```

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 :

```
1 sudo systemctl restart chrony
```

### Étape 1g : installer les packages

```
1 sudo apt-get install -y libsasl2-2
2
3 sudo apt-get install -y libgtk2.0-0
```

### Étape 1h : ajouter des référentiels pour installer les dépendances nécessaires

Pour Debian 11, ajoutez la ligne `deb http://deb.debian.org/debian/ bullseye main` au fichier `/etc/apt/sources.list`.

### Étape 1i : installer et spécifier la base de données à utiliser

#### Remarque :

- Nous vous recommandons d'utiliser SQLite pour le mode VDI uniquement et d'utiliser PostgreSQL pour un modèle de mise à disposition de bureaux partagés hébergés.
- Pour Easy Install et MCS, vous pouvez spécifier SQLite ou PostgreSQL sans avoir à les installer manuellement. Sauf indication contraire dans `/etc/xdl/db.conf`, le Linux VDA utilise PostgreSQL par défaut.
- Pour les installations manuelles, vous devez installer SQLite, PostgreSQL ou les deux manuellement. Si vous installez SQLite et PostgreSQL, vous pouvez spécifier l'un d'entre eux à utiliser en modifiant `/etc/xdl/db.conf` après avoir installé le package Linux VDA.

Cette section explique la procédure d'installation de PostgreSQL et SQLite, et comment spécifier l'utilisation de l'un ou l'autre.

### Installer PostgreSQL

 Exécutez les commandes suivantes pour installer PostgreSQL :

```
1 sudo apt-get update
2
3 sudo apt-get install -y postgresql
4
5 sudo apt-get install -y libpostgresql-jdbc-java
```

Exécutez les commandes suivantes pour démarrer PostgreSQL au démarrage de la machine ou immédiatement, respectivement :

```
1 sudo systemctl enable postgresql
2
3 sudo systemctl start postgresql
```

**Installer SQLite** Pour Debian, exécutez la commande suivante pour installer SQLite :

```
1 sudo apt-get install -y sqlite3
```

**Spécifier la base de données à utiliser** Si vous installez SQLite et PostgreSQL, vous pouvez spécifier l'un d'entre eux à utiliser en modifiant `/etc/xdl/db.conf` après avoir installé le package Linux VDA.

1. Exécutez `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omettez cette étape s'il s'agit d'une nouvelle installation.
2. Modifiez `/etc/xdl/db.conf` pour spécifier la base de données à utiliser.
3. Exécutez le fichier `ctxsetup.sh`.

**Remarque :**

Vous pouvez également utiliser `/etc/xdl/db.conf` pour configurer le numéro de port de PostgreSQL.

## Étape 2 : préparer l'hyperviseur

Certaines modifications sont requises pour l'exécution du Linux VDA en tant que VM 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 XenServer (anciennement Citrix Hypervisor)

Lorsque la fonctionnalité de synchronisation de l'heure de XenServer est activée, vous rencontrez des problèmes avec NTP et XenServer au sein de chaque machine virtuelle Linux paravirtualisée. 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 XenServer VM Tools installé, vous pouvez vérifier si la fonctionnalité de synchronisation de l'heure de XenServer est présente et activée à partir de la VM Linux :

```
1 su -
2 cat /proc/sys/xen/independent_wallclock
```

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 désactivée, désactivez-la en entrant 1 dans le fichier :

```
1 sudo echo 1 > /proc/sys/xen/independent_wallclock
```

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 :

```
1 su -
2 cat /proc/sys/xen/independent_wallclock
```

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 XenServer (anciennement 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 VM Linux au domaine Windows

Les méthodes suivantes sont disponibles pour ajouter des machines Linux au domaine Active Directory (AD) :

- [Samba Winbind](#)
- Service d'authentification Quest
- [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

```
1 sudo apt-get install winbind samba libnss-winbind libpam-winbind krb5-config krb5-locales krb5-user
```

**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 :

```
1 sudo systemctl enable winbind
```

**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
```

Dans ce contexte, le paramètre **domain-dns-name** est le nom de domaine DNS, tel que **exemple.com**. L'élément **REALM** est le nom du royaume Kerberos en majuscules, tel que **EXEMPLE.COM**.

**Configurer l'authentification Winbind** Ouvrez `/etc/samba/smb.conf` en exécutant la commande `vim /etc/samba/smb.conf`, puis définissez les paramètres suivants :

```
[global]
workgroup = WORKGROUP
security = ADS
realm = REALM
encrypt passwords = yes
idmap config *:range = 16777216-33554431
```

```
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: files systemd winbind
```

```
group: files 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 :

```
1 sudo net ads join <Kerberos realm name in uppercase> -U <domain user  
with permission to add computers to the domain>
```

#### Redémarrer Winbind

```
1 sudo systemctl restart winbind
```

**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
```

#### 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 si la machine est associée à un domaine :

```
1 sudo net ads testjoin
```

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

```
1 sudo net ads info
```

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

```
1 sudo klist -ke
```

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 :

```
1 sudo kinit -k MACHINE$@REALM
```

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 inversée (\) 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 :

```
1 sudo klist
```

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

```
1 sudo net ads status
```

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

```
1 wbinfo --krb5auth=domain\username%password
```

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.

```
1 ssh localhost -l domain\username
2
3 id -u
```

**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** :

```
1 ls /tmp/krb5cc_uid
```

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

```
1 klist
```

Quittez la session.

```
1 exit
```

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 :

```
1 reboot
```

### 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 :

```
1 sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-  
interval 32400  
2  
3 sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-  
auth false
```

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 :

```
1 sudo /opt/quest/bin/vastool configure pam  
2  
3 sudo /opt/quest/bin/vastool configure nss
```

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

```
1 sudo /opt/quest/bin/vastool -u user join domain-name
```

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.

Redémarrez la machine Linux une fois le domaine rejoint.

**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 :

```
1 sudo /opt/quest/bin/vastool info domain
```

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.

```
1 ssh localhost -l domain\username  
2  
3 id -u
```

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

```
1 ls /tmp/krb5cc_uid
```

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

```
1 /opt/quest/bin/vastool klist
```

Quittez la session.

```
1 exit
```

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` :

```
1 su -
2 adjoin -w -V -u user domain-name
```

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, Windows ou Linux, aient un objet ordinateur dans Active Directory. Pour vérifier qu'une machine Linux associée à Centrify se trouve sur le domaine :

```
1 su -
2
3 adinfo
```

Vérifiez que la valeur **Joined to domain** est valide et que le **mode CentrifyDC** 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 :

```
1 adinfo --sysinfo all
2
3 adinfo --diag
```

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

```
1 adinfo --test
```

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 :

```
1 sudo apt-get install krb5-user
```

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
rdns = 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 royaume Kerberos en majuscules, tel que `EXEMPLE.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**.

```
1 sudo apt-get install adcli
```

2. Rejoignez le domaine avec **adcli**.

Supprimez l'ancien fichier keytab du système et rejoignez le domaine à l'aide de :

```
1 su -
2
3 rm -rf /etc/krb5.keytab
4
5 adcli join domain-dns-name -U user -H hostname-fqdn
```

**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.

```
1 sudo apt-get install samba krb5-user
```

##### 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.

```
1 sudo net ads join <the Kerberos realm name in uppercase> -U <
  domain user with permission to add computers to the domain>
```

**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 :

```
1 sudo apt-get install sssd
```

Si les packages sont déjà installés, une mise à jour est recommandée :

```
1 sudo apt-get install --only-upgrade sssd
```

**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/sss/sss.conf` n'est pas installé par défaut et doit être créé manuellement. En tant qu'utilisateur racine, créez ou ouvrez `/etc/sss/sss.conf` et configurez les paramètres suivants :

```
[sss]
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`.

Dans ce contexte, le paramètre **domain-dns-name** est le nom de domaine DNS, tel que `exemple.com`. L'élément *REALM* est le nom du royaume Kerberos en majuscules, tel que `EXEMPLE.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
```

**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 :

```
1 sudo systemctl start sssd
2
3 sudo systemctl enable sssd
```

**Configuration de PAM** Exécutez la commande suivante et assurez-vous que les options **SSS authentication** et **Create home directory on login** sont sélectionnées :

```
1 sudo pam-auth-update
```

**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 VDA Linux, vérifiez que le fichier keytab système a été créé et contient des clés valides :

```
1 sudo klist -ke
```

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 :

```
1 sudo kinit -k MACHINE$@REALM
```

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 inversée (\) 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 :

```
1 sudo klist
```

**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.

```
1 ssh localhost -l domain\username
2
3 id -u
4
5 klist
6
7 exit
```

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
```

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

```
1 sudo wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

### Rendre le script d'installation PBIS exécutable

```
1 sudo chmod +x pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

### Exécuter le script d'installation PBIS

```
1 sudo sh pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

**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 /opt/pbis/bin/domainjoin-cli join domain-name user
```

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 :

```
1 /opt/pbis/bin/domainjoin-cli query
```

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.

```
1 sudo ssh localhost -l domain\user
2
3 id -u
```

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

```
1 ls /tmp/krb5cc_uid
```

Quittez la session.

```
1 exit
```

Passez à l'[étape 6 : installer le Linux VDA](#) après vérification de la jonction du domaine.

## Étape 4 : installer .NET Runtime 6.0

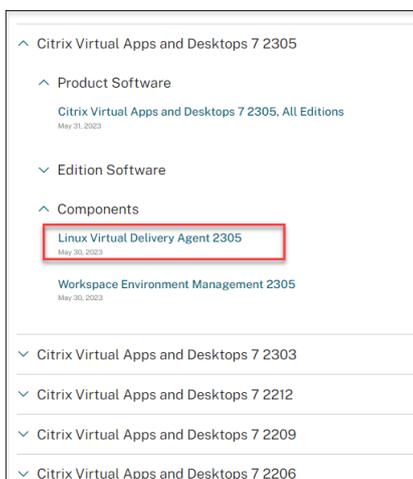
Avant d'installer Linux VDA, installez .NET Runtime 6.0 conformément aux instructions de l'article <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers>.

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

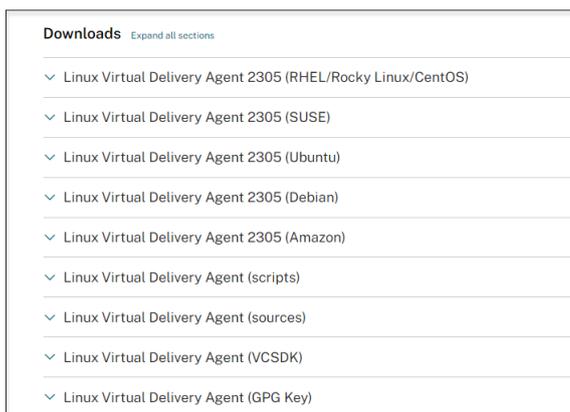
En fonction de la sortie de la commande, définissez le chemin binaire de .NET Runtime. Par exemple, si la sortie de la commande est /aa/bb/dotnet, utilisez /aa/bb comme chemin binaire .NET.

## 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. Développez **Components** pour trouver le Linux VDA. Par exemple :

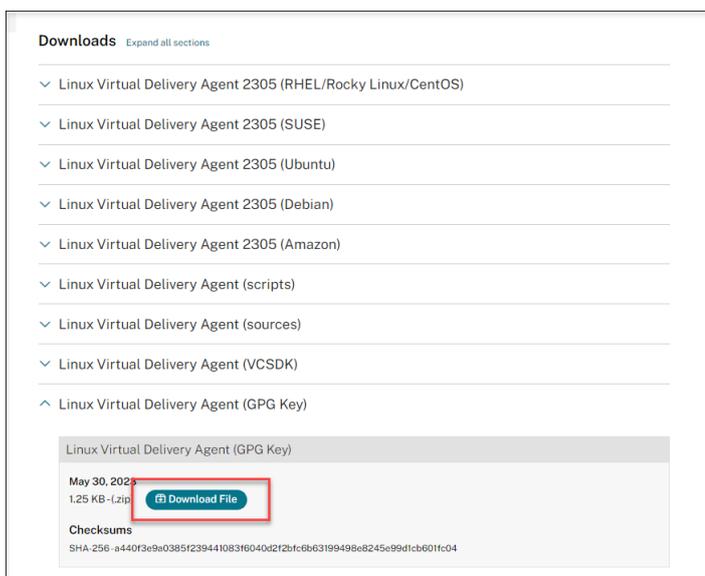


4. Cliquez sur le lien Linux VDA pour accéder aux téléchargements de Linux VDA.



5. Téléchargez le package Linux VDA correspondant à votre distribution Linux.

6. Téléchargez la clé publique GPG que vous pouvez utiliser pour vérifier l'intégrité du package Linux VDA. Par exemple :



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

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

## 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 :

```
1 sudo dpkg -i xendesktopvda_<version>.debian11_amd64.deb
```

**Liste des dépendances pour Debian 11 :**

```
1 libnss3-tools >= 2:3.61
2
3 libfuse2 >= 2.9
4
5 openjdk-11-jdk >= 11
6
7 imagemagick >= 8:6.9.10
8
9 ufw >= 0.36
10
11 desktop-base >= 10.0.2
12
13 libxrandr2 >= 2:1.5.1
14
15 libxtst6 >= 2:1.2.3
16
17 libxm4 >= 2.3.8
18
19 util-linux >= 2.33
20
21 gtk3-nocsd >= 3
22
23 bash >= 5.0
24
25 findutils >= 4.6.0
26
27 sed >= 4.7
28
29 cups >= 2.2
30
31 ghostscript >= 9.53~
32
33 libmspack0 >= 0.10
34
35 ibus >= 1.5
36
37 libgoogle-perftools4 >= 2.7~
38
39 libpython3.9 >= 3.9~
40
41 libsasl2-modules-gssapi-mit >= 2.1.~
42
43 libqt5widgets5 >= 5.5~
44
45 mutter >= 3.38.6~
46
47 libqrencode4 >= 4.0.0
48
49 libimlib2 >= 1.5.1
```

**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)

Le Linux VDA prend en charge les mises à niveau depuis la version la plus récente. Par exemple, vous pouvez mettre à niveau le Linux VDA de 2308 à 2311 et de 1912 LTSR à 2203 LTSR.

```
1 sudo dpkg -i <PATH>/<Linux VDA deb>
```

**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 :

- [XenServer](#)
- [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

**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 sur 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**.

Après l'installation du package, vous devez configurer le VDA Linux 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 pré-configurées. Consultez l'aide sur le script avant de continuer :

```
1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
```

### Configuration avec invites

Exécutez une configuration manuelle avec questions :

```
1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

### 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\_NON\_DOMAIN\_JOINED='Y|N'** : indique s'il faut associer la machine à un domaine . La valeur par défaut est "n". Pour les scénarios liés à un domaine, définissez la valeur sur "n".
- **CTX\_XDL\_AD\_INTEGRATION='winbind|sssd|centrify|pbis|quest'** : 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.
- **CTX\_XDL\_DDC\_LIST='<list-ddc-fqdns>'** : 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\_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\_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 VDA doit être configuré pour le mode Bureaux VDI (session unique), c'est-à-dire, CTX\_XDL\_VDI\_MODE='y'.
- **CTX\_XDL\_START\_SERVICE='y|n'** : indique si les services Linux VDA sont lancés une fois la configuration de Linux VDA terminée.
- **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 Virtual Desktop 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\_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 par défaut configuré sur le VDA est utilisé.

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**

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

– **Pour le bureau GNOME Classic**

```
1 GSESSION="$(type -p gnome-session)"
2 if [ -n "$GSESSION" ]; then
3     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\_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 service Broker Agent. Le chemin d'accès par défaut est `/usr/bin`.
- **CTX\_XDL\_VDA\_PORT=***port-number* : le Linux VDA communique avec les composants Delivery Controller via un port TCP/IP.
- **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`. Pour accélérer les requêtes LDAP dans une forêt Active directory, 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\_SUPPORT\_DDC\_AS\_CNAME='y|n'** : le Linux VDA prend en charge la spécification d'un nom de composant Delivery Controller à l'aide d'un enregistrement DNS CNAME.

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

```

1 export CTX_XDL_NON_DOMAIN_JOINED='n'
2 export CTX_XDL_AD_INTEGRATION=winbind|centrify|sssd|pbis|quest
3 export CTX_XDL_DDC_LIST='<list-ddc-fqdns>'
4 export CTX_XDL_VDI_MODE='y|n'
5 export CTX_XDL_HDX_3D_PRO='y|n'

```

```

6 export CTX_XDL_START_SERVICE='y|n'
7 export CTX_XDL_REGISTER_SERVICE='y|n'
8 export CTX_XDL_ADD_FIREWALL_RULES='y|n'
9 export CTX_XDL_DESKTOP_ENVIRONMENT= gnome|gnome-classic|mate| '<none>'
10 export CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime>'
11 export CTX_XDL_VDA_PORT='<port-number>'
12 export CTX_XDL_SITE_NAME='<dns-site-name>' | '<none>'
13 export CTX_XDL_LDAP_LIST='<list-ldap-servers>' | '<none>'
14 export CTX_XDL_SEARCH_BASE='<search-base-set>' | '<none>'
15 export CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n'
16 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh --silent

```

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_NON_DOMAIN_JOINED='n' \
2 CTX_XDL_AD_INTEGRATION=winbind|centrify|sssd|pbis|quest \
3 CTX_XDL_DDC_LIST='<list-ddc-fqdns>' \
4 CTX_XDL_VDI_MODE='y|n' \
5 CTX_XDL_HDX_3D_PRO='y|n' \
6 CTX_XDL_START_SERVICE='y|n' \
7 CTX_XDL_REGISTER_SERVICE='y|n' \
8 CTX_XDL_ADD_FIREWALL_RULES='y|n' \
9 CTX_XDL_DESKTOP_ENVIRONMENT= gnome|gnome-classic|mate| '<none>' \
10 CTX_XDL_DOTNET_RUNTIME_PATH='<path-to-install-dotnet-runtime>' \
11 CTX_XDL_VDA_PORT='<port-number>' \
12 CTX_XDL_SITE_NAME='<dns-site-name>' | '<none>' \
13 CTX_XDL_LDAP_LIST='<list-ldap-servers>' | '<none>' \
14 CTX_XDL_SEARCH_BASE='<search-base-set>' | '<none>' \
15 CTX_XDL_SUPPORT_DDC_AS_CNAME='y|n' \
16 /opt/Citrix/VDA/sbin/ctxsetup.sh --silent

```

## 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
```

Pour supprimer les modifications de configuration :

```
1 sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
```

**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
```

Pour afficher des informations plus détaillées :

```
1 apt-cache show xendesktopvda
```

Pour désinstaller le logiciel Linux VDA :

```
1 dpkg -r xendesktopvda
```

**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 :

```
1 sudo systemctl start ctxhdx
2
3 sudo systemctl start ctxvda
```

### Arrêter Linux VDA :

Pour arrêter les services Linux VDA :

```
1 sudo systemctl stop ctxvda
2
3 sudo systemctl stop ctxhdx
```

#### Remarque :

Avant d'arrêter les services **ctxvda** et **ctxhdx**, exécutez la commande **systemctl stop ctxmonitord** 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 systemctl stop ctxvda
2
3 sudo systemctl restart ctxhdx
4
5 sudo systemctl restart ctxvda
```

### Vérifier l'état de Linux VDA :

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

```
1 sudo systemctl status ctxvda
2
3 sudo systemctl status ctxhdx
```

## Étape 11 : créer des catalogues de machines

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 vous 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 des groupes de mise à disposition

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 2311](#).

## Configurer

August 20, 2024

Cette section détaille les fonctionnalités du Linux VDA, notamment la description des fonctionnalités, la configuration et le dépannage.

## Administration

August 20, 2024

Cette section contient les rubriques suivantes :

- [Programme de collecte de données Linux VDA](#)
- [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](#)
- [Dépannage](#)
- [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 de collecte de données Linux VDA

August 21, 2024

Vous participez automatiquement au programme de collecte de données après avoir installé le Linux VDA. Le programme de collecte de données collecte des statistiques et des données d'utilisation et les envoie à Citrix Analytics pour améliorer la qualité et les performances des produits Citrix. Le chargement des données a lieu lorsque vous lancez une session.

### Paramètres de registre

Le programme de collecte de données Linux VDA est activé par défaut. Vous pouvez activer ou désactiver le programme via les paramètres de registre suivants :

**Emplacement** : HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\CEIP

**Nom** : CEIPSwitch

**Valeur** : 1 = désactivé, 0 = activé (par défaut)

Lorsqu'il n'est pas spécifié, le programme de collecte de données Linux VDA est activé.

Vous pouvez exécuter la commande suivante pour désactiver le programme de collecte de données Linux VDA :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP" -v "CEIPSwitch" -d "1"
```

### Données collectées depuis le Linux VDA

Le tableau suivant présente des exemples de types de données collectées.

Point de données	Nom de la clé	Description
GUID de machine	<b>machine_guid</b>	Chaîne GUID identifiant la machine d'où les données proviennent
Version et nom du système d'exploitation Linux	<b>os_name_version</b>	Chaîne indiquant le nom et la version du système d'exploitation Linux de la machine

Point de données	Nom de la clé	Description
Solution Active Directory	<b>ad_solution</b>	Chaîne indiquant la méthode de jonction du domaine de la machine
Version du noyau Linux	<b>kernel_version</b>	Chaîne indiquant la version du noyau de la machine
Type de GPU	<b>gpu_type</b>	Indique le type de processeur graphique de la machine
Cœurs d'UC	<b>cpu_cores</b>	Entier indiquant le nombre de cœurs d'UC de la machine
Fréquence du processeur	<b>cpu_frequency</b>	Nombre flottant indiquant la fréquence du processeur en MHz
Taille de la mémoire physique	<b>memory_size</b>	Entier indiquant la taille de la mémoire physique en Ko
Version LVDA	<b>vda_version</b>	Chaîne indiquant la version installée du Linux VDA.
Mise à jour LVDA ou nouvelle installation	<b>update_or_fresh_install</b>	Chaîne indiquant que le package Linux VDA actuel est en cours de mise à jour ou d'installation
Mode VDI activé ou non	<b>vdi_mode</b>	Chaîne indiquant si le mode VDI est activé
<b>Méthode d'installation de LVDA</b>	install_method	Chaîne 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	<b>hdx_3d_pro</b>	Chaîne indiquant si HDX 3D Pro est activé sur la machine
BCR activé ou non	<b>bcr</b>	Chaîne indiquant si la redirection du contenu du navigateur (BCR) est activée sur cette machine
Paramètres régionaux système	<b>system_locale</b>	Chaîne indiquant les paramètres régionaux de cette machine
Identifiant de la batterie de serveurs	<b>farm_id</b>	Chaîne indiquant l'identifiant de la batterie de serveurs.

Point de données	Nom de la clé	Description
Type de virtualisation du VDA	<b>vda_virtualisation</b>	Chaîne indiquant l'hyperviseur qui a créé le VDA
Clé de session	<b>session_key</b>	Identification de la session d'où les données proviennent
Type de ressource	<b>resource_type</b>	Chaîne indiquant le type de ressource de la session lancée : bureau ou <appname>
Type de client Receiver	<b>receiver_type</b>	Entier indiquant le type d'application Citrix Workspace utilisé pour lancer la session
Version du client Receiver	<b>receiver_version</b>	Chaîne indiquant la version de l'application Citrix Workspace utilisée pour lancer la session
Nombre d'impressions	<b>printing_count</b>	Entier indiquant le nombre de fois que la session utilise la fonction d'impression
Nombre de redirections USB	<b>usb_redirecting_count</b>	Entier indiquant le nombre de fois que la session utilise un périphérique USB
Type de fournisseur <b>Gfx</b>	<b>gfx_provider_type</b>	Chaîne indiquant le type de fournisseur de graphiques de la session
Nombre d'observations	<b>shadow_count</b>	Entier indiquant le nombre de fois que la session a été observée
Langue sélectionnée par l'utilisateur	<b>ctxism_select</b>	Chaîne longue composée contenant toutes les langues sélectionnées par les utilisateurs
Nombre de redirections de carte à puce	<b>scard_redirecting_count</b>	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

Point de données	Nom de la clé	Description
Type de codec vidéo	<b>type_code_vidéo_graphique</b>	Chaîne indiquant le codec vidéo utilisé pour Thinwire.
Type d'identifiant d'ouverture de session	<b>credentials_type</b>	Entier indiquant le type d'informations d'identification utilisé pour se connecter au Linux VDA
Filigrane	<b>Filigrane</b>	Chaîne indiquant si le filigrane de session est activé ou non
Transparence du filigrane	<b>watermark_transparency</b>	Entier indiquant la transparence du filigrane
<b>Longueur du texte personnalisé dans un filigrane</b>	<b>watermark_custom_text_len</b>	Entier indiquant la longueur du texte personnalisé dans un filigrane
MTU	<b>mtu</b>	Chaîne indiquant si l'unité de transmission maximale (MTU) est utilisée dans cette session
MTU MSS	<b>mtu_mss</b>	Entier indiquant la taille maximale des segments (MSS)
Transfert de fichiers	<b>filetrans</b>	Entier indiquant les paramètres de la stratégie de transfert de fichiers
Nombre de chargements et transferts de fichiers	<b>filetrans_upload_count</b>	Entier indiquant le nombre de fois que l'icône « Charger » est utilisée pour les transferts de fichiers au cours de la session
Nombre de téléchargements et transferts de fichiers	<b>filetrans_download_count</b>	Entier indiquant le nombre de fois que l'icône « Télécharger » est utilisée pour les transferts de fichiers au cours de la session

---

## HDX Insight

August 20, 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
```

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
  VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP" -d "0x00000001"
  --force
```

## Dépannage

### 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.

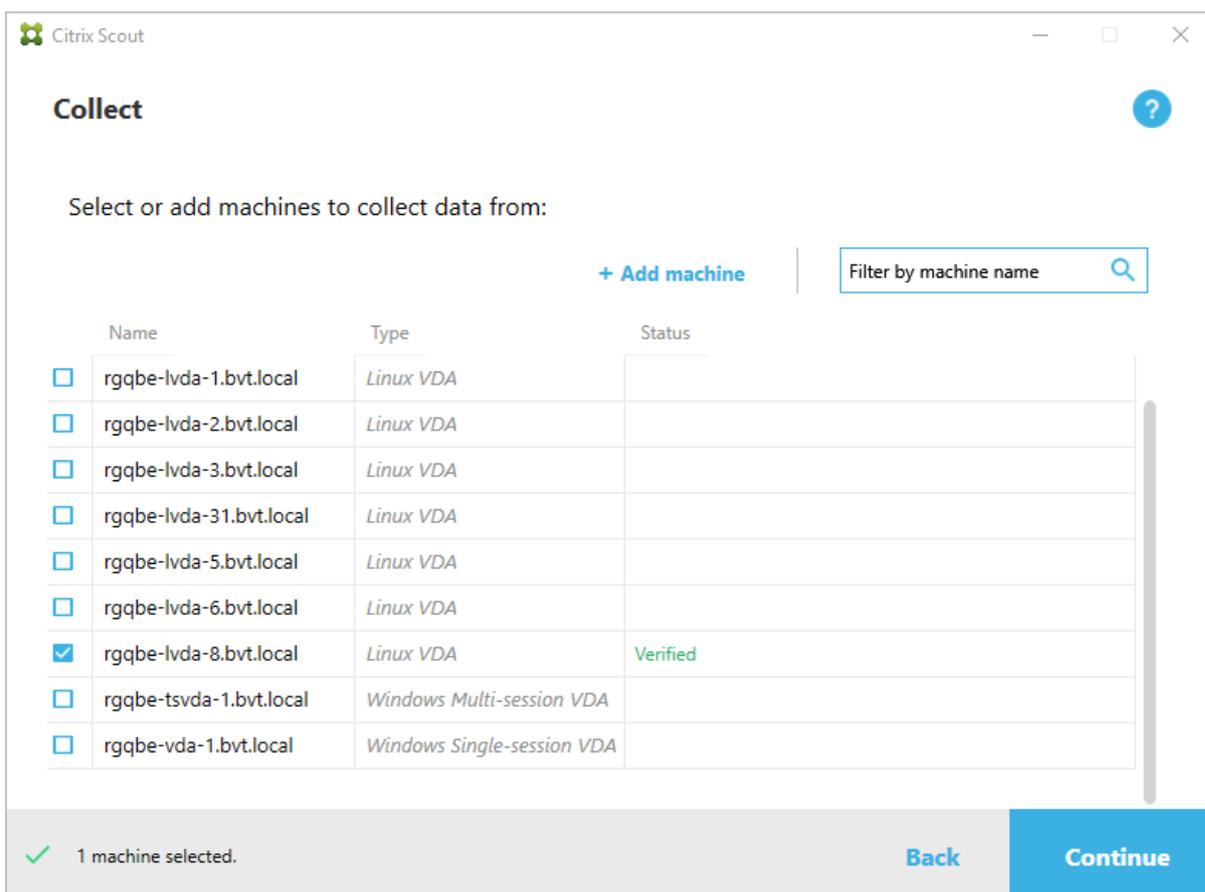
### Aucun point de données d'application n'est affiché

Vérifiez que le canal virtuel transparent est activé et qu'une application transparente est exécutée.

## Intégration avec Citrix Telemetry Service

August 20, 2024

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.



### 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.

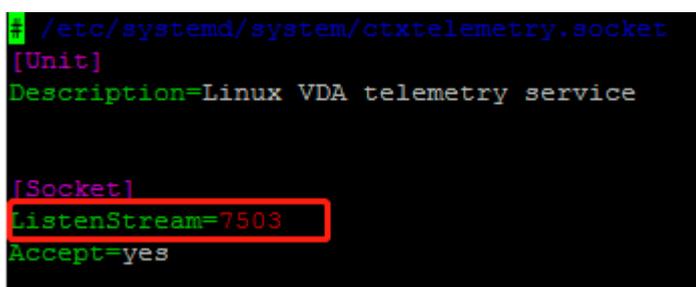
Pour modifier les ports après avoir installé votre VDA, procédez comme suit :

1. Pour modifier un port de communication avec Scout, exécutez la commande suivante.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent" -t REG_DWORD -v "TelemetryServicePort" -d <port number> --force
```

2. Pour modifier le port de socket pour l'écoute de Scout, exécutez la commande suivante pour ouvrir et modifier le fichier `ctxtelemetry.socket`.

```
1 sudo vi /etc/systemd/system/ctxtelemetry.socket
```



```
1 /etc/systemd/system/ctxtelemetry.socket
[Unit]
Description=Linux VDA telemetry service

[Socket]
ListenStream=7503
Accept=yes
```

3. Exécutez les commandes suivantes pour redémarrer le port de socket.

```
1 sudo systemctl daemon-reload
2 sudo systemctl stop ctxtelemetry.socket
3 sudo systemctl start ctxtelemetry.socket
```

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.

#### Remarque :

Vous pouvez également exécuter `ctxsetup.sh` à la place pour automatiser les étapes 3 et 4 précédentes.

## Mode de 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.

```
1 sudo vi /opt/Citrix/VDA/sbin/ctxtelemetry
```

```

#!/bin/sh

export PATH=/usr/lib/jvm/java-8-openjdk-amd64/jre/bin:/usr/lib/jvm/java-8-openjdk-amd64/bin:${PATH}
# Set this flag to 1 to enter debugging mode
DebugMode=1
# Set this flag to 1 to enter interactive debugging mode
InteractiveDebugMode=0

```

2. Arrêtez manuellement le service de télémétrie Citrix ou attendez 15 minutes que le service s'arrête automatiquement.

```

administrator@RGQBE-LVDA-3:~$ sudo netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:139             0.0.0.0:*                LISTEN      1447/smbd
tcp        0      0 127.0.0.53:53          0.0.0.0:*                LISTEN      971/systemd-resolve
tcp        0      0 0.0.0.0:22             0.0.0.0:*                LISTEN      1309/sshd
tcp        0      0 127.0.0.1:631          0.0.0.0:*                LISTEN      25158/cupsd
tcp        0      0 127.0.0.1:5432         0.0.0.0:*                LISTEN      998/postgres
tcp        0      0 0.0.0.0:445            0.0.0.0:*                LISTEN      1447/smbd
tcp6       0      0 :::2598                 :::*                    LISTEN      28100/ctxhdx
tcp6       0      0 :::139                  :::*                    LISTEN      1447/smbd
tcp6       0      0 :::7502                 :::*                    LISTEN      1958/java
tcp6       0      0 :::7303                 :::*                    LISTEN      1/init
tcp6       0      0 :::80                   :::*                    LISTEN      1610/java
tcp6       0      0 :::1494                 :::*                    LISTEN      28100/ctxhdx
tcp6       0      0 :::22                   :::*                    LISTEN      1309/sshd
tcp6       0      0 :::1:631                 :::*                    LISTEN      25158/cupsd
tcp6       0      0 :::445                   :::*                    LISTEN      1447/smbd
administrator@RGQBE-LVDA-3:~$

```

Dans cet exemple, vous pouvez exécuter les commandes suivantes pour arrêter le service de télémétrie Citrix.

```

1 sudo netstat -ntlp
2 Kill -9 1958

```

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

```

## 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

August 20, 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 :

```
1 {  
2
```

```

3  "Version": "21.04.200.4",
4  "Distributions": [
5  {
6
7  "TargetOS": "RHEL7_9",
8  "PackageName": "",
9  "PackageHash": ""
10 }
11 ,
12 {
13
14 "TargetOS": "UBUNTU20_04",
15 "PackageName": "",
16 "PackageHash": ""
17 }
18
19 ]
20 }

```

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) ou UBUNTU20\_04. Le démon **ctxmonitord** 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

```

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 <b>mise à jour automatique</b> est désactivée. Vous pouvez définir ce paramètre sur 1 pour activer la <b>mise à jour automatique</b> .
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.
ScheduledTime	Ce paramètre est requis. Vous pouvez le définir sur <b>Immediate</b> ou <b>NextStart</b> . <b>Immediately</b> 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. <b>NextStart</b> signifie l'exécution d'une mise à jour au prochain démarrage de <b>ctxmonitord</b> . Cette option est appropriée lorsque la vitesse de téléchargement n'est pas élevée et que votre mise à jour n'est pas urgente.

Paramètre de registre	Description
CaCertificate	<p>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, mais il n'est PAS pris en charge sur Ubuntu ou Debian, car la commande <code>curl</code> ne peut pas fonctionner comme prévu lors de la vérification du pair à l'aide du fichier de certificat spécifié sur Ubuntu ou Debian.</p> <p>Assurez-vous de définir les principes du moindre privilège sur le certificat.</p>

Au redémarrage de **ctxmonitord**, le service interroge d'abord l'**Url** pour obtenir le fichier Update-Info.json et récupère la version de mise à jour à partir du fichier JSON. Ensuite, **ctxmonitord** 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 **ScheduledTime**. Dans un déploiement local, vous pouvez redémarrer **ctxmonitord** 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, **ctxmonitord** 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.
- Pour effectuer un téléchargement à partir de l'URL fournie, vous devez installer `curl` sur la machine virtuelle cible.
- 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

August 20, 2024

Le tableau suivant répertorie certaines mesures disponibles pour les machines virtuelles Linux et les sessions Linux.

Métrique	Min. Version du VDA requise	Description	Remarques
Latence ICA	2311	La latence ICA est en fait la latence du réseau. Cette mesure indique si le réseau est lent. Pour accéder à cette mesure, ouvrez la vue <b>Détails de la session</b> .	Disponible à la fois dans Citrix Director et dans l'onglet Surveiller.
Stratégies	2311	Toutes les stratégies appliquées à la session en cours sont affichées dans l'onglet <b>Stratégies</b> de la vue <b>Détails de la session</b> .	Disponible à la fois dans Citrix Director et dans l'onglet Surveiller.

Métrique	Min. Version du VDA requise	Description	Remarques
Durée d'ouverture de session	2109	<p>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 cette mesure de session, accédez à l'onglet <b>Monitor</b> de Citrix DaaS. La console Monitor est disponible en tant que console Director pour surveiller et résoudre les problèmes liés aux déploiements de la version actuelle et LTSR de Citrix Virtual Apps and Desktops. Dans l'onglet <b>Surveiller</b>, cliquez sur <b>Afficher la tendance historique</b> dans la section <b>Durée moyenne d'ouverture de session</b>. Sur la page <b>Performances d'ouverture de session</b>, définissez les conditions de filtre et cliquez sur <b>Appliquer</b> pour afficher les mesures.</p>	Disponible uniquement dans l'onglet Surveiller.

Métrique	Min. Version du VDA requis	Description	Remarques
Nombre de reconnexions automatiques de sessions	2109	<p>Pour afficher le nombre de reconnexions automatiques au cours d'une session, accédez à la vue <b>Tendances</b>. Définissez les conditions et cliquez sur <b>Appliquer</b> pour affiner les résultats de recherche. La colonne <b>Nombre de reconnexions automatiques de sessions</b> affiche le nombre de reconnexions automatiques dans une session. La <b>reconnexion automatique</b> est activée lorsque la stratégie <b>Fiabilité de session</b> ou <b>Reconnexion automatique du client</b> sont en vigueur. Pour plus d'informations sur les reconnexions de session et les stratégies, consultez les articles suivants.</p> <p><a href="#">Sessions</a></p>	Disponible à la fois dans Citrix Director et dans l'onglet Surveiller.

Métrique	Min. Version du VDA requise	Description	Remarques
		<a href="#">Paramètres de stratégie Reconnexion automatique des clients</a> <a href="#">Paramètres de stratégie Fiabilité de session</a>	
Délai d'inactivité	2103	Pour accéder à cette mesure, ouvrez la boîte de dialogue <b>Toutes les sessions</b> en sélectionnant <b>Filtres &gt; Sessions &gt; Toutes les sessions</b> .	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.
Protocole	1909	Le protocole de transport d'une session Linux est indiqué par UDP ou TCP dans la vue <b>Détails de la session</b> .	Disponible à la fois dans Citrix Director et dans l'onglet Surveiller.

Métrique	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 <b>Calcul des boucles ICA</b> et <b>Intervalle de calcul des boucles ICA</b> dans Citrix Studio.	Disponible à la fois dans Citrix Director et dans l'onglet Surveiller.

---

## Collecte de journaux

August 20, 2024

### Présentation du mécanisme de journalisation

Le tableau suivant présente une vue d'ensemble du mécanisme de journalisation pour l'agent Linux VDA.

Module de journalisation	Format du nom du fichier journal	Exemple de nom de fichier journal	Étendue de journalisation	Taille maximale d'un seul fichier	Seuil de rotation (par défaut)	Configuration
HDX	hdx.log[.n]	hdx.log, hdx.log.1	Graphisme, ouverture de session, audio, clavier, souris	200 Mio	1 actuel, 2 anciens	Configurable via l'utilitaire setlog
Jproxy	jproxy.log[.n.log]	jproxy.log, jproxy.log.1.log	Enregistrement VDA, authentification des utilisateurs	20 Mio	1 actuel, 10 anciens	Configurable via l'utilitaire setlog ou /etc/xdl/log4j2.xml
VDA	vda.YYYY-MM-DD.hh.mm.ss.log	vda.2024-05-06.20.18.40.log	Enregistrement de VDA	10 Mio	1 actuel, 100 anciens	Configurable via l'utilitaire setlog ou /etc/xdl/broker-agent.conf

**Remarque :**

- Le nom du premier fichier journal ne comporte pas de numéro et les fichiers suivants sont numérotés avec « .n », où « n » représente le numéro de fichier. Par exemple, « hdx.log » est le premier fichier journal HDX et « hdx.log.1 » est le second.
- La taille maximale d'un seul fichier journal est mesurée en mébioctets (Mio).
- Un fichier journal qui est en cours de génération et qui n'a pas encore atteint la taille maximale d'un seul fichier est appelé fichier journal « actuel ». Lorsqu'un fichier journal « actuel » atteint la taille maximale d'un seul fichier, il est remplacé et devient un « ancien » fichier journal.
- Le seuil de rotation est configurable pour limiter le nombre d'« anciens » fichiers journaux pouvant être conservés. Les fichiers journaux les plus anciens seront supprimés lorsque la limite sera atteinte.

## Journalisation de la configuration

Cette section fournit des informations supplémentaires sur la configuration de la journalisation, en complément des informations décrites dans le tableau ci-dessus.

### La journalisation est activée par défaut pour l'agent Linux VDA

Le démon `ctxlogd` et l'utilitaire `setlog` sont maintenant inclus dans le package du Linux VDA. Par défaut, le démon `ctxlogd` démarre après l'installation et la configuration du Linux VDA. 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.

### Configurer la journalisation du VDA via `/etc/xdl/brokeragent.conf`

#### Remarque :

Si vous souhaitez configurer uniquement les niveaux de journalisation pour le VDA sans entrer dans d'autres paramètres de journalisation tels que la taille maximale d'un seul fichier journal, vous pouvez exécuter l'utilitaire `setlog` décrit plus loin dans cet article. Sinon, utilisez `/etc/xdl/brokeragent.conf`.

Le fichier `/etc/xdl/brokeragent.conf` du VDA est disponible pour configurer la journalisation du VDA. Par exemple :

```
<!-- VDA trace settings -->
<add key="TraceProvider.Type" value="QueuedLogFileProvider"/>
<add key="TraceProvider.BaseFilename" value="/var/log/xdl/vda.log"/>
<add key="TraceProvider.AppendMode" value="true"/>
<add key="TraceProvider.SizeLimit" value="50"/>
<add key="TraceProvider.TrailCount" value="2"/>
<add key="TraceProvider.ProcessSafe" value="true"/>
<add key="TraceProvider.CategoryFilter" value="All" />
```

#### Remarque :

Par défaut, le nombre maximal d'« anciens » fichiers journaux VDA pouvant être conservés est de 100. Ajustez-le selon vos besoins.

### Configurer la journalisation Jproxy via `/etc/xdl/log4j2.xml`

#### Remarque :

Si vous souhaitez configurer uniquement les niveaux de journalisation Jproxy sans entrer

dans d'autres paramètres de journalisation tels que la taille maximale d'un seul fichier journal, vous pouvez exécuter l'utilitaire `setlog` décrit plus loin dans cet article. Sinon, utilisez `/etc/xdl/log4j2.xml`.

Voici un exemple de configuration de la journalisation Jproxy via `/etc/xdl/log4j2.xml`, dont le paramètre **SizeBasedTriggeringPolicy** spécifie la taille maximale d'un seul fichier journal Jproxy et le paramètre **DefaultRollerStrategy** définit le nombre total de fichiers journaux Jproxy qui peuvent être conservés.

```
<!-- Logging Properties -->
<Properties>
  <Property name="LOG_PATTERN">%d{yyyy-MM-dd HH:mm:ss.SSS}{GMT} [%-5p] [%tid] - %m%n</Property>
  <Property name="logfile">/var/log/xdl/jproxy.log</Property>
  <Property name="perflogfile">/var/log/xdl/jproxyperf.log</Property>
</Properties>

<Appenders>

  <Console name="CONSOLE" target="SYSTEM_OUT">
    <PatternLayout pattern="${LOG_PATTERN}"/>
  </Console>

  <RollingFile name="logfile" fileName="${sys:logfile}"
    filePattern="${sys:logfile}.%i.log">
    <PatternLayout pattern="${LOG_PATTERN}"/>
    <Policies>
      <SizeBasedTriggeringPolicy size="19500KB" />
    </Policies>
    <DefaultRolloverStrategy max="10"/>
  </RollingFile>

  <RollingFile name="perflogfile" fileName="${sys:perflogfile}"
    filePattern="${sys:perflogfile}.%i.log">
    <PatternLayout pattern="${LOG_PATTERN}"/>
    <Policies>
      <SizeBasedTriggeringPolicy size="19500KB" />
    </Policies>
    <DefaultRolloverStrategy max="10"/>
  </RollingFile>
```

## Configurer la journalisation HDX via l'utilitaire `setlog`

L'utilitaire `setlog` se trouve sous le chemin `/opt/Citrix/VDA/bin/`. Seul l'utilisateur racine est autorisé à l'exécuter. Vous pouvez utiliser l'interface graphique ou exécuter des commandes pour afficher et modifier vos options de configuration, notamment les valeurs (chemin du fichier journal, limite de taille de fichier unique et seuil de rotation) et les niveaux de journalisation. Pour obtenir de l'aide sur l'utilitaire `setlog`, exécutez la commande suivante :

```
1 setlog help
```

**Valeurs** Par défaut, les journaux HDX sont enregistrés sous `/var/log/xdl/hdx.log`, la taille limite d'un seul fichier journal HDX est de 200 Mio et vous pouvez enregistrer jusqu'à deux « anciens » fichiers journaux HDX sous `/var/log/xdl/hdx.log`.

Pour afficher toutes les valeurs de `setlog` actuelles, exécutez la commande suivante :

```
1 setlog values
2
3 log_path (Log Output Path) = /var/log/xdl/hdx.log
4
5 log_size (Max Log Size (MiB)) = 200
6
7 log_count (Max Old Log Files) = 2
```

Pour afficher ou définir une seule valeur de setlog, exécutez la commande suivante :

```
1 setlog value <name> [<value>]
```

Par exemple :

```
1 setlog value log_size 100
```

**Niveaux** Par défaut, les niveaux de journalisation sont définis sur **Information** (non sensibles à la casse).

Lorsque vous rencontrez un problème nécessitant un dépannage, nous vous recommandons de définir le niveau de journalisation sur **détaillé** dans la plupart des scénarios. Ensuite, reproduisez le problème et collectez les journaux.

Pour définir les niveaux de journalisation (tels que Désactivé, Hérité, Trace, Détaillé, Information, Avertissements, Erreurs et Erreurs fatales), exécutez la commande suivante :

```
1 setlog level <class> [<level>]
```

---

Niveau du journal	Paramètre de commande (non sensible à la casse)
Désactivé	none
Inherited	inherit
Trace	trace
Détaillé	détaillé
Information	info
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 « tous ». Par exemple :

```
1 setlog level all error
```

Pour afficher toutes les classes ou tous les composants pris en charge, exécutez la commande suivante :

```
1 setlog levels
```

**Restaurer paramètres par défaut** Rétablir les paramètres par défaut de tous les niveaux et de toutes les valeurs :

```
1 setlog default
```

#### 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.

## Collecte de journaux

Vous pouvez exécuter la commande **bash /opt/Citrix/VDA/bin/xdlcollect.sh** pour collecter les journaux. Le script Bash **xdlcollect** utilisé pour collecter les journaux est intégré dans le logiciel Linux VDA et se trouve dans **/opt/Citrix/VDA/bin**.

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 téléchargement 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.

## Dépannage

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 :

```
1 Apr 1 02:28:21 RH72 citrix-ctxlogd[17881]: Failed to open logging configuration file.
```

```
2
3 Apr 1 02:28:21 RH72 systemd: ctxlogd.service: main process exited, code
   =exited, status=1/FAILURE
4
5 Apr 1 02:28:21 RH72 systemd: Unit ctxlogd.service entered failed state.
6
7 Apr 1 02:28:21 RH72 systemd: ctxlogd.service failed.
```

Pour résoudre ce problème, exécutez `setlog` en tant qu'utilisateur `root` pour créer le fichier `/var/xdl/.ctxlog`. Redémarrez le service `ctxlogd` dont dépendent d'autres services.

## Observation de session

August 20, 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).

```
1 sudo pip3 install websockify
2 sudo yum install x11vnc
```

**(Pour RHEL 7.x)** Résolvez `python-websockify` et `x11vnc` en activant Extra Packages for Enterprise Linux (EPEL) et les référentiels RPM facultatifs :

- EPEL

Le référentiel EPEL est requis pour `x11vnc`. Pour activer le référentiel EPEL, exécutez la commande suivante :

```
1 yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

- RPM facultatifs

Exécutez la commande suivante pour activer le référentiel de RPMs facultatifs pour l'installation de certains packages de dépendances de `x11vnc` :

```
1 subscription-manager repos --enable rhel-7-server-optional-rpms
  --enable rhel-7-server-extras-rpms
```

**Pour RHEL 9.2/9.0/8.x et Rocky Linux 9.2/9.0/8.x :**

Exécutez les commandes suivantes pour installer `python-websocketify` et `x11vnc` (`x11vnc` version 0.9.13 ou ultérieure).

```
1 sudo pip3 install websocketify
2 sudo yum install x11vnc
```

Résolvez `x11vnc` en activant les référentiels EPEL et CodeReady Linux Builder :

```
1 dnf install -y --nogpgcheck https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
2
3 subscription-manager repos --enable "codeready-builder -for-rhel-8-x86_64-rpms"
```

**Pour Ubuntu :**

Exécutez les commandes suivantes pour installer `python-websocketify` et `x11vnc` (`x11vnc` version 0.9.13 ou ultérieure).

```
1 sudo pip3 install websocketify
2 sudo apt-get install x11vnc
```

**Pour SUSE :**

Exécutez les commandes suivantes pour installer `python-websocketify` et `x11vnc` (`x11vnc` version 0.9.13 ou ultérieure).

```
1 sudo pip3 install websocketify
2 sudo zypper install x11vnc
```

**Pour Debian :**

Exécutez les commandes suivantes pour installer `python-websocketify` et `x11vnc` (`x11vnc` version 0.9.13 ou ultérieure).

```
1 sudo pip3 install websocketify
2 sudo apt-get install x11vnc
```

## 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 CA racine dans l'onglet **Autorités** du gestionnaire de certificats.

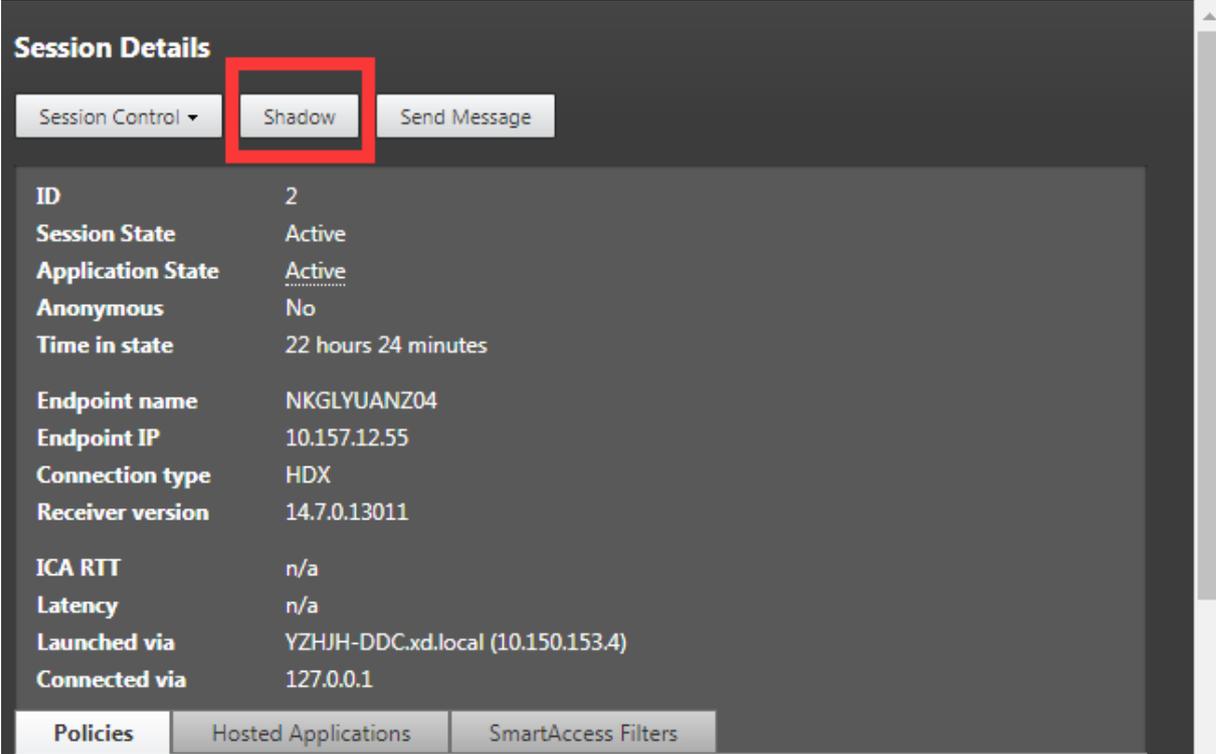
**Installer un certificat de serveur et sa clé sur chaque serveur Linux VDA** Appelez les certificats de serveur « shadowingcert.\* » et le fichier de clé « shadowingkey.\* » (\* peut indiquer le format, par exemple, shadowingcert.pem et shadowingkey.key). Placez les certificats de serveur et les fichiers de clés sous le chemin d'accès **/etc/xdl/shadowingssl** et protégez-les correctement avec des autorisations

restreintes, pour ne permettre l'accès en lecture qu'à ctxsrvr. 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. Les commandes sont les suivantes :

```
1 cp <vda's-public-key> /etc/xdl/shadowingssl/shadowingcert.pem
2 cp <vda's-server-private-key> /etc/xdl/shadowingssl/shadowingkey.key
3 sudo chown ctxsrvr:ctxadm /etc/xdl/shadowingssl/shadowingcert.pem
4 sudo chown ctxsrvr:ctxadm /etc/xdl/shadowingssl/shadowingkey.key
```

## 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.

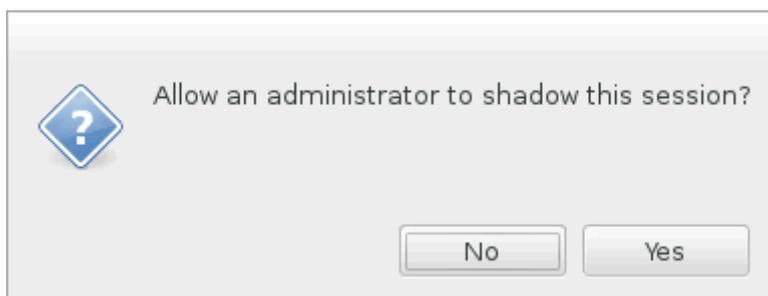


The screenshot shows the 'Session Details' interface in Citrix Director. At the top, there are three buttons: 'Session Control' (with a dropdown arrow), 'Shadow' (highlighted with a red box), and 'Send Message'. Below these buttons is a table of session details:

ID	2
Session State	Active
Application State	Active
Anonymous	No
Time in state	22 hours 24 minutes
Endpoint name	NKGLYUANZ04
Endpoint IP	10.157.12.55
Connection type	HDX
Receiver version	14.7.0.13011
ICA RTT	n/a
Latency	n/a
Launched via	YZHJH-DDC.xd.local (10.150.153.4)
Connected via	127.0.0.1

At the bottom of the page, there are three tabs: 'Policies', 'Hosted Applications', and 'SmartAccess Filters'.

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 :

```
1 <!-- Broker Agent Plugin - Director VDA plugin Logger -->
2
3 <logger name="com.citrix.dmc">
4
5 <level value="trace"/>
6
7 </logger>
```

3. Exécutez la commande `systemctl restart ctxvda` 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

August 20, 2024

Le démon du service de surveillance (**ctxmonitord**) 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.

```
1 systemctl restart ctxmonitord
```

- **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.

```
MonitorUser: all
MonitorType: 3
ProcessName: ctxhdx
Operation: 4
DBRecord: false
MonitorUser: all
MonitorType: 3
ProcessName: ctxvda
Operation: 4
DBRecord: false
MonitorUser: all
MonitorType: 3
ProcessName: ctxpolicyd
Operation: 4
DBRecord: false
MonitorUser: all
MonitorType: 3
ProcessName: Xorg
Operation: 8
DBRecord: false
```

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

## Dépannage

August 20, 2024

Cet article explique comment utiliser **XDPing** pour le dépannage et comment interroger les données de session à l'aide de l'utilitaire **ctxsdcutil**.

### 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.

## Installer l'outil XDPing Linux

L'exécution de `ctxsetup.sh` n'installe pas **XDPing**. Pour installer **XDPing**, exécutez `sudo /opt/Citrix/VDA/bin/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
```

## Tâches pouvant être effectuées avec XDPing

L'outil **XDPing** est fourni avec l'exécutable unique nommé `xdping` qui est exécuté à partir de l'interface de commande.

Le tableau suivant décrit les différentes tâches qui peuvent être effectuées avec les commandes **XDPing** correspondantes :

Tâche	Commande <b>XDPing</b>	Remarques
Pour afficher les options de la ligne de commande	<b>sudo /opt/Citrix/VDA/bin/xdping -h</b>	S/O
Pour exécuter la suite complète de tests	<b>sudo /opt/Citrix/VDA/bin/xdping</b> (exécutez <b>XDPing</b> sans aucune option de ligne de commande)	L'outil Linux <b>XDPing</b> effectue plus de 150 tests individuels sur le système. Pour plus d'informations, consultez la section Tests individuels plus loin dans cet article.
Pour vérifier l'état d'enregistrement d'un VDA	<b>sudo /opt/Citrix/VDA/bin/xdping -a</b>	Pour plus d'informations, consultez la section Aperçu des vérifications de l'état d'enregistrement plus loin dans cet article.

Tâche	Commande <b>XDPing</b>	Remarques
Pour sauvegarder les données clés d'un VDA	<b>sudo</b> <b>/opt/Citrix/VDA/bin/xdping -b</b>	Pour plus d'informations, consultez la section Sauvegarder et comparer les données VDA plus loin dans cet article.
Pour comparer les deux dernières copies des données de sauvegarde du VDA	<b>sudo</b> <b>/opt/Citrix/VDA/bin/xdping -diff</b>	Pour plus d'informations, consultez la section Sauvegarder et comparer les données VDA plus loin dans cet article.
Pour comparer deux copies spécifiques des données de sauvegarde du VDA	**sudo <b>/opt/Citrix/VDA/bin/xdping -diff=:**</b>	Pour plus d'informations, consultez la section Sauvegarder et comparer les données VDA plus loin dans cet article.
Pour vérifier l'environnement avant d'installer le package du VDA Linux	<b>sudo</b> <b>/opt/Citrix/VDA/bin/xdping -preflight</b>	S/O
Pour exécuter uniquement des catégories de test spécifiques, par exemple les tests liés à l'heure, à Kerberos et à la base de données	<b>sudo</b> <b>/opt/Citrix/VDA/bin/xdping -T time,kerberos,database</b>	S/O
Pour analyser un Delivery Controller spécifique	**sudo <b>/opt/Citrix/VDA/bin/xdping -d</b> **	S/O

**Tests individuels** L'outil **XDPing** Linux effectue plus de 150 tests individuels sur le système, qui sont généralement classés comme suit :

- Vérifiez si la configuration système du VDA Linux est respectée.
- Identifiez et affichez les informations de la machine, y compris les distributions Linux.
- Vérifiez la compatibilité du noyau Linux.
- Vérifiez les problèmes de distribution Linux connus qui peuvent avoir un impact sur le fonctionnement du VDA Linux.
- Vérifiez le mode de sécurité Security-Enhanced Linux (SELinux) et sa compatibilité.
- Identifiez les interfaces réseau et vérifiez les paramètres réseau.

- Vérifiez le partitionnement du stockage et l'espace disque disponible.
- Vérifiez la configuration du nom d'hôte et du nom de domaine de la machine.
- Vérifiez la configuration DNS et effectuez des tests de recherche.
- Identifiez les hyperviseurs sous-jacents et vérifiez la configuration de la machine virtuelle. Prise en charge de :
  - XenServer (anciennement Citrix Hypervisor)
  - Microsoft HyperV
  - VMware vSphere
- Vérifiez les paramètres d'heure et vérifiez si la synchronisation de l'heure réseau est opérationnelle.
- Vérifiez si le service PostgreSQL est correctement configuré et opérationnel.
- Vérifiez si SQLite est correctement configuré et opérationnel.
- Vérifiez si le pare-feu est activé et si les ports requis sont ouverts.
- Vérifiez la configuration de Kerberos et effectuez des tests d'authentification.
- Vérifiez l'environnement de recherche LDAP pour Group Policy Engine Service.
- Vérifiez 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
- Vérifiez l'intégrité de l'objet ordinateur Linux dans Active Directory.
- Vérifiez la configuration du module d'authentification enfichable (PAM).
- Vérifiez le modèle de l'image mémoire.
- Vérifiez si les packages requis par le VDA Linux sont installés.
- Identifiez le package du VDA Linux et vérifiez l'intégrité de l'installation.
- Vérifiez l'intégrité de la base de données de registre PostgreSQL.
- Vérifiez si les services du VDA Linux sont correctement configurés et opérationnels.
- Vérifiez l'intégrité de la configuration VDA et HDX.
- Analysez la configuration de chaque Delivery Controller pour vérifier que le Broker Service est accessible, opérationnel et réactif.
- Vérifiez si la machine est enregistrée auprès de la batterie du Delivery Controller.
- Vérifiez l'état de chaque session HDX active ou déconnectée.
- Analysez les fichiers journaux pour les erreurs et avertissements liés au VDA Linux.
- Vérifiez si la version de Xorg est adaptée.
- Vérifiez si les dépendances requises sont installées.

**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/1]: [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.

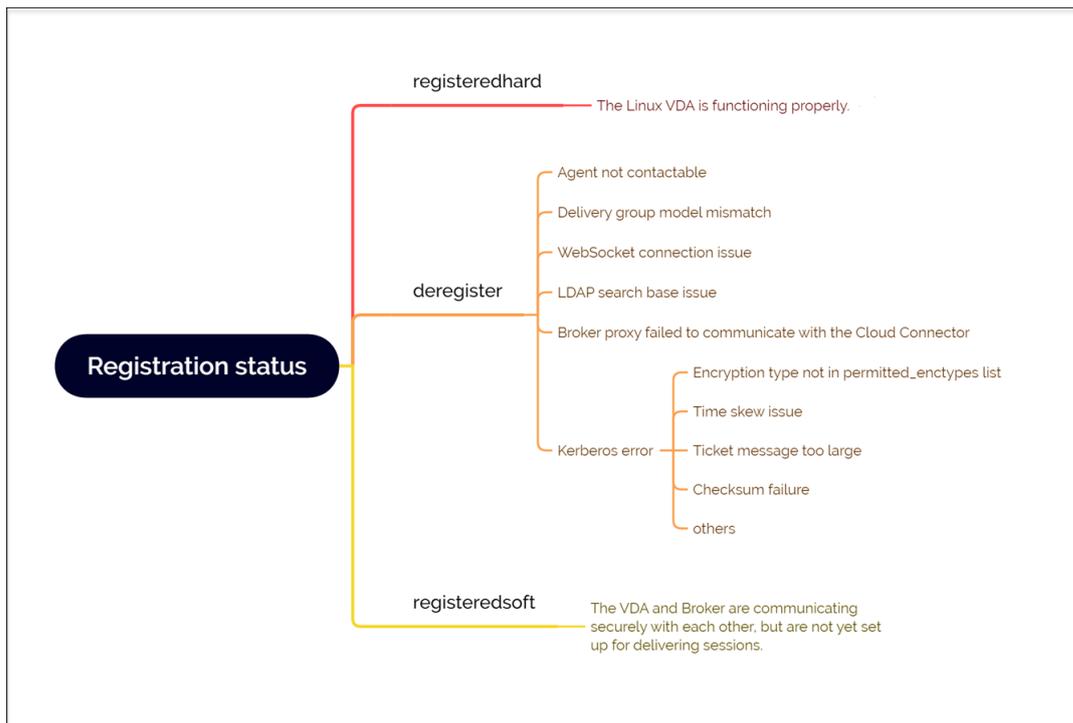
```

```

Verify Kerberos system keys for SPN exist [Pass]
Kerberos login: [FAILED AUTHENTICATION]
    Keytab contains no suitable keys for MYVDA1$@>
    while getting initial credentials
Verify KDC authentication [ERROR]
Failed to authenticate and obtain a Ticket Granting Ticket (TGT)
from the KDC authentication service for the machine account UPN
MYVDA1$@>. Check that the Kerberos configuration is
valid and the keys in the system keytab are current.

Summary -----
The following tests did not pass:
Verify Kerberos system keys for UPN exist [ERROR]
Verify KDC authentication [ERROR]
    
```

**Aperçu des vérifications de l'état d'enregistrement d'un VDA** L'outil Linux **XDPing** fournit également un module d'analyse pour vous aider à vérifier et à analyser l'état d'enregistrement de votre VDA. Pour obtenir un aperçu des vérifications de l'état d'enregistrement, consultez la capture d'écran suivante :



**Sauvegarder et comparer les données VDA** À partir de Linux VDA 2305, l'outil **XDPing** introduit un module de sauvegarde VDA. Ce module vous permet de sauvegarder les données clés d'un VDA à tout moment, telles que la configuration, la base de données et les données d'autorisation binaires. Vous pouvez sauvegarder les données clés d'un VDA lorsqu'il fonctionne correctement. En cas de défaut-

lance ultérieure du VDA, sauvegardez une autre copie des données et comparez les deux copies pour faciliter le dépannage. Le tableau suivant décrit la sauvegarde des données VDA et la comparaison avec les commandes **XDPing** correspondantes :

Tâche	Commande <b>XDPing</b>	Remarques
Pour sauvegarder les données clés d'un VDA	<b>sudo /opt/Citrix/VDA/bin/xdping -b</b>	Chaque fois que vous exécutez la commande de sauvegarde, une copie des données de sauvegarde est générée et enregistrée dans un répertoire situé sous <b>/var/ctxbackup</b> . Les répertoires de données de sauvegarde sont nommés selon la date et l'heure actuelles au format <b>aaaa-mm-jj-hh_mm_ss</b> , par exemple, <b>2023-02-27-16_31_27</b> . Par défaut, le nombre maximum de répertoires de données de sauvegarde est de 30 et l'outil <b>XDPing</b> alterne ou supprime les anciens répertoires de données de sauvegarde lorsque ce nombre est dépassé. Pour personnaliser le nombre de répertoires, exécutez la commande suivante : <pre>sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent\Backup"-t "REG_DWORD"-v "MaxDirRotationCount"-d "0x00000005"--force</pre>
Pour comparer les deux dernières copies des données de sauvegarde du VDA	<b>sudo /opt/Citrix/VDA/bin/xdping -diff</b>	S/O

Tâche	Commande <b>XDPing</b>	Remarques
Pour comparer deux copies spécifiques des données de sauvegarde du VDA	<b>**sudo</b> <code>/opt/Citrix/VDA/bin/xdping -diff=:**</code>	S/O

## 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**

## Autres

August 20, 2024

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

August 20, 2024

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

August 20, 2024

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.

### Logiciels requis

- 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

Pour créer un environnement virtuel Python3, procédez comme suit :

1. Installez les dépendances Python3.

#### Pour Amazon Linux 2 :

```
1 yum -y install python3 python3-devel krb5-devel gcc
```

#### Pour RHEL et Rocky Linux :

```
1 yum -y install python3-devel krb5-devel gcc
```

#### 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 :

```
1 apt-get -y install python3-dev python3-pip python3-venv libkrb5-dev
```

**Pour SUSE :**

```
1 zypper -n install lsb-release python3-devel python3-setuptools
   krb5-devel gcc libffi-devel libopenssl-devel
```

## 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 :**

```
1 sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
```

**Pour SUSE :**

```
1 sudo ln -s /usr/lib/mit/bin/krb5-config /usr/bin/krb5-config
2
3 export PATH=$PATH:/usr/lib/mit/bin:/usr/lib/mit/sbin
4
5 sudo mkdir -p /usr/lib/mit/include/gssapi/
6
7 sudo ln -s /usr/include/gssapi/gssapi_ext.h/usr/lib/mit/include/
   gssapi/gssapi_ext.h
8
9 sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
```

## 3. Installez les dépendances LDAPS.

```
1 sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install --
   upgrade pip==21.3.1
2
3 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
```

4. Installez les dépendances **XDPing**.

```
1 sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install --
   upgrade pip==21.3.1
2
3 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  
4  
5 sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install /  
opt/Citrix/VDA/sbin/ctxpython3/packages/xdping-*.whl
```

## Intégrer NIS avec Active Directory

August 20, 2024

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 de la section [Installer le Linux VDA manuellement pour Amazon Linux 2, CentOS, RHEL et Rocky Linux](#). Pour une distribution Ubuntu, suivez les instructions de la section [Installer le Linux VDA manuellement sur 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 :

```
1 yum -y install ypbind rpcbind oddjob-mkhomedir
```

Définissez le domaine NIS :

```
1 ypdomainname nis.domain
2 echo "NISDOMAIN=nis.domain" >> /etc/sysconfig/network
```

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** :

```
1 sudo authconfig --enablenis --nisdomain=nis.domain --nisserver=server.
  nis.domain --enablemkhomedir --update
```

**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 :

```
1 sudo systemctl start rpcbind ypbind
2
3 sudo systemctl enable rpcbind ypbind
```

Assurez-vous que la configuration NIS est correcte :

```
1 ypwhich
```

Vérifiez que les informations de compte sont disponibles à partir du serveur NIS :

```
1 getent passwd nisaccount
```

### 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
```

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
```

**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

#### Remarque

L'utilisation de SSSD avec le démon NSCD (Name Service Cache Daemon) peut entraîner un comportement inattendu. Pour plus d'informations, consultez la page [Using NSCD with 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/sss/sss.conf** Exemple de configuration **sssd.conf** (des options supplémentaires peuvent être ajoutées si nécessaire) :

```
1 [sssd]
2 config_file_version = 2
3 domains = EXAMPLE
4 services = nss, pam
5
6 [domain/EXAMPLE]
7 # Uncomment if you need offline logins
8 # cache_credentials = true
9 re_expression = (((?P<domain>[^\]+)\(?P<name>.+$$)|((?P<name>[^\@]+)@(P
    <domain>.+$$)|(^(?P<name>[^\@]+)$$))
10 id_provider = proxy
11 proxy_lib_name = nis
12 auth_provider = ad
13 access_provider = ad
14
15 # Should be specified as the long version of the Active Directory
    domain.
16 ad_domain = EXAMPLE.COM
17
18 # Kerberos settings
19 krb5_ccachedir = /tmp
20 krb5_ccname_template = FILE:%d/krb5cc_%U
21
22 # Uncomment if service discovery is not working
23 # ad_server = server.ad.example.com
24
25 # Comment out if the users have the shell and home dir set on the AD
    side
26 default_shell = /bin/bash
27 fallback_homedir = /home/%d/%u
28
29 # Uncomment and adjust if the default principal SHORTNAME$@REALM is not
    available
30 # 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](#).

Définissez les autorisations et les propriétaires du fichier **sssd.conf** :

```
chown root:root /etc/sss/sss.conf
chmod 0600 /etc/sss/sss.conf
```

```
restorecon /etc/sss/sss.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 :

```
1 authconfig --enablesssd --enablesssdauth --enablemkhomedir --update
2
3 sudo systemctl start sssd
4
5 sudo systemctl enable sssd
```

#### 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 :

```
1 sudo klist -ke
```

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 :

```
1 sudo kinit -k MACHINE$@REALM
```

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 inversée (\) 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 :

```
1 sudo klist -ke
```

## 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 :

```
1 sudo getent passwd DOMAIN\username
```

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.

```
1 sudo ssh localhost -l DOMAIN\username
2
3 id -u
```

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

```
1 ls /tmp/krb5cc_{
2 uid }
```

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

```
1 klist
```

## IPv6

August 20, 2024

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"
```

La valeur de **OnlyUseIPv6ControllerRegistration** doit être définie 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
```

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
```

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](#).

## Dépannage

Vérifiez l'environnement réseau IPv6 de base et utilisez ping6 pour vérifier si AD et Delivery Controller sont accessibles.

## LDAPS

August 20, 2024

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
```

### 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 l'agent Linux VDA, exécutez le script **enable\_ldaps.sh** (vous devez être connecté en tant qu'administrateur). Pour exécuter le script **enable\_ldaps.sh** en mode non interactif, exportez les variables suivantes vers votre environnement :

```
1 #CTX_LDAPS_KEYSTORE_PASSWORD=  
2  
3 #CTX_LDAPS_LDAP_SERVERS=
```

- Pour activer LDAP sur SSL/TLS avec le certificat CA racine fourni :

```
1 /opt/Citrix/VDA/sbin/enable_ldaps.sh -Enable pathToRootCA
```

- Pour activer LDAP sur SSL/TLS avec liaison de canal :

```
1 /opt/Citrix/VDA/sbin/enable_ldaps.sh -Enablecb pathToRootCA
```

**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 d'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
```

- Pour revenir à LDAP sans SSL/TLS

```
““
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Disable
““
```

The Java keystore dedicated for LDAPS resides in **`/etc/xdl/keystore`**. Affected registry keys include:

```
““
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
““
```

## 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 Amazon Linux 2, RHEL, Rocky Linux, CentOS et SUSE) ou **/etc/ldap/ldap.conf** (pour Debian et 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.

## Dépannage

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/xdm/.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

August 20, 2024

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 :

```
1 # xauth -f ~/.Xauthority
2
3 # > list
4
5 # > us01msip06:107 MIT-MAGIC-COOKIE-1
   fb228d1b695729242616c5908f11624b
```

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 :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "
   XauthEnabled" -d "0x00000001" --force
2
3 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "ListenTCP"
   -d "0x00000001" --force
```

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 :

```
1 export DISPLAY={
2   Display number stored in the Xauthority file }
3
4
5 export XAUTHORITY={
6   the file path of .Xauthority }
```

### 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.

## Dépannage

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 :

```
1 ps aux | grep -i xorg
```

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 :

```
1 /var/xdm/xauth/.Xauthority110
```

Affichez les cookies à l'aide de la commande **Xauth** :

```
1 Xauth -f /var/xdm/xauth/.Xauthority110
```

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 :

```
1 telnet 10.158.11.11 6160
```

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

August 20, 2024

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](#)
- [Accès des utilisateurs non authentifiés \(anonymes\)](#)

## Authentification avec Azure Active Directory

August 20, 2024

### 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
- RHEL 8.8, 8.6, 7.9
- SUSE 15.5

Pour plus d'informations, veuillez consulter cet [article Microsoft](#).

### Problèmes connus et solutions

Sur RHEL 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.

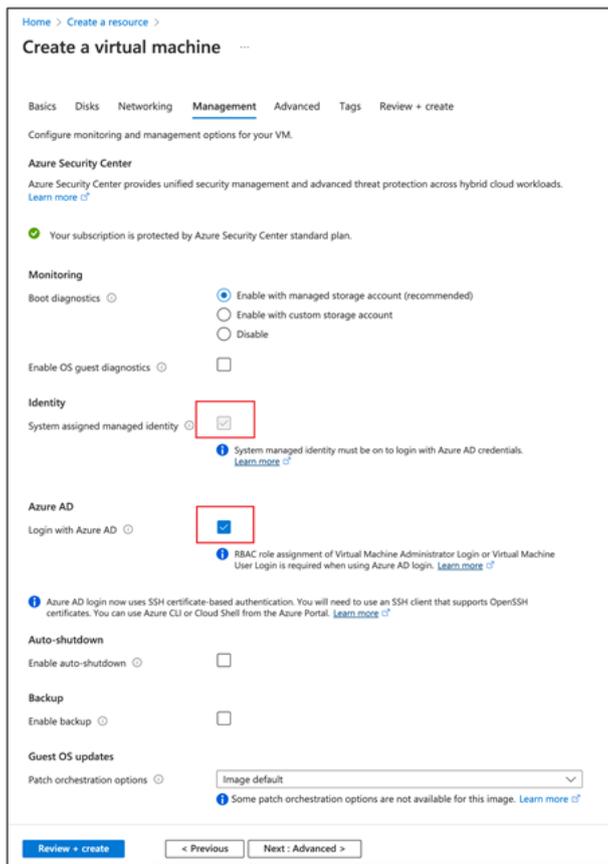
Pour contourner ce problème, dans `/etc/pam.d/remote`, commentez la ligne `Session required pam_loginuid.so`. Reportez-vous à la capture d'écran suivante pour un exemple.

```
#%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, consultez cet [article Microsoft](#).

## Étape 2 : préparer une image principale sur la VM modèle

Pour préparer une image principale, consultez les instructions de l'[Étape 3 : préparer une image principale](#).

## 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.

```
1 Modify /var/xdl/mcs/mcs_util.sh
```

2. Localisez `function read_non_domain_joined_info()`, puis remplacez la valeur `NonDomainJoined` par 2. Consultez le bloc de code dans l'exemple suivant.

```
1 function read_non_domain_joined_info()
2 {
3
4 log "Debug: Enter read_non_domain_joined_info"
5 # check if websocket enabled
6 TrustIdentity=`cat ${
7 id_disk_mnt_point }
8 ${
9 ad_info_file_path }
10 | grep '[TrustIdentity]' | sed 's/\s//g'`
11 if [ "$TrustIdentity" == "[TrustIdentity]" ]; then
12 NonDomainJoined=2
13 fi
14 ...
15 }
```

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.

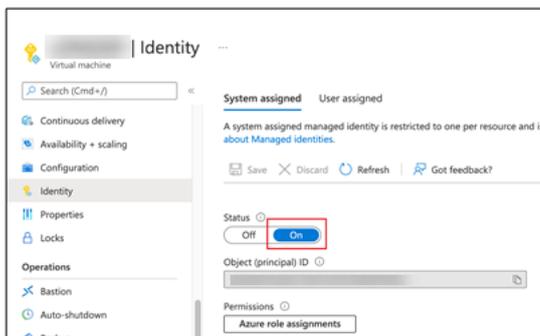
3. Dans **Catalogues de machines**, choisissez d'utiliser Machine Creation Services pour créer les machines virtuelles Linux à partir de la VM modèle. Pour plus d'informations, consultez [VDA n'appartenant pas à un domaine](#) dans le document Citrix DaaS.

## Étape 5 : Attribuer des comptes utilisateurs AAD aux machines virtuelles Linux

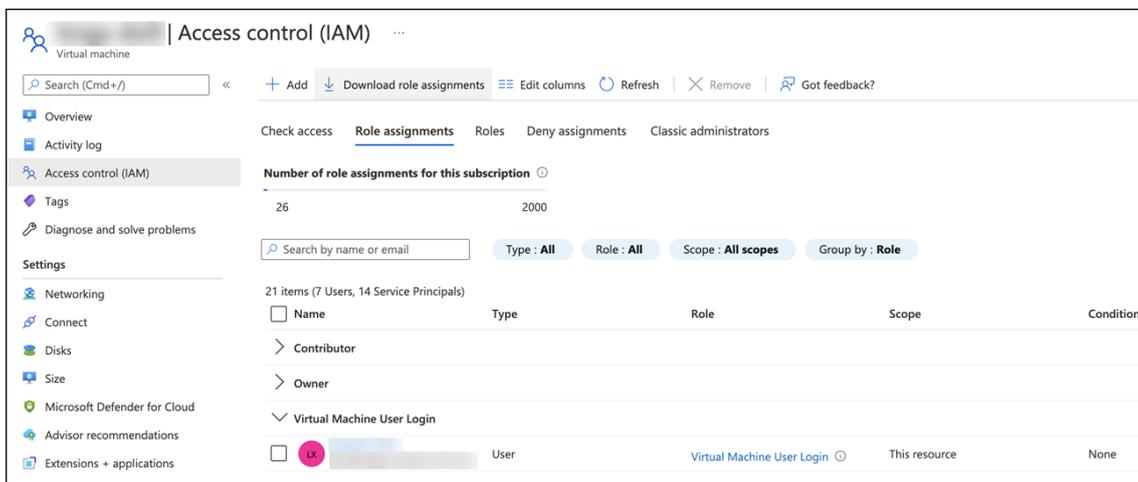
Après avoir créé les machines virtuelles n'appartenant pas à un domaine, attribuez-leur des comptes utilisateur AAD.

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`.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
  Services\CitrixBrokerAgent\WebSocket" -t "REG_DWORD" -v "
  AADAcctPwdAuthEnable" -d "0x00000001" --force
```

#### 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

August 20, 2024

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.

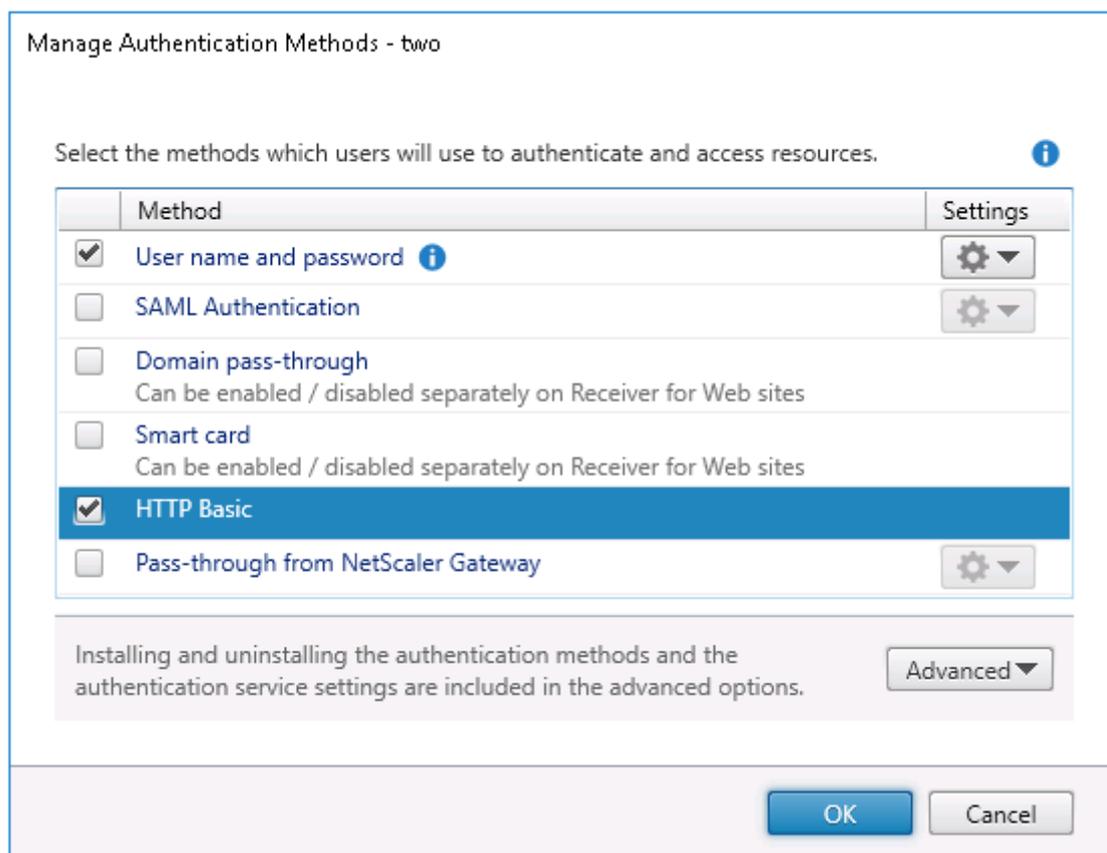
Pour activer la fonctionnalité :

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 :

```

1 <Protocols>
2   <HTTPBasic>
3     <Enabled>True</Enabled>
4   </HTTPBasic>
5 </Protocols>

```

4. Exécutez les commandes suivantes pour installer le certificat racine dans le répertoire spécifié.

```

1 cp rootcert.pem $ICAROOT/keystore/cacerts/
2 $ICAROOT/util/ctx_rehash $ICAROOT/keystore/cacerts/

```

5. Exécutez la commande suivante pour activer la fonctionnalité :

```

1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
  CurrentControlSet\Control\Citrix" -v "LurSsonEnabled" -d "0
  x00000001"

```

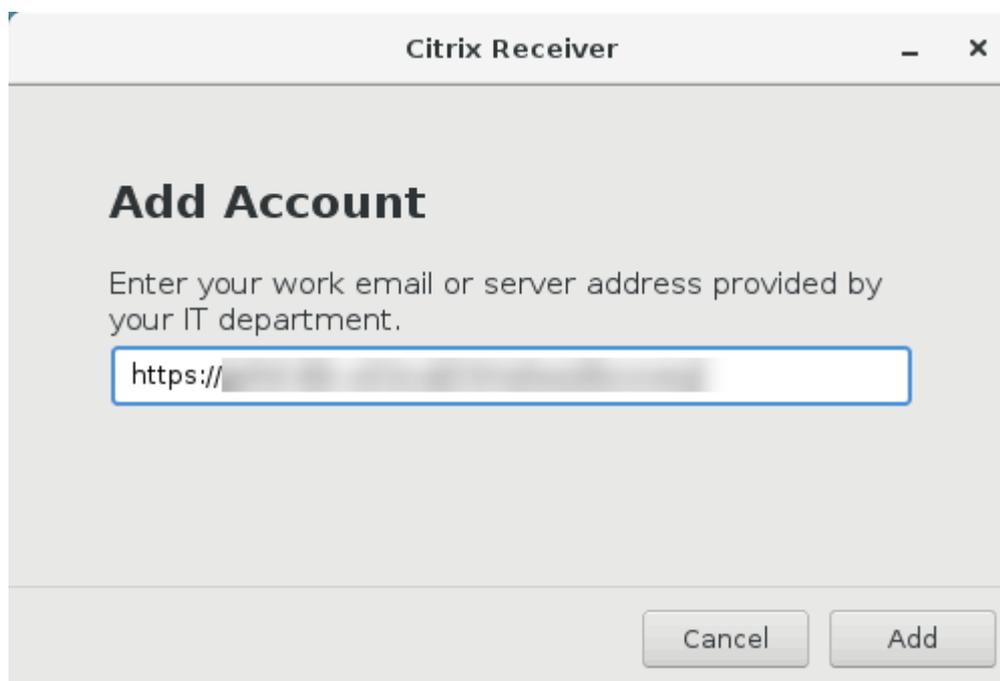
6. Lancez une session de bureau virtuel Linux et démarrez l'application Citrix Workspace pour Linux ou Citrix Receiver pour Linux 13.10 dans cette session.

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

August 20, 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.

## Distributions prises en charge

FAS prend en charge des distributions Linux limitées et des méthodes de jonction de domaines. Reportez-vous à la matrice suivante :

	Winbind	SSSD	Centrify	PBIS
Amazon Linux 2	Oui	Oui	Oui	Oui
Debian 11.7/11.3	Oui	Oui	Oui	Oui
RHEL 9.2/9.0	Oui	Oui	Non	Non
RHEL 8.8/8.6	Oui	Oui	Oui	Oui
RHEL 7.9, CentOS 7.9	Oui	Oui	Oui	Oui
Rocky Linux 9.2/9.0	Oui	Oui	Non	Non
Rocky Linux 8.8/8.6	Oui	Oui	Non	Non
SUSE 15.5	Oui	Oui	Oui	Non
Ubuntu 22.04/20.04	Oui	Oui	Oui	Oui

## Configurer FAS sur le Linux VDA

### Prise en charge de FAS sur RHEL/Rocky Linux 8.x et versions ultérieures

FAS dépend du module `pam_krb5`, qui est obsolète sur RHEL/Rocky Linux 8.x et versions ultérieures. Les étapes suivantes sont requises si vous souhaitez utiliser le FAS sur des machines RHEL/Rocky Linux 8.x ou version ultérieure fournies en mode OS multi-session. Si vous utilisez le FAS sur les machines RHEL/Rocky Linux 8.x et versions ultérieures fournies en mode OS mono-session (VDI), vous pouvez ignorer les étapes suivantes.

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](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`.

```
1 yum install make gcc krb5-devel pam-devel autoconf libtool
2
3 rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio -div
4
5 tar xvzf pam_krb5-2.4.8.tar.gz
```

```
6
7 cd pam_krb5-2.4.8
8
9 ./configure --prefix=/usr
10
11 make
12
13 make install
```

3. Vérifiez que `pam_krb5.so` existe sous `/usr/lib64/security/`.

```
1 ls -l /usr/lib64/security | grep pam_krb5
```

## 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 CA 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 le télécharger 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.

Par exemple, pour convertir un fichier DER (.crt, .cer, .der) en PEM, exécutez une commande similaire à la suivante :

```
1 sudo openssl x509 -inform der -in root.cer -out root.pem
```

Installez ensuite le certificat d'autorité de certification racine dans le répertoire `openssl` en exécutant la commande suivante :

```
1 sudo cp root.pem /etc/pki/CA/certs/
```

### Remarque :

ne placez pas le certificat d'autorité de certification racine sous le chemin d'accès `/root`. Sinon, le FAS ne dispose pas de l'autorisation de lecture sur le certificat CA racine.

## Exécuter `ctxfascfg.sh`

Exécutez le script `ctxfascfg.sh` pour configurer FAS :

```
1 sudo /opt/Citrix/VDA/sbin/ctxfascfg.sh
```

Vous pouvez exécuter `ctxfascfg.sh` en mode silencieux. Avant d'exécuter le script en mode silencieux, définissez les variables d'environnement suivantes :

- **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 (KDC) 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. Si vous disposez de plusieurs Delivery Controllers, ajoutez les noms d'hôte de tous les KDC du domaine à `pkinit_kdc_hostname` dans le fichier `/etc/krb5.conf`. Pour obtenir davantage d'informations, veuillez consulter l'article [CTX322129](#) du centre de connaissances.
- **CTX\_FAS\_SERVER\_LIST='list-fas-servers'** : les serveurs du service d'authentification fédérée (FAS) sont configurés via la stratégie de groupe AD. Pour plus d'informations sur la définition de la stratégie FAS sur l'objet de stratégie de groupe du domaine, consultez [Configurer la stratégie de groupe](#). 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'`.

Pour mettre à niveau une installation Linux VDA existante, vous pouvez exécuter les commandes suivantes pour configurer les serveurs FAS et redémarrer le service `ctxvda` afin que vos paramètres soient pris en compte.

```
1 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  
2  
3 systemctl restart ctxjproxy  
4  
5 systemctl restart ctxvda
```

Pour mettre à jour les serveurs FAS via `ctxreg`, exécutez les commandes suivantes :

---

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
  VirtualDesktopAgent\Authentication\UserCredentialService" -v "
  Addresses" -d "<Your-FAS-Server-List>"
2
3 systemctl restart ctxjproxy
4
5 systemctl restart ctxvda
```

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.

### Désactiver FAS

Pour désactiver FAS sur le Linux VDA, supprimez tous les serveurs FAS de ConfDB à l'aide des commandes suivantes :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
  VirtualDesktopAgent\Authentication\UserCredentialService" -t "REG_SZ
  " -v "Addresses" -d "" --force
2
3 systemctl restart ctxjproxy
4
5 systemctl restart ctxvda
```

### Limitation

- 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 dépanner le FAS, assurez-vous que :

- Le Linux VDA est correctement installé et configuré.
- Une session non FAS peut être lancée avec succès sur le magasin commun à l'aide de l'authentification par mot de passe.

Si les sessions non FAS fonctionnent correctement, définissez le niveau de journalisation HDX de la classe **Loggin** 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](#).

Vous pouvez également utiliser l'outil Linux **XDPing** pour vérifier les problèmes de configuration courants susceptibles de survenir dans votre environnement VDA Linux.

### 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 :

```
1 2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user: [
    Logon Type] Federated Authentication Logon.
2
3 2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas:
    entry
4
5 2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: connect_fas: start
    connect to server 0
6
7 2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: connect_fas0:
    failed to connect: Connection refused.
8
9 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 configured in condb
10
11 2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: exit
    , 43
12
13 2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user:
    failed to validate fas credential
14
15 2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: LoginBoxValidate:
    failed validation of user 'user1@CTXDEV.LOCAL', INVALID_PARAMETER
```

**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>.

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep "UserCredentialService"
```

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 :

```
1 2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
   get_logon_certificate: entry
2
3 2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin: check_caller:
   current process: pid [30656], name [/opt/Citrix/VDA/bin/ctxlogin]
4
5 2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
   get_public_certificate: entry
6
7 2021-01-28 01:47:46.211 <P30656:S5> citrix-ctxlogin: query_fas: waiting
   for response...
8
9 2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin: query_fas: query
   to server success
10
11 2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin:
   get_public_certificate: exit
12
13 2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin: fas_base64_decode:
   input size 1888
14
15 2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: fas_base64_decode:
   output size 1415
16
17 2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin:
   get_logon_certificate: get logon certificate success
18
19 2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: cache_certificate:
   cache certificate success
20
21 2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin:
   get_logon_certificate: exit, 0
22
23 2021-01-28 01:47:48.060 <P30656:S5> citrix-ctxlogin: validate_user:
```

```
pam_authenticate err,can retry for user user1@CTXDEV.LOCAL
```

**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 :

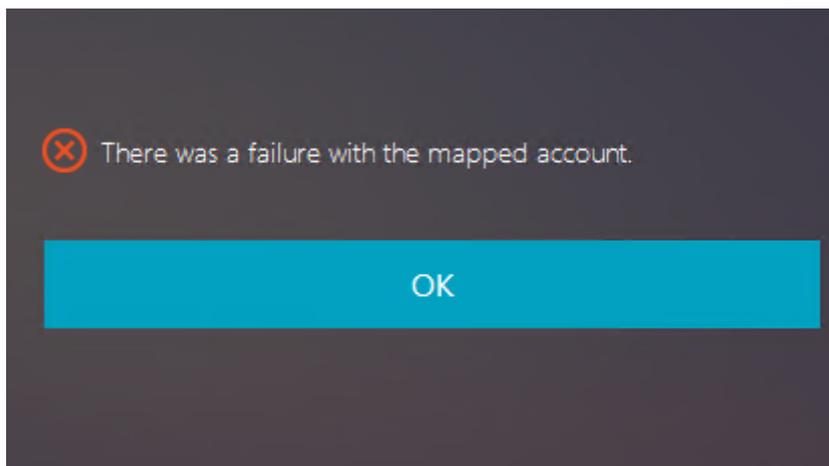
```
1  [realms]
2
3  EXAMPLE.COM = {
4
5
6      .....
7
8      pkinit_anchors = DIR:/etc/pki/CA/certs/
9
10     .....
11
12 }
```

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.

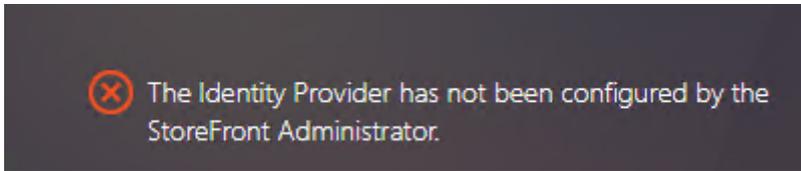


Cette erreur indique que l'utilisateur ADFS a été vérifié, mais qu'aucun utilisateur fictif n'est configuré sur AD.

**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 vous configurez le magasin FAS pour utiliser l'authentification SAML mais que le déploiement ADFS est manquant.

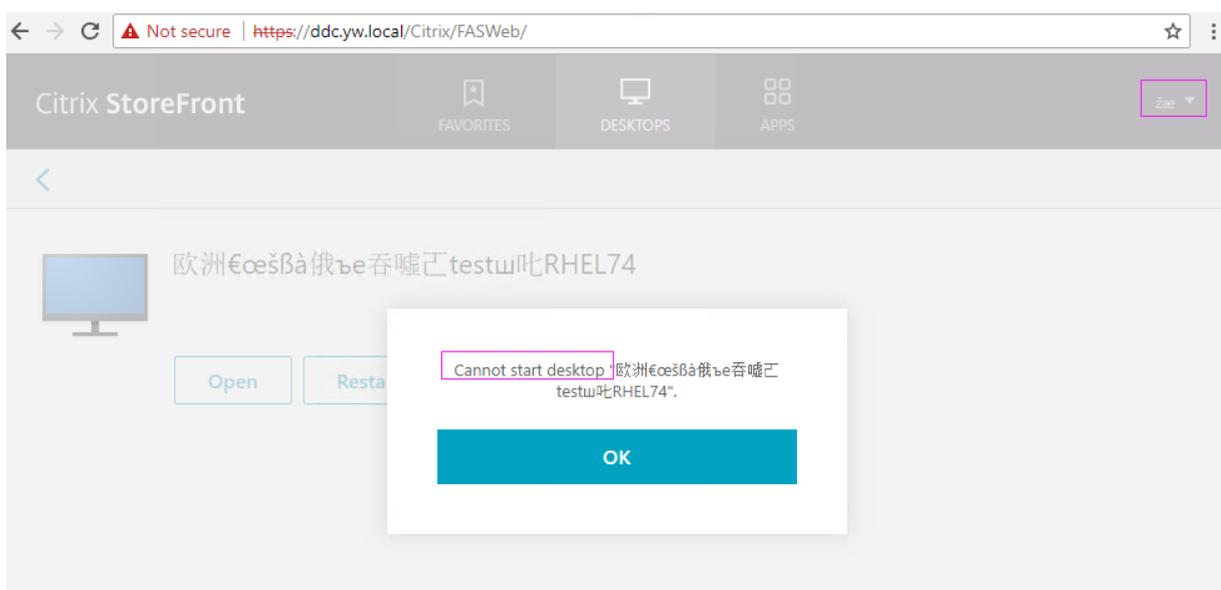
**Solution** Déployez le fournisseur d'identité ADFS du Service d'authentification fédérée. Pour plus d'informations, consultez la section [Déploiement ADFS du Service d'authentification fédérée](#).

## 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](#).

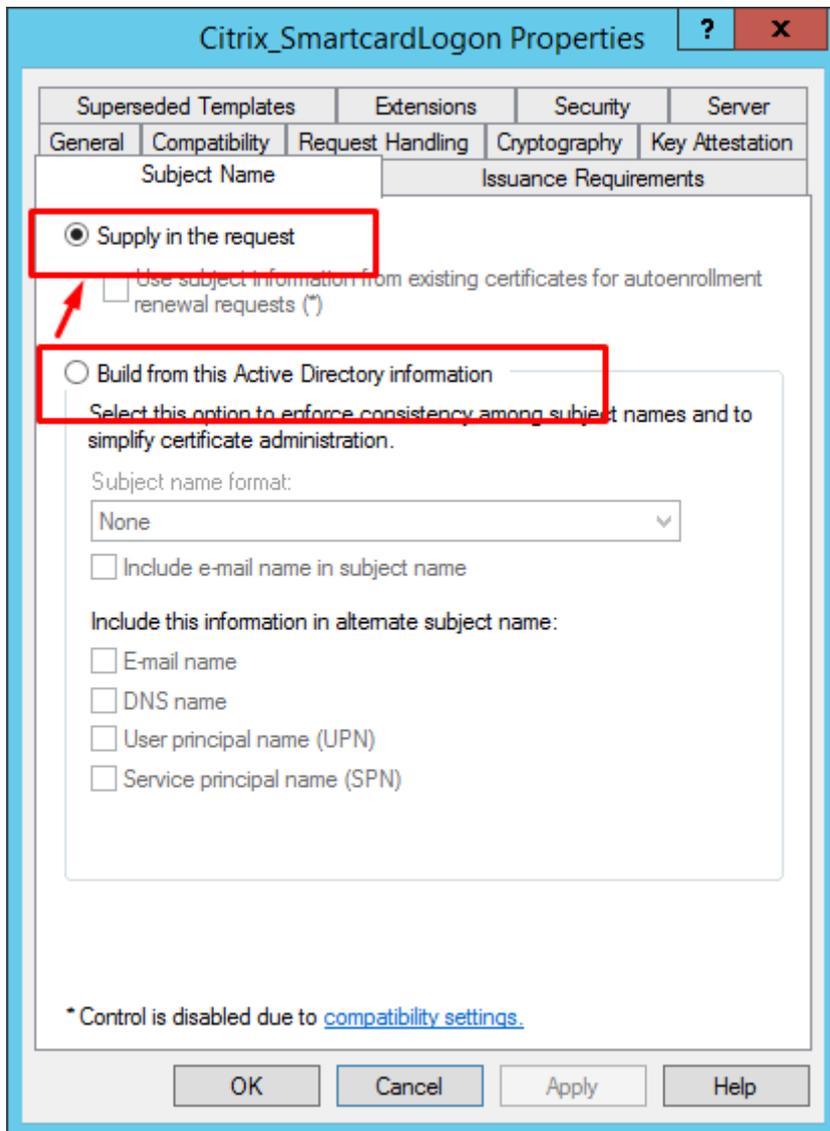
## Problèmes connus

Lorsque FAS est utilisé, la tentative de lancement d'une session de bureau ou d'application publiée avec des caractères non anglais peut échouer.



## 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** :



## FIDO2 (version Technical Preview)

August 20, 2024

Vous pouvez configurer l'authentification FIDO2 pour accéder aux sites Web à l'aide de Google Chrome hébergé sur le Linux VDA.

**Remarque :**

Cette fonctionnalité est disponible dans la Tech Preview. Les fonctionnalités de la version Technical Preview peuvent ne pas être entièrement localisées et sont recommandées pour une utilisation dans des environnements hors production. Le support technique de Citrix ne traite pas les problèmes rencontrés avec les fonctionnalités Technical Preview.

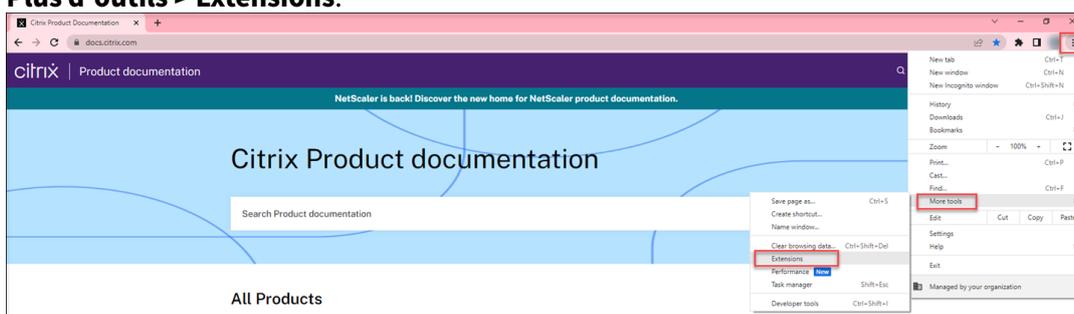
Le Linux VDA prend uniquement en charge la combinaison de FIDO2 et de Google Chrome.

Pour configurer l'authentification FIDO2, procédez comme suit :

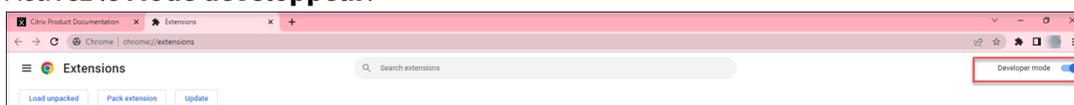
1. Téléchargez le package d'extension Citrix FIDO2.
  - a) Accédez à la [page de téléchargement de Citrix Virtual Apps and Desktops](#).
  - b) Développez la version appropriée de Citrix Virtual Apps and Desktops.
  - c) Cliquez sur **Composants** pour trouver le Linux VDA.
  - d) Cliquez sur le Linux VDA pour ouvrir sa page de téléchargement.
  - e) Téléchargez le package « sources ».
  - f) Décompressez le package « sources » et localisez le fichier **FIDO2-JavaScript-Extensions.zip**.
  - g) Décompressez le package d'extension FIDO2. Le répertoire des extensions FIDO2 est disponible dans **extensions > chrome > fido2**.

2. Ajoutez l'extension Citrix FIDO2 dans Google Chrome :

- a) Ouvrez Google Chrome hébergé sur le Linux VDA.
- b) Cliquez sur le menu à trois points situé à droite de la barre d'adresse, puis sélectionnez **Plus d'outils > Extensions**.



c) Activez le **Mode développeur**.



- d) Cliquez sur **Charger l'extension non empaquetée** et sélectionnez le répertoire de l'extension dans **extensions > chrome > fido2**.

3. Sur le site Web pour lequel vous souhaitez utiliser l'authentification FIDO2, enregistrez une clé de sécurité FIDO2 pour utiliser l'authentification FIDO2.

- a) Insérez une clé de sécurité FIDO2 dans le client sur lequel l'application Citrix Workspace est installée.
- b) Activez l'authentification multifacteur et ajoutez FIDO2 comme méthode d'authentification.

Une fois l'authentification FIDO2 configurée, vous serez invité à toucher la clé de sécurité pour accéder correctement au site Web.

## Pas d'authentification unique

August 20, 2024

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
FAS	Nom d'utilisateur
FAS	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
```

## Cartes à puce

August 20, 2024

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.

## Logiciels requis

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 9.2/9.0
  - RHEL 8.8/8.6
  - RHEL 7, CentOS 7
  - Rocky Linux 9.2/9.0
  - Rocky Linux 8.8/8.6
  - Ubuntu 22.04
  - Ubuntu 20.04
  - Debian 11.7/11.3

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](#).

## 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 :

```
1 pkcs11-tool --module opensc-pkcs11.so --list-slots
```

## 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.

```
1 openssl x509 -inform der -in certnew.cer -out certnew.pem
```

2. Installez le certificat racine dans le répertoire `openssl`. Le fichier **certnew.pem** est utilisé à titre d'exemple.

```
1 cp certnew.pem <path where you install the root certificate>
```

Pour créer un chemin d'accès pour l'installation du certificat racine, exécutez `sudo mkdir -p <path where you install the root certificate>`.

### Créer le module pam\_krb5 sur RHEL 8.x/9.x et Rocky Linux 8.x/9.x

L'authentification par carte à puce dépend du module pam\_krb5, qui est obsolète sur RHEL 8.x et Rocky Linux 8.x. Les étapes suivantes sont requises si vous souhaitez utiliser l'authentification par carte à puce sur les machines RHEL 8.x et Rocky Linux 8.x fournies en mode OS multi-session. Si vous utilisez l'authentification par carte à puce sur les machines RHEL 8.x et Rocky Linux 8.x fournies en mode OS mono-session (VDI), vous pouvez ignorer les étapes suivantes.

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](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.x et Rocky Linux 8.x.

```
1 yum install -y opensc pcsc-lite pcsc-lite-libs pcsc-lite-ccid nss-  
  tools  
2 yum install gcc krb5-devel pam-devel autoconf libtool  
3 rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio -div  
4 tar xvzf pam_krb5-2.4.8.tar.gz  
5 cd pam_krb5-2.4.8  
6 ./configure --prefix=/usr  
7 make  
8 make install
```

3. Vérifiez que pam\_krb5.so existe sous /usr/lib64/security/.

```
1 ls -l /usr/lib64/security | grep pam_krb5
```

### Configurer l'environnement de la carte à puce

Vous pouvez utiliser le script ctxsmartlogin.sh pour configurer l'environnement de carte à puce ou effectuer la configuration manuellement.

#### (Option 1) Utiliser le script ctxsmartlogin.sh pour configurer l'environnement de carte à puce

##### Remarque :

Le script ctxsmartlogin.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 ctxsmartlogin.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`.

```
1 sudo /opt/Citrix/VDA/sbin/ctxsmartlogon.sh
```

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
```

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 9.2/9.0/8.x, Rocky Linux 9.2/9.0/8.x, RHEL 7/CentOS 7 :**

```
1 yum install pcsc-lite pcsc-lite-ccid pcsc-lite-libs
```

**Ubuntu 22.04, Ubuntu 20.04, Debian 11.7, Debian 11.3 :**

```
1 apt-get install -y libpcsclite1 libccid
```

**Installer le pilote de la carte à puce** OpenSC est un pilote de carte à puce largement utilisé. Si OpenSC n'est pas installé, exécutez la commande suivante pour l'installer :

**RHEL 9.2/9.0/8.x, Rocky Linux 9.2/9.0/8.x, RHEL 7/CentOS 7 :**

```
1 yum install opensc
```

**Ubuntu 22.04, Ubuntu 20.04, Debian 11.7, Debian 11.3 :**

```
1 apt-get install -y opensc
```

**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 :**

```
1 yum install pam_krb5 krb5-pkinit
```

**RHEL 9.2/9.0/8.x, Rocky Linux 9.2/9.0/8.x :**

```
1 yum install krb5-pkinit
```

**Ubuntu 22.04, Ubuntu 20.04 :**

```
1 apt-get install libpam-krb5 krb5-pkinit
```

**Debian 11.7, Debian 11.3 :**

```
1 apt-get install -y libpam-krb5 krb5-pkinit
```

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 :

```
1 authconfig --enablekrb5 --update
```

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 :

```
1 EXAMPLE.COM = {
2
3
4     kdc = KDC.EXAMPLE.COM
5
6     auth_to_local = RULE:[1:$1@$0]
7
8     pkinit_anchors = FILE:<path where you install the root certificate
9         >/certnew.pem
10
11     pkinit_kdc_hostname = KDC.EXAMPLE.COM
12
13     pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature
```

```

13
14     pkinit_eku_checking = kpServerAuth
15
16 }

```

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

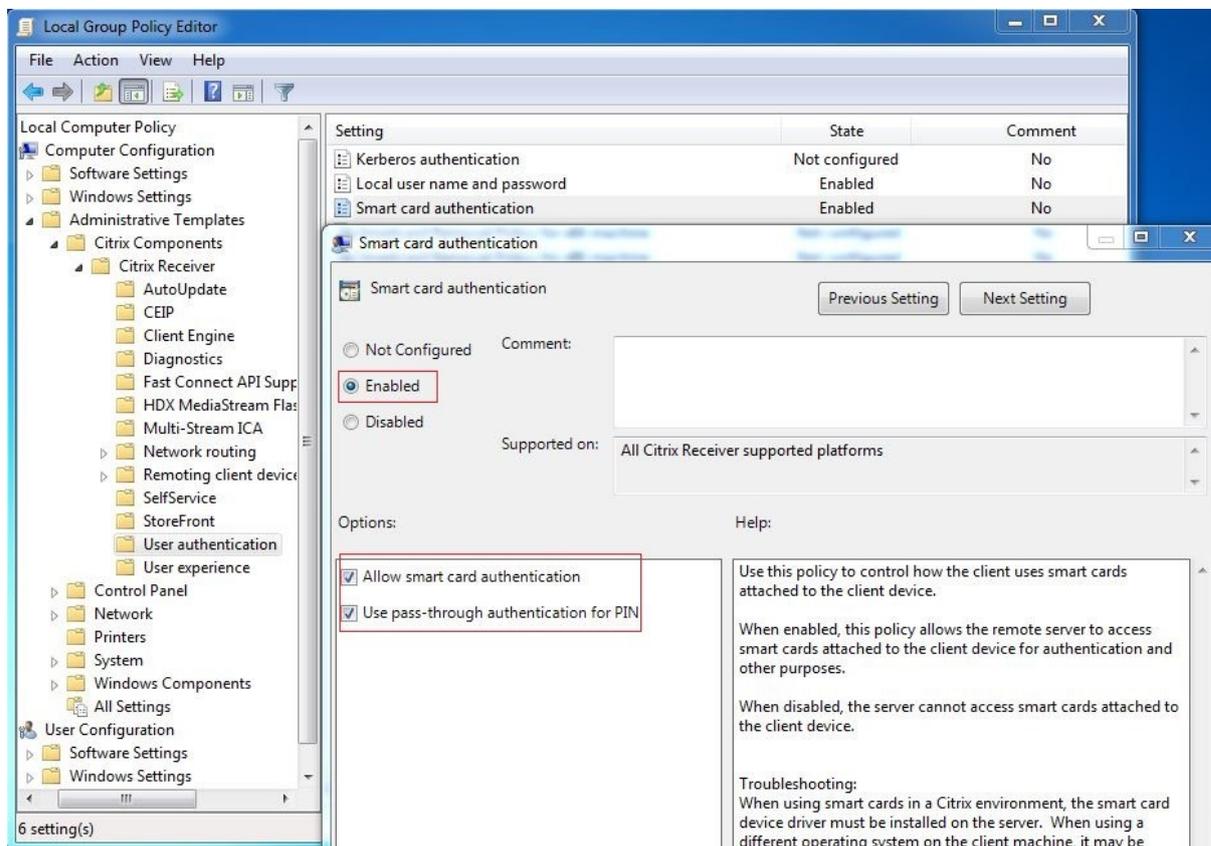
```

### (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, config-

urez 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 con-

nexion par carte à puce rapide, incluez le paramètre suivant dans le fichier default.ica du site StoreFront associé :

```
1 [WFClient]
2 SmartCardCryptographicRedirection=0n
```

**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.

### Exécuter XDPing

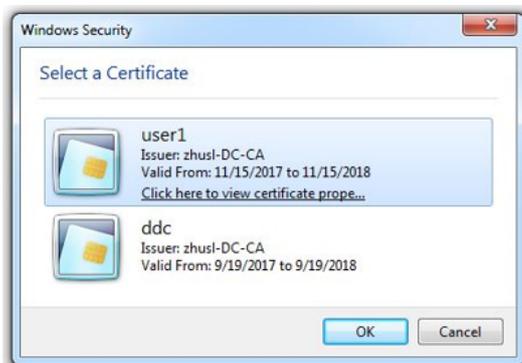
Après avoir effectué les étapes précédentes, vous pouvez utiliser l’outil Linux **XDPing** pour vérifier les problèmes de configuration courants susceptibles de survenir dans votre environnement Linux VDA.

### Utilisation

#### Se connecter au Linux VDA en utilisant une carte à puce

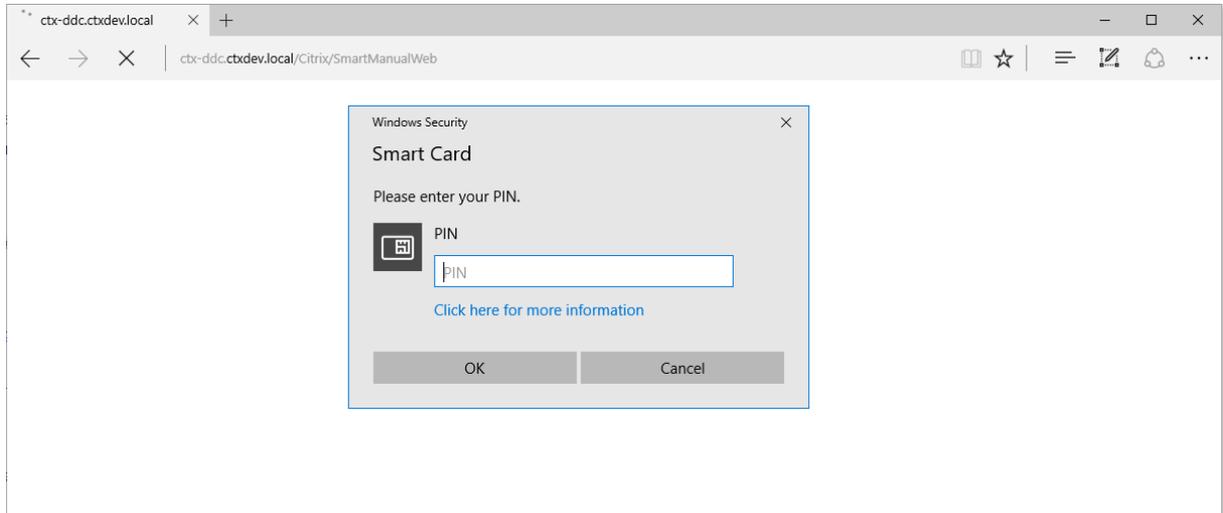
Vous pouvez utiliser une carte à puce pour vous connecter au Linux VDA dans les scénarios SSO et non SSO.

- 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.

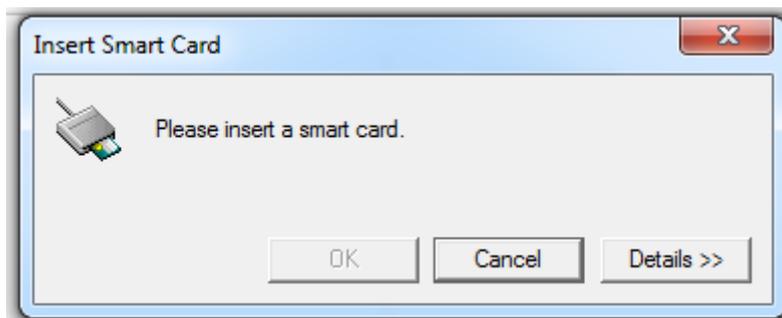
Le comportement est le même avec le VDA Windows.



### 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

### Prise en charge des distributions Linux limitées et des méthodes d'intégration AD

- L'authentification pass-through par carte à puce prend en charge les distributions Linux limitées et les méthodes d'intégration AD. Reportez-vous à la matrice suivante :

	Winbind	SSSD	Centrify
Debian 11.7/11.3	Oui	Oui	Oui
RHEL 9.2/9.0	Oui	Oui	Non
RHEL 8.8/8.6	Oui	Oui	Oui
RHEL 7.9, CentOS 7.9	Oui	Oui	Oui
Rocky Linux 9.2/9.0	Oui	Oui	Non
Rocky Linux 8.8/8.6	Oui	Oui	Non
Ubuntu 22.04/20.04	Oui	Oui	Oui

### Stratégie de retrait de carte à puce

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 :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
CurrentControlSet\Control\Citrix\VirtualChannels\Scard" -v "
PKCS11LibPath" -d "PATH"
```

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.

## Accès des utilisateurs non authentifiés (anonymes)

August 20, 2024

Vous pouvez autoriser les utilisateurs à accéder aux applications et aux bureaux sans présenter d'informations d'identification à StoreFront ou à l'application Citrix Workspace. Pour accorder l'accès à des utilisateurs non authentifiés, vous devez disposer d'un magasin StoreFront non authentifié et autoriser l'accès des utilisateurs non authentifiés dans un groupe de mise à disposition.

### Remarque :

L'accès des utilisateurs non authentifiés est pris en charge pour les VDA joints au domaine uniquement.

Le pré-démarrage de session n'est pas pris en charge pour les utilisateurs non authentifiés. Le pré-démarrage de session n'est pas non plus pris en charge sur l'application Citrix Workspace pour Android.

## Créer un magasin StoreFront non authentifié

1. Sélectionnez le nœud **Magasins** dans le panneau gauche de la console de gestion Citrix StoreFront, puis dans le panneau **Actions**, cliquez sur **Créer un magasin**.
2. Sur la page **Nom du magasin**, spécifiez un nom pour votre magasin, sélectionnez **Autoriser uniquement les utilisateurs non authentifiés (anonymes) à accéder à ce magasin**, puis cliquez sur **Suivant**.

Pour plus d'informations, consultez [Créer un magasin non authentifié](#).

## Autoriser l'accès des utilisateurs non authentifiés dans 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. Lorsque vous spécifiez qui peut utiliser les applications et les bureaux d'un groupe de mise à disposition, vous pouvez accorder l'accès à des utilisateurs non authentifiés. Pour plus d'informations, consultez la section

[Créer des groupes de mise à disposition](#).

## Définir le délai d'inactivité des sessions d'utilisateur non authentifié

Les sessions d'utilisateur non authentifié possèdent un délai d'inactivité par défaut de 10 minutes ; de plus, les sessions sont automatiquement fermées lorsque le client se déconnecte. Vous pouvez configurer un délai d'inactivité personnalisé via le paramètre de registre **AnonymousUserIdleTime**. Par exemple, pour définir un délai d'inactivité personnalisé de cinq minutes, exécutez la commande suivante :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
  CurrentControlSet\Control\Citrix" -v AnonymousUserIdleTime -d 0
  x00000005
```

## 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 d'utilisateur non authentifié 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, exécutez la commande suivante :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
  CurrentControlSet\Control\Citrix" -v MaxAnonymousUserNumber -d 0
  x00000020
```

### Important :

Limitez le nombre de sessions d'utilisateur non authentifié. Le lancement d'un trop grand nombre de sessions simultanées peut entraîner des problèmes sur le VDA, y compris la saturation de la mémoire.

## Dépannage

Tenez compte des éléments suivants lors de la configuration de sessions d'utilisateur non authentifié :

- **Impossible de se connecter à une session d'utilisateur non authentifié.**

Vérifiez que le registre a été mis à jour comme suit (défini sur 0):

```
1 sudo /opt/Citrix/VDA/bin/ctxreg read -k "HKLM\System\CurrentControlSet\
  \Control\Citrix" -v MaxAnonymousUserNumber
```

Vérifiez que le service **ncsd** est en cours d'exécution et qu'il est configuré pour activer le cache **passwd** :

```
1 ps uax | grep nscd
2 cat /etc/nscd.conf | grep 'passwd' | grep 'enable-cache'
```

Définissez la variable du cache **passwd** sur **no** s'il est activé, puis redémarrez le service **nscd**. 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 d'utilisateur non authentifié avec KDE.**

Le bouton et le menu de l'écran de verrouillage sont désactivés par défaut dans une session d'utilisateur non authentifié. 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 :

```
1 [KDE Action Restrictions]
2 action/lock_screen=false
```

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

August 20, 2024

Cette section contient les rubriques suivantes :

- [Copier-coller de fichiers](#)
- [Transfert de fichiers](#)

## Copier-coller de fichiers

August 20, 2024

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.
- Les noms de fichiers ne contiennent que des caractères ASCII et aucun caractère spécial.

## 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 du 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 des opérations 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

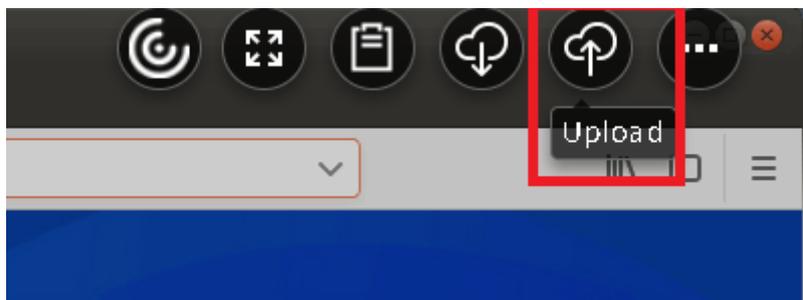
August 20, 2024

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 10 fichiers en même temps.



### Remarque :

Pour charger et télécharger des fichiers entre Linux VDA 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 :

Pour activer le téléchargement automatique, vous devez définir les stratégies **Transfert de fichiers pour l'application Citrix Workspace pour ChromeOS/HTML5** et **Téléchargement de**

## fichiers pour l'application Citrix Workspace pour ChromeOS/HTML5 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

Par défaut, le transfert de fichiers est activé. Utilisez Citrix Studio pour modifier ces stratégies. Elles se trouvent sous **Paramètres utilisateur > ICA\Redirection de dossiers**. Tenez compte de ce qui suit lors de l'utilisation des stratégies de transfert de fichiers :

**Transfert de fichiers pour l'application Citrix Workspace pour ChromeOS/HTML5** : autorise ou empêche les utilisateurs de transférer des fichiers entre une session Citrix Virtual Apps and Desktops ou Citrix DaaS et leurs appareils.

**Charger un fichier pour l'application Citrix Workspace pour ChromeOS/HTML5** : autorise ou empêche les utilisateurs de charger des fichiers. depuis leur appareil sur une session Citrix Virtual Apps and Desktops ou Citrix DaaS.

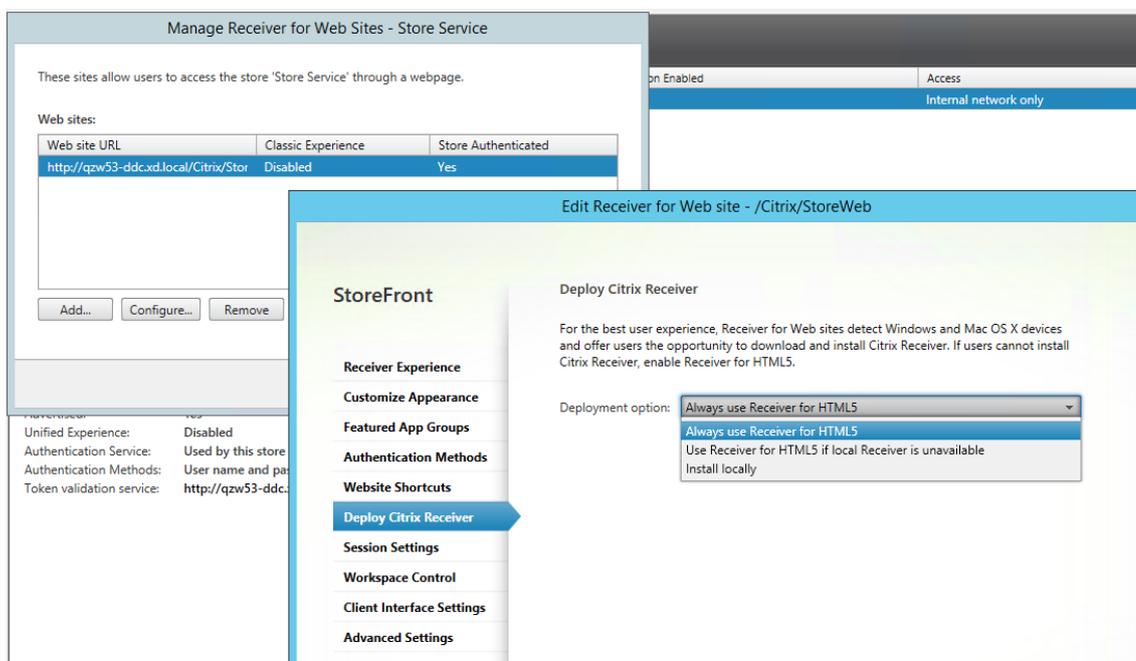
**Télécharger le fichier pour l'application Citrix Workspace pour ChromeOS/HTML5** : autorise ou empêche les utilisateurs de télécharger des fichiers Cette opération peut s'effectuer depuis une session Citrix Virtual Apps and Desktops ou Citrix DaaS vers l'appareil de l'utilisateur.

## 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**.



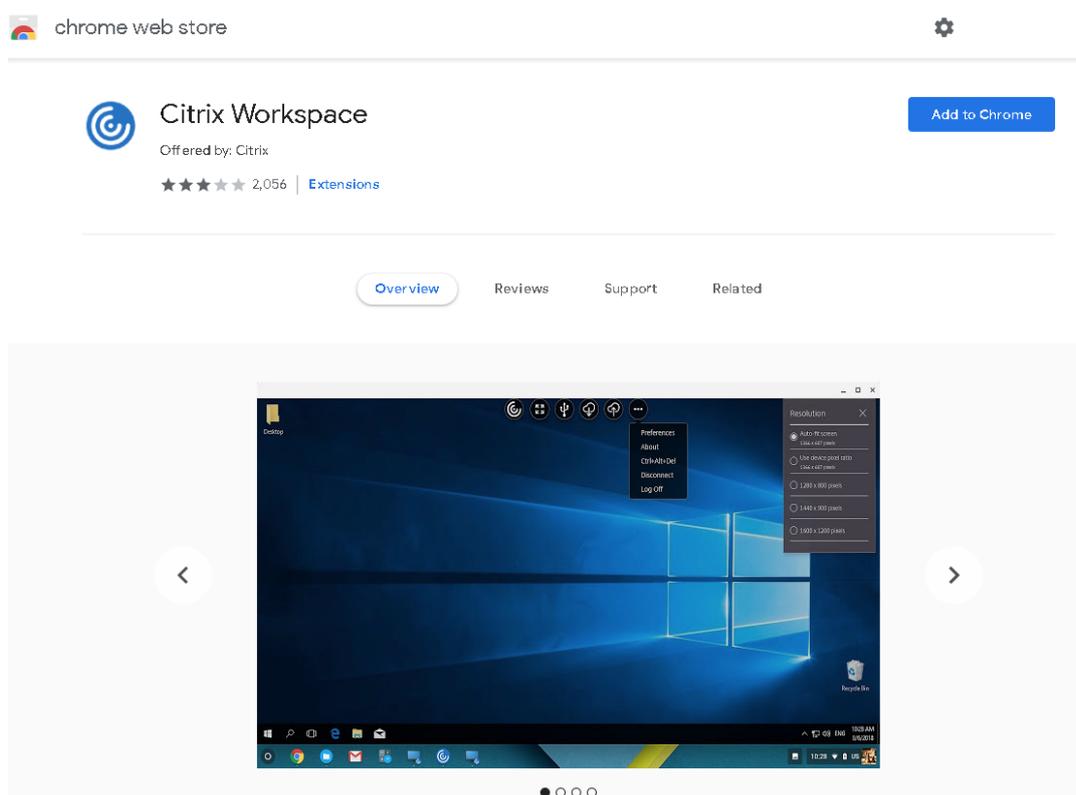
4. Lancez une session de bureau virtuel ou d'application de navigateur Web. Effectuez un ou plusieurs transferts de fichiers entre le VDA Linux et votre machine cliente.

#### **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

August 20, 2024

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](#)
- [GPU non virtualisés](#)
- [Filigrane de session](#)
- [Affichage progressif Thinwire](#)

## Mise à l'échelle DPI automatique

August 20, 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	Dimension de l'écran
Inférieur ou égal à 174 %	96 (1 x 96)	100 %
175 %–274 %	192 (2 x 96)	200 %
275 %–399 %	288 (3 x 96)	300 %
Supérieur ou égal à 400 %	384 (4 x 96)	400 %

---

**Remarque :**

La machine Linux VDA a une capacité de montée en charge jusqu'à 200 % pour les bureaux MATE.

## Affichage de l'état de la batterie client

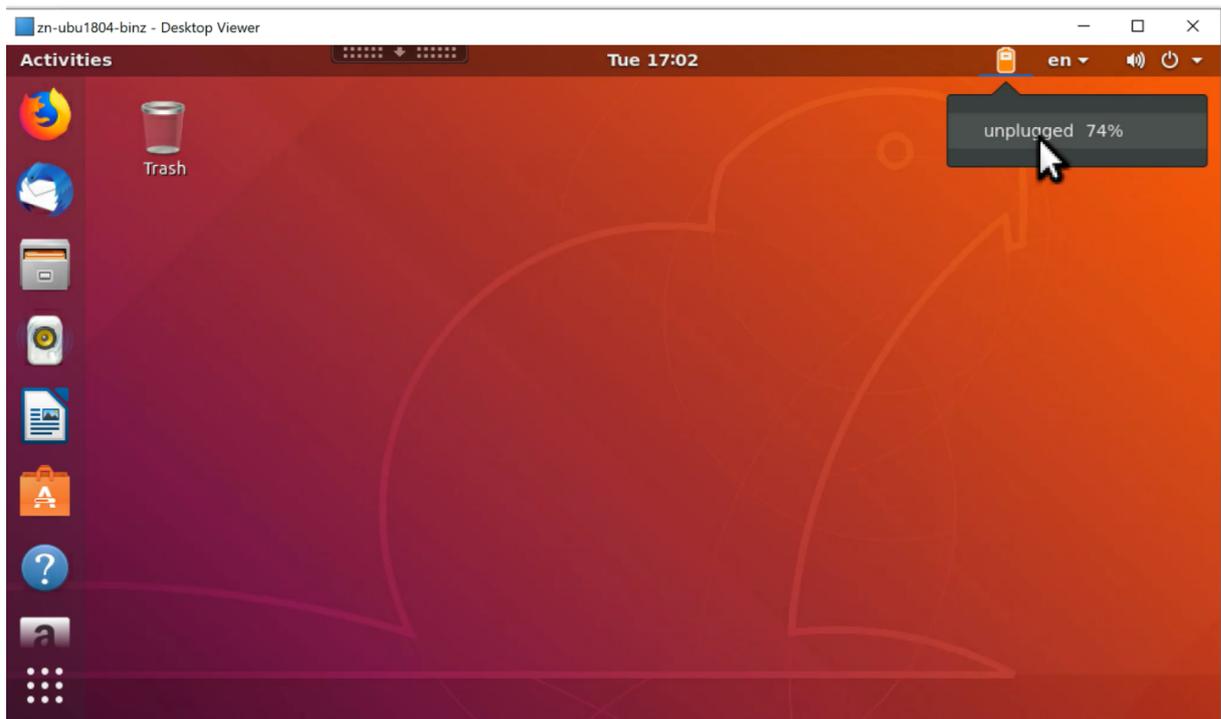
August 20, 2024

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 %
	Pas en cours de charge, indiqué par un symbole « + »	Élevé, indiqué par une couleur verte	=80 %

Icône de batterie	État de charge	Niveau d'autonomie restante	Pourcentage d'autonomie restante
	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 :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\MrVc" -v "Enabled" -d "0x00000000"
```

Pour activer cette fonctionnalité, exécutez la commande suivante :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\MrVc" -v "Enabled" -d "0x00000001"
```

### 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, effectuez les étapes supplémentaires pour activer la fonctionnalité. Pour plus d'informations, consultez la section [Activer la barre d'état système](#).

## Configuration et réglage précis des graphiques

August 20, 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.

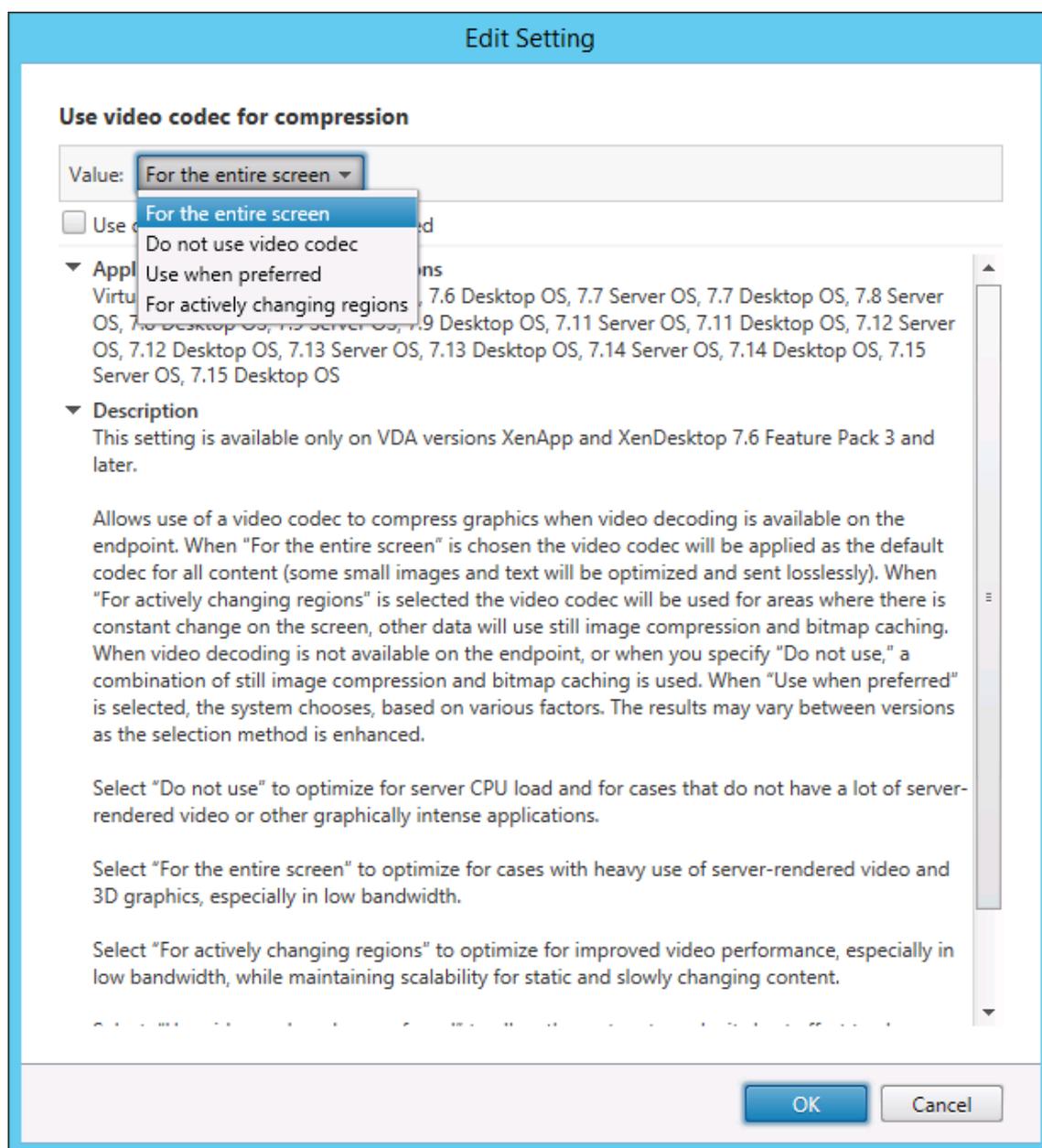
### Codec vidéo pour la compression

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 AV1, H.264 ou H.265 uniquement dans la partie de l'écran sur laquelle l'image est en mouvement. L'utilisation sélective du codec vidéo AV1, H.264 ou H.265 permet à HDX Thinwire de détecter et de coder des parties de l'écran qui sont fréquemment mises à jour. 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 avec des images de haute qualité. L'utilisation sélective du codec vidéo AV1 ou H.265 n'est pas prise en charge lorsque la stratégie **Qualité visuelle** est définie sur **Toujours sans perte** ou sur **Sans perte si possible**.



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 AV1/H.265/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. L'accélération matérielle du GPU optimise l'utilisation des ressources matérielles et améliore considérablement les performances des images par seconde (FPS).

L'accélération matérielle du GPU couvre tous les modes graphiques définis par la stratégie [Utiliser codec vidéo pour la compression](#) :

- **Utiliser au choix**
- **Pour l'écran entier**
- **Pour les zones changeant constamment**

Pour activer la compression vidéo matérielle, procédez comme suit :

1. Définissez la stratégie **Utiliser le codage matériel pour le codec vidéo** sur **Activé**.
2. Définissez le paramètre **Utiliser codec vidéo pour la compression** sur **Utiliser au choix, Pour l'écran entier** ou **Pour les zones changeant constamment**. Assurez-vous que le paramètre n'est pas réglé sur **Ne pas utiliser de codec vidéo**.

Pour pouvoir être utilisé, le codec vidéo AV1 ou H.265 doit être pris en charge et activé à la fois sur le VDA et l'application Citrix Workspace. AV1 obtient la préférence sur H.265 et H.264 lors de la négociation du codec. Lorsque AV1 n'est pas pris en charge, H.265 est négocié. Si AV1 et H.265 ne sont pas pris en charge, les sessions recommencent à utiliser le codec vidéo H.264. Si le matériel GPU n'est pas disponible, le VDA utilise le codage basé sur l'UC avec le codec vidéo logiciel.

### **Exigences relatives à l'encodage matériel AV1**

#### **VDA**

- VDA : 2311 ou version ultérieure
- Unité de traitement graphique : **NVIDIA Ada Lovelace ou version ultérieure** (pour obtenir une matrice des codecs vidéo pris en charge par les GPU NVIDIA, consultez le document NVIDIA à l'adresse <https://developer.nvidia.com/video-encode-and-decode-gpu-support-matrix-new>.)
- Pilote graphique NVIDIA 522.25 ou version ultérieure (SDK du codec vidéo v12.0)

#### **Client**

- Application Citrix Workspace 2305 pour Windows ou version ultérieure

- GPU client prenant en charge le décodage AV1 :
  - NVIDIA Ampere ou version ultérieure
  - Intel 11e génération/Arc ou version ultérieure
  - AMD Radeon RX 6000/Radeon Pro W6000 series (RDNA2) ou version ultérieure

## Exigences relatives à l'encodage matériel H.265

### Client

- Citrix Receiver pour Windows 4.10 à 4.12
- Application Citrix Workspace 1808 pour Windows et versions ultérieures

Pour activer le codage matériel H.265 sur votre client, consultez la section [Codage vidéo H.265](#).

## Compression sans perte H.265/H.264

La prise en charge de la compression sans perte H.265/H.264 est disponible pour l'accélération matérielle HDX 3D PRO par les GPU NVIDIA. La compression sans perte H.265 nécessite l'application Citrix Workspace 2305 pour Windows et versions ultérieures. La compression sans perte H.264 nécessite les clients suivants :

- Application Citrix Workspace 2303 pour Windows et versions ultérieures
- Application Citrix Workspace 2301 pour Mac et versions ultérieures avec la puce Apple M1

Pour activer la compression sans perte H.265/H.264, procédez comme suit :

1. Définissez la stratégie **Utiliser le codage matériel pour le codec vidéo** sur **Activé**.
2. Définissez la stratégie **Utiliser codec vidéo pour la compression** sur **Pour l'écran entier**.
3. Définissez la stratégie **Qualité visuelle** sur **Toujours sans perte** ou **Sans perte si possible**.

## 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.

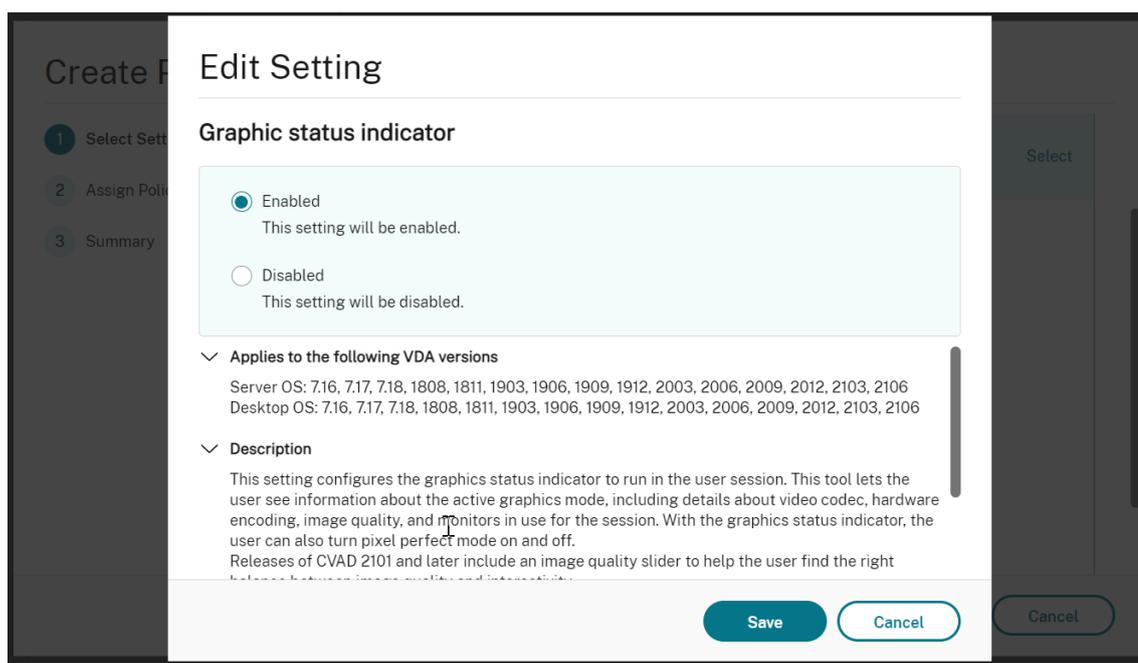
Pour plus d'informations sur les paramètres de stratégie **Qualité visuelle** et **Utiliser codec vidéo pour la compression**, consultez la section [Paramètres de stratégie Affichage visuel](#) et [Paramètres de stratégie Graphiques](#).

## 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.

- Vous pouvez lancer l'interface utilisateur du curseur à la fois depuis le terminal et depuis la [barre d'état système](#).



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.

Cette fonctionnalité est activée par défaut. Pour la 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
```

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
```

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 :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
  CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
  ParallelProcessing" -d "0x00000001" --force
```

### 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) :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep GraphicsMode
```

Le résultat se présente comme suit :

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "GraphicsMode"-d "0x00000000"--force
```

#### Vérifier que l'AV1 est en cours d'utilisation

##### Remarque :

Pour vérifier quel codec vidéo est utilisé pour la session en cours, exécutez la commande ci-dessous ou vérifiez l'état graphique dans la barre d'état [système](#).

Exécutez la commande suivante pour vérifier si AV1 est en cours d'utilisation (**0** signifie qu'il n'est pas utilisé ; **1** signifie qu'il est utilisé) :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep AV1
```

Par exemple, le résultat peut se présenter comme suit :

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"  
-v "AV1"-d "0x00000000"--force
```

### Vérifiez que H.265 est utilisé

Exécutez la commande suivante pour vérifier que H.265 plein écran est en cours d'utilisation (**0** signifie qu'il n'est pas utilisé ; **1** signifie qu'il est utilisé) :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H265
```

Par exemple, le résultat peut se présenter comme suit :

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"  
-v "H265"-d "0x00000000"--force
```

### Vérifier que H.264 est utilisé

Exécutez la commande suivante pour vérifier que H.264 est en cours d'utilisation (**0** signifie qu'il n'est pas utilisé ; **1** signifie qu'il est utilisé) :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H264
```

Par exemple, le résultat peut se présenter comme suit :

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"  
-v "H264"-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
```

Par exemple, le résultat peut se présenter comme suit :

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"  
-v "YUVFormat"-d "0x00000000"--force
```

### Vérifier que le codage logiciel YUV444 est utilisé

Exécutez la commande suivante pour vérifier que le codage logiciel YUV444 est utilisé :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep Graphics
```

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 que HDX 3D Pro est activé

Exécutez les commandes suivantes pour vérifier que HDX 3D Pro est activé :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep ProductEdition  
2  
3 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep StackSessionMode  
4  
5 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep 3DPro
```

Lorsque HDX 3D Pro est activé, le résultat se présente comme suit :

```
create -k "HKLM\Software\Citrix\VirtualDesktopAgent\State"-t "REG_SZ"  
-v "ProductEdition"-d "<PLT or ENT>"--force  
create -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\  
tcp"-t "REG_DWORD"-v "StackSessionMode"-d "0x00000000"--force  
create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD"  
-v "3DPro"-d "0x00000000"--force
```

Pour vérifier que les bibliothèques NVIDIA requises sont chargées pour HDX 3D Pro, exécutez la commande **nvidia-smi** sur le Linux VDA. Le résultat se présente comme suit :

```

1 Tue Apr 12 10:42:03 2016
2 +-----+
3 | NVIDIA-SMI 361.28      Driver Version: 361.28      |
4 |-----+-----+
5 | GPU   Name           Persistence-M| Bus-Id        Disp.A | Volatile
6 | Fan  Temp  Perf    Pwr:Usage/Cap|      Memory-Usage | GPU-Util
7 | Compute M. |
8 |-----+-----+
9 |    0  GRID K1              Off   | 0000:00:05.0   Off   |
10 | N/A   42C    P0              N/A   | 14W / 31W     | 207MiB / 4095MiB |    8%
11 | Default |
12 +-----+-----+
13 | Processes:                                                    GPU
14 |   Memory |
15 | GPU      PID  Type  Process name
16 | Usage    |
17 |-----+-----+
18 |    0      2164  C+G  /usr/local/bin/ctxgfx
19 | 106MiB |
20 |    0      2187    G    Xorg
21 | 85MiB |
22 +-----+-----+

```

### Vérifier que 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
```

Lorsque 3D Pro est utilisé, le résultat se présente comme suit :

```
create -k "HKLM\Software\Citrix\Ica\Session\1\Graphics"-t "REG_DWORD"
-v "HardwareEncoding"-d "0x00000001"--force
```

### 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 :

```

1 +-----+
2 | NVIDIA-SMI 352.70      Driver Version: 352.70      |
3 |-----+-----+
4 | GPU   Name           Persistence-M| Bus-Id        Disp.A | Volatile
   |   Uncorr. ECC |
5 | Fan  Temp  Perf    Pwr:Usage/Cap|      Memory-Usage | GPU-Util
   |   Compute M. |
6 |=====+=====+
7 |    0   Tesla M60                Off      | 0000:00:05.0    Off  |
   |               Off  |
8 | N/A   20C    P0     37W / 150W |      19MiB /  8191MiB |      0%
   |   Default |
9 +-----+-----+
10
11 +-----+-----+
12 | Processes:                                                       GPU
   |   Memory |
13 | GPU       PID  Type  Process name
   |   Usage   |
14 |=====+=====+
15 |   No running processes found
16 +-----+-----+

```

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 XenServer (anciennement Citrix Hypervisor) affiche l'écran de la session de bureau ICA

**Solution** : désactivez la console VGA locale de la machine virtuelle en exécutant la commande suivante :

```
1 [root@xenserver ~]# xe vgpu-param-set uuid=vgpu-uuid extra_args=
  disable_vnc=1
```

### 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** pourrait engendrer une erreur indiquant que le **rendu dans cette texture n'est pas pris en charge (tampon de trame incomplet)**.

## Partage d'écran HDX

August 20, 2024

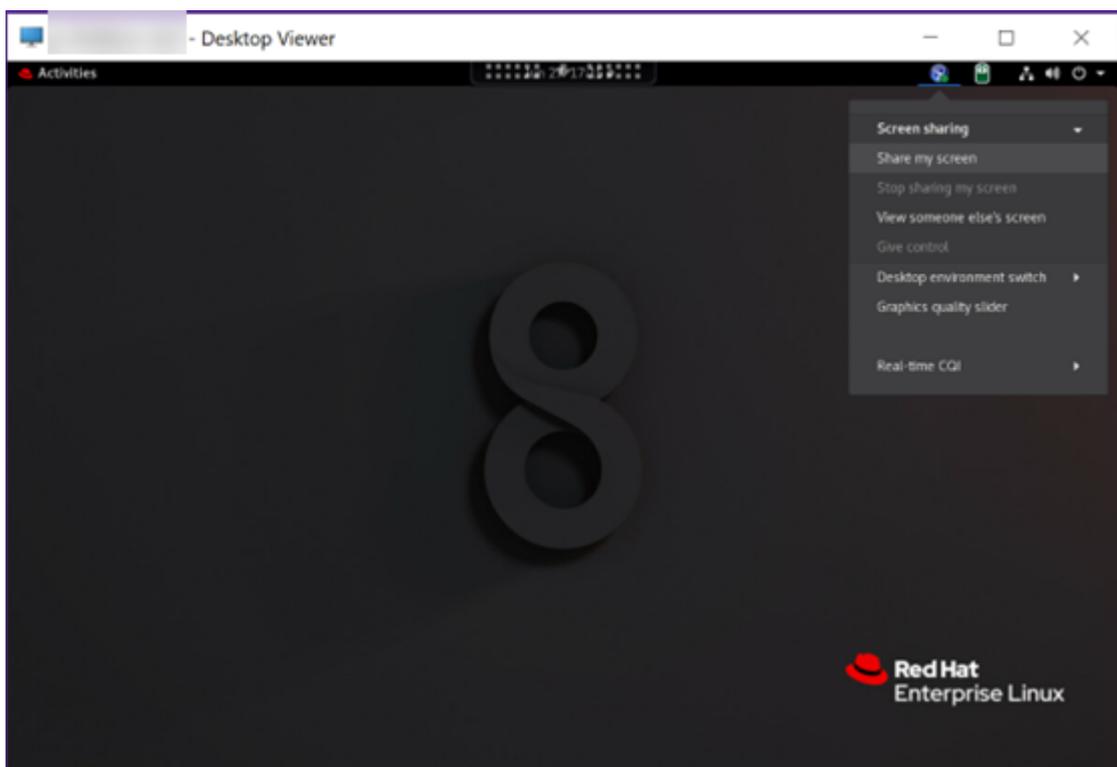
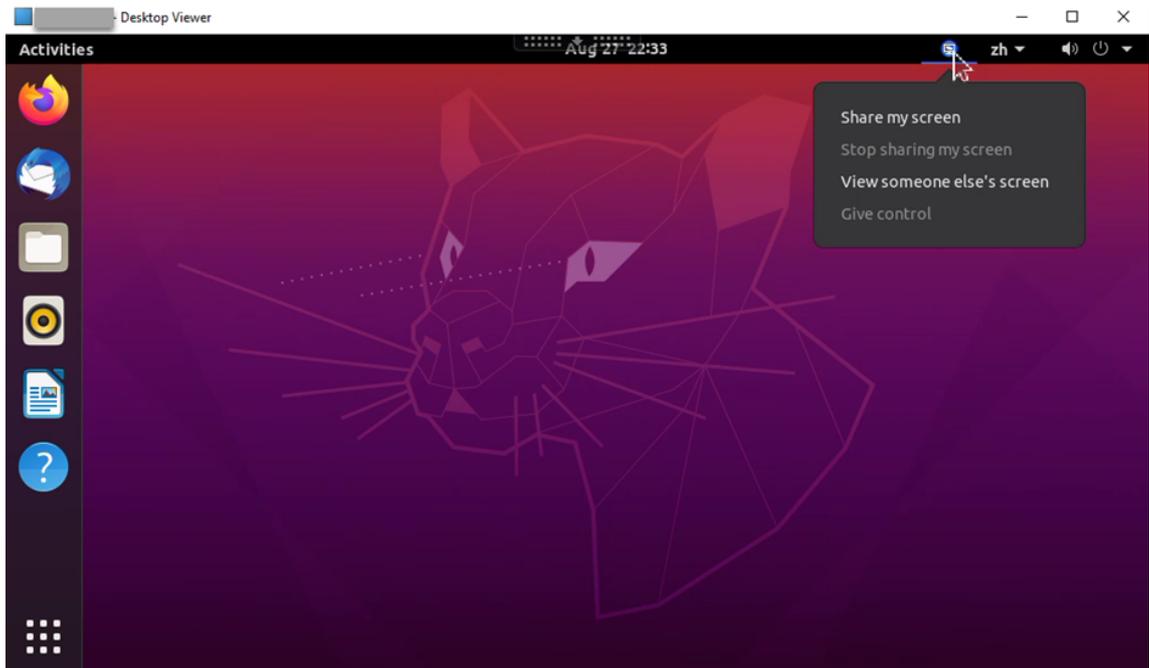
### Vue d'ensemble

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.

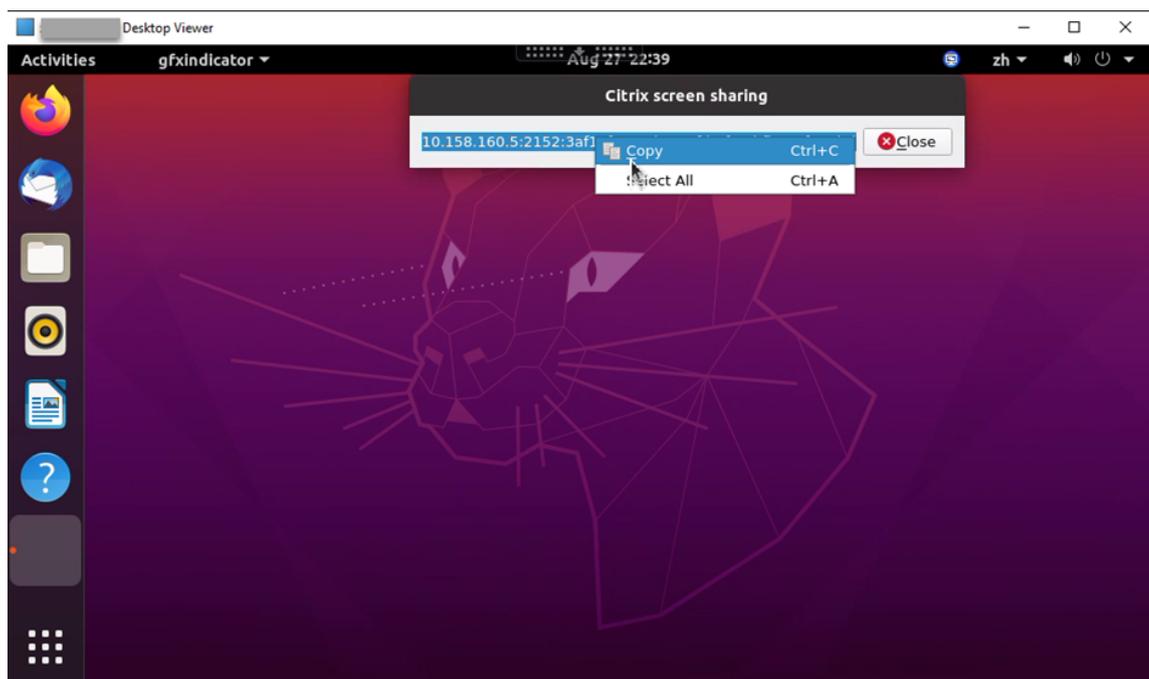
#### Pour partager un écran :

1. Dans la zone de notification de votre bureau virtuel, cliquez sur l'icône de la barre d'état système et sélectionnez **Partage d'écran > Partager mon écran**.



2. Cliquez sur **Copier et fermer**.

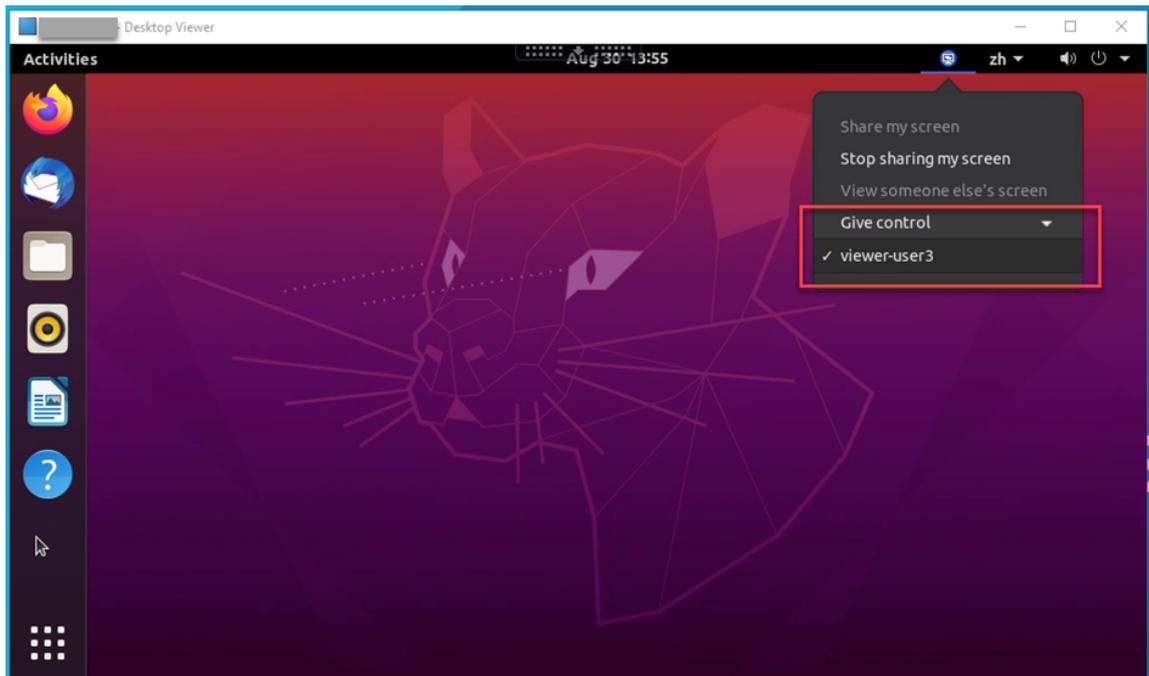
Le code de partage d'écran actuel persiste jusqu'à ce que vous arrêtez et recommencez le partage de votre écran.



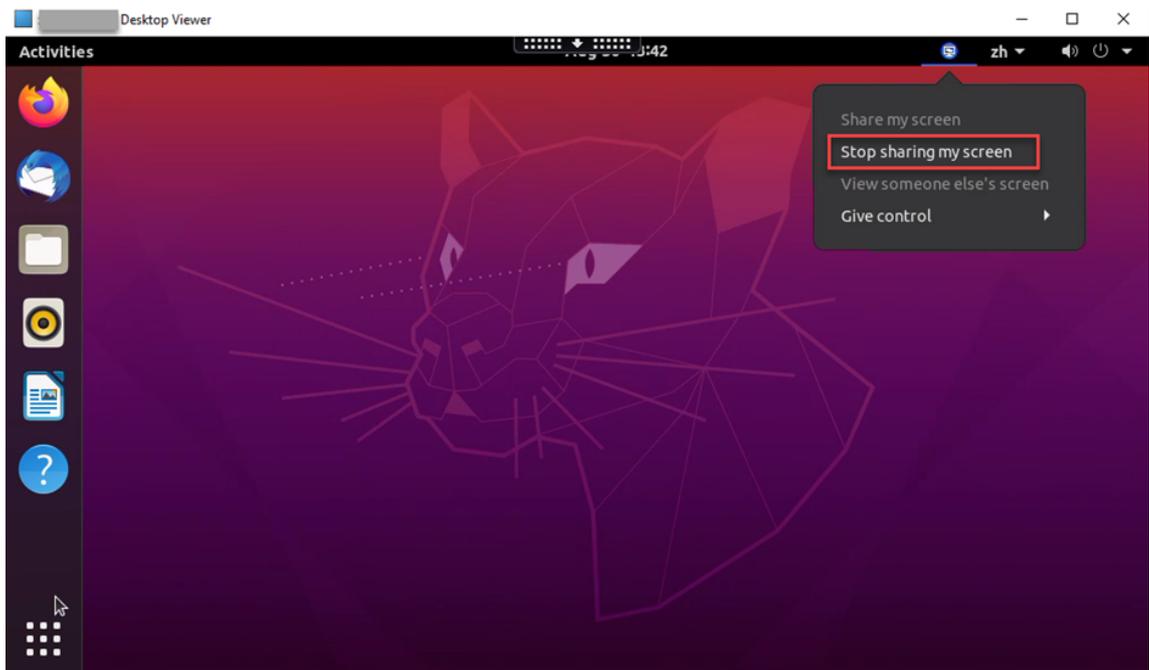
**Conseil :**

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.

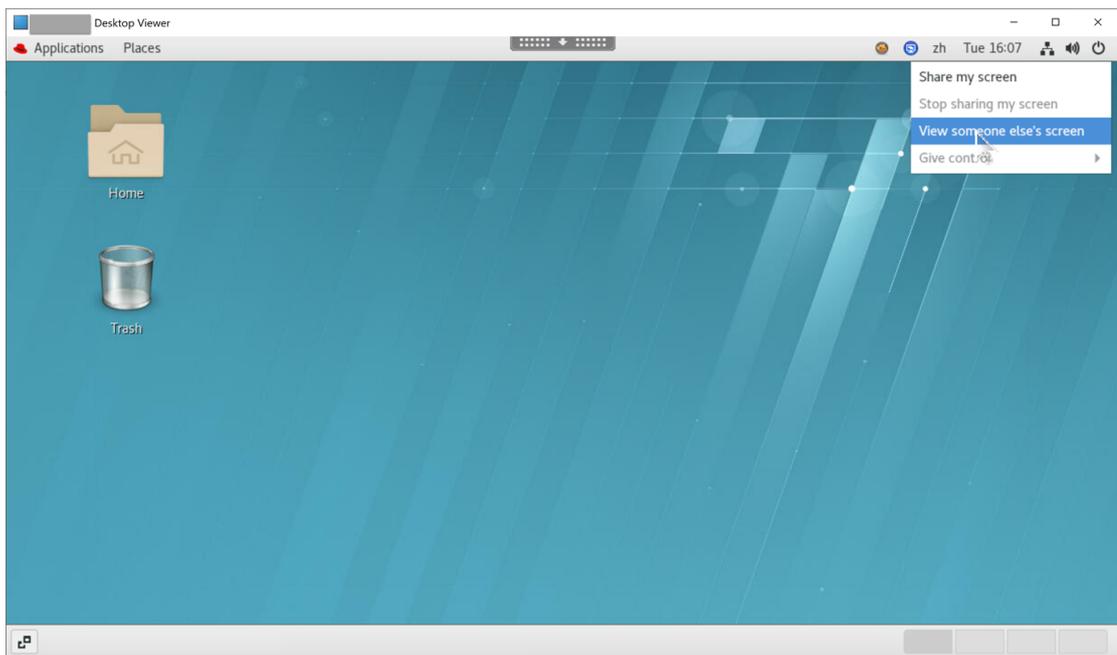


5. Pour arrêter le partage de votre écran, sélectionnez **Arrêter de partager mon écran**.

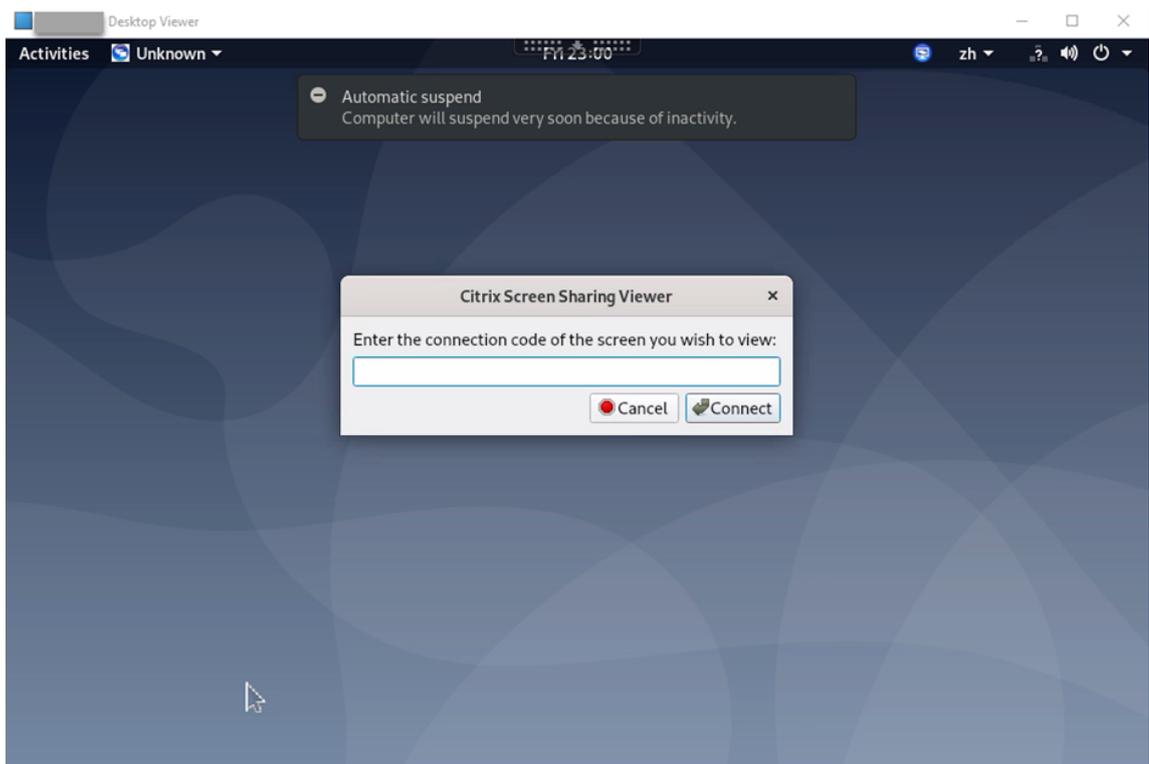


**Pour afficher l'écran d'un autre utilisateur :**

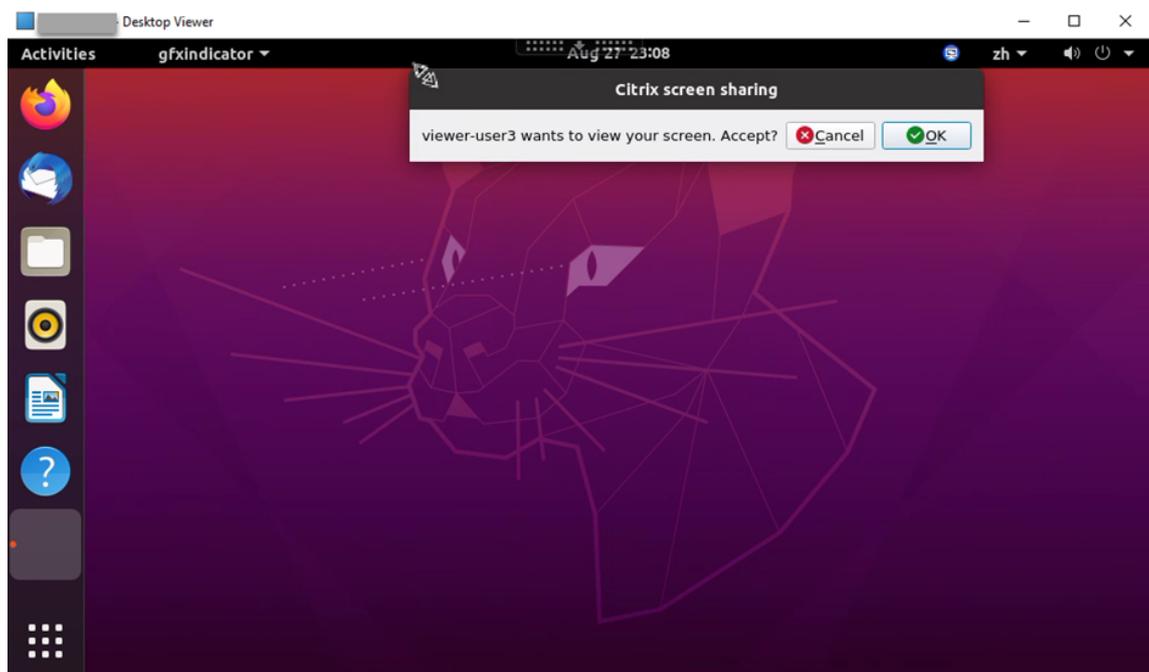
1. Dans la zone de notification de votre bureau virtuel, cliquez sur l'icône de **partage d'écran** et sélectionnez **Afficher l'écran de quelqu'un d'autre**.



2. Entrez le code de connexion de l'écran que vous souhaitez afficher, puis cliquez sur **Connecter**.



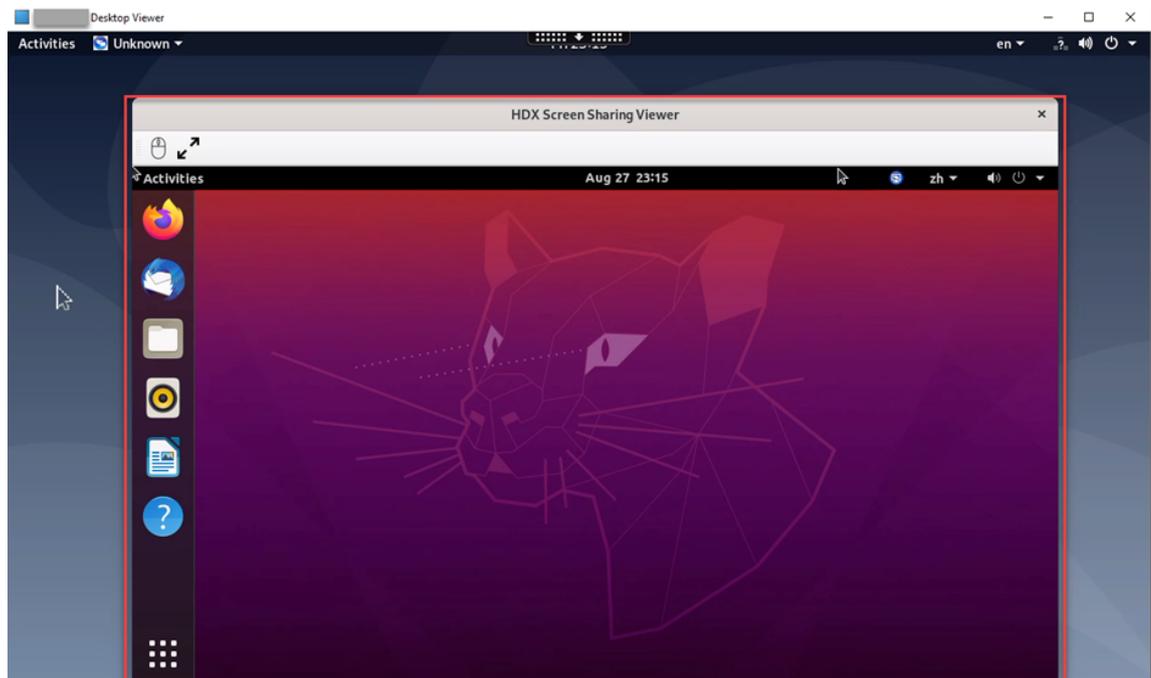
3. Attendez que l'utilisateur effectuant le partage d'écran accepte votre demande. Par exemple :



**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.

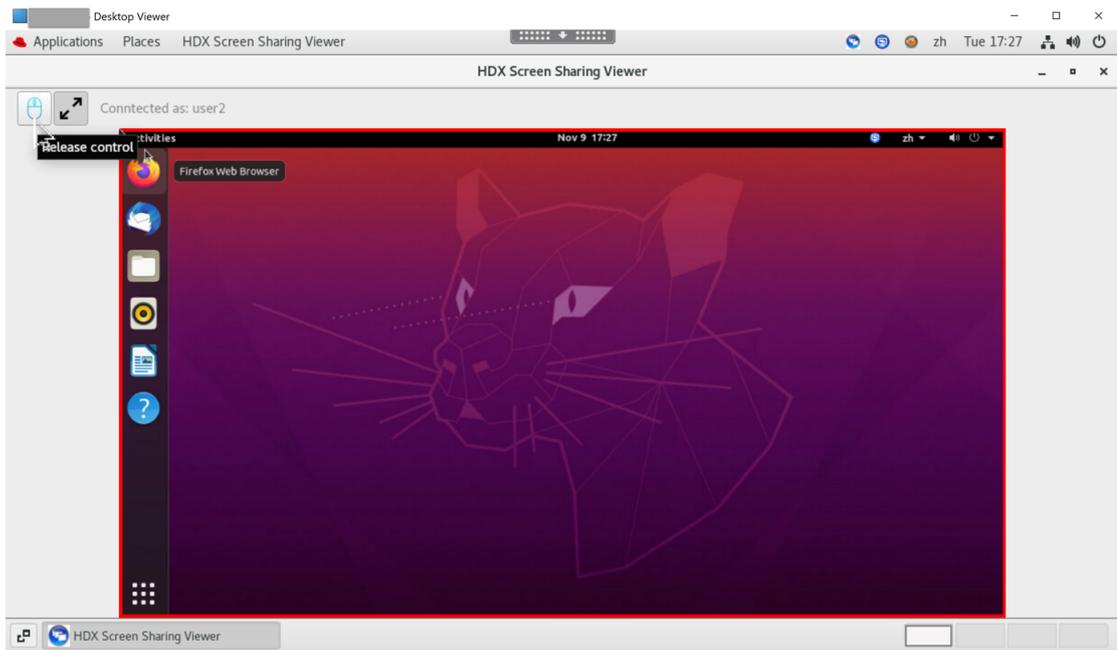


5. Pour demander le contrôle de l'écran partagé, cliquez sur l'icône de la souris dans le coin supérieur gauche.

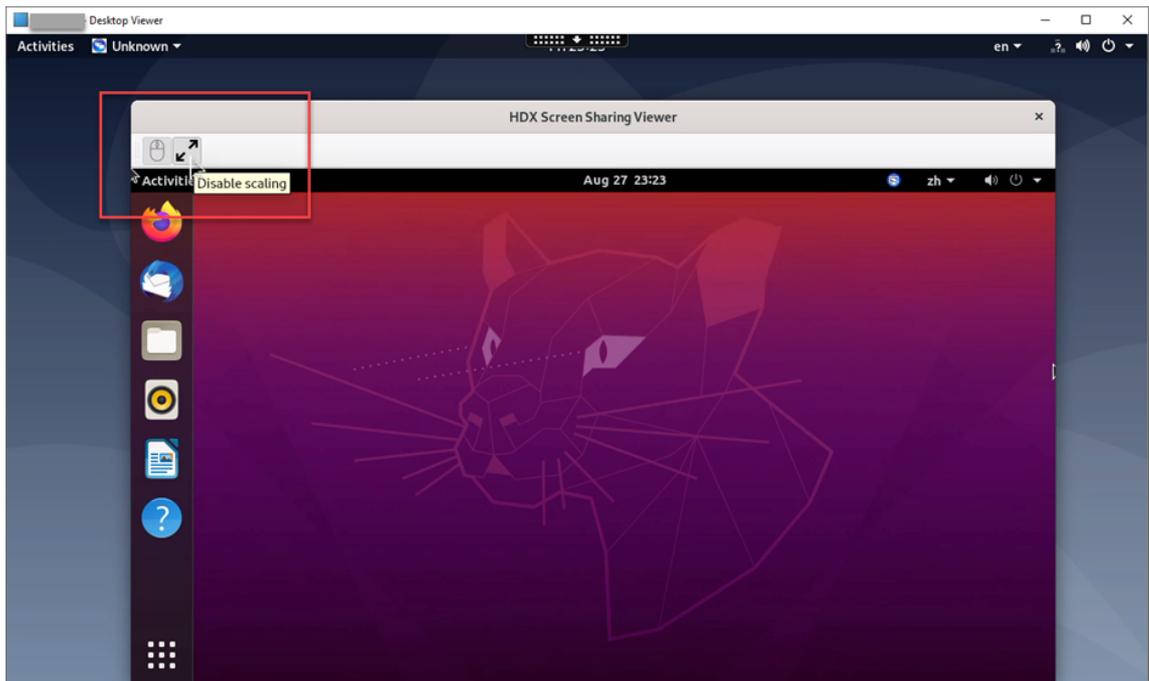
**Conseil :**

- 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 barre d'état système.](#)
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 :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
  CurrentControlSet\Control\Citrix\Thinwire" -v "
  EnableScreenSharing" -d "0x00000001"
```

4. Autorisez les ports 52525 - 52625 dans votre pare-feu.

## 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.

## Prise en charge multi-moniteurs

August 20, 2024

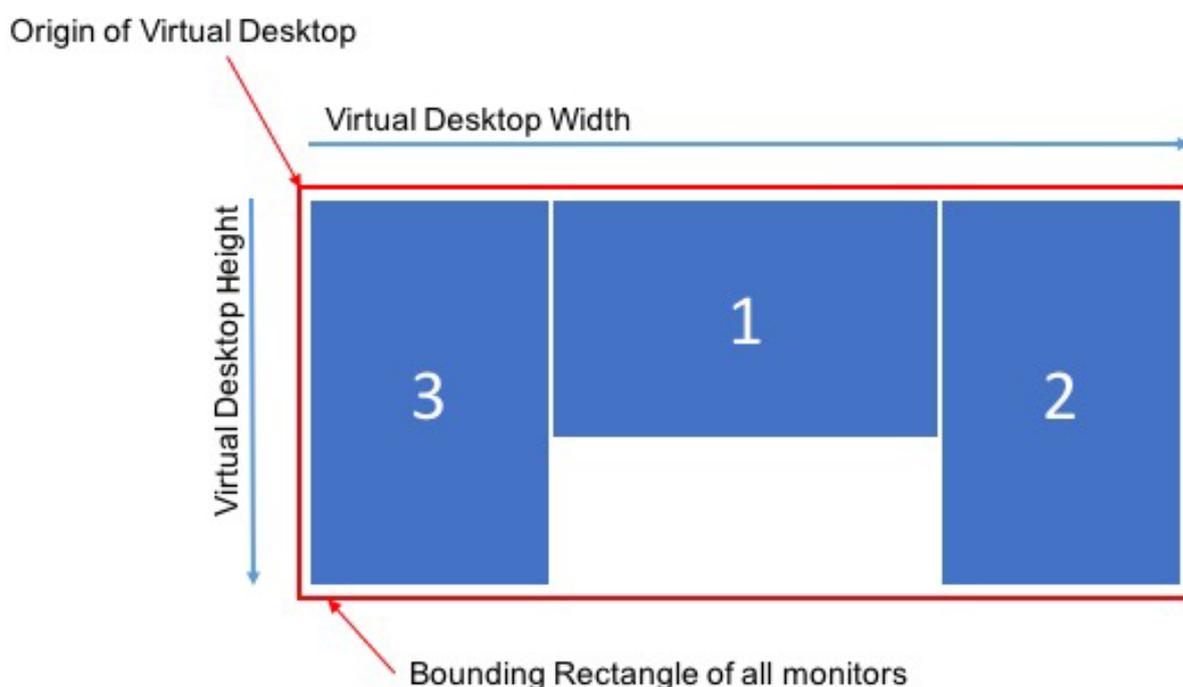
### Vue d'ensemble

Le VDA Linux fournit une prise en charge multi-moniteurs prête à l'emploi avec une résolution par défaut de 2 560 × 1 600 par moniteur. Les VDA standard prennent en charge jusqu'à neuf moniteurs, tandis que les VDA HDX 3D Pro prennent en charge jusqu'à quatre moniteurs.

Cet article explique comment configurer le VDA Linux pour différentes résolutions et configurations de moniteur.

## Bureau de la session virtuelle

À l'instar du VDA Windows, le VDA Linux repose sur le concept d'un bureau virtuel multi-moniteurs. Il est basé sur le cadre de délimitation de tous les moniteurs, et non sur la disposition réelle des moniteurs. Ainsi, la surface du bureau virtuel peut théoriquement être plus grande que la zone couverte par les écrans du client.



## Taille du bureau de la session virtuelle

L'origine du bureau de la session virtuelle est calculée à partir du coin supérieur gauche du cadre de délimitation de tous les moniteurs. Ce point se situe à  $X = 0$ ,  $Y = 0$ , où  $X$  et  $Y$  sont respectivement les axes horizontal et vertical.

**La largeur du bureau de la session virtuelle correspond à la distance horizontale, en pixels, entre l'origine et le coin supérieur droit du cadre de délimitation de tous les moniteurs.**

**De même, la hauteur du bureau de la session virtuelle correspond à la distance verticale, en pixels, entre l'origine et le coin inférieur gauche du cadre de délimitation de tous les moniteurs.**

Ce calcul est important pour les raisons suivantes :

- Permettre différentes dispositions de moniteur client
- Comprendre l'utilisation de la mémoire sur le VDA Linux

## Permettre différentes dispositions de moniteur client

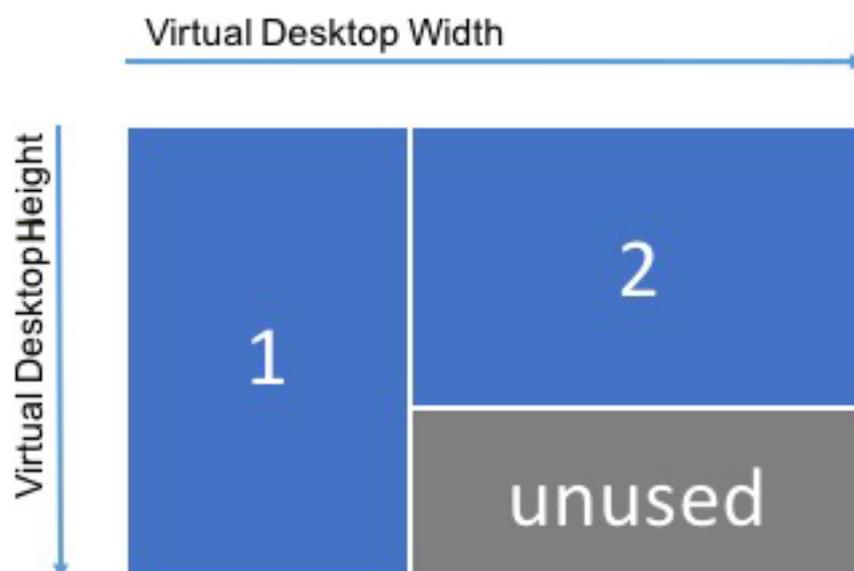
Connaître la taille maximale du bureau virtuel pour vos différentes dispositions de moniteur client vous permet de configurer le VDA Linux de manière à ce qu'il soit flexible en termes de configurations de moniteur client.

Tenez compte de la configuration du moniteur client suivante :



Le schéma ci-dessus montre une configuration multi-moniteurs prête à l'emploi avec deux moniteurs, chacun ayant une résolution de 2 560 x 1 600.

À présent, envisagez de vous connecter au même VDA Linux avec la configuration de moniteur client suivante :



Si chaque moniteur du schéma ci-dessus a une résolution de 2 560 x 1 600, les paramètres de configuration multi-moniteurs prêts à l'emploi sont insuffisants. La hauteur maximale est trop petite pour

accueillir le bureau de la session virtuelle adapté à cette configuration de moniteur. Pour s'adapter à la configuration du moniteur client dans cet exemple, vous devez définir le bureau virtuel Linux VDA sur une taille de  $4\,160 \times 2\,560$ .

Pour une flexibilité maximale dans une configuration multi-moniteurs, trouvez le plus petit cadre de délimitation parmi toutes les configurations de moniteurs que vous souhaitez prendre en charge. Pour les configurations avec deux moniteurs  $2\,560 \times 1\,600$ , les configurations possibles incluent :

- **Moniteur 1**  $2\,560 \times 1\,600$  et **Moniteur 2**  $2\,560 \times 1\,600$
- **Moniteur 1**  $1\,600 \times 2\,560$  et **Moniteur 2**  $2\,560 \times 1\,600$
- **Moniteur 1**  $2\,560 \times 1\,600$  et **Moniteur 2**  $1\,600 \times 2\,560$
- **Moniteur 1**  $1\,600 \times 2\,560$  et **Moniteur 2**  $1\,600 \times 2\,560$

Pour s'adapter à toutes les configurations ci-dessus, vous avez besoin d'un bureau virtuel de  $5\,120 \times 2\,560$ . Il s'agit du plus petit cadre de délimitation pouvant contenir toutes les dispositions souhaitées.

Si tous vos utilisateurs disposent d'un moniteur unique dans la configuration paysage classique, définissez la taille maximale du bureau virtuel sur la résolution la plus élevée du moniteur.



Dans cet exemple, le bureau virtuel doit être défini sur une taille de  $2\,560 \times 1\,600$ . La configuration par défaut étant de  $5\,120 \times 1\,600$  avec 2 moniteurs, une modification de configuration est nécessaire pour optimiser l'utilisation de la mémoire pour les déploiements à moniteur unique.

**Remarque :**

Si un bureau s'affiche avec une résolution incorrecte dans une configuration multi-moniteurs, réglez les paramètres DPI (points par pouce) dans l'application Citrix Workspace. Pour plus d'informations, consultez l'article [CTX230017](#) du centre de connaissances.

## Comprendre l'utilisation de la mémoire sur le VDA Linux

Connaître la taille du bureau virtuel vous permet de calculer la quantité de mémoire utilisée par chaque session HDX. Cette mémoire est la mémoire allouée à chaque session pour ses données graphiques au début de la session. Cela ne change pas pendant toute la durée de la session. Bien que cette mémoire ne soit pas la quantité totale de mémoire utilisée pour la session, c'est le moyen le plus simple de calculer l'utilisation de la mémoire par session.

Pour calculer la quantité de mémoire allouée à chaque session HDX, utilisez la formule suivante :

$$M = X \times Y \times Z,$$

Où :

- **M** est la quantité de mémoire utilisée pour les graphiques de session.
- **X** est la largeur du bureau de la session virtuelle.
- **Y** est la hauteur du bureau de la session virtuelle.
- **Z** est la profondeur de couleur de la fenêtre de session HDX. La valeur est en octets et non en bits. Utilisez donc 4 pour une couleur 32 bits.

### REMARQUE :

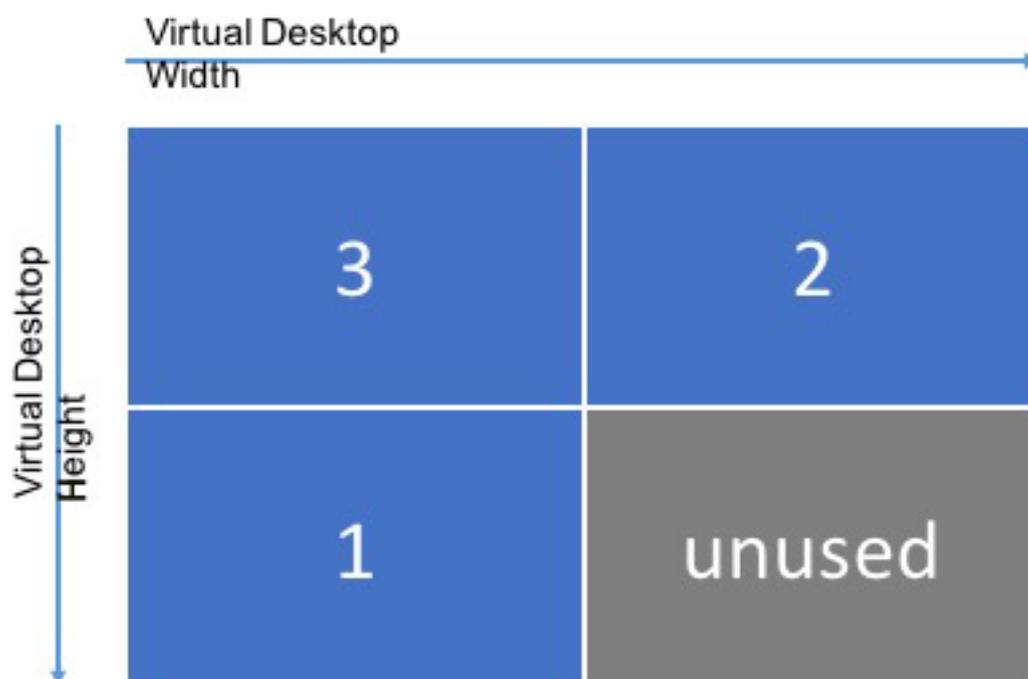
La profondeur de couleur du serveur X est fixe et ne peut pas changer pendant la durée de vie de la session (**de la connexion aux déconnexions/reconnexions jusqu'à la fermeture de session**). Par conséquent, le VDA Linux alloue toujours le bureau de la session virtuelle sous forme d'échantillons 32 bits et moins selon la profondeur de couleur demandée pour la session.

Par exemple, pour une session 1 024 × 768, la mémoire utilisée est la suivante :

$$1024 \times 768 \times 4/2^{20} \text{ MO} = 3 \text{ Mo}$$

Il est important de comprendre l'utilisation de la mémoire pour augmenter la densité de session sur chaque VDA Linux.

Tenez compte de la configuration du moniteur client suivante :



Si chaque moniteur a une résolution de 2 560 x 1 600, pour s'adapter à cette configuration de moniteur client, la taille du bureau de la session virtuelle doit être de 5 120 × 3 200. Notez que la zone grise n'est pas utilisée et équivaut à 16 384 000 (soit 2 560 x 1 600 x 4) octets de mémoire gaspillée.

### Paramètres de configuration multi-moniteurs Citrix

Vous pouvez contrôler la fonctionnalité multi-moniteurs du VDA Linux à l'aide des paramètres de configuration suivants :

- **MaxScreenNum**

**Paramètre :** HKEY\_LOCAL\_MACHINE/System/CurrentControlSet/Control/Citrix/Thinwire/MaxScreenNum

**Description :** nombre de moniteurs à prendre en charge

**Type :** DWORD

**Par défaut :** 2

**Maximum :** 9 pour le VDA standard, 4 pour le VDA HDX 3D Pro

- **MaxFbWidth**

**Paramètre :** HKEY\_LOCAL\_MACHINE /System/CurrentControlSet/Control/Citrix/Thinwire/MaxFbWidth

**Description :** largeur maximale d'un bureau de session virtuelle

**Type :** DWORD

**Par défaut :** 5 120

**Maximum :** 16 384 (8 192 x 2)

- **MaxFbHeight**

**Paramètre :** HKEY\_LOCAL\_MACHINE /System/CurrentControlSet/Control/Citrix/Thinwire/MaxFbHeight

**Description :** hauteur maximale d'un bureau de session virtuelle

**Type :** DWORD

**Par défaut :** 1 600

**Maximum :** 16 384 (8 192 x 2)

## Modifier la configuration multi-moniteurs du VDA Linux

La section suivante explique comment activer, configurer et désactiver la fonctionnalité multi-moniteurs sur le VDA Linux.

Définissez le nombre maximum de moniteurs en utilisant :

```
1 sudo ctxreg create -k " HKEY_LOCAL_MACHINE \System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "MaxScreenNum" -d " NumMons" --force
```

Où **NumMons** est une valeur comprise entre 1 et 9 pour un VDA standard ou entre 1 et 4 pour un HDX 3D Pro VDA.

Définissez la largeur maximale d'un bureau de session virtuelle en utilisant :

```
1 sudo ctxreg create -k " HKEY_LOCAL_MACHINE \System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "MaxFbWidth" -d " MaxWidth" --force
```

Où **MaxWidth** est une valeur comprise entre **1,024** et **16,384**.

Définissez la hauteur maximale d'un bureau de session virtuelle en utilisant :

```
1 sudo ctxreg create -k " HKEY_LOCAL_MACHINE \System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "MaxFbHeight" -d " MaxHeight" --force
```

Où **MaxHeight** est une valeur comprise entre **1,024** et **16,384**.

## GPU non virtualisés

August 20, 2024

Dans la documentation du Linux VDA, les GPU non virtualisés font référence à :

- GPU utilisés dans les scénarios Remote PC Access
- GPU transmis par un hyperviseur

Cet article fournit des informations sur la prise en charge des GPU non virtualisés.

### Activer HDX 3D Pro pour les GPU NVIDIA qui prennent en charge le SDK NVIDIA Capture pour Linux

Pour les GPU NVIDIA qui prennent en charge le [SDK NVIDIA Capture pour Linux](#), activez HDX 3D Pro en définissant **CTX\_XDL\_HDX\_3D\_PRO** sur **Y** lors de l'installation du Linux VDA. Aucune configuration supplémentaire n'est requise. L'accélération matérielle est activée par défaut après l'activation de HDX 3D Pro.

### Compatibilité avec les GPU NVIDIA qui ne prennent pas en charge le SDK NVIDIA Capture pour Linux et les GPU d'autres fabricants tels qu'AMD et Intel

**Remarque :**

Dans ce scénario, seul le codage logiciel est pris en charge.

#### Étape 1 : définissez CTX\_XDL\_HDX\_3D\_PRO sur Y lors de l'installation du Linux VDA

Pour plus d'informations sur les variables d'environnement, consultez [Étape 8 : définir l'environnement d'exécution afin de terminer l'installation](#).

#### Étape 2 : installez Xdamage

Par exemple, vous pouvez exécuter **sudo apt-get install -y libxdamage1** pour installer XDamage sur Ubuntu 20.04. En règle générale, XDamage existe sous forme d'extension de XServer.

#### Étape 3 : activez XDamage en exécutant la commande suivante

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\System\
  CurrentControlSet\Control\Citrix\XDamage" -t "REG_DWORD" -v "
  XDamageEnabled" -d "0x00000001" --force
```

#### Étape 4 : modifier les fichiers de configuration Xorg

Vous trouverez les quatre fichiers de configuration de modèle suivants dans **/etc/X11**. En fonction du nombre de moniteurs connectés, modifiez l'un des fichiers de configuration de modèle avec le nombre correspondant dans son nom. Par exemple, si un seul moniteur est connecté, modifiez le fichier de configuration de modèle dont le nom comporte le chiffre 1, c'est-à-dire `ctx-driver_name-1.conf`. Si deux moniteurs sont connectés, modifiez le fichier de configuration de modèle dont le nom contient le chiffre 2, c'est-à-dire `ctx-driver_name-2.conf`.

- `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 du GPU fourni par le fabricant pour obtenir des informations sur la configuration. Un fichier de configuration natif peut être généré. Vérifiez que votre GPU peut fonctionner dans un environnement local à l'aide du fichier de configuration natif.
  - 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
```

## 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 GPU non virtualisés.

Les distributions Linux entièrement testées qui prennent en charge cette fonctionnalité incluent Ubuntu 20.04 et Debian 11.

La fonction est désactivée par défaut. Pour l'activer, procédez comme suit :

1. Installez le package `evdi-dkms` basé sur votre distribution Linux :

```
1 sudo apt install evdi-dkms
```

2. Activez le téléchargement de l'affichage graphique vers l'EVDI :

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
  CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
  EVDI" -d "0x00000001" --force
```

3. Si vous utilisez un GPU Intel, désactivez le gestionnaire d'affichage. Dans le cas contraire, le gestionnaire d'affichage occupe et rend le GPU Intel indisponible pour les sessions distantes Citrix.

```
1 sudo systemctl disable --now gdm
```

## 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/bin/setlog` et définissez `GFX_X11` sur `Détaillé` afin de collecter les informations de trace à des fins de débogage.

## Filigrane de session

August 20, 2024

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 une fonctionnalité 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 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, l'option **Style de filigrane de session** est définie 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 <b>Unique</b> .
<rotation>	Rotation du filigrane selon un certain angle	-180–180	0	-
<transparency>	Opacité du filigrane	0–100	17	-
<font>	-	Police prise en charge par le système	Sans	-
<fontsize>	-	20–50	0 (calculé automatiquement)	-

Option de syntaxe	Description	Paramètre valide (sensible à la casse)	Valeur par défaut	Remarques
<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	-
<time>	Espace réservé pour l'heure de connexion à la session (HH:MM)	S/O	S/O	-

Option de syntaxe	Description	Paramètre valide (sensible à la casse)	Valeur par défaut	Remarques
<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 au moins une option 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.

## Accélération du GPU partagé sur un VDA Linux multi-session

August 20, 2024

HDX 3D PRO ne prend en charge que les VDA Linux configurés pour les bureaux VDI (mode session unique). Pour un Linux VDA multi-session, vous pouvez activer l’accélération du GPU partagé afin d’accélérer les applications OpenGL 3D.

### Remarque :

Le serveur d’affichage Wayland n’est pas pris en charge pour l’accélération du GPU partagé.

## Configuration

Pour activer l’accélération du GPU partagé sur un VDA Linux multi-session afin d’accélérer les applications OpenGL 3D, suivez les étapes de configuration suivantes :

### Étape 1 : installer VirtualGL

Téléchargez et installez **VirtualGL** depuis <https://sourceforge.net/projects/virtualgl/files>. Téléchargez les packages **.deb** pour les distributions Linux basées sur Debian et les packages **.rpm** pour les distributions Linux basées sur RHEL.

## Étape 2 : configurer VirtualGL

1. Arrêtez le gestionnaire d'affichage Linux, par exemple LightDM ou GNOME Display Manager (GDM).
2. Exécutez le script de configuration VirtualGL en exécutant :

```
1 #/opt/VirtualGL/bin/vglserver_config
```

Nous vous recommandons d'effectuer les sélections suivantes lors de l'exécution du script :

- Sélectionnez « 1 - Configure server for use with VirtualGL (GLX + EGL back ends) » pour configurer le serveur pour une utilisation avec VirtualGL (backends GLX + EGL).
  - Sélectionnez « n - Restrict 3D X server access to **vglusers** group » pour restreindre l'accès au serveur 3D X au groupe vglusers.
  - Sélectionnez « n - Restrict framebuffer devices access to **vglusers** group » pour restreindre l'accès des périphériques de tampon de trame (framebuffer) au groupe vglusers.
  - Sélectionnez « n - Disable XTEST extension » pour désactiver l'extension XTEST.
3. Quittez le script de configuration et redémarrez le gestionnaire d'affichage Linux.

## Étape 3 : exécuter des applications OpenGL 3D avec accélération du GPU

Il existe deux méthodes pour exécuter des applications OpenGL 3D avec l'accélération du GPU dans une session de VDA Linux :

- **Méthode 1** : activer l'accélération du GPU partagé pour toutes les applications OpenGL 3D

Pour ce faire, ouvrez un terminal bash sur le VDA Linux, exécutez la commande suivante, puis redémarrez le terminal bash. Cette approche permet une accélération du GPU partagé pour toutes les applications OpenGL 3D lancées depuis le terminal bash.

```
1 #/opt/Citrix/VDA/sbin/ctxgpushare.sh enable
```

- **Méthode 2** : activer l'accélération du GPU partagé pour une application OpenGL 3D spécifique :

Pour ce faire, ouvrez un terminal sur le VDA Linux et exécutez la commande suivante avec le nom de l'application spécifiée :

```
1 #vglrun <AppName>
```

## Limitations

- L'accélération du GPU partagé fonctionne en étroite collaboration avec le gestionnaire d'affichage du VDA Linux. Il est recommandé d'utiliser LightDM comme gestionnaire d'affichage

pour l'accélération du GPU partagé afin d'obtenir les fonctionnalités et les performances attendues.

- L'accélération matérielle WebGL est prise en charge dans Firefox sur Ubuntu et Debian uniquement.

## Capacité à monter en charge

Le nombre maximal de sessions simultanées pouvant partager un processeur graphique dépend du processeur et de la mémoire système. Cela dépend également fortement de la mémoire vidéo maximale du processeur graphique.

Par exemple :

---

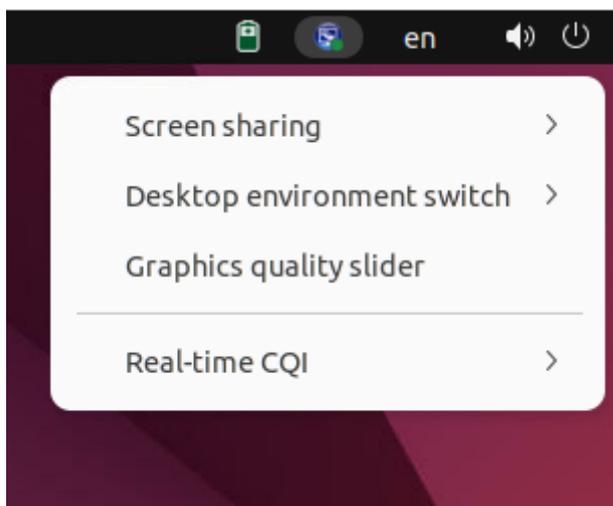
Si	Alors
Si le vGPU NVIDIA <b>M10-2B</b> dispose de 2 048 Mo de mémoire vidéo et qu'une application OpenGL telle que le lecteur VariCAD utilise 100 Mo de mémoire vidéo pour sa charge de travail à chaque session,	en théorie, le nombre maximum de sessions simultanées prises en charge ne peut pas dépasser 20.

---

## Barre d'état système

August 20, 2024

Les utilisateurs de session peuvent cliquer sur l'icône de la barre d'état système suivante pour effectuer les actions ou afficher les indicateurs :



## Présentation des éléments de la barre d'état système

Chaque élément de menu correspond à une fonctionnalité dotée d'un bouton Activer/désactiver. Lorsque la fonctionnalité correspondant à un élément de menu est désactivée, l'élément de menu est masqué et n'est pas affiché.

- **Partage d'écran**

Pour plus d'informations sur cette fonctionnalité, consultez la section [Partage d'écran HDX](#).

- **Commutateur d'environnement de bureau**

Cet élément de menu est une interface graphique pour **ctxdesktopswitch.sh**. Pour plus d'informations, consultez [Environnements de bureau personnalisés par utilisateurs de session](#).

La personnalisation de l'environnement de bureau par les utilisateurs de session est activée par défaut. Pour la désactiver, exécutez la commande suivante :

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
  CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
  EnableDesktopSwitch" -d "0x00000000" --force
```

- **Curseur pour la qualité des graphiques**

Pour plus d'informations, consultez la section [Curseur pour la qualité graphique](#) dans l'article sur la configuration graphique.

- **CQI en temps réel**

Actuellement, les données relatives à la durée des boucles (RTT) et à la latence sont affichées. Pour plus d'informations, consultez [Utilitaire permettant d'interroger les données de session](#).

L'icône de la barre d'état système s'affiche différemment en fonction de la latence du CQI en temps réel :



Il existe des seuils qui contrôlent le changement d'affichage de l'icône. Par défaut, ils sont définis comme suit :

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
  CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
  HighLatencyThreshold" -d "0x000000dc" --force
```

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
  CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
  LowLatencyThreshold" -d "0x00000078" --force
```

Lorsque la latence réelle est inférieure ou égale à **LowLatencyThreshold**, l'icône est marquée en vert. Lorsque la latence réelle est supérieure à **HighLatencyThreshold**, l'icône est marquée en rouge. Dans les autres cas, l'icône est marquée en jaune. Si le CQI en temps réel est désactivé, l'icône n'a pas de marque de couleur.

Le CQI en temps réel est activé et affiché par défaut. Pour le désactiver et le masquer, et pour que l'icône de la barre d'état ne comporte pas de marque de couleur, exécutez la commande suivante :

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
  CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
  EnableCqiShow" -d "0x00000000" --force
```

#### • État des graphiques

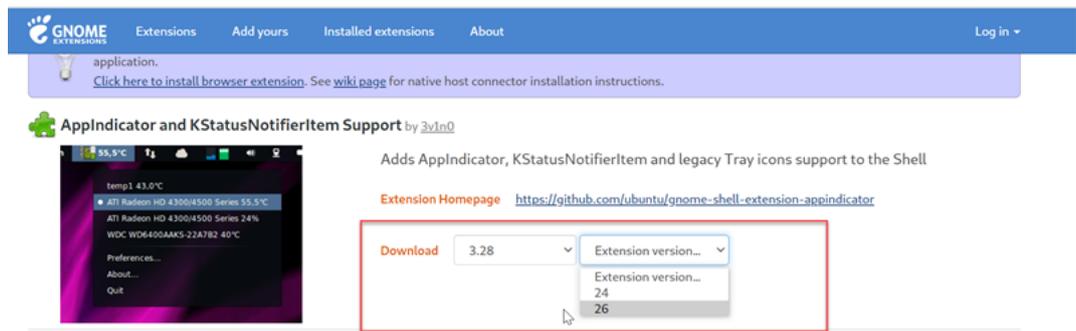
Cet indicateur indique les paramètres graphiques de la session en cours. Ce paramètre est activé par défaut. Pour la désactiver, exécutez la commande suivante :

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
  CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
  EnableGfxInfo" -d "0x00000000" --force
```

## Activer la barre d'état système

La barre d'état système ainsi que l'[affichage de l'état de la batterie du client](#) sont activés par défaut. Dans certaines conditions, vous devez toutefois effectuer une configuration supplémentaire pour activer la barre d'état système, et l'affichage de l'état de la batterie du client. Les détails sont les suivants :

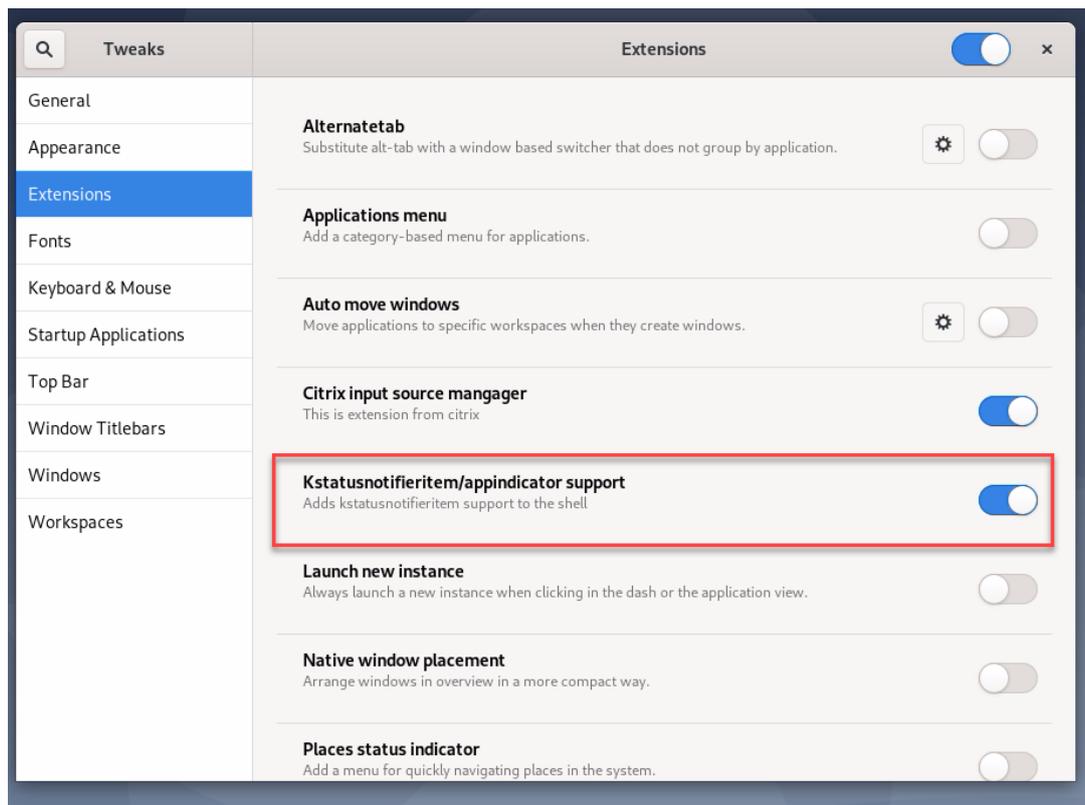
1. Activez la stratégie Indicateur d'état des graphiques dans Citrix Studio.
2. (**Cette étape n'est requise que si vous utilisez RHEL 8.x/9.x, Rocky Linux 8.x/9.x, Debian 11 ou SUSE 15.x installé avec GNOME.**) Installez une extension compatible pour votre shell GNOME afin d'activer la prise en charge 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.



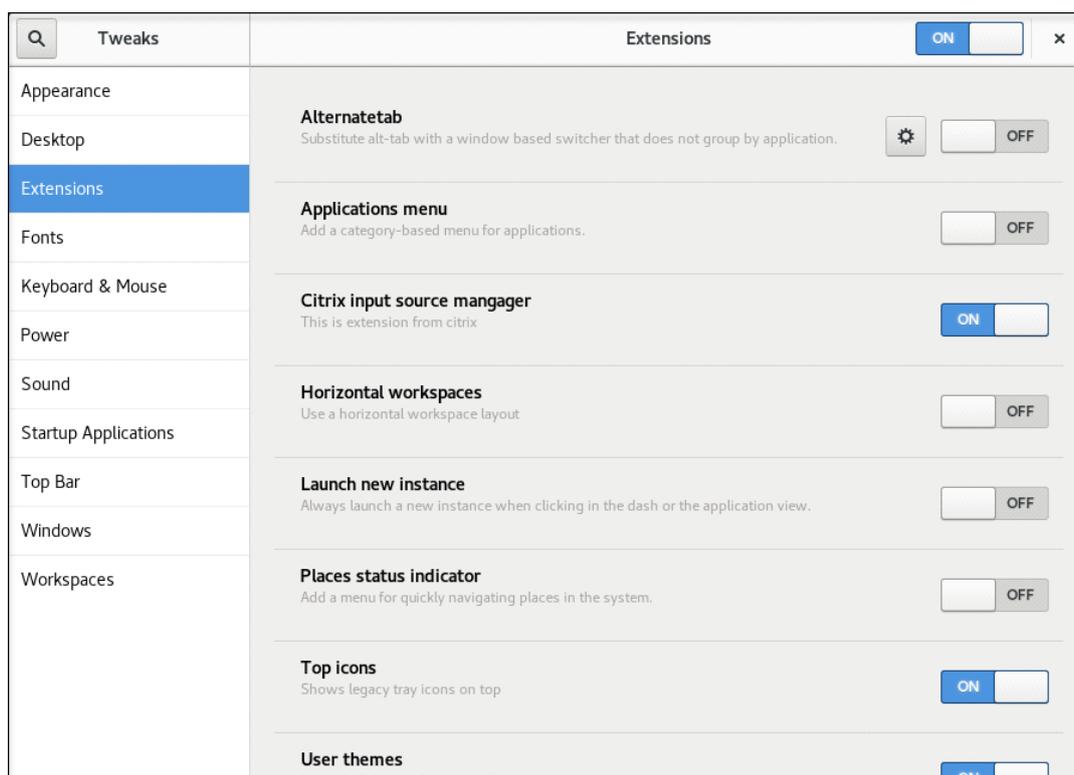
- c) Décompressez le package téléchargé et renommez le répertoire décompressé **appindicatorsupport@rgcjonas.gmail.com**. Vérifiez que la valeur **uuid** dans le fichier **metadata.json** du package est définie sur **appindicatorsupport@rgcjonas.gmail.com**.
  - d) Exécutez la commande `mv` pour déplacer 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, puis activez **KStatusNotifierItem/AppIndicator Support** dans l'outil Tweaks ou Extensions.
3. (**Cette étape n'est requise que si vous utilisez Debian 11 installé avec GNOME.**) Procédez comme suit pour installer et activer les icônes de la barre d'état système de 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**.



4. (**Cette étape est requise si vous utilisez RHEL 7.9 installé avec GNOME.**) Procédez comme suit pour installer et activer les icônes de la barre d'état système de GNOME.
  - a) Recherchez l'outil Tweaks dans l'écran **Activities**.
  - b) Sélectionnez **Extensions** dans l'outil Tweaks.
  - c) Activez **les principales icônes**.



d) Déconnectez-vous de la session, puis rouvrez-la.

## Affichage progressif Thinwire

August 20, 2024

L'interactivité de session peut se dégrader sur des connexions 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.

## Features



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.

## Features



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
```

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
```

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
```

où <value> est le <seuil en ms> (par défaut = 200)

Exemple : 100 = bascule en mode progressif si le réseau descend sous 100 ms.

## Redirection de contenu générale

August 20, 2024

### Mappage des lecteurs clients et redirection des dossiers clients

---

Si	Alors
Vous activez uniquement le mappage du lecteur client sur l'hôte (VDA).	Les volumes complets côté client sont automatiquement mappés aux sessions du sous-répertoire <b>ctxmnt</b> du répertoire de base.
Vous activez la redirection des dossiers clients sur l'hôte (VDA) et l'utilisateur la configure sur la machine utilisateur (client).	La partie du volume local spécifiée par l'utilisateur est redirigée.

---

### Redirection de périphérique USB

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.

### Mappage des lecteurs clients

August 20, 2024

Vous pouvez utiliser le mappage des lecteurs clients et la redirection des dossiers clients pour rendre les fichiers côté client accessibles sur la session côté hôte. La comparaison entre le mappage des lecteurs clients et la redirection des dossiers clients est la suivante :

---

Si	Alors
Vous activez uniquement le mappage du lecteur client sur l'hôte (VDA).	Les volumes complets côté client sont automatiquement mappés aux sessions du sous-répertoire <b>ctxmnt</b> du répertoire de base.

Si	Alors
Vous activez la redirection des dossiers clients sur l'hôte (VDA) et l'utilisateur la configure sur la machine utilisateur (client).	La partie du volume local spécifiée par l'utilisateur est redirigée.

---

## Activer le mappage des lecteurs clients

Pour activer le mappage des lecteurs clients, définissez la stratégie de **redirection des lecteurs clients** sur **Autorisé** dans Citrix Studio. Pour plus d'informations sur cette stratégie, consultez la section [Paramètres de stratégie de la redirection de fichiers](#).

## Activer la redirection des dossiers clients et spécifier les dossiers à rediriger

Pour activer la redirection des dossiers clients, exécutez la commande suivante sur le VDA :

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\Client
  Folder Redirection" -t "REG_DWORD" -v "CFROnlyModeAvailable" -d "0
  x00000001" --force
```

Pour spécifier les dossiers à rediriger du client vers la session côté hôte, procédez comme suit sur la machine utilisateur :

1. Vérifiez que la dernière version de l'application Citrix Workspace est installée.
2. À partir du répertoire d'installation de l'application Citrix Workspace, démarrez **CtxCFRUI.exe**.
3. Sélectionnez le bouton radio **Personnaliser** et ajoutez, modifiez ou supprimez des dossiers.
4. Déconnectez-vous et reconnectez-vous à vos sessions pour que le paramètre prenne effet.

## Redirection de périphérique USB

August 20, 2024

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 de périphérique USB lorsque la latence réseau est inférieure à 100 millisecondes. N'utilisez pas la redirection de périphérique USB lorsque la

latence réseau est supérieure à 200 millisecondes.

La redirection de périphérique USB contient trois domaines de fonctionnalité :

- Projet USB/IP Open Source
- Module de session USB Citrix
- Module de service USB Citrix

#### **Projet USB/IP Open Source :**

Le projet USB/IP 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.

Le Linux VDA implémente la redirection de périphérique USB sur la base du projet USB/IP Open Source et réutilise le pilote noyau et les bibliothèques en mode utilisateur de l'USB/IP. Toutefois, tous les transferts de données USB entre le Linux VDA et l'application Citrix Workspace sont encapsulés dans le protocole USB ICA de Citrix.

#### **Module de session USB Citrix :**

Le module de session USB Citrix agit comme un pont de communication entre le module noyau USB/IP et l'application Citrix Workspace.

#### **Module de service USB Citrix :**

Le module de service USB Citrix gère toutes les opérations sur les périphériques USB, par exemple, connecter ou détacher des périphériques USB.

### **Fonctionnement de la redirection de périphérique 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 depuis le client.

### **Périphériques USB pris en charge**

**Conseil :**

La prise en charge des ports USB 3.0 a été ajoutée. Vous pouvez insérer des périphériques USB 3.0 dans les ports USB 3.0 d'un appareil client.

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 :

---

Périphérique de stockage de masse USB	VID:PID	Système de fichiers
Netac Technology Co., Ltd	0dd8:173c	FAT32, NTFS
Kingston Datatraveler 101 II	0951:1625	FAT32, NTFS
Kingston Datatraveler GT101 G2	1567:8902	FAT32, NTFS
SanDisk SDCZ80 flash drive	0781:5580	FAT32, NTFS
WD HDD	1058:10B8	FAT32, NTFS
Toshiba Kingston DataTraveler 3.0 USB device	0930:6545	FAT32, NTFS
Taiwan OEM – OBSOLETE VendorCo ProductCode Disk 2.0	FFFF:5678	FAT32, NTFS
TD-RDF5A Transcend USB device	8564:4000	FAT32, NTFS

---

**Remarque :**

Pour utiliser NTFS sur Amazon Linux 2, CentOS, RHEL, Rocky Linux et SUSE, activez d'abord le support NTFS sur ces distributions.

---

Souris 3D USB	VID:PID
3DConnexion SpaceMouse Pro	046d: c62b

---

---

Scanner USB	VID:PID
Epson Perfection V330 photo	04B8: 0142

---

---

Yubico USB	VID:PID
Yubico YubiKey OTP+FIDO+CCID - Keyboard, HID	1050:0407

---

---

Webcam USB	VID:PID
Logitech composite USB device - WebCam, Audio	0460:0825

---

## Configurer la redirection de périphérique USB

### (pour CentOS, RHEL et Rocky Linux uniquement) Installer ou compiler le module noyau USB/IP

Le Linux VDA utilise USB/IP comme contrôleur hôte virtuel pour la redirection de périphérique USB. Le module noyau USB/IP étant publié dans la plupart des cas avec la version 3.17 et ultérieure du noyau Linux, vous n'avez pas besoin de créer le module noyau par défaut. Toutefois, le module noyau USB/IP n'est pas disponible pour CentOS, RHEL et Rocky Linux. Pour utiliser la redirection de périphérique USB avec ces distributions Linux, vous devez installer ou compiler le module noyau USB/IP. Téléchargez et installez le module noyau USB/IP depuis <https://pkgs.org/download/kmod-usbip> en fonction de votre distribution Linux.

### Définir les stratégies de redirection de périphérique USB

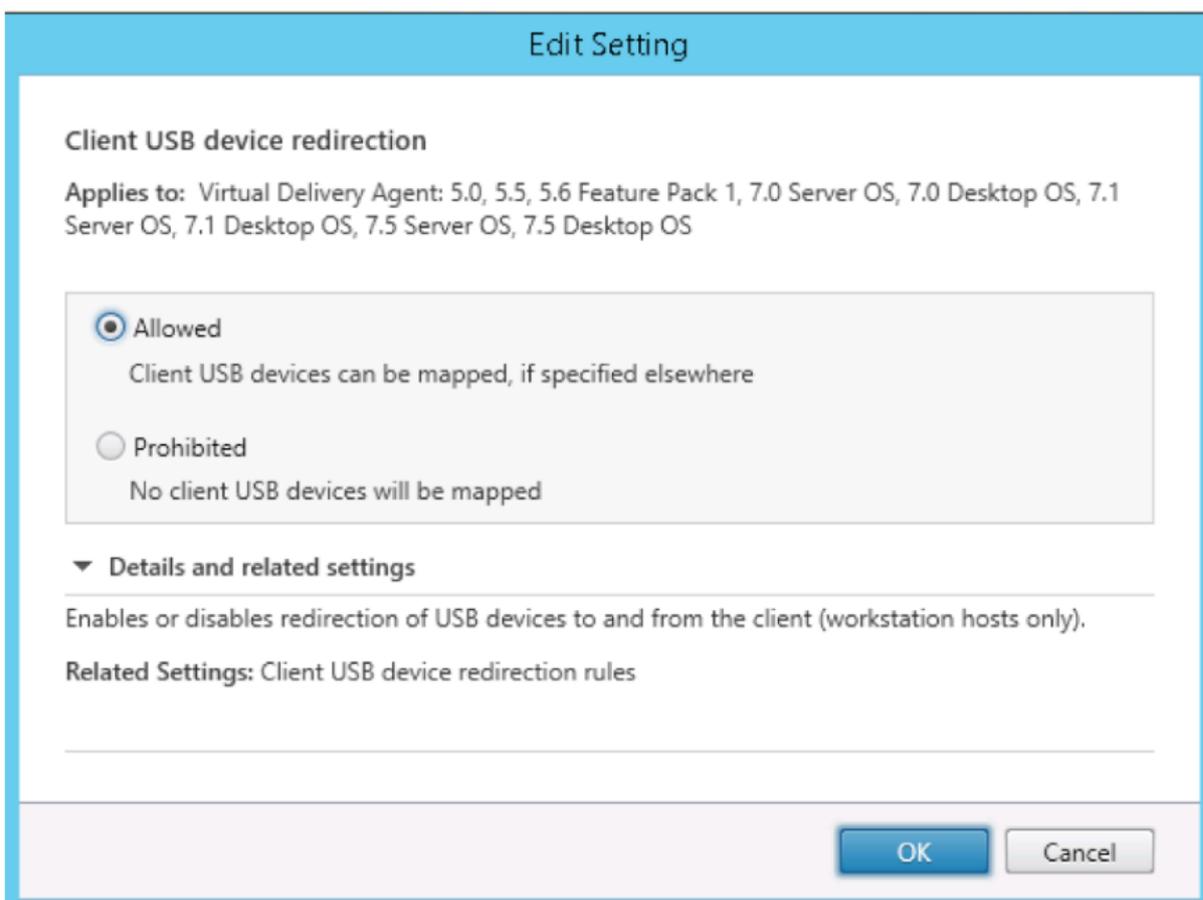
Une stratégie Citrix détermine si la redirection de périphérique USB est activée ou désactivée. Le type de périphérique peut également être spécifié à l'aide d'une stratégie Delivery Controller. Lors de la configuration de la redirection de périphérique USB pour les Linux VDA, configurez les stratégies et règles suivantes :

- Stratégie de redirection de périphérique USB client
- Règles de redirection de périphérique USB client

**Activer la redirection de périphérique USB** Dans Citrix Studio, activez (ou désactivez) la redirection de périphérique USB depuis le client (hôtes de station de travail uniquement).

Dans la boîte de dialogue **Modifier le paramètre** :

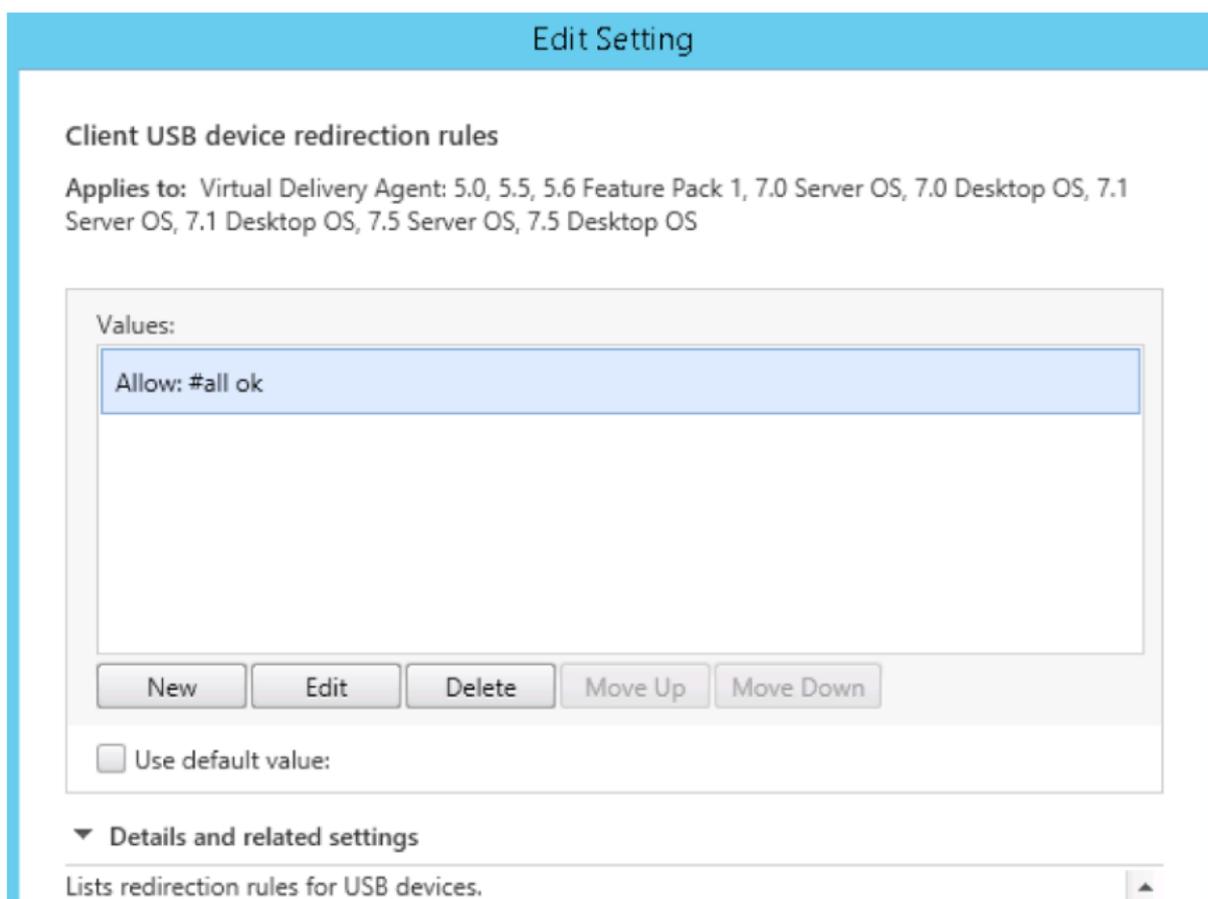
1. Sélectionnez **Autorisé**.
2. Cliquez sur **OK**.



**Définir des règles de redirection de périphérique 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**.



**Edit Setting**

**Client USB device redirection rules**

Applies to: Virtual Delivery Agent: 5.0, 5.5, 5.6 Feature Pack 1, 7.0 Server OS, 7.0 Desktop OS, 7.1 Server OS, 7.1 Desktop OS, 7.5 Server OS, 7.5 Desktop OS

Values:

Allow: #all ok
----------------

Use default value:

▼ **Details and related settings**

Lists redirection rules for USB devices.

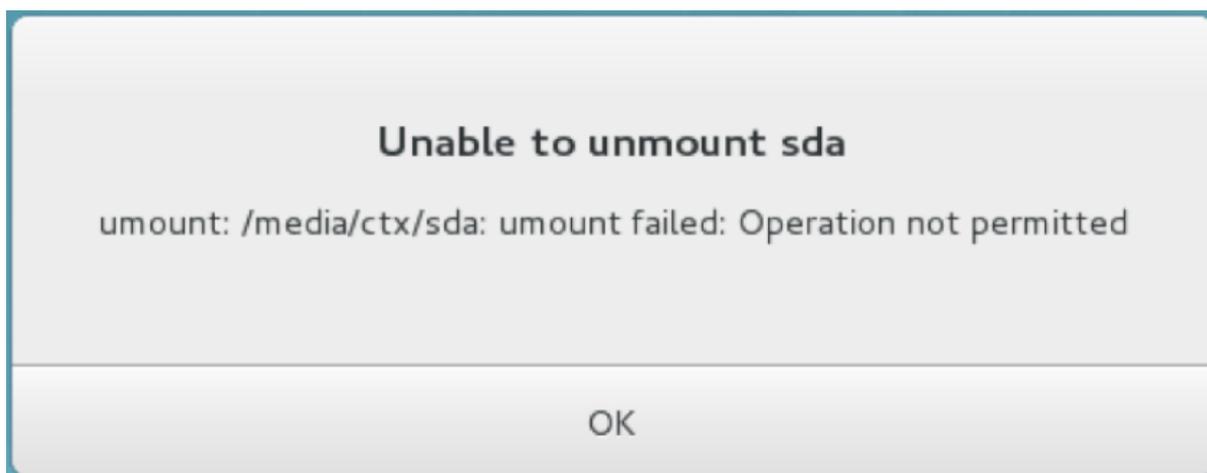
Pour de plus amples informations sur la configuration de la redirection de périphérique USB générique, reportez-vous au [Guide de configuration de la redirection USB générique Citrix](#).

## Résolution des problèmes de redirection de périphérique 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.



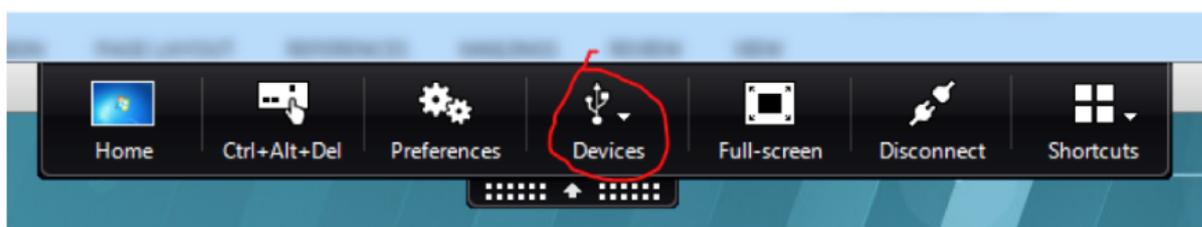
### Le fichier est perdu lorsque vous arrêtez la redirection d'un disque USB

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 **sync** 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 de périphérique USB.
- Le module de service USB Citrix est en cours d'exécution.

Si la stratégie n'est pas définie correctement, corrigez-la en consultant la section [Définir les stratégies de redirection de périphérique USB](#) de cet article.

Si le module de service USB Citrix n'est pas en cours d'exécution, procédez comme suit :

1. Vérifiez si un module noyau USB/IP est disponible sur votre distribution Linux à l'aide de la commande suivante :

```
1 modinfo usbip-core
```

2. Si la sortie s'affiche comme suit, installez ou compilez le module noyau USB/IP en fonction de votre distribution Linux :

```
1 modinfo: ERROR: Module usbip-core not found.
```

- Pour Amazon Linux 2, CentOS, RHEL et Rocky Linux, consultez la section [Installer ou compiler le module noyau USB/IP](#) de cet article.
- Pour SUSE, téléchargez et installez le package USB/IP à partir de <https://software.opensuse.org/package/usbip>.
- Pour Ubuntu/Debian, procédez comme suit pour compiler et installer le module noyau USB/IP :

- a) Téléchargez le code source du module noyau USB/IP.

Accédez au référentiel du noyau Linux accessible sur <https://github.com/torvalds/linux/tree/master/drivers/usb/usbip>, sélectionnez la balise de version cible du noyau Linux (v4.15 ou ultérieure) et obtenez le lien tel que <https://github.com/torvalds/linux/tree/v4.15/drivers/usb/usbip>.

Accédez à [DownGit](#) et entrez le lien précédent pour créer un lien de téléchargement permettant de télécharger le code source USB/IP.

- b) Décompressez le fichier source à l'aide des commandes suivantes :

```
1 unzip ${
2   USBIP_SRC }
3   .zip
4
5 cd usbip
```

- c) Modifiez le fichier **Makefile** comme suit :

```
1 # SPDX-License-Identifier: GPL-2.0
2
3 ccflags-$(CONFIG_USBIP_DEBUG) := -DDEBUG
4
5 obj-$(CONFIG_USBIP_CORE) += usbip-core.o
6
7 usbip-core-y := usbip_common.o usbip_event.o
8
9 obj-$(CONFIG_USBIP_VHCI_HCD) += vhci-hcd.o
10
```

```
11 vhci-hcd-y := vhci_sysfs.o vhci_tx.o vhci_rx.o vhci_hcd.o
12
13 #obj-$(CONFIG_USBIP_HOST) += usbip-host.o
14
15 #usbip-host-y := stub_dev.o stub_main.o stub_rx.o stub_tx.o
16
17 #obj-$(CONFIG_USBIP_VUDC) += usbip-vudc.o
18
19 #usbip-vudc-y := vudc_dev.o vudc_sysfs.o vudc_tx.o vudc_rx.o
    o vudc_transfer.o vudc_main.o
```

d) Compilez le code source :

```
1 apt-get install linux-headers-`uname -r`
2
3 make -C /lib/modules/`uname -r`/build M=$PWD
```

e) Installez le module noyau USB/IP :

```
1 cp usbip-core.ko vhci-hcd.ko /opt/Citrix/VDA/lib64/
```

f) Redémarrez le service **ctxusbsd** pour charger le module du noyau USB/IP :

```
1 systemctl restart ctxusbsd
```

### Échec de redirection lorsque des périphériques USB sont visibles dans la barre d'outils de l'application Citrix Workspace, mais avec la mention « Limité par une stratégie »

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.

## Redirection du Presse-papiers

August 20, 2024

La redirection du Presse-papiers vous permet de copier et coller des données entre les applications exécutées dans la session VDA et les applications exécutées sur l'appareil client.

Cet article décrit les stratégies Citrix disponibles qui vous permettent de réaliser la redirection du Presse-papiers.

### Stratégies Citrix pour la redirection du Presse-papiers

#### Redirection du Presse-papiers client

Ce paramètre permet d'autoriser ou d'empêcher le mappage du Presse-papiers sur la machine utilisateur au Presse-papiers du VDA.

Par défaut, la redirection du Presse-papiers est définie sur **Autorisé**.

Pour empêcher le transfert des données par copier-coller entre une session et le Presse-papiers local, sélectionnez **Interdire**. Les utilisateurs peuvent toujours copier-coller des données entre les applications exécutées dans les sessions.

#### Limite de bande passante de redirection du Presse-papiers

Ce paramètre spécifie la bande passante maximale autorisée (Kbits/s) pour le transfert des données entre la session et les Presse-papiers locaux.

### **Pourcentage de la limite de la bande passante de redirection du Presse-papiers**

Ce paramètre spécifie la bande passante maximale autorisée pour le transfert de données entre la session et les Presse-papiers locaux sous forme de pourcentage de la bande passante totale de session.

### **Limiter le client du presse-papiers à la taille de transfert de la session**

Ce paramètre spécifie la taille maximale des données du Presse-papiers qu'un utilisateur peut transférer d'une machine cliente vers une session virtuelle au cours d'une opération de copier-coller unique.

Pour limiter la taille du transfert du Presse-papiers, activez le paramètre **Limiter le client du Presse-papiers à la taille de transfert de la session**. Ensuite, dans le champ **Limite de taille**, entrez une valeur en kilo-octets pour définir la taille du transfert de données entre le Presse-papiers local et une session.

Par défaut, ce paramètre est désactivé et aucune limite sur les transferts entre le client et une session n'est définie.

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

Ce paramètre spécifie la taille maximale des données du Presse-papiers qu'un utilisateur peut transférer d'une session virtuelle vers une machine cliente au cours d'une opération de copier-coller unique.

Pour limiter la taille du transfert du Presse-papiers, activez le paramètre **Limiter la session du Presse-papiers à la taille de transfert du client**. Ensuite, dans le champ **Limite de taille**, entrez une valeur en kilo-octets pour définir la taille du transfert de données entre une session et le Presse-papiers local.

Par défaut, ce paramètre est désactivé et aucune limite sur les transferts entre le client et une session n'est définie.

### **Restreindre écriture dans le Presse-papiers client ET Formats d'écriture autorisés dans le Presse-papiers client**

L'activation de ces deux paramètres vous permet d'autoriser le copier-coller de formats de données spécifiques depuis la session vers le client (écriture dans le client).

Les formats de Presse-papiers suivantes sont définis par le système :

- CF\_TEXT

- CF\_BITMAP
- CF\_METAFILEPICT
- CF\_SYLK
- CF\_OEMTEXT
- CF\_DIB
- CF\_PALETTE
- CF\_UNICODETEXT
- CF\_LOCALE
- CF\_DIBV5
- CF\_HDROP

### **Restreindre écriture dans le Presse-papiers de session ET Formats d'écriture autorisés dans le Presse-papiers de session**

L'activation de ces deux paramètres vous permet d'autoriser le copier-coller de formats de données spécifiques depuis le client vers la session (écriture dans la session).

Les formats de Presse-papiers suivantes sont définis par le système :

- CF\_TEXT
- CF\_BITMAP
- CF\_METAFILEPICT
- CF\_SYLK
- CF\_OEMTEXT
- CF\_DIB
- CF\_PALETTE
- CF\_UNICODETEXT
- CF\_LOCALE
- CF\_DIBV5
- CF\_HDROP

## **Clavier**

August 20, 2024

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

August 20, 2024

### 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 la fonctionnalité d'éditeur IME client.

### Problèmes connus

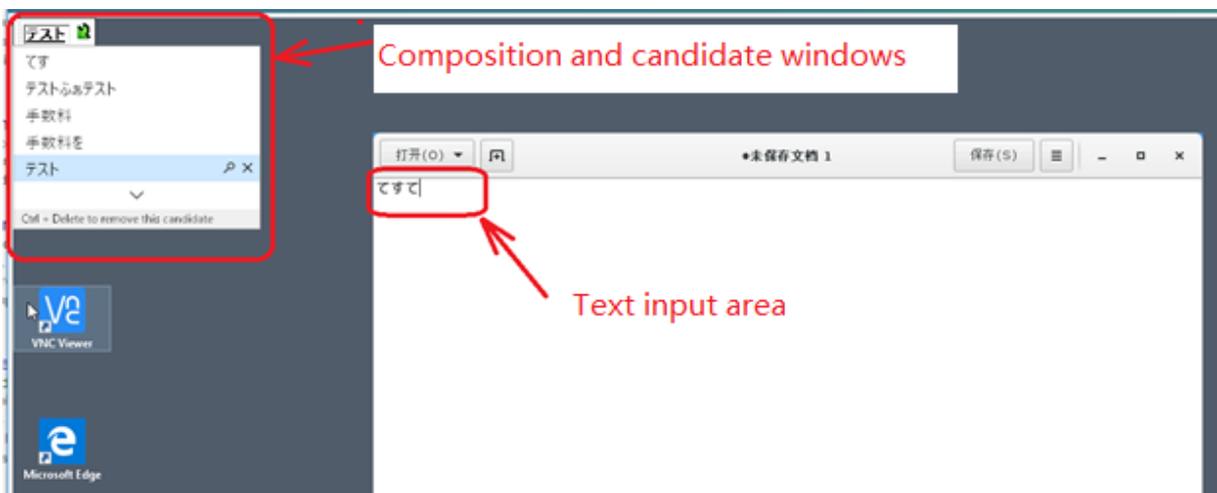
- Vous devez double-cliquer sur une cellule dans une feuille de calcul Google avant de pouvoir utiliser la fonctionnalité d'éditeur IME client pour saisir des caractères dans la cellule.
- La fonctionnalité d'éditeur IME client n'est pas automatiquement désactivé dans les champs de mot de passe.
- L'interface 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

August 20, 2024

### 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](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.

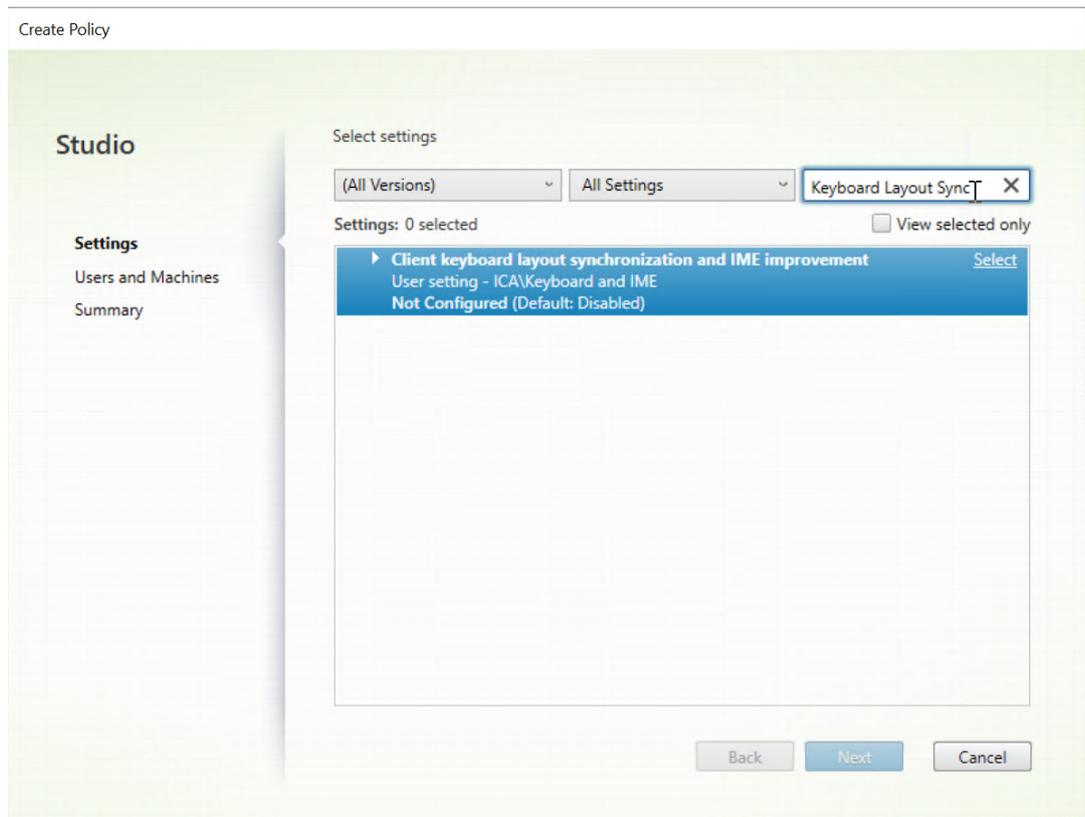
## Activer et désactiver la fonctionnalité

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`.

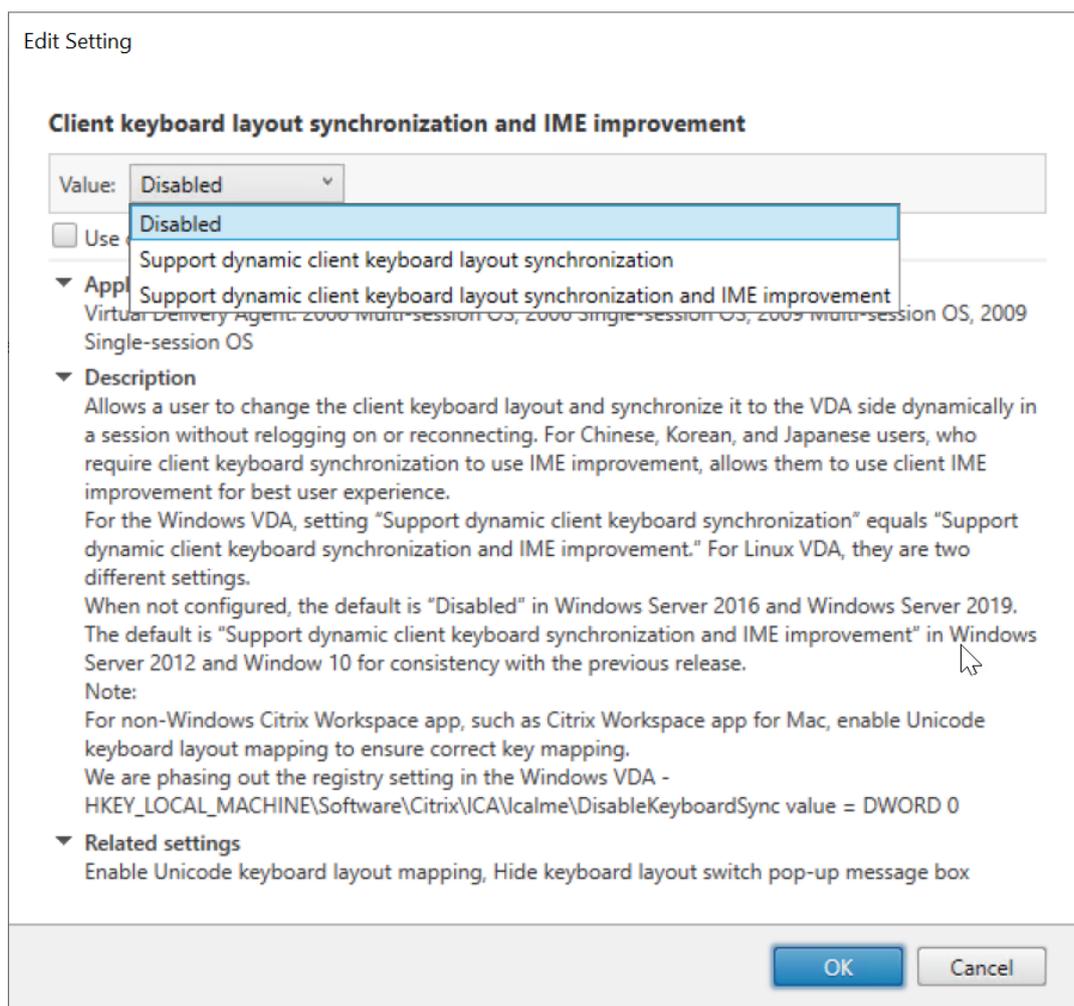
### Remarque :

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"
```

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"
```

## Synchronisation dynamique de la disposition du clavier

August 20, 2024

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

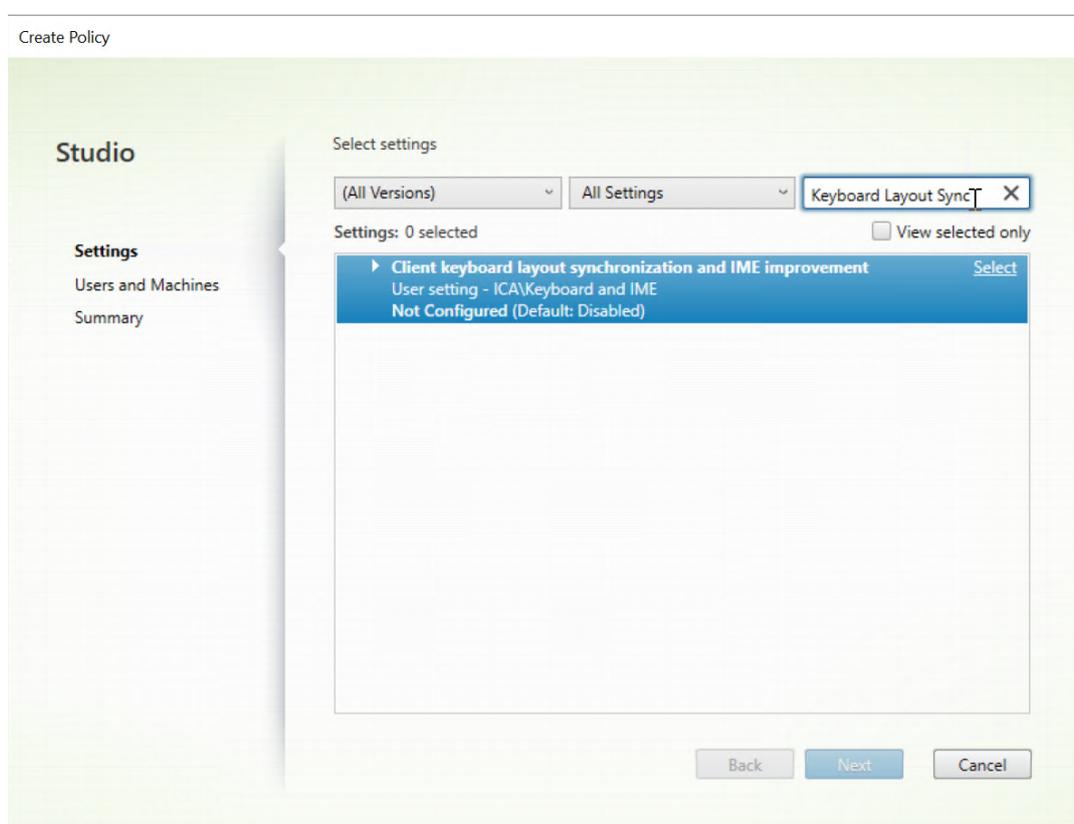
La fonctionnalité de synchronisation dynamique de la disposition du clavier est désactivée par défaut. Pour activer ou désactiver la fonctionnalité, définissez la stratégie **Synchronisation de la disposition du clavier client et améliorations apportées à l'éditeur IME** ou modifiez le Registre via l'utilitaire `ctxreg`.

### Remarque :

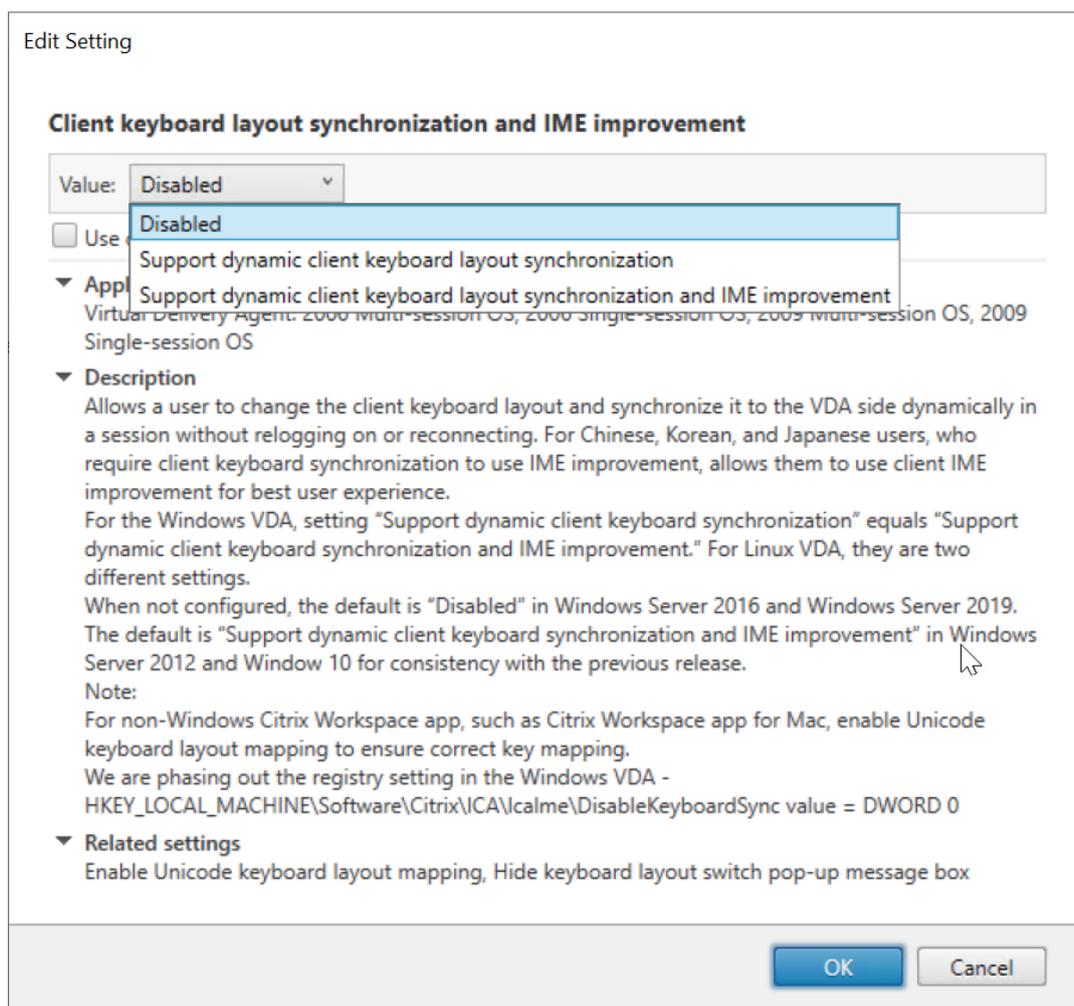
La stratégie **Synchronisation de la disposition du clavier client et améliorations apportées à l'éditeur IME** prend la priorité sur les paramètres du Registre et peut être appliquée aux objets

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"
```

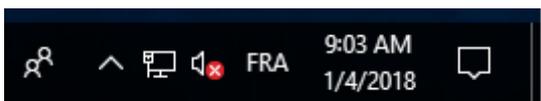
Pour désactiver cette fonctionnalité, exécutez la commande :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar" -v "SyncKeyboardLayout" -d "0x00000000"
```

## Utilisation

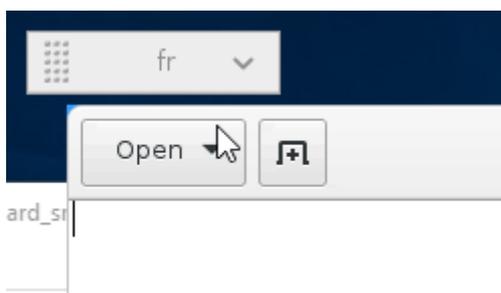
Lorsque cette fonctionnalité est activée, si la disposition du clavier change sur la machine cliente pendant une session, la disposition du clavier de la session change en conséquence.

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 :



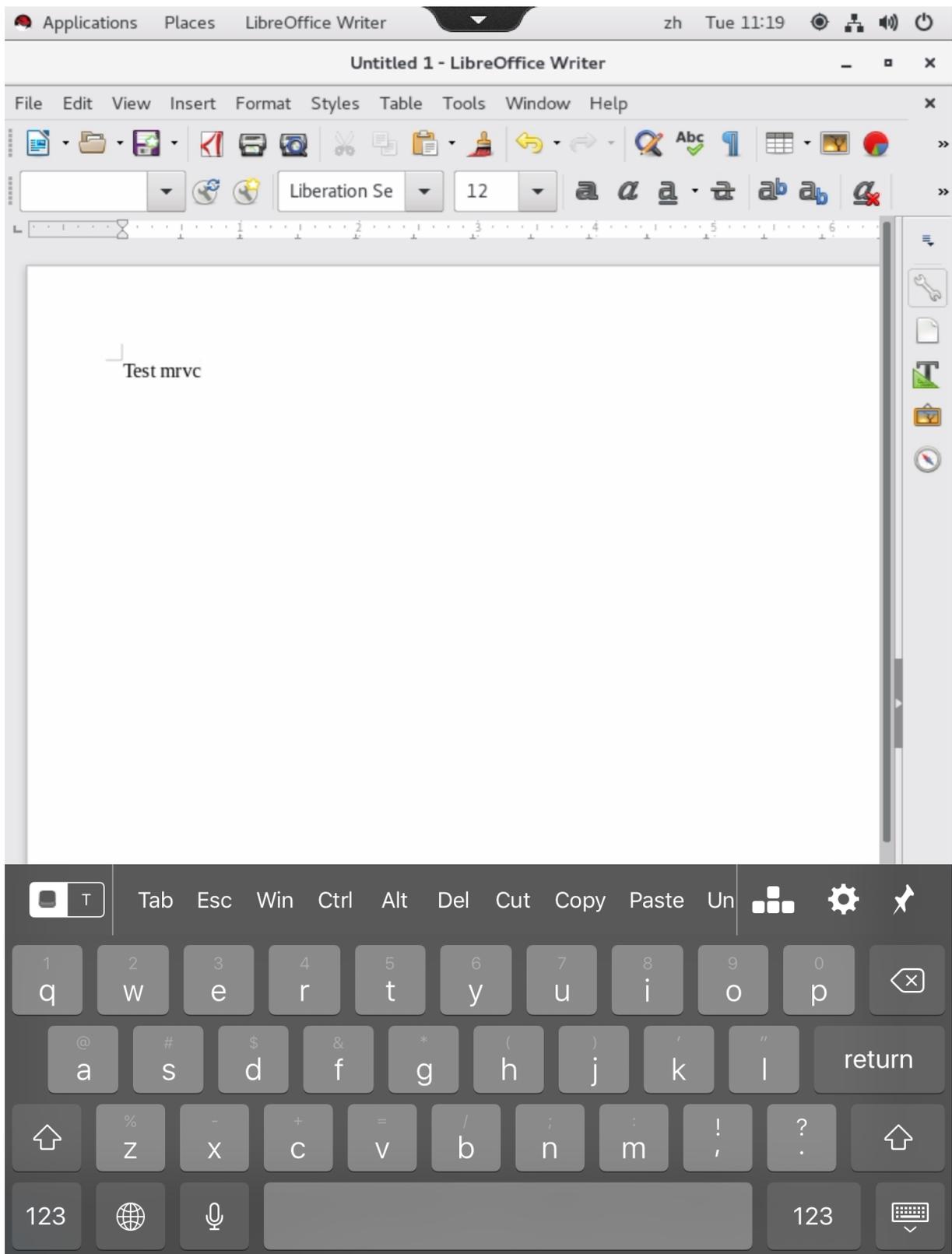
Dans une session de bureau, cette modification automatique est affichée dans la barre des tâches :



## Clavier logiciel

August 20, 2024

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 prise en charge sur l'application Citrix Workspace pour iOS et Android.

**Activer et désactiver la fonctionnalité**

La 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 :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
  CurrentControlSet\Control\Citrix\VirtualChannels\MrVc" -v "
  Enabled" -d "0x00000001"
```

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 :

```
1 echo "GTK_IM_MODULE=ibus" >>/etc/bashrc
```

Pour désactiver cette fonctionnalité, exécutez la commande suivante :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\
  Control\Citrix\VirtualChannels\MrVc" -v "Enabled" -d "0x00000000"
```

**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

August 20, 2024

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"
```

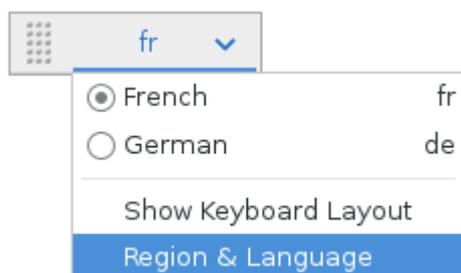
Pour désactiver cette fonctionnalité, exécutez la commande :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
  CurrentControlSet\Control\Citrix\LanguageBar" -v "Enabled" -d "0
  x00000000"
```

## 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

August 20, 2024

Cette section contient les rubriques suivantes :

- [Fonctionnalités audio](#)
- [Redirection de contenu du navigateur](#)
- [Compression vidéo pour Webcam HDX](#)

## Fonctionnalités audio

August 20, 2024

### 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 et Rocky Linux 8.x.

## Prise en charge de plusieurs périphériques audio (version Technical Preview)

### Vue d'ensemble

À partir de la version 2311, le Linux VDA introduit une fonctionnalité de redirection audio. Cette fonctionnalité permet de rediriger vers la session Linux VDA distante plusieurs périphériques audio sur la machine cliente sur laquelle l'application Citrix Workspace est installée.

Lorsque cette fonctionnalité est activée :

- Tous les périphériques audio locaux de la machine cliente sont affichés au cours d'une session. Au lieu d'indiquer CitrixAudioSink (sortie audio) ou CitrixAudioSource (entrée audio), les périphériques audio sont affichés avec leur nom d'appareil respectif. Vous pouvez sélectionner un périphérique audio dans une application dans une session ou utiliser le périphérique audio par défaut pendant une session qui est également le périphérique audio par défaut de la machine cliente. Si nécessaire, vous pouvez modifier le périphérique audio par défaut à partir des paramètres système de l'ordinateur client. Une fois le périphérique audio par défaut de la machine cliente mis à jour, le nouveau périphérique apparaît comme périphérique audio par défaut dans la session.
- Les sessions sont mises à jour de manière dynamique lorsque vous branchez ou supprimez des périphériques audio.

## Configuration

Pour utiliser cette fonctionnalité, activez-la sur le Linux VDA et choisissez une application Citrix Workspace prise en charge.

**Activer la fonctionnalité sur le Linux VDA** La fonction de redirection audio qui permet la prise en charge de plusieurs périphériques audio est désactivée par défaut. Pour l'activer, exécutez la commande suivante sur la session Linux VDA :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
  CurrentControlSet\Control\Citrix\VirtualChannels\Audio" -v "
  fEnableCamV4" -t BIN -d "1"
```

Pour désactiver ou réactiver la fonctionnalité, exécutez les commandes suivantes, respectivement :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
  CurrentControlSet\Control\Citrix\VirtualChannels\Audio" -v "
  fEnableCamV4" -d "0"
```

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
  CurrentControlSet\Control\Citrix\VirtualChannels\Audio" -v "
  fEnableCamV4" -d "1"
```

**Exigences et paramètres du client** La fonctionnalité n'est prise en charge que pour les clients suivants :

- Application Citrix Workspace pour Windows
- Application Citrix Workspace pour Linux version minimale 2212
- Application Citrix Workspace pour HTML5 version minimale 2306
- Application Citrix Workspace pour Chrome version minimale 2306
- Application Citrix Workspace pour Mac version minimale 2311

Pour que la fonctionnalité fonctionne comme prévu, des paramètres appropriés doivent être définis dans l'application Citrix Workspace. Pour plus d'informations, consultez la documentation de l'[application Citrix Workspace](#).

## Problèmes connus

En raison d'un [problème](#) avec PulseAudio, les tentatives de commutation entre les périphériques audio peuvent échouer lors d'une session Ubuntu 22.04. Pour résoudre le problème, supprimez la configuration PulseAudio pour l'utilisateur de la session en cours du VDA, puis rouvrez la session. Pour supprimer la configuration PulseAudio, exécutez la commande `$ rm -r ~/.config/pulse`.

## Redirection de contenu du navigateur

August 20, 2024

### Vue d'ensemble

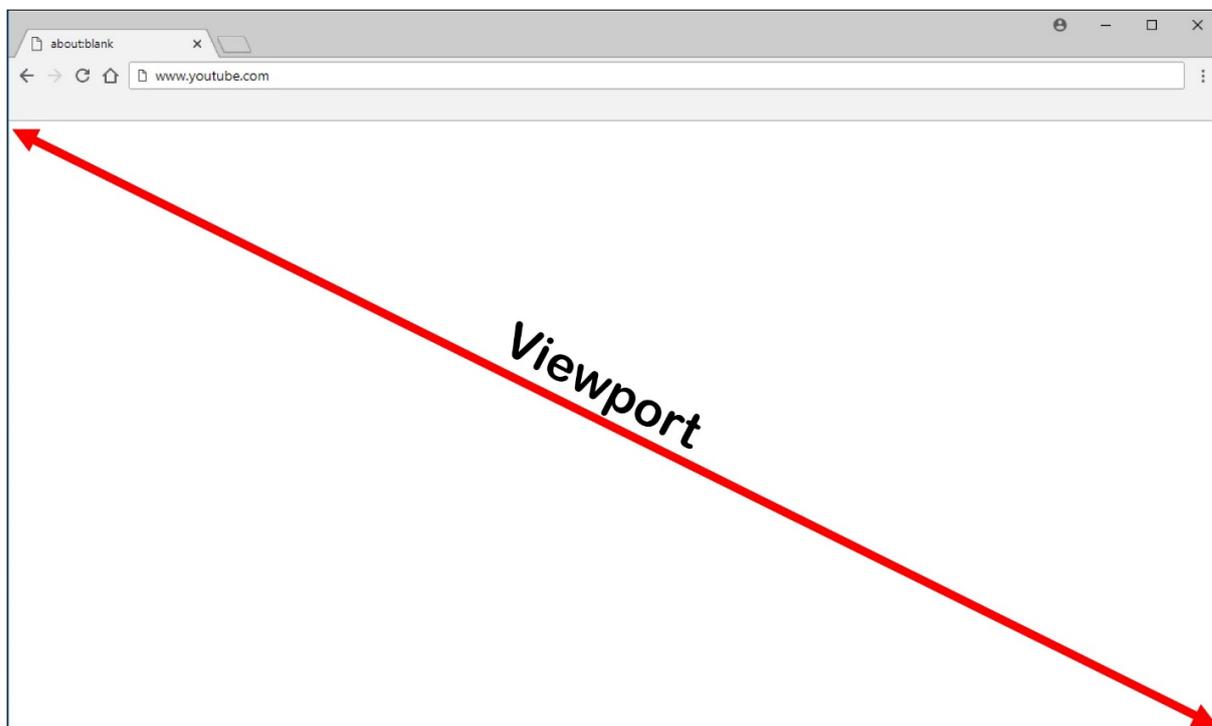
La redirection du contenu du navigateur permet d'afficher les pages Web dans la liste verte du côté client. Cette fonctionnalité utilise l'application Citrix Workspace pour instancier un moteur de rendu correspondant côté client, qui récupère le contenu HTTP et HTTPS de l'URL.

#### Remarque :

Le VDA Linux prend en charge la redirection du contenu du navigateur dans Google Chrome.

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.

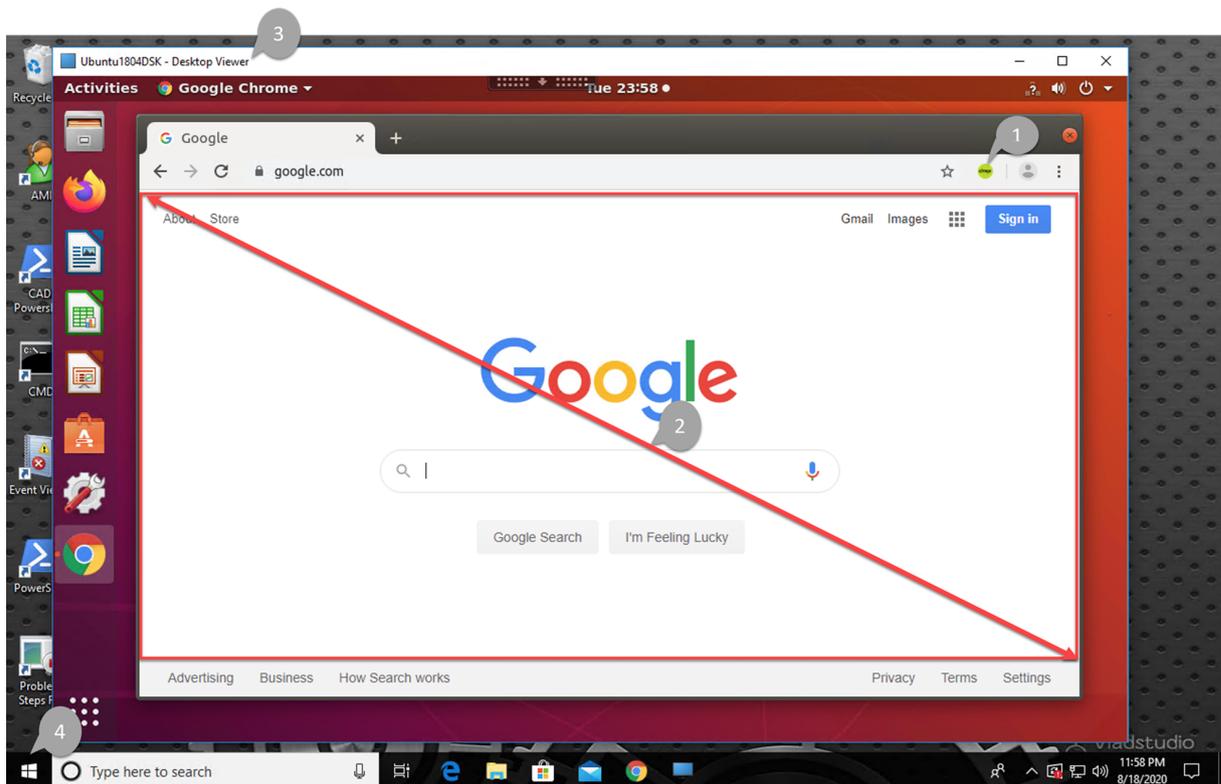


Configurez une stratégie Studio qui spécifie une liste de contrôle d'accès contenant les URL de la liste

verte pour la redirection. Configurez une liste rouge qui désactive la redirection pour des URL spécifiques.

Si une correspondance avec une URL est trouvée dans une liste verte 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

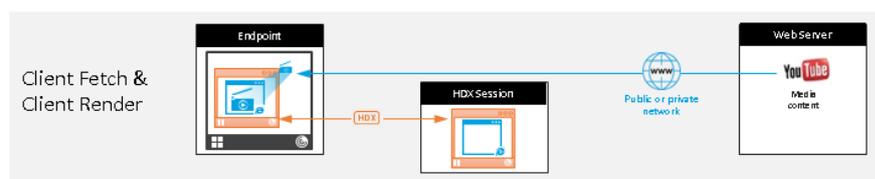
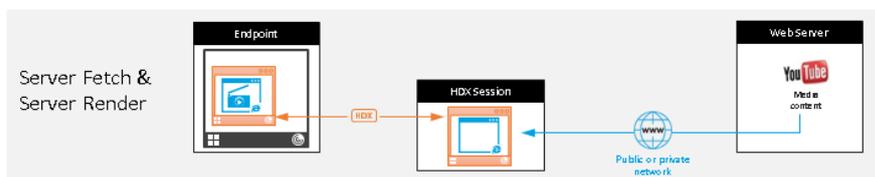
2. Affichage sur le client ou reproduit sur le bureau virtuel

3. Linux VDA

4. Client Windows

L'application Citrix Workspace peut récupérer le contenu de trois façons :

## Redirection scenarios



### Benefits:

- Better end user experience (Adaptive Bit Rate (ABR))
- Reduced VDA resource usage (CPU/RAM/IO)
- Reduced bandwidth consumption

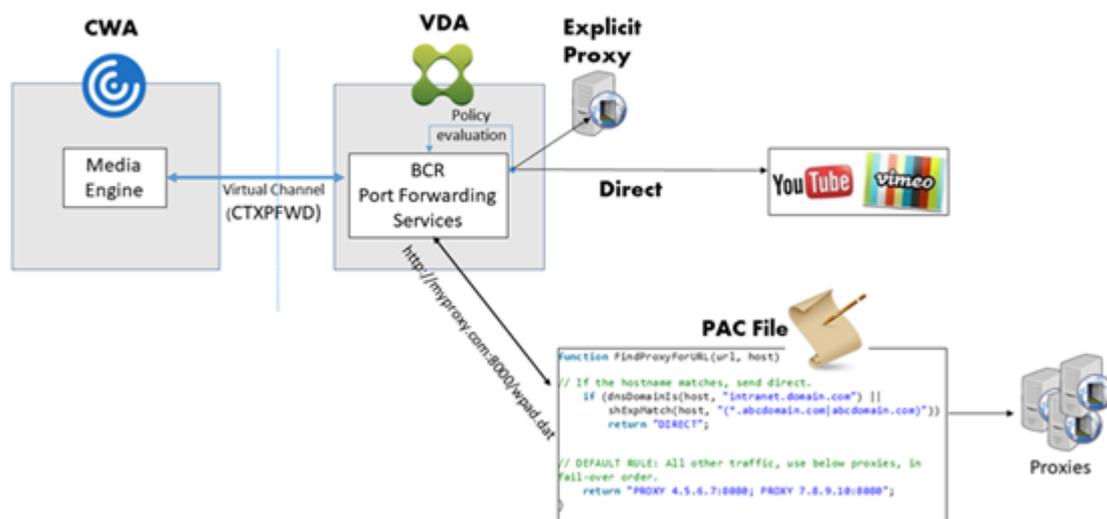
- **Récupération serveur et rendu serveur** : il n'y a pas de redirection car vous n'avez pas ajouté le site à la liste verte ou la redirection a échoué. Nous revenons au rendu de page Web sur le VDA et utilisons Thinwire pour utiliser à distance les graphiques. Utiliser les stratégies pour contrôler le comportement de secours. Ce scénario provoque une consommation élevée de CPU, de RAM et de bande passante sur le VDA.
- **Récupération serveur et restitution client** : l'application Citrix Workspace contacte et récupère le contenu depuis le serveur Web via le VDA à l'aide d'un canal virtuel (CTXPFWD). Cette option est utile lorsque le client n'a pas accès au serveur Web (par exemple, les clients légers). Elle réduit la consommation du processeur et de la RAM sur le VDA, mais la bande passante est consommée sur le canal virtuel ICA.

Il existe trois modes de fonctionnement pour ce scénario. CTXPFWD transmet les données à une machine proxy par laquelle le VDA passe pour accéder au serveur Web.

Quelle option de stratégie choisir :

- Proxy explicite - Si vous avez un seul proxy explicite dans votre centre de données.
- Direct ou Transparent - Si vous n'avez pas de proxy, ou si vous utilisez des proxy transparents.
- Fichiers PAC - Si vous utilisez des fichiers PAC pour que les navigateurs du VDA puissent automatiquement choisir le serveur proxy approprié pour récupérer une URL spécifiée.

Pour plus d'informations, consultez le paramètre **Configuration du proxy de redirection du contenu de navigateur** décrit plus loin dans cet article.



- **Récupération client et restitution 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.

Avantages :

- Meilleure expérience pour l'utilisateur final (débit binaire adaptatif (ABR))
- Réduction de l'utilisation des ressources VDA (CPU/RAM/IO)
- Réduction de la consommation de bande passante

## Configuration système requise

### Client Windows :

- Application Citrix Workspace 1809 pour Windows ou version ultérieure

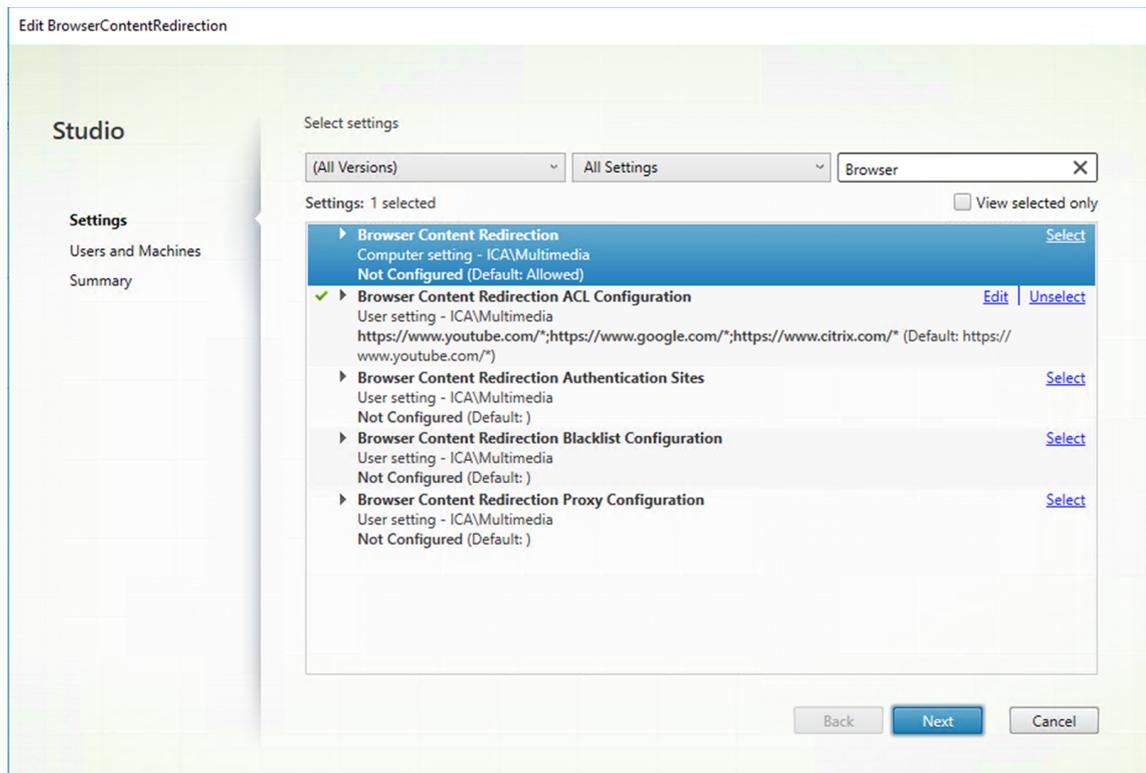
### Linux VDA :

- 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

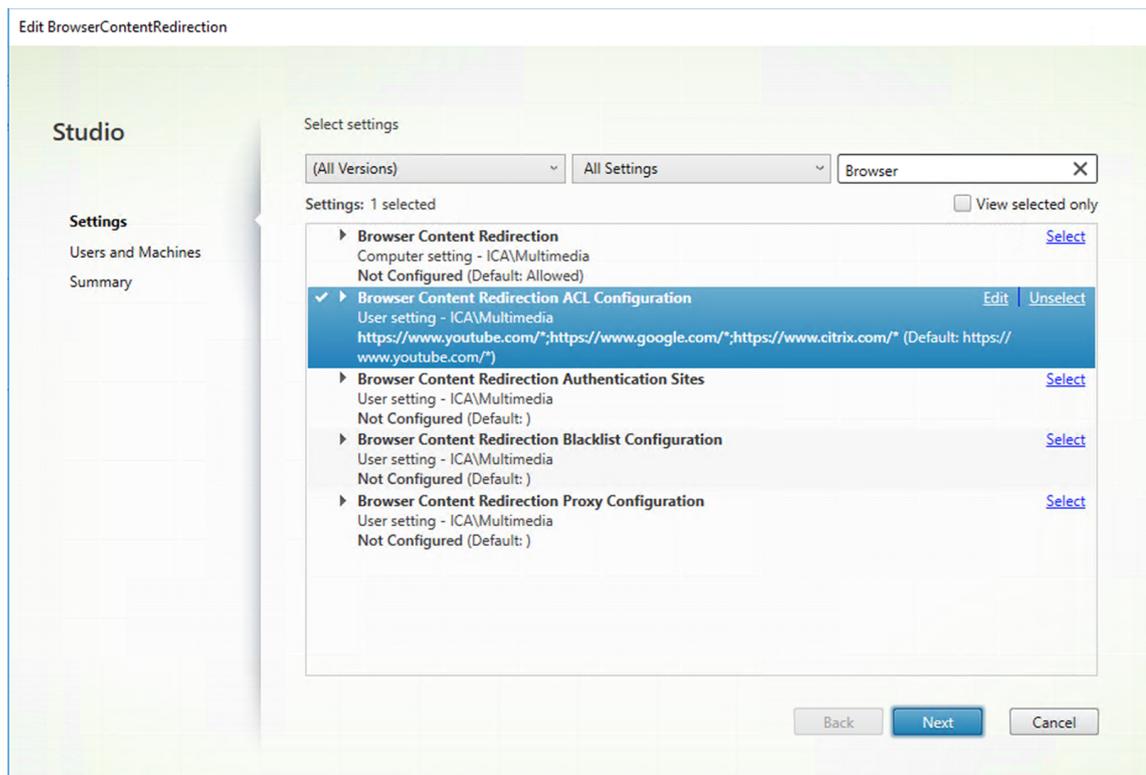
Pour utiliser la redirection du contenu du navigateur, configurez les stratégies pertinentes et installez l'extension de redirection de contenu du navigateur dans Google Chrome. Pour ce faire, procédez comme suit :

1. Dans Citrix Studio, définissez **Redirection du contenu de navigateur** sur **Autorisé** pour activer la redirection du contenu du navigateur.



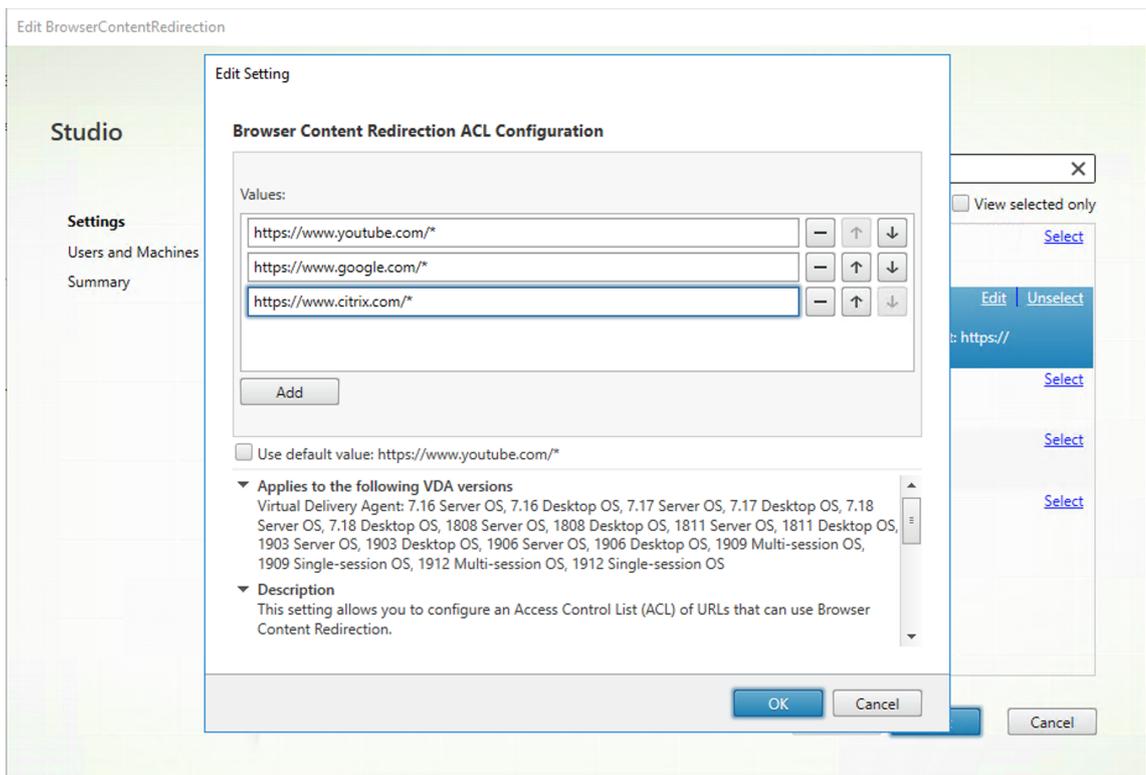
2. Spécifiez une liste verte d'URL dont le contenu peut être redirigé vers le client et une liste rouge qui désactive la redirection pour des URL spécifiques. La configuration d'une liste rouge est facultative.

Le paramètre **Configuration de l'ACL de redirection du contenu de navigateur** spécifie une liste verte d'URL dont le contenu peut être redirigé vers le client. Lorsque vous spécifiez des URL, vous pouvez utiliser le caractère générique \* pour représenter tous les composants de l'URL à l'exception du protocole.

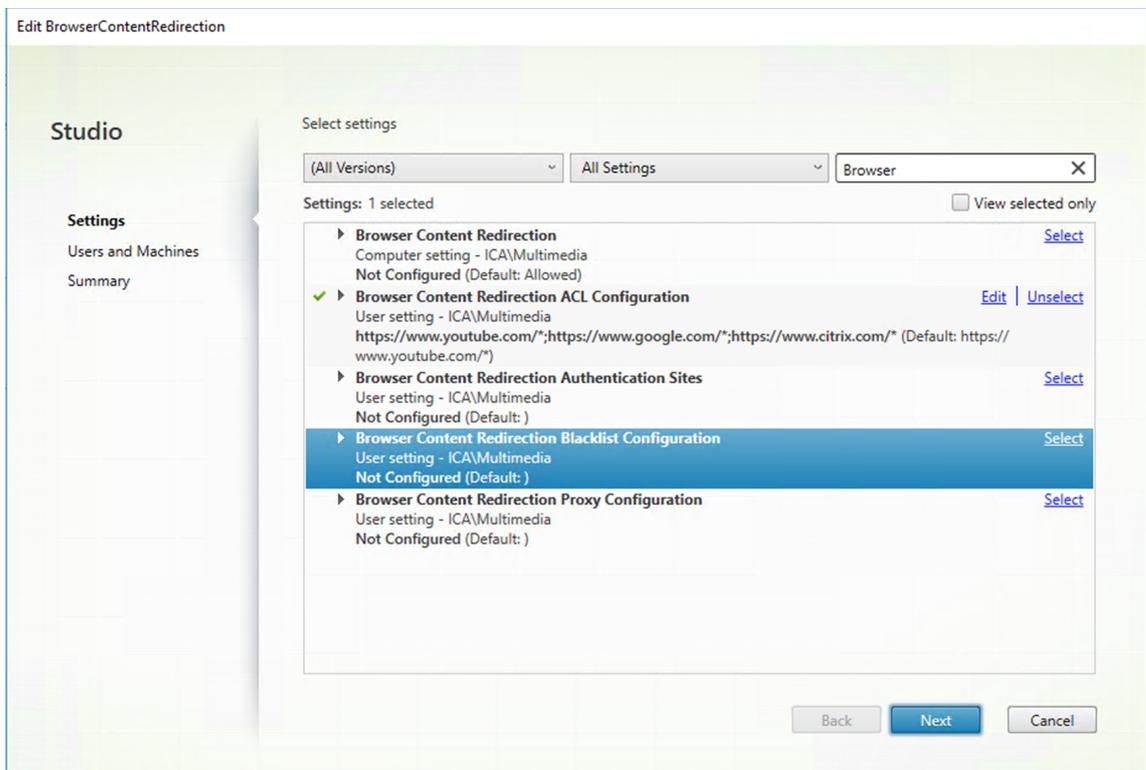


Les exemples suivants sont autorisés :

- `http://www.xyz.com/index.html` (Vous pouvez obtenir une meilleure granularité en spécifiant des chemins d'accès dans l'URL. Par exemple, si vous spécifiez `https://www.xyz.com/sports/index.html`, seule la page `index.html` est redirigée.)
- `https://www.xyz.com/*`
- `http://www.xyz.com/*videos*`
- `http://*.xyz.com/`
- `http://*.*.com/`



Le paramètre **Configuration d'une liste noire de redirection du contenu de navigateur** spécifie une liste rouge qui désactive la redirection pour des URL spécifiques.



3. Pour activer la récupération serveur et la restitution client, configurez le paramètre **Configuration du proxy de redirection du contenu de navigateur**.

Ce paramètre fournit des options de configuration pour les paramètres proxy sur le VDA pour la redirection du contenu du navigateur. Si cette option est activée avec une adresse proxy et un numéro de port valides, une URL PAC/WPAD ou un paramètre Direct/Transparent, l'application Citrix Workspace essaie toujours d'effectuer la récupération serveur et la restitution client en premier. Pour plus d'informations, consultez la section Mécanisme de secours.

Si cette option est désactivée ou non configurée et utilise une valeur par défaut, l'application Citrix Workspace tente une récupération client et une restitution client.

Par défaut, cette option est définie sur **Interdit**.

#### **Modèle autorisé pour un proxy explicite :**

`http://\<hostname/ip address>:\<port\>`

Exemple :

`http://proxy.example.citrix.com:80 http://10.10.10.10:8080`

#### **Modèles autorisés pour des fichiers PAC/WPAD :**

`http://<hostname/ip address>:<port>/<path>/<Proxy.pac>`

Exemple : `http://wpad.myproxy.com:30/configuration/pac/Proxy.pac`

`https://<hostname/ip address>:<port>/<path>/<wpad.dat>`

Exemple : `http://10.10.10.10/configuration/pac/wpad.dat`

#### **Modèles autorisés pour des proxys directs ou transparents :**

Tapez le mot **DIRECT** dans la zone de texte de la stratégie.

##### **Remarque :**

Vous pouvez également définir un proxy en modifiant la valeur de registre `HKLM\Software\Citrix\HdxMediastream\WebBrowserRedirectionProxyAddress` .. En outre, la valeur de registre `HKLM\Software\Citrix\HdxMediastream\AllowNonTlsPacUri` vous permet de décider d'autoriser ou non le téléchargement de fichiers PAC via HTTP. La valeur par défaut est 0, ce qui signifie que le protocole HTTP n'est pas autorisé.

Options de remplacement du registre pour les paramètres de stratégie Pour obtenir la liste des clés de registre pertinentes, consultez la section Remplacements de clé du registre de redirection de contenu du navigateur.

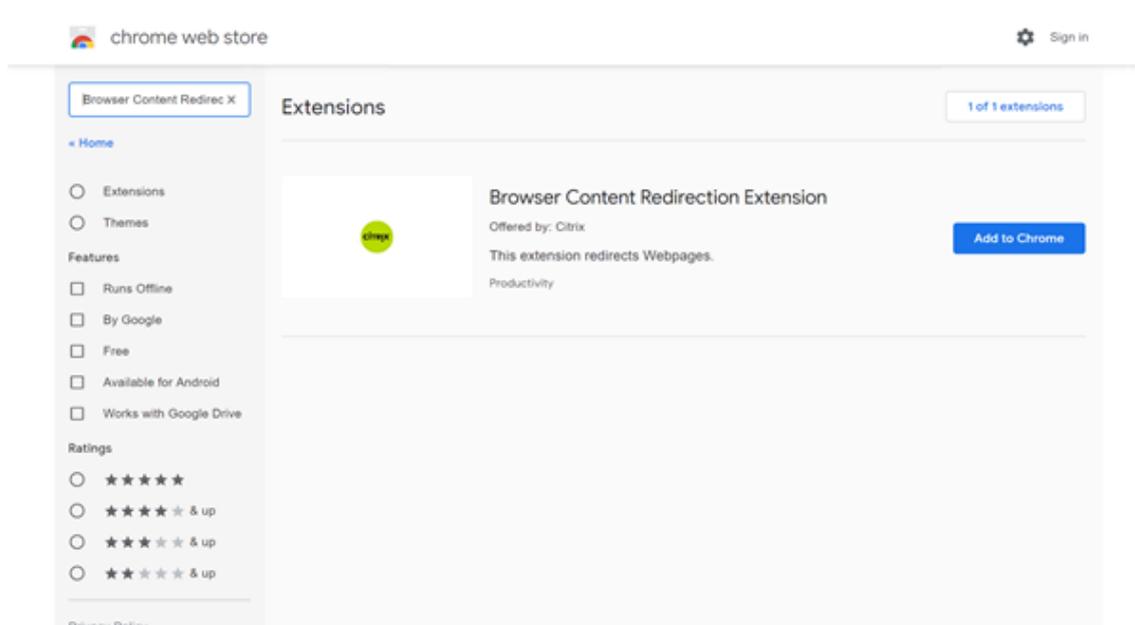
4. Cliquez sur **Ajouter à Chrome** sur le VDA pour ajouter l'extension de redirection de contenu du

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 verte ou une liste rouge.

### 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.



## Mécanisme de secours

Si vous activez la stratégie **Configuration du proxy de redirection du contenu de navigateur**, Citrix Receiver tente uniquement une récupération serveur et une restitution client. Si la récupération serveur et la restitution client échouent, le système revient automatiquement à la récupération client et à la restitution client. Si la machine cliente n'a pas accès au serveur Web, le navigateur du VDA peut alors recharger et afficher la page sur le serveur (récupération serveur et restitution serveur).

## Remplacements de clé du registre de redirection de contenu de navigateur

### Avertissement :

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

votre registre avant de le modifier.

HKLM\Software\Citrix\HdxMediastream

Nom	Type	Valeur
<b>WebBrowserRedirection</b>	DWORD	1=Autorisé, 0=Interdit
<b>WebBrowserRedirectionAcl</b>	REG_MULTI_SZ	/
<b>WebBrowserRedirectionProxyAddresses</b>	REG_SZ	Si vous définissez ce paramètre sur l'un des modes suivants, la restitution client de récupération serveur est activée : <b>Proxy explicite</b> - Si vous avez un seul proxy explicite dans votre centre de données. <b>Direct ou Transparent</b> - Si vous n'avez pas de proxy, ou si vous utilisez des proxy transparents. <b>Fichiers PAC</b> - Si vous utilisez des fichiers PAC pour que les navigateurs du VDA puissent automatiquement choisir le serveur proxy approprié pour récupérer une URL spécifiée.
<b>WebBrowserRedirectionBlacklist</b>	REG_MULTI_SZ	/
<b>AllowNonTlsPacUri</b>	DWORD	Détermine si le téléchargement de fichiers PAC via HTTP est autorisé. La valeur par défaut est 0, ce qui signifie que le protocole HTTP n'est pas autorisé. Si vous définissez ce paramètre sur 1, <b>HDXWebProxy.exe</b> peut télécharger les fichiers PAC via HTTP (pas uniquement via HTTPS).

## Compression vidéo pour Webcam HDX

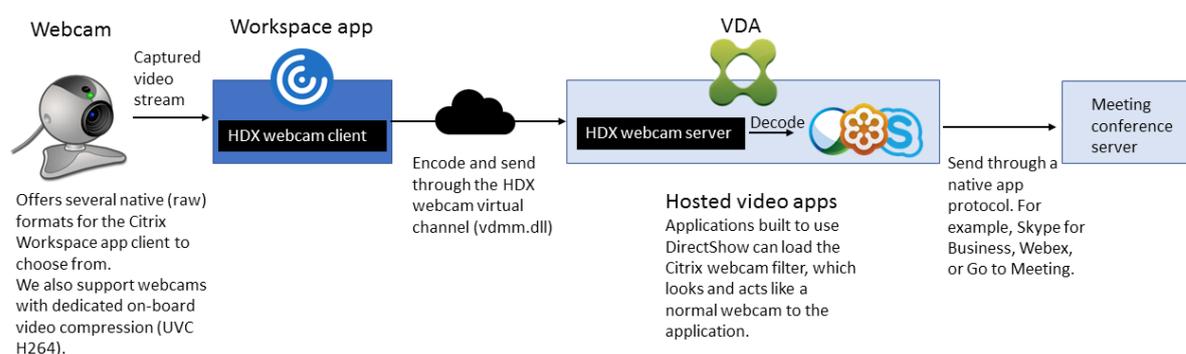
August 20, 2024

### 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.

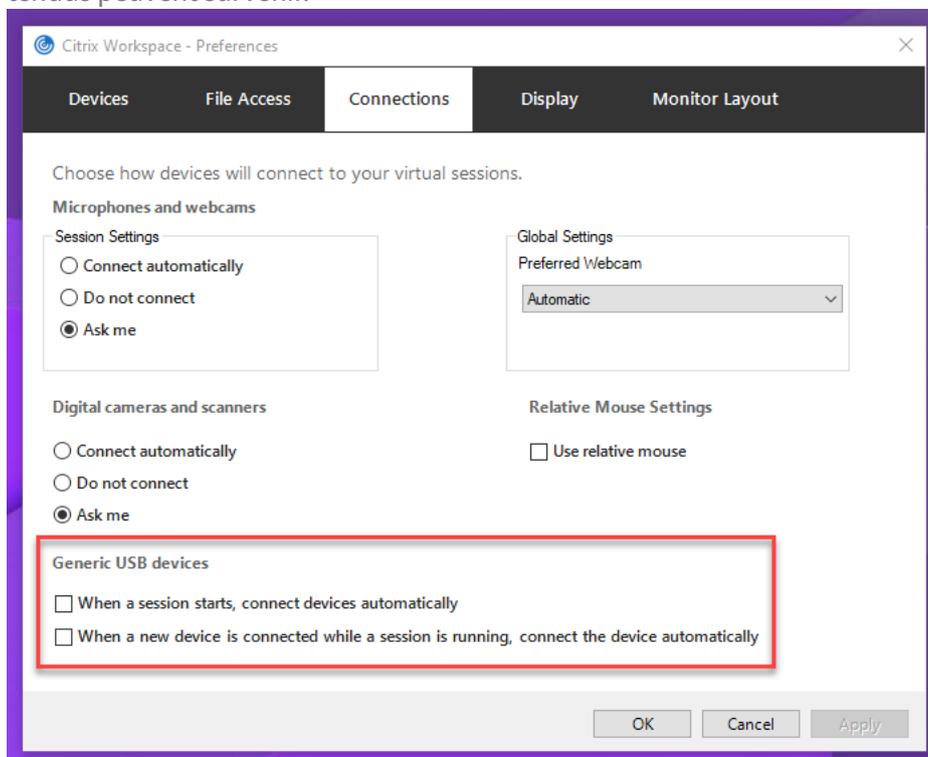
Le client gère la communication avec la webcam. Le client envoie alors la vidéo uniquement au serveur qui peut l'afficher correctement. Le serveur ne communique pas directement avec la webcam, mais il est intégré pour vous offrir la même expérience sur votre bureau. L'application Workspace compresse 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.

---

Plateforme	Processeur
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 :

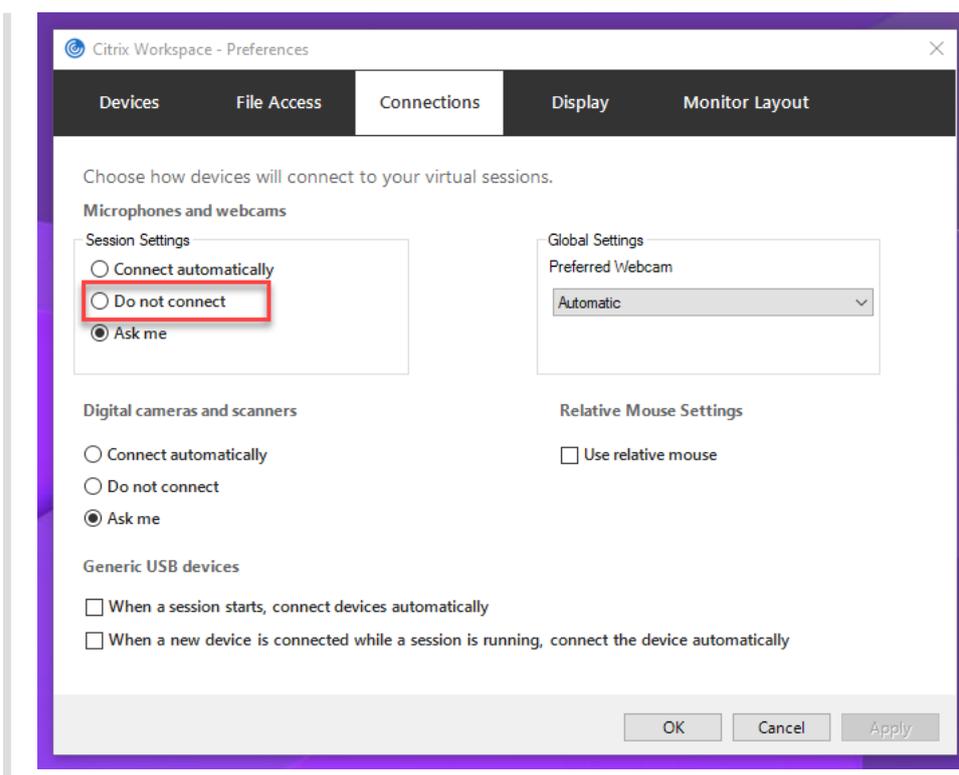
- Logitech HD Webcam C270
- Logitech Webcam C930e
- Microsoft-LifeCam-HD3000

## Configuration

Cette fonctionnalité est activée par défaut. 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 de Desktop Viewer **Ne pas se connecter** sous **Micros et webcams**.



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 :

```
1 sudo apt-get update
2 sudo apt-get dist-upgrade
3 sudo reboot
```

Si votre VDA est déployé sur SUSE 15, exécutez les commandes suivantes pour effectuer la mise à jour vers la dernière version du noyau et redémarrer :

```
1 zypper up kernel-default
2 reboot
```

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 systemctl restart ctxwcamsd`. 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, exécutez la commande `sudo mkdir -p /var/xdl`.
  - c) Copiez `/var/xdl/configure_*` depuis votre VDA vers la machine sous `/var/xdl/`.
  - d) Sur la machine, 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 sur votre VDA et placez-le sous `/opt/Citrix/VDA/lib64/`.

- f) Sur votre VDA, exécutez la commande `sudo systemctl restart ctxwcamsd` pour redémarrer le service de webcam et chargez le module de noyau `v4l2loopback`.

## VDA Linux non joints à un domaine

August 20, 2024

### Vue d'ensemble

Avec les VDA non joints à un domaine, vous n'avez plus besoin de joindre des VDA à des domaines Active Directory pour l'authentification des VDA et des utilisateurs. Lorsque vous créez un VDA non joint à un domaine, vous générez une paire de clés publique-privée pour enregistrer le VDA dans le plan de contrôle du cloud. Il n'est donc plus nécessaire de joindre un domaine Active Directory. Lorsqu'un utilisateur lance une session à partir du VDA non joint à un domaine, le VDA crée un compte de mappage local en utilisant le nom d'utilisateur que l'utilisateur utilise pour se connecter à l'application Citrix Workspace. Le VDA attribue un mot de passe aléatoire que le compte de mappage local utilise pour l'authentification unique et la reconnexion de session. Si vous modifiez le mot de passe aléatoire, l'authentification unique et la reconnexion de session échouent. Pour désactiver l'authentification unique, consultez la section [Pas d'authentification unique](#).

#### Important :

- Les VDA non joints à un domaine sont pris en charge pour Citrix DaaS.
  - Votre plan de contrôle doit être déployé via Citrix DaaS.
  - Vous pouvez déployer des VDA non joints à un domaine dans un cloud public ou un centre de données sur site. Le plan de contrôle de Citrix DaaS gère les VDA non joints à un domaine.
  - Pour créer des VDA non liés à un domaine, vous devez activer [Rendezvous V2](#). Les composants Cloud Connector ne sont nécessaires que si vous envisagez de provisionner des machines sur des hyperviseurs locaux ou si vous souhaitez utiliser Active Directory comme fournisseur d'identité dans Workspace.
- Pour créer des VDA non joints à un domaine, vous pouvez utiliser Machine Creation Services (MCS) et Easy Install. Pour plus d'informations, consultez [Créer des VDA Linux non joints à un domaine à l'aide de MCS](#) et [Créer un Linux VDA non joint à un domaine à l'aide d'Easy Install](#).
  - MCS ne prend pas en charge les serveurs bare metal.

## Fonctionnalités disponibles pour les VDA Linux 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, tels que 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. Spécifiez les attributs suivants dans le script `/var/xdm/getuidgid.sh` situé sous le chemin d'installation du VDA :

Attribut	Requis ou facultatif	Description
<code>uid</code>	Obligatoire	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.
<code>gid</code>	Obligatoire	Un identificateur de groupe (GID) est un nombre utilisé pour représenter un groupe spécifique.
<code>homedir</code>	Facultatif	Le répertoire de base Linux est un répertoire destiné à un utilisateur particulier.
<code>shell</code>	Facultatif	Un shell d'ouverture de session est un shell donné à un utilisateur lors de la connexion à 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.

```
1 #!/bin/bash
2
3 #####
4 #
5 # Citrix Virtual Apps & Desktops For Linux Script: Get uid and gid
   for the user
6 #
7 # Copyright (c) Citrix Systems, Inc. All Rights Reserved.
8 #
9
10 export LC_ALL="en_US.UTF-8"
11
12 function get_uid_gid_for_user()
13 {
14
15 echo "uid:12345"
16 echo "gid:1003"
17 echo "homedir:/home/$1"
18 echo "shell:/bin/sh"
19 }
20
21
22 get_uid_gid_for_user $1
```

**Pas d'authentification unique**

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. Pour plus d'informations, consultez [Pas d'authentification unique](#).

**Authentification avec Azure Active Directory**

Les VDA non joints à un domaine que vous déployez dans Azure s'intègrent au service d'identité AAD pour fournir l'authentification des utilisateurs. Pour plus d'informations, consultez [Authentification avec Azure Active Directory](#).

## Rendezvous V2

Les VDA non joints à un domaine sont pris en charge pour utiliser Rendezvous V2 afin de contourner les Citrix Cloud Connector. Pour plus d'informations, consultez [Rendezvous V2](#).

## Liste des stratégies prises en charge

August 20, 2024

### Liste des stratégies prises en charge avec le Linux VDA

Nom	Valeur
Stratégie de la Studio clé	par Module défaut
<b>Utiliser l'heure locale du client</b>	UseLocalTimeOfICAController de fuseau horaire du serveur
<b>Calcul des boucles ICA</b>	IcaroundTripCheckFinalité de l'utilisateur final
<b>Intervalle de calcul des boucles ICA</b>	IcaroundTripCheckFinalité de l'utilisateur final

Nom	Valeur
Stratégie de la Studio clé	par Module défaut
<b>Calcul des boucles ICA pour les connexions inactives</b>	IcaroundTripTimeCAControlled (0) de l'utilisateur final
<b>Limite de bande passante de session générale</b>	LimitOverallBandwidthCA\Bandwidth pas-sante
<b>Limite de bande passante de la redirection audio</b>	LimitAudioBandwidthCA\Bandwidth pas-sante

Nom	Valeur
Stratégie de la Studio clé	par Module défaut

---

**Pourcentage de limite de bande passante de la redirection audio** LimitAudioBandwidth CA\Band0 pas-sante

**Limite de bande passante de redirection du périphérique USB client** LimitUSBBandwidth CA\Band0 pas-sante

Nom	Valeur
Stratégie de la Studio clé	par Module défaut

---

**Pourcentage de bande pas-sante de redirection du périphérique USB client** LimitCdm\BwRate\CA\Band0

**Limite de bande pas-sante de redirection de fichier** LimitCdm\BwRate\CA\Band0

Nom	Valeur
Stratégie de la Studio clé	par Module défaut

---

**Pourcentage de bande passante de redirection de fichier**

LimitPrinters\Bandwidth

de bande passante de redirection de fichier

LimitPrinters\Bandwidth

de bande passante de redirection

d'imprimante

Nom	Valeur
Stratégie de la Studio clé	par Module défaut

---

**Pourcentage de bande passante de redirection de l'imprimante**

**de bande passante de redirection de l'imprimante**

**Connexions WebSockets**

**Numéro de port WebSockets**

Nom	Valeur
Stratégie de la Studio clé	par Module défaut

**Liste des serveurs d'origine approuvés Web-Sockets**

**Persistance ICA** **ICA** **Persistance** **Non**

en-  
voyer  
de  
mes-  
sages  
de  
persis-  
tance  
ICA (0)

**Délai d'expiration de persistance ICA**

**ICA** **Persistance** **60** **sec-**  
**ondes**

Nom				Valeur
Stratégie de la Studio	clé	Type	Module	par défaut
<b>Numéro de port de l'écouteur ICA</b>	ICAListenPort	Port	1494	
<b>Transport adaptatif HDX</b>	HDXoverUD	Préférence	Préféré (2)	
<b>Connexion de fiabilité de session</b>	SessionReliability	Métrique de session	(1)	
<b>Niveau de transparence de l'interface durant la reconnexion</b>	ReconnectTransparency	Niveau de transparence des clients		

Nom	Valeur
Stratégie de la Studio clé	par Module défaut

**Numéro de port de la fiabilité de session** SessionReliabilityPort 2598

**Expiration de délai de la fiabilité de session** SessionReliabilityTimeout 180 s

**Reconnexion automatique des clients** AutoClientReconnect 1

**Redirection audio cliente** AudioRedirection 1

**Redirection d'imprimante cliente** PrinterRedirection 1

	Nom	Valeur
Stratégie de la Studio	clé	Type Module par défaut
<b>Créer automatiquement l'imprimante universelle PDF</b>	AutoCreatePDFPrinter	Désactivé (0)
<b>Mappage et compatibilité du pilote d'imprimante</b>	PrinterMapping	Microsoft XPS Document Writer *, Deny ; Send to Microsoft OneNote *, Deny "
<b>Redirection du Presse-papiers client</b>	ClipboardRedirection	Autorisé (1)

Nom	Valeur
Stratégie de la Studio clé Type Module	par défaut
<b>Limite le client du presse- papiers à la taille de trans- fert de la ses- sion</b>	LimitClipboardSizeC2H Désactivé (0)
<b>Limite la ses- sion du Presse- papiers à la taille de trans- fert du client</b>	LimitClipboardSizeH2C Désactivé (0)

Nom		Valeur	
Stratégie de la			par
Studio	clé	Type	Module défaut
<b>Limite de bande pas-sante de redirection du Presse-papiers</b>	LimitClipboardMaterialCA\Band		0
<b>Pourcentage de la limite de la bande pas-sante de redirection du Presse-papiers</b>	LimitClipboardMaterialCA\Band		0
<b>Restriction de l'écriture dans le Presse-papiers client</b>	RestrictClipboardWrite		Désactivé
			papiers (0)

Nom	Valeur
Stratégie de la Studio clé	par Module défaut

**Formats ClientClipboardAllowedFormats**  
**d'**  
**écriture**  
**au-**  
**torisés**  
**dans**  
**le**  
**Presse-**  
**papiers**  
**client**

**RestrictionsSessionClipboardDisabled**  
**écriture**  
**dans**  
**le**  
**Presse-**  
**papiers**  
**de**  
**ses-**  
**sion**

**Formats SessionClipboardAllowedFormats**  
**d'**  
**écriture**  
**au-**  
**torisés**  
**dans**  
**le**  
**Presse-**  
**papiers**  
**de**  
**ses-**  
**sion**

Nom		Valeur	
Stratégie de la Studio	clé	Type	Module par défaut
<b>Redirection de périphérique USB client</b>	USBDeviceFilter	Boolean	Interdit (0)
<b>Règles de redirection de périphérique USB client</b>	USBDeviceFilter	String	""
<b>Compression d'images en mouvement</b>	ImageStreaming	Boolean	Activé (1)
<b>Compression de couleur supplémentaire</b>	ColorCompression	Boolean	Désactivé (0)
<b>Taux de trame minimum cible</b>	TargetedUtilization	Integer	10

Nom	Valeur
Stratégie de la Studio clé	par Module défaut
<b>Taux de trames cible</b>	FramesPerSecondThinwire 30 fps
<b>Qualité visuelle</b>	VisualQualityUserThinwire Moyenne (3)
<b>Utiliser le codec vidéo pour la compression</b>	VideoCodecUserThinwire Utiliser au choix (3)
<b>Utiliser le codage matériel pour le codec vidéo</b>	UseHardwareEncoderHighPerformanceVideoCodec (1)
<b>Autoriser la compression visuelle sans perte</b>	AllowVisualLosslessCompression (0)

Nom	Valeur
Stratégie de la Studio clé Type Module	par défaut
<b>Optimiser pour la charge des graphiques 3D</b>	OptimizeFor3DWire Désactivé (0)
<b>Nombre de couleurs préféré pour les graphiques simples</b>	PreferredColorDepth 24 bits par pixel (1)
<b>Qualité audio</b>	SoundQualityAudio Élevée : audio à définition élevée (2)
<b>Redirection du microphone client</b>	AllowMicrophoneAudio Autorisé (1)
<b>Nombre maximum de sessions</b>	MaximumOrdnateOfSessions 250 de la charge

Nom	Valeur
Stratégie de la Studio clé	par Module défaut
<b>Tolérance d'ouvertures de session simultanées</b>	Concurrente 2
<b>Activer la mise à jour automatique des contrôleurs</b>	EnableAutoupdate Fonctionnel Virtual (1) Deliv-ery Agent
<b>Mode de mise à jour de la sélection du Presse-papiers</b>	Clipboard Selection Presse-papiers

	Nom	Valeur
Stratégie de la Studio	clé	Type Module par défaut
<b>Mode de mise à jour de la sélection principale</b>	PrimarySelection	UpstreamMode papiers
<b>Qualité speex maximale</b>	MaxSpeexQuality	Audio 5
<b>Connecteur au-toma-tique-les lecteurs clients</b>	AutoConnectDrives	RedirectionActivé (1) fichier\CDM
<b>Lecteurs optiques clients</b>	AllowCDROMDrives	RedirectionAutorisé (1) fichier\CDM
<b>Lecteurs fixes clients</b>	AllowFixedDrives	RedirectionAutorisé (1) fichier\CDM
<b>Lecteurs de disquette clients</b>	AllowFloppyDrives	RedirectionAutorisé (1) fichier\CDM

Nom	Type	Valeur
Stratégie de la Studio	clé	par Module défaut
<b>Lecteurs réseau clients</b>	AllowNetworkClients	Redirection de fichier\CDM Autorisé (1)
<b>Redirection de lecteur client</b>	AllowDriveRedirection	Redirection de fichier\CDM Autorisé (1)
<b>Accès en lecture unique sur le lecteur client</b>	ReadOnlyMappedDrive	Redirection de fichier\CDM Désactivé (0)
<b>Affichage automatique du clavier</b>	AllowAutomaticKeyboard	Redirection de fichier\CDM Désactivé (0)
<b>Autoriser le transfert de fichiers entre le bureau et le client</b>	AllowFileTransfer	Transfert de fichiers Autorisé

Nom	Valeur
Stratégie de la Studio clé	par Module défaut
<b>Télécharger des fichiers depuis le bureau</b>	AllowFileDownloadTransfert Autorisé de fichiers
<b>Charger des fichiers sur le bureau</b>	AllowFileUploadTransfert Autorisé de fichiers
<b>Horloge inactive de session</b>	EnableSessionIdleTimeouts Activé de ses- (1) sion
<b>Intervalle d'horloge inactive de session</b>	SessionIdleTimeoutInterval 1440 de ses- min- sion utes
<b>Horloge de session dé-connectée</b>	EnableSessionDisconnectTimeouts Désactivé de ses- (0) sion

Nom	Valeur
Stratégie de la Studio clé	par Module défaut
<b>Intervalle d'horloge de session de dé-con-nec-tée</b>	Session Distribution Interval: 40 minutes
<b>Redirection de contenu du navigateur</b>	Web Browser Redirection Multimedia
<b>Configuration de l'ACL de redirection du contenu de navigateur</b>	Web Browser Redirection Multimedia :// www. youtube .com /*

Nom	Valeur
Stratégie de la Studio clé	par Module défaut

**Configuration d'une liste rouge de redirection du contenu de navigateur**

**Configuration du proxy de redirection du contenu de navigateur**

**Activer le filtrage de session** EnableSessions Watermark Content  
 Désactivé

Nom	Valeur
Stratégie de la Studio clé	par Module défaut
<b>Inclure adresse IP du client</b>	IncludeClientAddress\Session Water- mark\Watermark Con- tent
<b>Inclure l' heure de con- nex- ion</b>	IncludeClientTime\Session Water- mark\Watermark Con- tent
<b>Inclure nom d'util- isa- teur de con- nex- ion</b>	IncludeLoginName\Session Water- mark\Watermark Con- tent
<b>Inclure nom d' hôte du VDA</b>	IncludeVDAHostName\Session Water- mark\Watermark Con- tent
<b>Inclure adresse IP du VDA</b>	IncludeVDAAddress\Session Water- mark\Watermark Con- tent

---

Nom		Valeur	
Stratégie de la			par
Studio	clé	Type	Module défaut

---

**Style de filigrane de session** Watermark\Style\CA\Session\Multiple  
Watermark\Watermark\Style

**Transparence du filigrane** Watermark\Time\CA\Session  
Watermark\Watermark\Style

	Nom		Valeur
	Stratégie de la		par
	Studio clé	Type	Module défaut
<b>Texte personnalisé en filigrane</b>	Watermark\CustomText	Text	<pre> Session Water- config- mark\Watermark Con- tion tent de texte per- son- nal- isée valide peut ressem- bler à ceci : &lt; font = Arial  Unicode MS &gt;&lt; domain &gt;&lt; newline &gt;&lt; fontsize =47&gt;&lt; username &gt;&lt; newline &gt;&lt; fontzoom =120&gt; Citrix &lt; newline </pre>

**Remarque :**

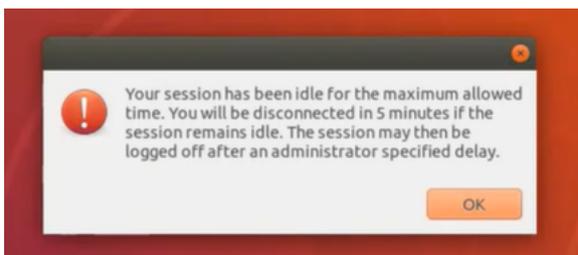
Seul le Virtual Delivery Agent (VDA) pour Windows prend en charge l'audio via UDP (User Datagram Protocol). Le VDA Linux ne prend pas en charge cette fonctionnalité. Pour de plus amples informations, consultez la section [Transport en temps réel audio via UDP \(User Datagram Protocol\)](#).

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 :

### Primary selection update mode

Value: Selection changes are not updated on neither client nor host

Use Selection changes are not updated on neither client nor host

Host selection changes are not updated to client

Client selection changes are not updated to host

Selection changes are updated on both client and host

OS, 7.1 Desktop OS, 7.5 Server OS, 7.1 Desktop OS, 7.8 Server OS, 7.8 Desktop OS, 7.9 Server OS, 7.9 Desktop OS, 7.11 Server OS, 7.11 Desktop OS, 7.12 Server OS, 7.12 Desktop OS, 7.13 Server OS, 7.13 Desktop OS, 7.14 Server OS, 7.14 Desktop OS, 7.15 Server OS, 7.15 Desktop OS, 7.16 Server OS, 7.16 Desktop OS, 7.17 Server OS, 7.17 Desktop OS, 7.18 Server OS, 7.18 Desktop OS, 7.19 Server OS, 7.19 Desktop OS

▼ Description

This setting is supported only by Linux VDA version 1.4 onwards.

PRIMARY selection is used for explicit copy/paste actions such as mouse selection and middle mouse button paste. This setting controls whether PRIMARY selection changes on the Linux VDA can be updated on the client's clipboard (and vice versa). It can include one of the following selection changes:

Selection changes are not updated on the client or the host. PRIMARY selection changes do not update a client's clipboard. Client clipboard changes do not update PRIMARY selection.

Host selection changes are not updated on the client. PRIMARY selection changes do not update a client's clipboard. Client clipboard changes update the PRIMARY selection.

Client selection changes are not updated on the host. PRIMARY selection changes update the client's clipboard. Client clipboard changes do not update the PRIMARY selection.

Selection changes are updated on both the client and host. PRIMARY selection change updates the client's clipboard. Client clipboard changes update the PRIMARY selection.

▼ Related settings

Clipboard selection update mode

- **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

- ClipboardSelectionMode

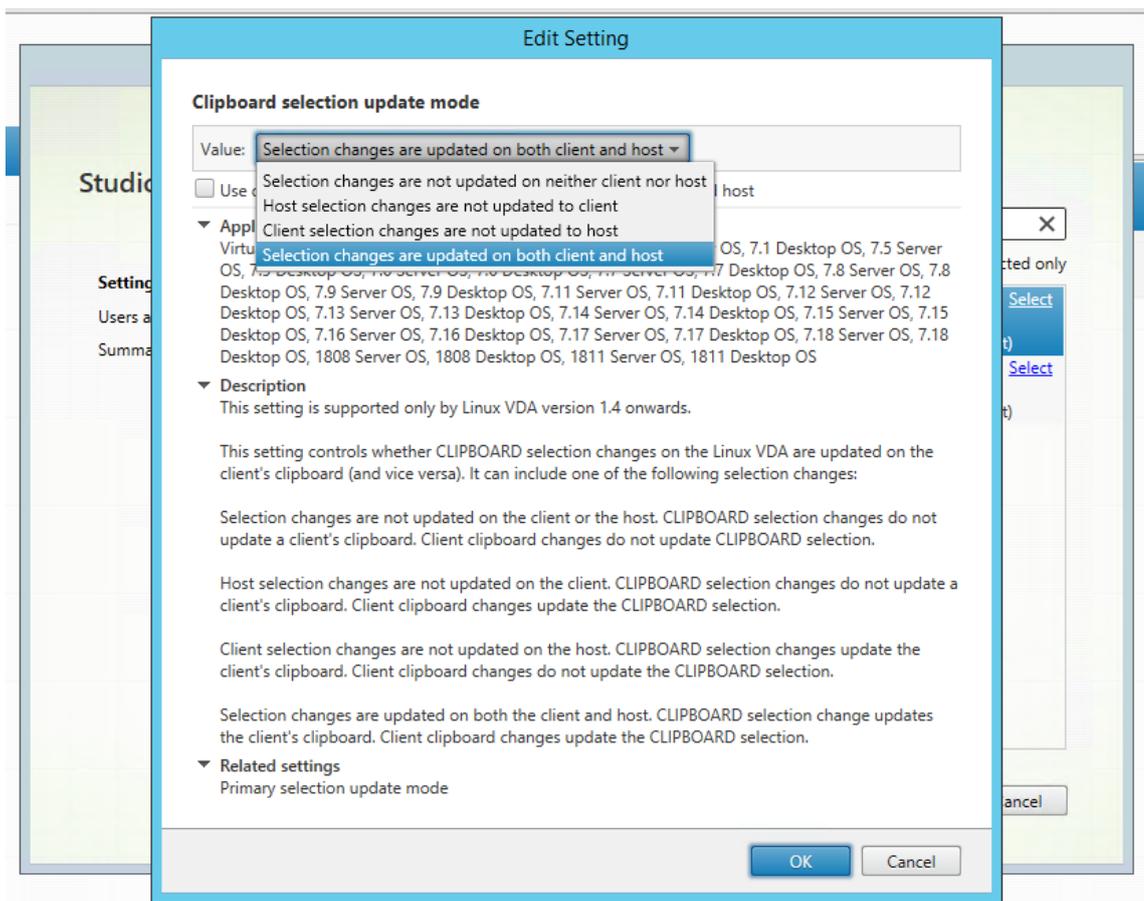
**Valeur (enum)** : [0, 1, 2, 3]

**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

August 20, 2024

Cette section contient les rubriques suivantes :

- [Meilleures pratiques d'impression](#)
- [Impression PDF](#)

## Meilleures pratiques d'impression

August 20, 2024

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 :**

```
1 sudo yum -y install cups
2
3 sudo yum -y install foomatic-filters
```

## Paramètres de stratégie Impression

### Redirection d'imprimante cliente

Ce paramètre contrôle si les imprimantes clientes sont mappées sur une session VDA. Par défaut, le mappage des imprimantes clientes est autorisé.

### Créer automatiquement les imprimantes clientes

Ce paramètre spécifie les imprimantes clientes qui peuvent être mappées dans des sessions VDA. Par défaut, il est configuré pour **Créer automatiquement toutes les imprimantes clientes**, ce qui signifie que toutes les imprimantes clientes sont mappées à des sessions VDA. Pour plus d'informations sur ce paramètre, consultez la section [Créer automatiquement les imprimantes clientes](#) dans la documentation de Citrix Virtual Apps and Desktops.

### Créer automatiquement l'imprimante universelle PDF

Pour utiliser la fonctionnalité [Impression PDF](#), définissez cette stratégie sur **Activé**.

### Mappage et compatibilité du pilote d'imprimante

Citrix fournit trois types de pilotes d'imprimante universels (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.

Edit Setting

**Printer driver mapping and compatibility**

Driver Name	Action	Settings	Se
Microsoft XPS Document Writer *	Do not create	Unmodified	
Send to Microsoft OneNote *	Do not create	Unmodified	
FX FPS Color Class Driver	Replace with	/u	

**Edit driver mapping** [X]

Driver Name:

Allow  
 Do not create  
 Create with universal driver only  
 Replace with

Use default v

▼ Applies to the  
 Virtual Deliv  
 Server OS, 7.  
 Server OS, 7.  
 Server OS, 7.  
 7.15 Server C  
 OS, 7.18 Server OS, 7.18 Desktop OS

▼ Description  
 Lists driver substitution rules for auto-created client printers. When you define these rules, you can allow or prevent printers to be created with the specified driver. Additionally, you can allow created printers to use only universal printer drivers.  
 Driver substitution overrides (or maps) printer driver names the client provides, substituting an

**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. Toutes les imprimantes clientes peuvent être mappées à une session VDA. Les noms d'imprimante doivent être différents pour les bureaux et les applications.

- Pour les bureaux publiés :  
`<client printer name>:$CLIENT_NAME:dsk$SESSION_ID`
- Pour les applications publiées :  
`<client printer name>:$CLIENT_NAME:app$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.

## Dépannage

### 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
```

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 :

```
1 systemctl status ctxcups
```

### 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** :

```
1 sudo systemctl stop cups
2
3 sudo vi /etc/systemd/system/printer.target.wants/cups.service
4
5 PrivateTmp=false
6
7 sudo systemctl start cups
8
9 sudo systemctl daemon-reload
```

**Remarque :**

Cette configuration sert uniquement à collecter le journal d'impression complet lorsqu'un prob-

lème 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 `~/.CtulpProfile$CLIENT_NAME` :

```
1 [DEFAULT_PRINTER]
2
3 printername=
4
5 model=
6
7 ppdpath=
8
9 drivertype=
```

#### 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** :

```
1 lpinfo -m
2
3 ...
4
5 xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
6
7 xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
8 xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
```

Vous pouvez ensuite définir le modèle pour qu'il corresponde à l'imprimante :

```
1 model=xerox/ph3115.ppd.gz
```

- 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` :

```
1 ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
```

- 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 :

```
1 drivertype=pcl5
```

### 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 :

```
1 deletespoolfile=no
```

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 spool 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 :

```
1 localhost:631
```

- c) Choisissez l'**imprimante mappée** `CitrixUniversalPrinter:$ClientName:app/dsk$SESSION_ID` et **modifiez l'imprimante**. Cette opération requiert des privilèges d'administrateur.
- d) Conservez la connexion **cups-ctx**, puis cliquez sur **Continuer** 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 `.CtxlpProfile$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 :

```
1 <Policy default>
2
3     # Job/subscription privacy...
4
5     JobPrivateAccess default
6
7     JobPrivateValues default
8
9     SubscriptionPrivateAccess default
10
11    SubscriptionPrivateValues default
12
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>
```

## Impression PDF

August 20, 2024

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, définissez les stratégies suivantes dans Citrix Studio :

- Définissez **Redirection d'imprimante cliente** sur **Autorisé** (**Autorisé** par défaut)
- Définissez **Créer automatiquement l'imprimante universelle PDF** sur **Activé** (**Désactivé** par défaut)
- Définissez **Créer automatiquement les imprimantes clientes** sur **Créer automatiquement toutes les imprimantes clientes**.

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

August 20, 2024

### 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

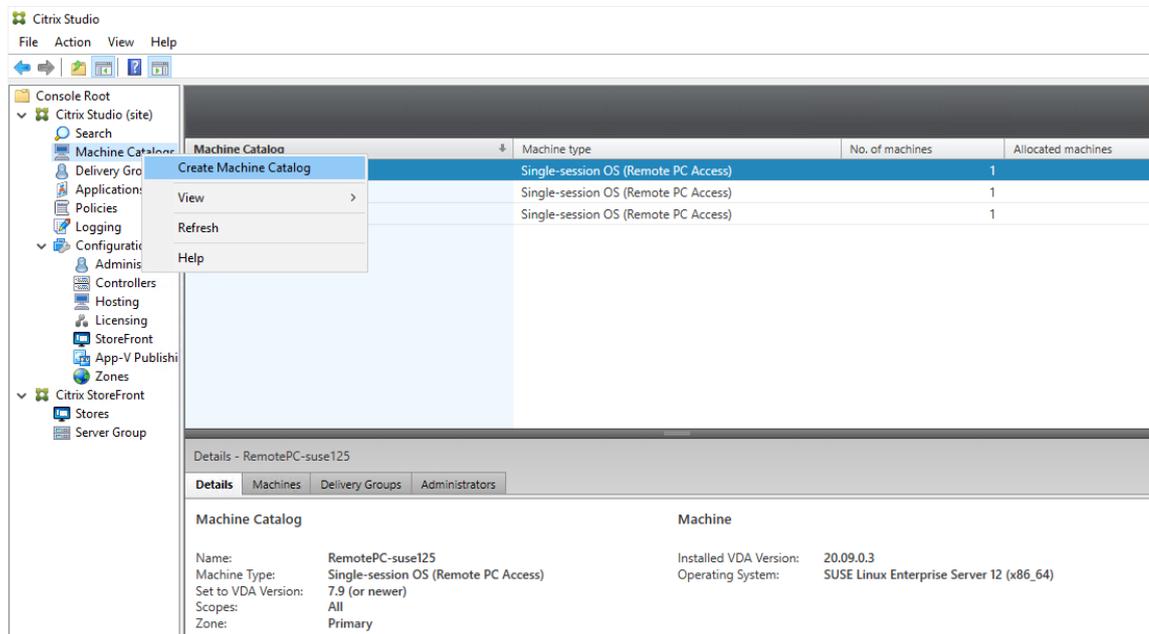
Pour fournir des sessions PC Linux, installez le Linux VDA sur les PC cibles, créez un catalogue de machines du type **Remote PC Access** et créez un groupe de mise à disposition pour rendre les PC du catalogue de machines disponibles pour les utilisateurs qui en demandent l'accès. La section suivante 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`.

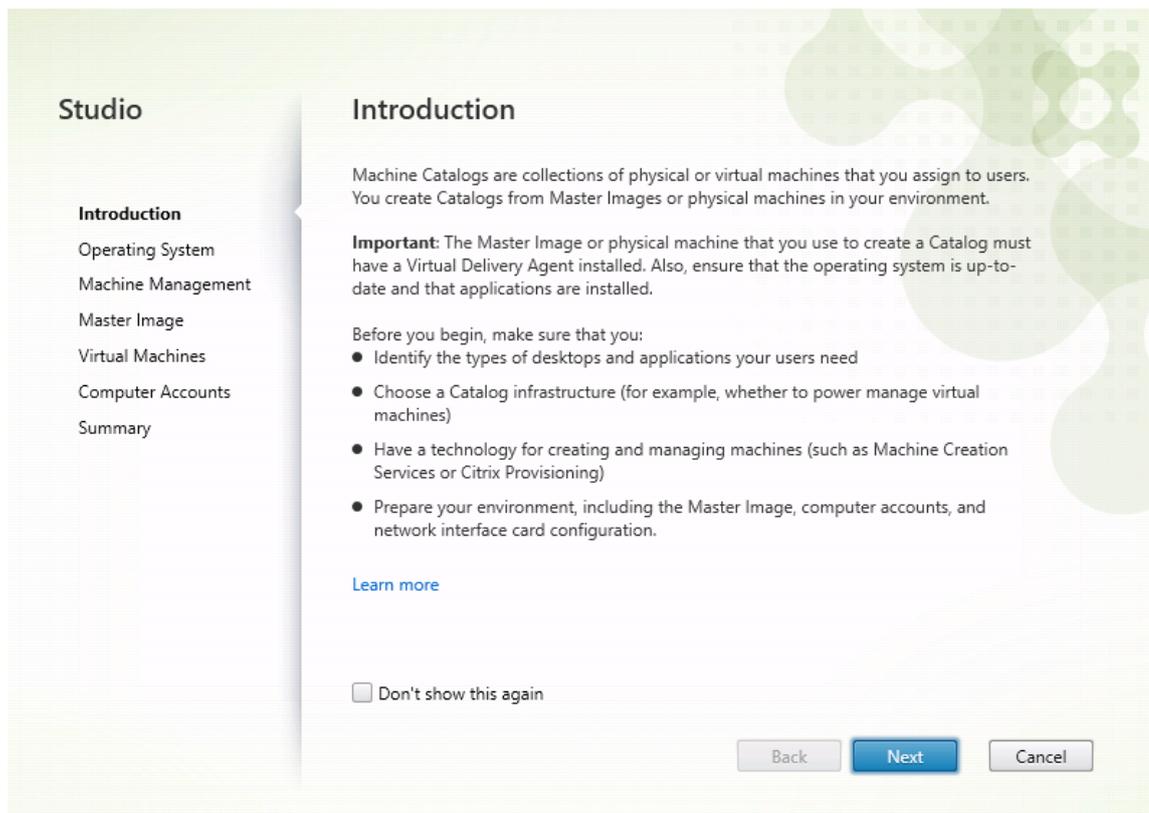
## Étape 2 : créer un catalogue de machines du type Remote PC Access

1. Dans Citrix Studio, cliquez avec le bouton droit sur **Catalogues de machines** et sélectionnez **Créer un catalogue de machines** dans le menu contextuel.

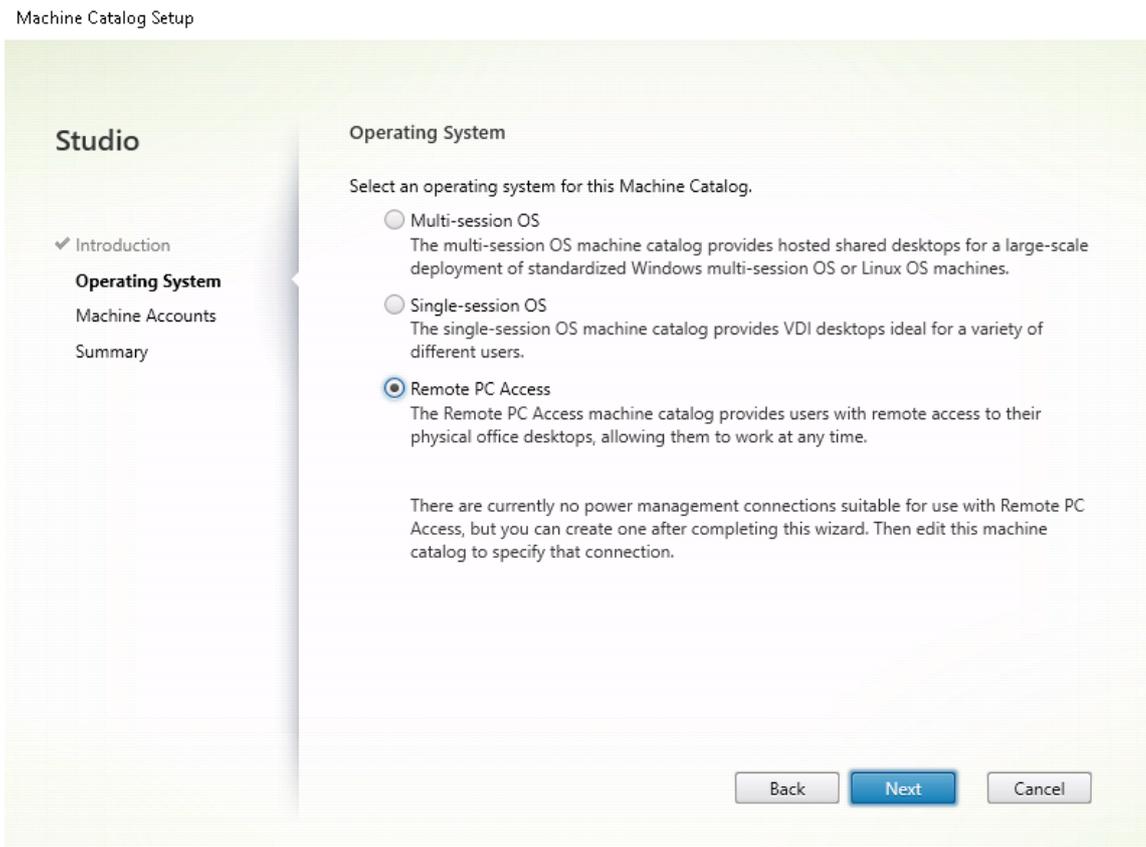


2. Cliquez sur **Suivant** sur la page **Introduction**.

Machine Catalog Setup

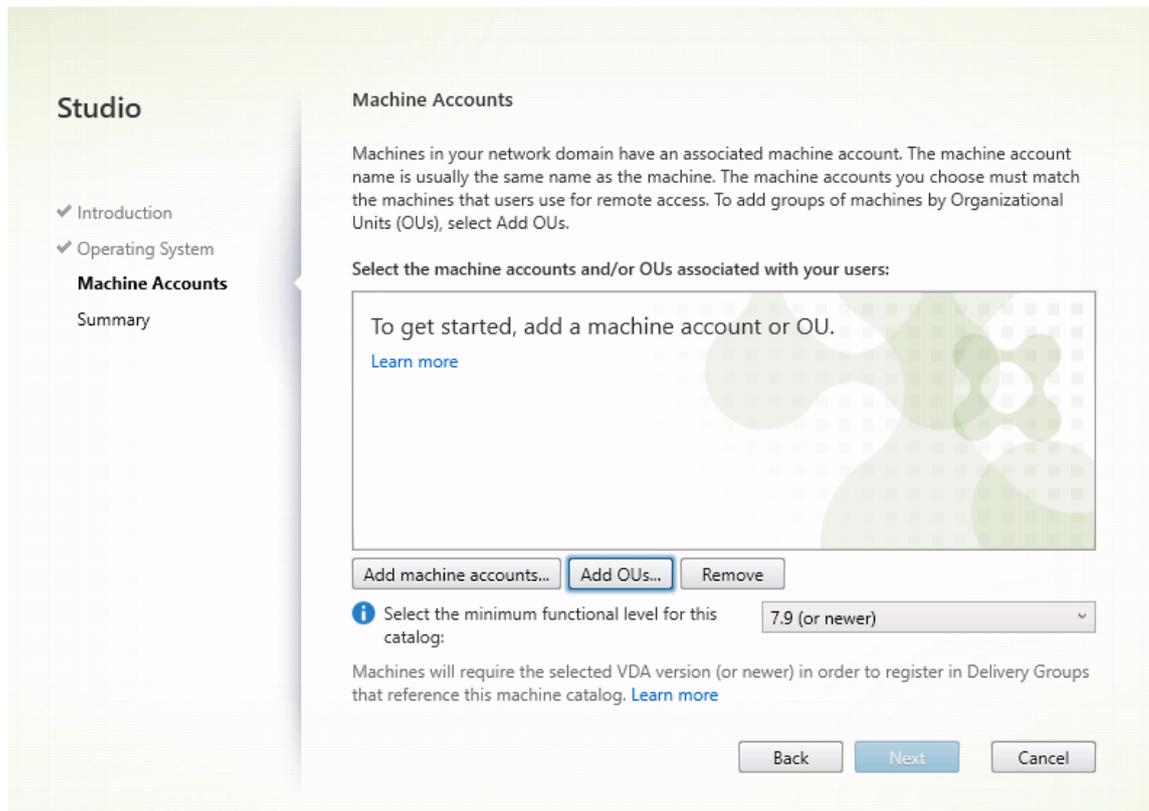


3. Sélectionnez **Remote PC Access** sur la page **Système d'exploitation**.



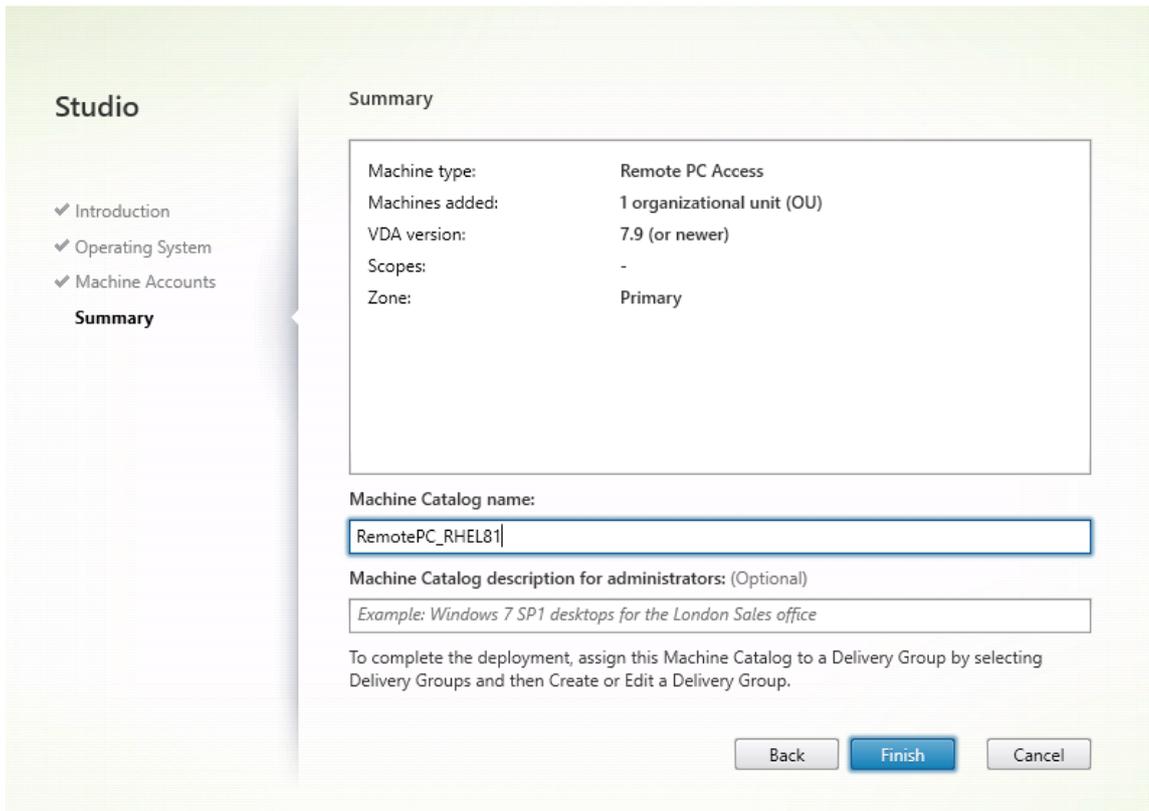
4. Cliquez sur **Ajouter des unités d'organisation** pour sélectionner des unités d'organisation contenant les ordinateurs cibles, ou cliquez sur **Ajouter des comptes de machines** pour ajouter des machines individuelles au catalogue de machines.

Machine Catalog Setup

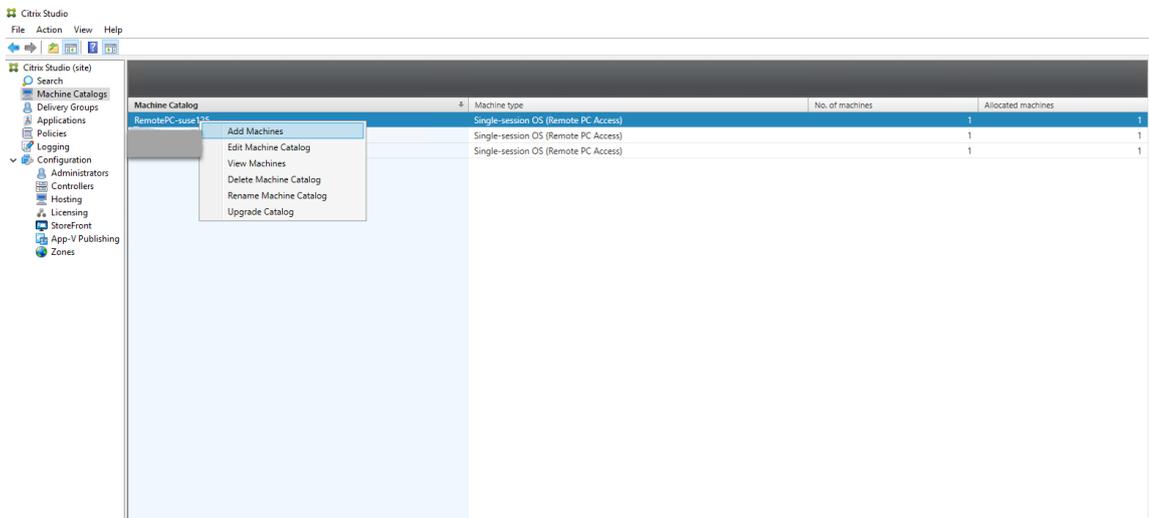


5. Nommez le catalogue de machines.

Machine Catalog Setup

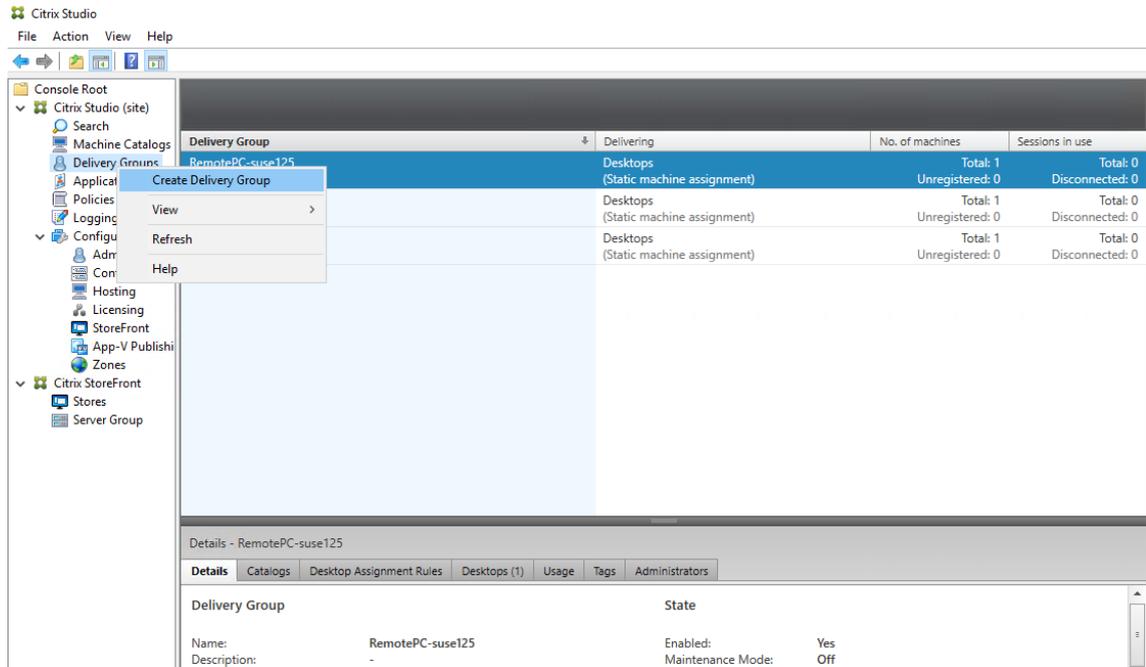


6. (Facultatif) Cliquez avec le bouton droit sur le catalogue de machines pour effectuer des opérations pertinentes.

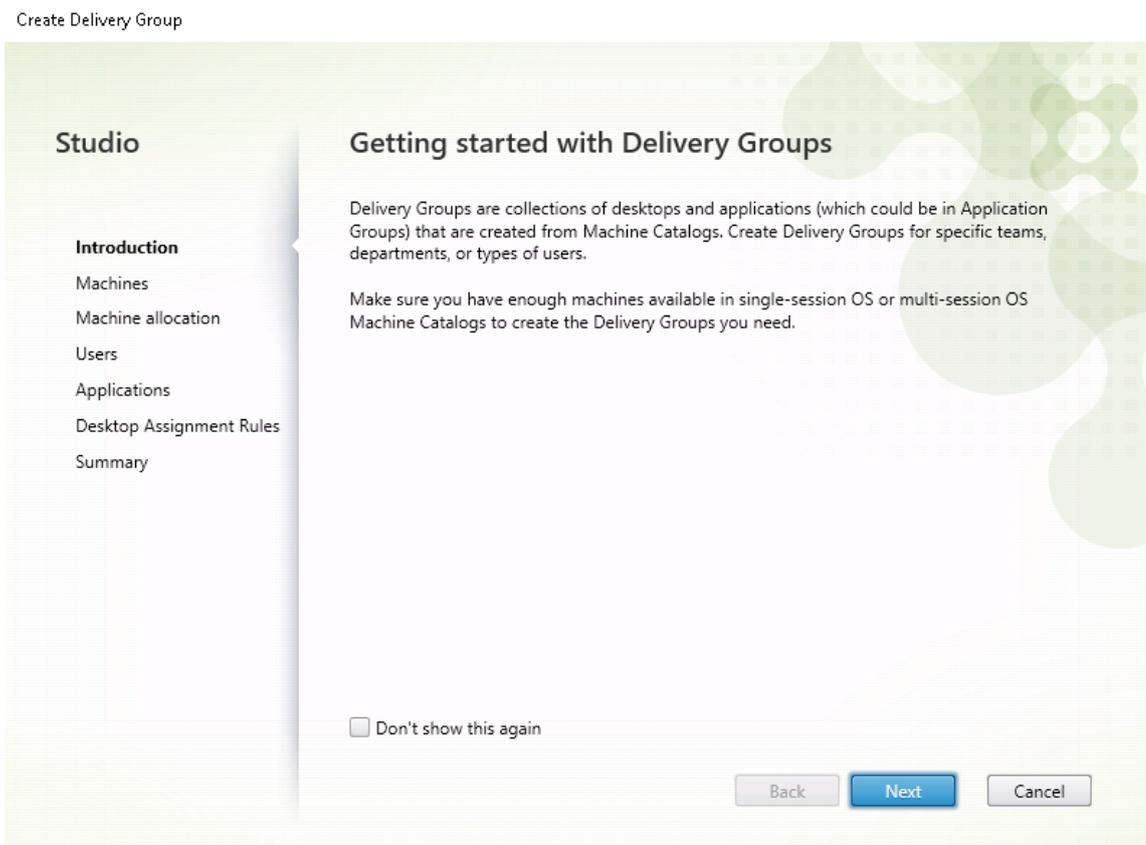


### Étape 3 : créer un groupe de mise à disposition pour rendre les PC du catalogue de machines disponibles auprès des utilisateurs qui demandent l'accès

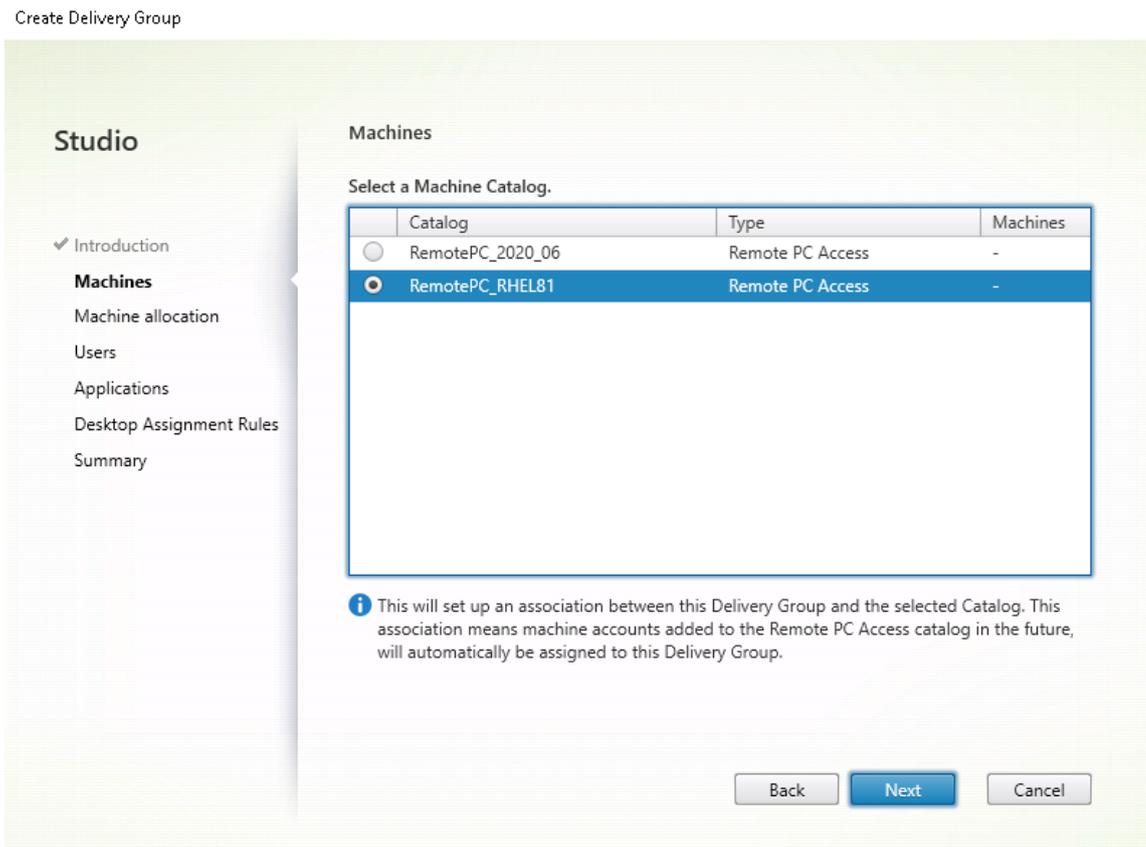
1. Dans Citrix Studio, cliquez avec le bouton droit sur **Groupe de mise à disposition** et sélectionnez **Créer un groupe de mise à disposition** dans le menu contextuel.



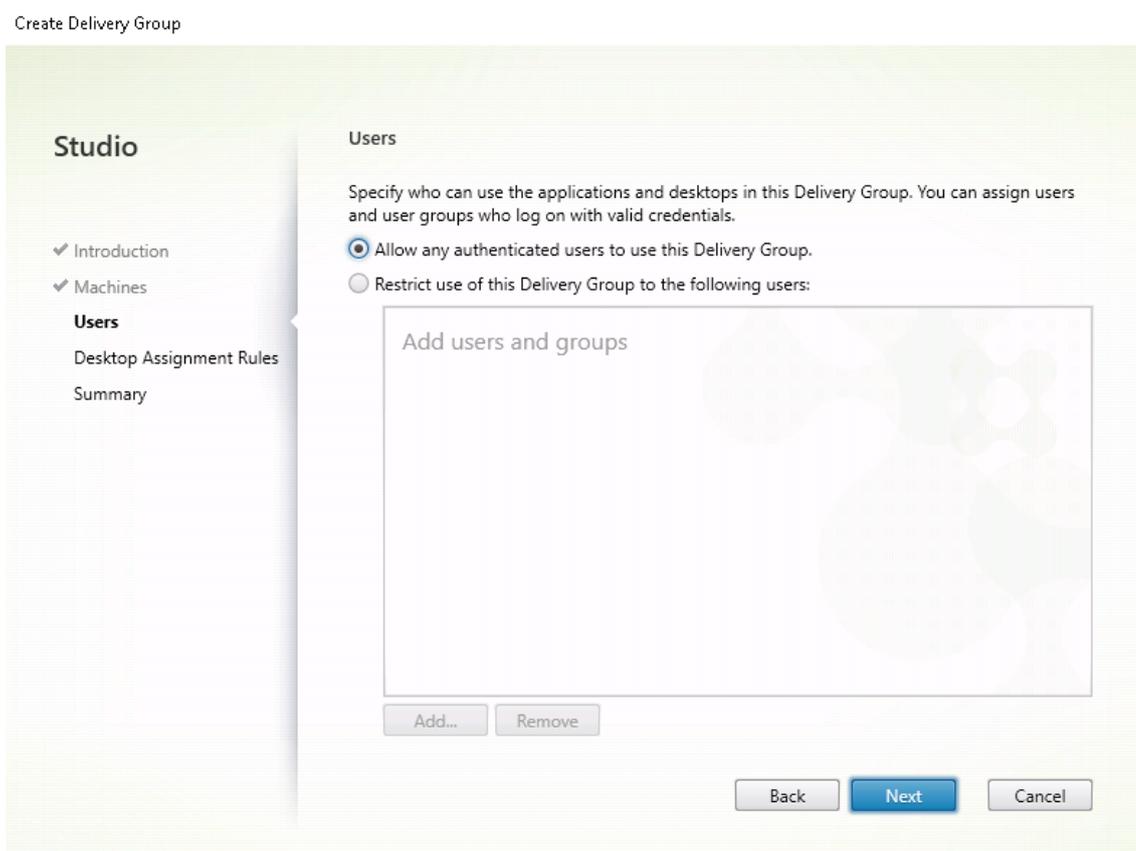
2. Cliquez sur **Suivant** sur la page **Présentation des groupes de mise à disposition**.



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 :

```
1 # Load Citrix SnapIns
2 Add-PSSnapIn -Name "*citrix*"
3
4 # Provide the name of the Wake on LAN host connection
5 [string]$connectionName = "Remote PC Access Wake on LAN"
6
7 # Create the hypervisor connection
8 $hypHc = New-Item -Path xdhyp:\Connections `
9             -Name $connectionName `
10            -HypervisorAddress "N/A" `
11            -UserName "woluser" `
12            -Password "wolpwd" `
13            -ConnectionType Custom `
```

```

14         -PluginId VdaWOLMachineManagerFactory `
15         -CustomProperties "<CustomProperties></
           CustomProperties>" `
16         -Persist
17
18 $bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
           $hypHc.HypervisorConnectionUid
19
20 # Wait for the connection to be ready before trying to use it
21 while (-not $bhc.IsReady)
22 {
23
24     Start-Sleep -s 5
25     $bhc = Get-BrokerHypervisorConnection -
           HypHypervisorConnectionUid $hypHc.HypervisorConnectionUid
26 }

```

Lorsque la connexion hôte est prête, exécutez les commandes suivantes pour récupérer l'identifiant unique de la connexion hôte :

```

1 $bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
2 $hypUid = $bhc.Uid

```

Après avoir récupéré l'identifiant unique de la connexion, exécutez les commandes suivantes pour associer la connexion au catalogue de machines Remote PC Access :

```

1 Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
   RemotePCHypervisorConnectionUid $hypUid

```

5. Activez la veille sur le réseau local, Wake on LAN, dans le BIOS et sur la carte d'interface réseau de 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 :

```
1 # ifupdown has been replaced by netplan(5) on this system.
   See
2 # /etc/netplan for current configuration.
3 # To re-enable ifupdown on this system, you can run:
4 # sudo apt install ifupdown
5 auto eth0
6 iface eth0 inet static
7     address 10.0.0.1
8     netmask 255.255.240.0
9     gateway 10.0.0.1
10    up ethtool -s eth0 wol g
```

**RHEL/SUSE :**

Ajoutez le paramètre suivant `ETHTOOL_OPTS` au fichier de configuration de l'interface `/etc/sysconfig/network-scripts/ifcfg-<NIC>` :

```
1 ETHTOOL_OPTS="-s ${
2   DEVICE }
3   wol g"
```

## 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](#).

## Session

August 20, 2024

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

August 20, 2024

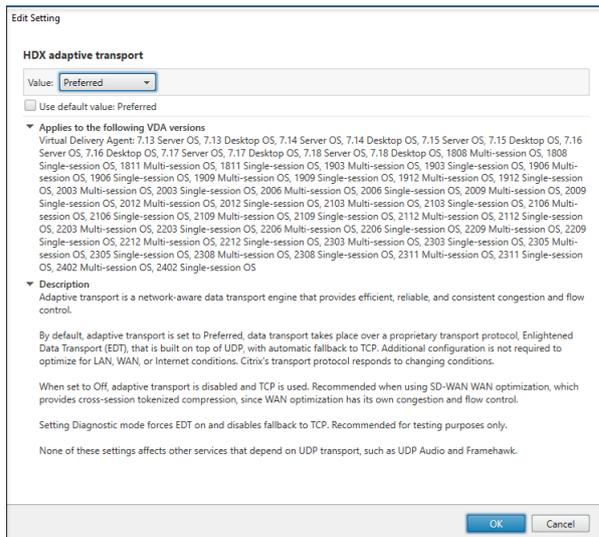
Le transport adaptatif est un mécanisme de Citrix Virtual Apps and Desktops qui permet d'utiliser Enlightened Data Transport (EDT) comme protocole de transport pour les connexions ICA. Le transport adaptatif bascule vers TCP lorsque EDT n'est pas disponible.

EDT est un protocole de transport propriétaire de Citrix basé sur le protocole UDP (User Datagram Protocol). Il offre une expérience utilisateur supérieure sur les connexions longue distance difficiles tout en maintenant la capacité à monter en charge du serveur. EDT améliore le débit de données de tous les canaux virtuels ICA sur des réseaux peu fiables, offrant ainsi une expérience utilisateur plus performante et plus cohérente.

Pour de plus amples informations, consultez la section [Transport adaptatif](#) dans la documentation Citrix Virtual Apps and Desktops.

### Activer ou désactiver le transport adaptatif

Le transport adaptatif est activé par défaut. Vous pouvez configurer les options suivantes à l'aide du paramètre de stratégie **Transport adaptatif HDX** :



- **Préfééré** : le transport adaptatif est activé, et il utilise EDT (Enlightened Data Transport) comme protocole de transport préféré, avec basculement vers TCP.
- **Mode de diagnostic** : le transport adaptatif est activé et il force l'utilisation d'EDT. Le basculement vers TCP est désactivé. Ce paramètre est recommandé uniquement pour les tests et le dépannage.
- **Désactivé**. Le transport adaptatif est désactivé et seul TCP est utilisé pour le transport.

## Vérifier si le transport adaptatif est activé

Pour vérifier si EDT est utilisé comme protocole de transport pour la session en cours, exécutez la commande suivante.

```
1 /opt/Citrix/VDA/bin/ctxquery -f iP
```

Si EDT est utilisé, les protocoles de transport affichés incluent le protocole UDP, par exemple :

```
root@j1-u20:~/Desktop$ ctxquery -f iP
SESSION:ID      TRANSPORT PROTOCOLS  RENDEZVOUS
j1-u20:0        -                    -
j1-u20:1        -                    -
j1-u20:2        -                    -
j1-u20:12      UDP-CGP-ICA         NONE
root@j1-u20:~/Desktop$
```

## Découverte MTU EDT

La découverte MTU permet à EDT de déterminer automatiquement l'unité de transmission maximale (MTU) lors de l'établissement d'une session. Cela empêche la fragmentation des paquets EDT, qui

pourrait entraîner une dégradation des performances ou l'échec de l'établissement d'une session.

Configuration système requise :

- Linux VDA version minimale 2012
- Application Citrix Workspace :
  - Windows : 1911 ou version ultérieure
- Citrix ADC :
  - 13.0.52.24 ou version ultérieure
  - 12.1.56.22 ou version ultérieure
- 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, reportez-vous à la section [CTX231821](#) pour plus d'informations sur la configuration de MTU EDT personnalisée adaptée à votre environnement.

### Contrôler la découverte MTU EDT sur le VDA

La découverte MTU EDT est activée sur le VDA par défaut. Vous pouvez l'activer ou la désactiver en définissant la clé de registre `MtuDiscovery` comme suit :

- 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 :

```
1 /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`.

#### **Avertissement :**

Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de **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.

### 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.

## Contrôle amélioré de la congestion EDT

Nous avons ajouté un algorithme de contrôle de la congestion pour optimiser le protocole EDT. Cette implémentation permet à EDT d'atteindre un débit plus élevé et de réduire la latence pour une expérience utilisateur améliorée.

Cette fonctionnalité est activée par défaut. Pour le désactiver et le réactiver, exécutez les commandes suivantes, respectivement, puis redémarrez le service `ctxhdx` :

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\icawd\Tds\udp\UDPStackParameters" -t "REG_DWORD" -v "edtBBR" -d "0x00000000" --force
```

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\icawd\Tds\udp\UDPStackParameters" -t "REG_DWORD" -v "edtBBR" -d "0x00000001" --force
```

## Débit adaptatif HDX

August 20, 2024

Le débit adaptatif HDX affine intelligemment le débit maximal de la session ICA en ajustant les tampons de sortie. Le nombre de tampons de sortie est initialement défini sur une valeur élevée. Cette valeur élevée permet de transmettre les données au client plus rapidement et efficacement, en particulier dans les réseaux à latence élevée. Cette fonctionnalité améliore l'expérience utilisateur. Elle offre une meilleure interactivité, des transferts de fichiers plus rapides, une lecture vidéo plus fluide, ainsi qu'une fréquence d'images et une résolution plus élevées. L'interactivité des sessions est constamment mesurée pour déterminer si des flux de données au sein de la session ICA nuisent à l'interactivité. Si c'est le cas, le débit diminue pour réduire l'impact du flux de données volumineux sur la session et permettre la récupération de l'interactivité.

**Important :**

Le débit adaptatif HDX modifie les tampons de sortie en déplaçant ce mécanisme du client vers

le VDA. Aucune configuration manuelle n'est nécessaire.

La fonctionnalité nécessite la version minimale 2311 du VDA. Elle est désactivée par défaut. Pour l'activer, exécutez la commande suivante sur le VDA :

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\icawd" -t "REG_DWORD" -v "AdaptiveScalingEnabled" -d "0x00000001" --force
```

La fonctionnalité ne s'applique qu'aux sessions lancées après son activation.

## Arrière-plans et messages de bannière personnalisés sur les écrans d'ouverture de session

August 20, 2024

### Ajouter un arrière-plan ou un message de bannière personnalisé aux écrans d'ouverture de session

#### Conseil :

Pour utiliser la fonctionnalité sur SUSE 15.5, installez `imlib2` à partir de <http://download.opensuse.org/distribution/leap/15.3/repo/oss/>.

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. Lorsque vous ouvrez une session, la page du message de bannière s'affiche en premier, puis la boîte de dialogue d'authentification apparaît.

Pour définir le titre d'un message de bannière personnalisé, exécutez :

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v "LogonDisplayStringTitle" -d "<Banner message title>" --force
```

#### La longueur maximale du titre d'un message de bannière est de 64 octets.

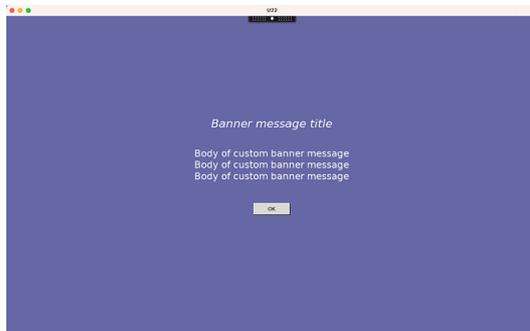
Pour définir le corps du texte d'un message de bannière personnalisé, exécutez :

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v "LogonDisplayString" -d "Body of custom banner message\nBody of custom banner message\n" --force
```

**La longueur maximale du corps d'un message de bannière est de 1 024 octets.**

**Conseil :**

L'élément \n crée un saut de ligne. Dans cet exemple, l'écran du message de bannière ressemble à ce qui suit :



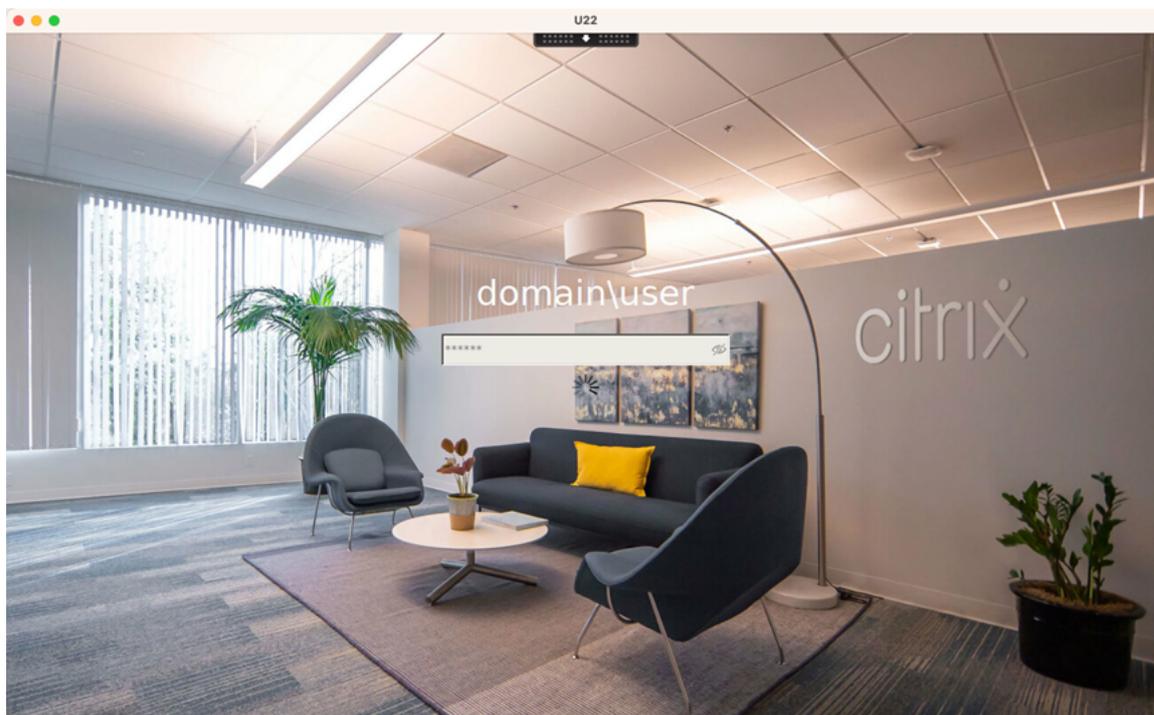
Pour vous assurer que votre message de bannière personnalisé s'affiche comme prévu, vous devrez peut-être utiliser des espaces. Par exemple, utilisez & pour représenter & en HTML et placez une barre oblique inversée (\*\*\\*\*) avant le caractère ! pour l'échapper dans les commandes Bash.

Pour ajouter un arrière-plan personnalisé aux écrans d'**ouverture de session**, exécutez :

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v "BackgroundImagePath" -d "<path to the background image>" --force
```

**Pour voir l'arrière-plan personnalisé, les utilisateurs de la session doivent avoir accès au chemin de l'image d'arrière-plan.**

Par exemple :



## Exemples d'écrans d'ouverture de session

Voici des exemples d'écrans d'ouverture de session dans différents scénarios :

- **Ouverture de session** dans des scénarios avec authentification unique (SSO) :



Le processus d'**ouverture de session** s'affiche.

- **Ouverture de session** dans des scénarios classiques sans authentification unique :

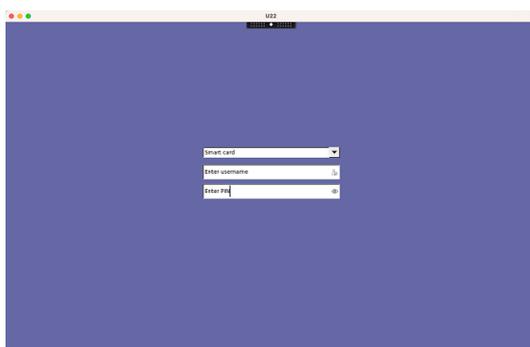


- Un mot de passe ou un code PIN est requis dans les scénarios sans authentification unique.
  - Les utilisateurs peuvent activer ou désactiver la visibilité des mots de passe et des codes PIN, ce qui leur permet de détecter facilement les saisies incorrectes.
- Ouverture de session dans des scénarios sans authentification unique lorsque les utilisateurs se connectent à des sessions VDA avec des informations d'identification différentes de celles utilisées pour se connecter à l'application Citrix Workspace :

Nom d'utilisateur et mot de passe utilisés pour la connexion à la session :



Carte à puce utilisée pour l'ouverture de session :



Pour les combinaisons de méthodes d'authentification utilisateur prises en charge dans les scénarios sans authentification unique, consultez la section [Pas d'authentification unique](#).

## Environnements de bureau personnalisés par utilisateurs de session

August 20, 2024

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 que les utilisateurs de session puissent utiliser 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
Debian 11.7/11.3	MATE, GNOME, GNOME-Classic, KDE
RHEL 8.8/8.6	MATE, GNOME, GNOME-Classic
RHEL 7.9	MATE, GNOME, GNOME-Classic, KDE
Rocky Linux 8.8/8.6	MATE, GNOME, GNOME-Classic, KDE
SUSE 15.5	MATE, GNOME, GNOME-Classic
Ubuntu 22.04/20.04	MATE, GNOME, GNOME-Classic, KDE

### Commandes de commutation de bureau

#### Remarque :

Vous pouvez passer d'un environnement de bureau à l'autre à partir du terminal et de la [barre d'état système](#).

Pour passer à un environnement de bureau cible à partir du terminal, exécutez la commande correspondante dans la session :

Si l'environnement de bureau cible est	Exécutez la commande
GNOME	<code>/opt/Citrix/VDA/bin/ctxdesktopswitch.sh GNOME</code>
GNOME Classic	<code>/opt/Citrix/VDA/bin/ctxdesktopswitch.sh GNOME-CLASSIC</code>

Si l'environnement de bureau cible est	Exécutez la commande
MATE	<code>/opt/Citrix/VDA/bin/ ctxdesktopswitch.sh MATE</code>
KDE	<code>/opt/Citrix/VDA/bin/ ctxdesktopswitch.sh KDE</code>

---

### 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 :

```
1 qt.qpa.xcb.xcberror.error=false
2 qt.qpa.xcb.warning=false
3 qt.qpa.xcb.error=false
```

- 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

August 20, 2024

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.	<pre>create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD"-v "LogNoHome"-d "0x00000001"--force</pre>
HomeMountPoint	Définit un point de montage local sur le Linux VDA. Par exemple, si <code>/mnt/home</code> est le point de montage, le répertoire de base d'un utilisateur est <code>/mnt/home/domain/&lt;user_name&gt;</code> . Assurez-vous que le point de montage est le même que le répertoire de base de l'utilisateur dans votre environnement. Ce paramètre prend effet uniquement lorsque <code>CheckUserHomeMountPoint</code> est défini sur 0.	<pre>create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_SZ"-v "HomeMountPoint"-d "&lt;A directory where the NFS share is to be mounted&gt;"--force</pre>
CheckUserHomeMountPoint	Détermine si des répertoires de base spécifiques à l'utilisateur doivent être définis comme point de montage sur le Linux VDA. Si vous souhaitez définir des répertoires de base spécifiques à l'utilisateur comme point de montage, définissez la valeur sur <b>1</b> . La valeur par défaut est <b>0</b> .	<pre>ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD"-v "CheckUserHomeMountPoint"-d "0x00000001"--force</pre>

Clé de registre	Description	Commande
<code>TempHomeDirectoryPath</code>	Définit un répertoire de base temporaire sur le Linux VDA en cas d'échec du point de montage. La valeur par défaut est <code>/tmp</code> . Le paramètre du répertoire de base temporaire ne prend effet que lorsque le point de montage déterminé par <code>HomeMountPoint</code> et <code>CheckUserHomeMountPoint</code> n'est pas disponible. Un répertoire de base temporaire pour un utilisateur est <code>/tmp/CTXSmf_user_id</code> .	<pre>create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_SZ"-v "TempHomeDirectoryPath"-d "&lt;/tmp by default &gt;"--force</pre>
<code>CheckMountPointRetryTime</code>	Définit le nombre de vérifications, à une fréquence d'une fois par seconde, pour vérifier si le montage est réussi. La valeur par défaut est 5.	<pre>ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD"-v "CheckMountPointRetryTime"-d "0x000000010"--force</pre>
<code>RemoveHomeOnLogoff</code>	Contrôle si les répertoires de base temporaires doivent être supprimés lors de la fermeture de session des utilisateurs. 1 signifie « activé », 0 « désactivé ».	<pre>create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD"-v "RemoveHomeOnLogoff"-d "0x00000000"--force</pre>

## Publier des applications

August 20, 2024

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**.
- Nous vous recommandons de créer des VDA et 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>.
- Les applications Linux disposent souvent d'une fenêtre À propos contenant des informations sur l'application utilisée, et des liens Web pour plus d'informations se trouvent généralement dans ces fenêtres. Cliquez sur les liens Web dans la fenêtre À propos pour lancer un navigateur Web à partir d'applications publiées telles que **calc**, **gedit**, **calendar** et **LibreOffice Suite**. Le lancement involontaire d'un navigateur Web contourne l'isolation des applications et peut compromettre la sécurité. Pour résoudre le problème, modifiez le navigateur Web par défaut en procédant comme suit :

1. Créez un fichier none.sh dans un emplacement personnalisé, par exemple :

```
1 sudo mkdir /home/none
2
3 sudo touch /home/none/none.sh
4
5 sudo chmod +x /home/none/none.sh
```

2. Ajoutez les lignes suivantes au fichier none.sh :

```
1 #!/bin/bash
2
3 echo "NONE"
```

3. Créez le fichier /etc/xdg/mimeapps.list avec sudo, puis ajoutez les lignes suivantes au fichier mimeapps.list :

```
1 [Default Applications]
2
3 text/html=none.desktop
4
5 x-scheme-handler/http=none.desktop
6
7 x-scheme-handler/https=none.desktop
8
9 x-scheme-handler/about=none.desktop
10
11 x-scheme-handler/unknown=none.desktop
```

4. Créez le fichier /usr/share/applications/none.desktop avec sudo, puis ajoutez les lignes suivantes au fichier none.desktop :

```
1 [Desktop Entry]
2
3 Encoding=UTF-8
```

```
4
5  Version=1.0
6
7  Type=Application
8
9  Terminal=false
10
11 Exec=/home/none/none.sh
12
13 Name=None
14
15 Icon=/home/none/none.sh
```

Comme vous pouvez placer le fichier none.sh dans un emplacement personnalisé, assurez-vous qu'aucun fichier .desktop ne peut référencer correctement le fichier none.sh.

## Rendezvous V1

August 20, 2024

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 Gateway et Citrix Workspace.
- 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](https://*.nssvc.net), y compris tous les sous-domaines. Si vous ne pouvez pas ajouter tous les sous-domaines à la liste d'autorisation de cette manière, utilisez [https://\\*.c.nssvc.net](https://*.c.nssvc.net) et [https://\\*.g.nssvc.net](https://*.g.nssvc.net) à la place. Pour plus d'informations, reportez-vous à la section [Exigences en termes de connexion Internet](#) de la documentation Citrix Cloud (sous 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. Ceci peut être fait de l'une de ces deux façons :
  - **Activez la résolution DNS pour le site.** Accédez à **Configuration complète > Paramètres** et activez le paramètre **Activer la résolution DNS**. Vous pouvez aussi utiliser le SDK Remote PowerShell Citrix Virtual Apps and Desktops et exécuter la commande `Set-BrokerSite -DnsResolutionEnabled $true`. Pour plus d'informations sur le SDK Remote PowerShell Citrix Virtual Apps and Desktops, consultez [SDK et API](#).
  - **Zone de recherche inversée DNS avec enregistrements PTR pour les VDA.** Si vous choisissez cette option, nous vous recommandons de configurer les VDA pour toujours tenter d'inscrire les enregistrements PTR. Pour ce faire, utilisez l'Éditeur de stratégie de groupe ou l'Objet de stratégie de groupe, accédez à **Configuration ordinateur > Modèles d'administration > Réseau > Client DNS**, puis définissez **Inscrire les enregistrements PTR** sur **Activé et Inscrire**. Si le suffixe DNS de la connexion ne correspond pas au suffixe DNS du domaine, vous devez également configurer le paramètre du **suffixe DNS spécifique à la connexion** afin que les machines puissent inscrire les enregistrements PTR correctement.

**Remarque :**

Si vous utilisez l'option de résolution DNS, les Cloud Connector doivent être en mesure de résoudre les noms de domaine complets (FQDN) des machines VDA. Dans le cas où les utilisateurs internes se connectent directement aux machines VDA, les machines clientes doivent également être en mesure de résoudre les noms de domaine des machines VDA.

Si vous utilisez une zone de recherche inversée DNS, les FQDN des enregistrements PTR doivent correspondre aux noms de domaine FQDN des machines VDA. Si l'enregistrement PTR contient un FQDN différent, la connexion Rendezvous échoue. Par exemple, si le FQDN de la machine est `vda01.domain.net`, l'enregistrement PTR doit contenir `vda01.domain.net`. Un FQDN différent tel que `vda01.sub.domain.net` ne fonctionne pas.

## Configuration du proxy

Le VDA prend en charge les connexions Rendezvous via 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 déchiffrement 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, déchiffré ou inspecté. Sinon, la connexion est interrompue.
- Les proxys 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 par négociation** 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 proxys 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 :

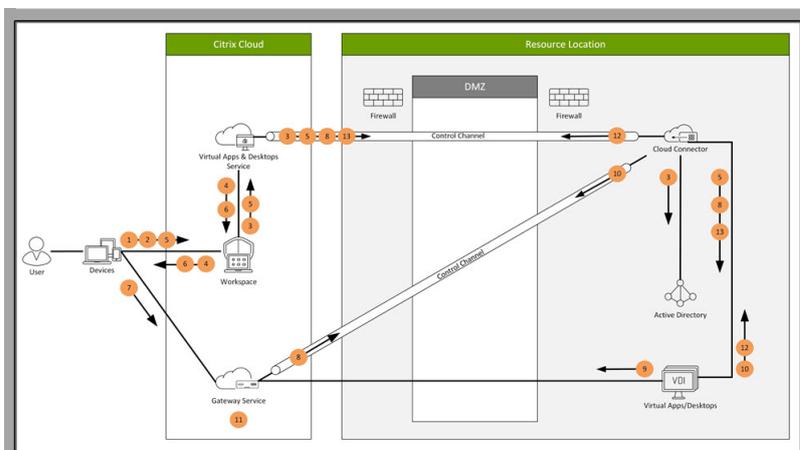
1. Lancez un terminal sur le VDA.
2. Exécutez `/opt/Citrix/VDA/bin/ctxquery -f iP`.
3. Les protocoles de transport utilisés indiqueront le type de connexion :
  - TCP Rendezvous : TCP - TLS - CGP - ICA
  - EDT Rendezvous : UDP - DTLS - CGP - ICA
  - Proxy via Cloud Connector : TCP - PROXY - SSL - CGP - 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

August 20, 2024

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://\\*.xendesktop.net](https://*.xendesktop.net) sur TCP 443. Si vous ne pouvez pas autoriser tous les sous-domaines de cette manière, vous pouvez utiliser [https://<customer\\_ID>.xendesktop.net](https://<customer_ID>.xendesktop.net), où <customer\_ID> est votre identifiant client Citrix Cloud, affiché sur le portail de l'administrateur Citrix Cloud.
  - [https://\\*.nssvc.net](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](https://*.c.nssvc.net) et [https://\\*.g.nssvc.net](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
```

### 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 proxys 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 de négociation d'authentification** 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 proxys 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 "0x00000001" --force
```

3. Redémarrez la machine VDA.
4. Créez une stratégie Citrix ou modifiez une stratégie existante :
  - Définissez le paramètre « Protocole Rendezvous » sur **Autorisé**. Le protocole Rendezvous est désactivé par défaut. Lorsque le protocole Rendezvous est activé (**Autorisé**), Rendezvous V2 est appliqué à la place de V1.
  - 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

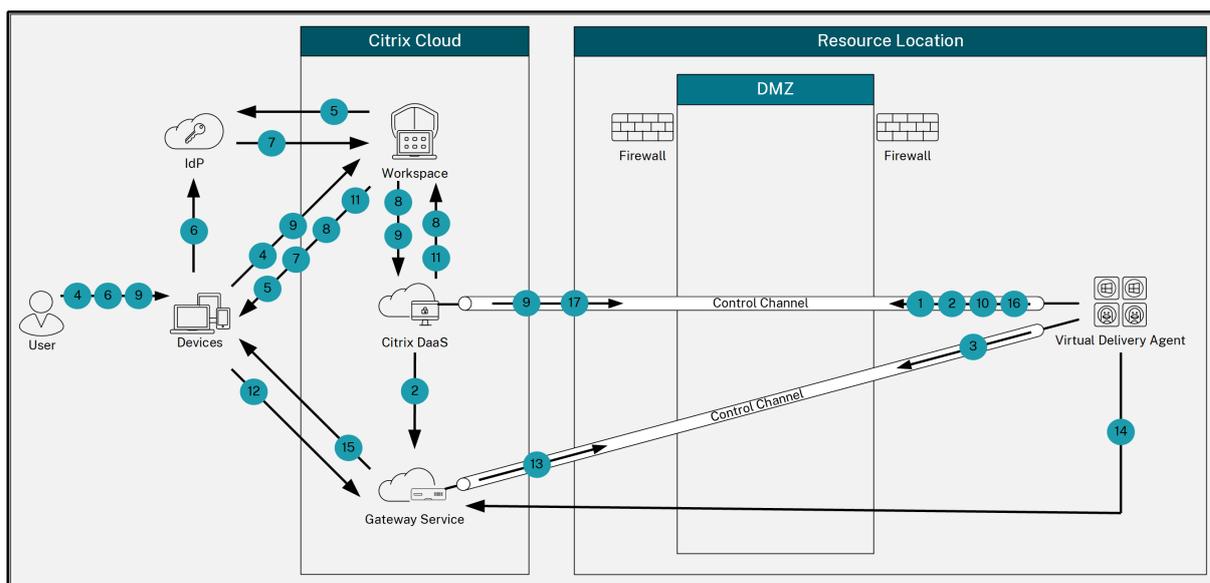
Si Rendezvous V2 est utilisé, la version du protocole affiche 2.0.

### 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.

## Flux de trafic Rendez-vous

Le schéma suivant illustre la séquence des étapes relatives au flux de trafic Rendezvous.



1. Le VDA établit une connexion WebSocket avec Citrix Cloud et s'enregistre.
2. Le VDA s'enregistre auprès de Citrix Gateway Service et obtient un jeton dédié.
3. Le VDA établit une connexion de contrôle permanente avec Gateway Service.
4. L'utilisateur accède à Citrix Workspace.
5. Workspace évalue la configuration de l'authentification et redirige les utilisateurs vers le fournisseur d'identité approprié pour l'authentification.
6. L'utilisateur saisit ses informations d'identification.
7. Une fois les informations d'identification de l'utilisateur validées, l'utilisateur est redirigé vers Workspace.
8. Workspace compte les ressources liées à l'utilisateur et les affiche.
9. L'utilisateur sélectionne un bureau ou une application dans Workspace. Workspace envoie la demande à Citrix DaaS qui négocie la connexion et demande au VDA de préparer la session.
10. Le VDA répond à l'aide de la fonctionnalité Rendezvous et de son identité.
11. Citrix DaaS génère un ticket de lancement et l'envoie à la machine utilisateur via Workspace.
12. Le point de terminaison de l'utilisateur se connecte à Gateway Service et fournit le ticket de lancement pour authentifier et identifier la ressource à laquelle se connecter.
13. Gateway Service envoie les informations de connexion au VDA.
14. Le VDA établit une connexion directe pour la session avec Gateway Service.
15. Gateway Service établit la connexion entre le point de terminaison et le VDA.
16. Le VDA vérifie les licences pour la session.
17. Citrix DaaS envoie les stratégies applicables au VDA.

## Secure HDX (Technical Preview)

August 20, 2024

Vous pouvez crypter les sessions ICA de bout en bout entre l'application Citrix Workspace (client) et le VDA (hôte de session).

La fonctionnalité de cryptage de bout en bout (E2EE) n'autorise aucun élément réseau intermédiaire, y compris Citrix Gateway, à déchiffrer le trafic ICA. Le cryptage de bout en bout améliore la sécurité de votre environnement et est facile à configurer et à gérer.

### Configuration système requise

- Linux VDA version minimale 2311
- Delivery Controller version minimale 2308
- StoreFront version minimale 2308
- Application Citrix Workspace pour Windows version minimale 2308

### Configuration

#### Activer le cryptage de bout en bout

La fonctionnalité de cryptage de bout en bout (E2EE) est désactivée par défaut. Pour l'activer, définissez la stratégie **Secure HDX** sur **Activé** dans Citrix Studio.

#### Programmer le renouvellement des certificats

La fonctionnalité de cryptage de bout en bout (E2EE) nécessite un certificat auto-signé et la clé privée associée gérée par le service **ctxcertmgr** sur le Linux VDA.

Un nouveau certificat auto-signé est créé au démarrage ou redémarrage du service **ctxcertmgr**. Par défaut, le service **ctxcertmgr** renouvelle le certificat (y compris sa clé privée) tous les 7 jours à 02:00 am. Vous pouvez également programmer le renouvellement des certificats avec des paramètres de registre similaires aux suivants :

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\SecureHDX" -  
   t "REG_SZ" -v "CaRotationStartDate" -d "2023-10-19" --force  
2  
3 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\SecureHDX" -  
   t "REG_SZ" -v "CaRotationTime" -d "00:45:30" --force  
4
```

```
5 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\SecureHDX" -  
t "REG_DWORD" -v "CaRotationPeriod" -d "0x00000005" --force
```

Dans l'exemple ci-dessus, l'heure de renouvellement du premier certificat est fixée à 00:45:30 le 19/10/2023. Ensuite, le service **ctxcermgr** renouvelle le certificat tous les 5 jours à 00:45:30. La date et l'heure programmées correspondent à la date et à l'heure sur le Linux VDA.

## Sécuriser les sessions utilisateur en utilisant DTLS

August 20, 2024

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 :

Linux VDA prend en charge DTLS 1.0, DTLS 1.2 et DTLS 1.3 et utilise DTLS 1.2 par défaut. Vérifiez quelle version de DTLS est utilisée sur votre application Citrix Workspace. Assurez-vous que la même version de DTLS est utilisée à la fois sur le Linux VDA et sur votre application Citrix Workspace. Si votre application Citrix Workspace prend uniquement en charge le protocole DTLS 1.0 (par exemple, Citrix Receiver pour Windows 4.11), définissez **SSLMinVersion** sur **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

August 20, 2024

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



## 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@xui804:~# /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/rootGR.cer"
Enable Linux VDA SSL using Root Certificate rootGR.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 :**

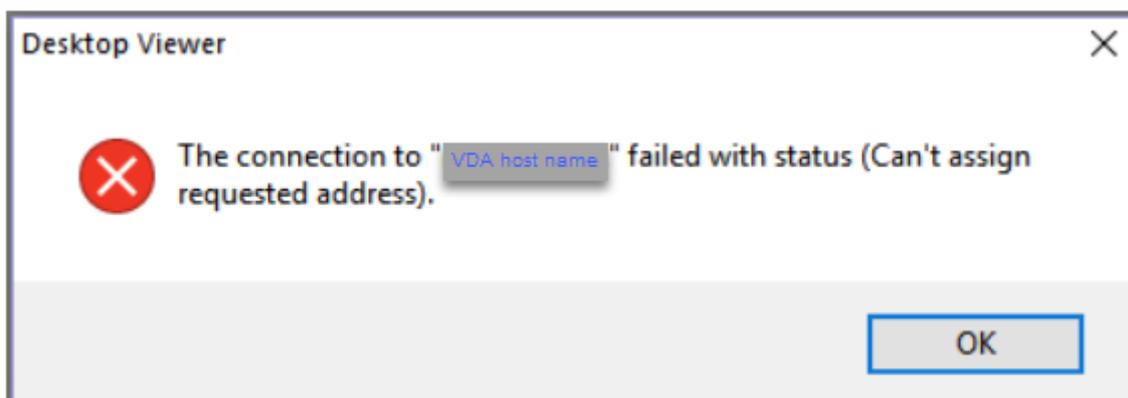
Pour vous assurer que seuls les noms de domaine complets VDA sont contenus dans un fichier de session ICA, vous pouvez également exécuter la commande `Set-BrokerSite -DnsResolutionEnabled $true`. La commande active la résolution DNS. Si vous désactivez la résolution DNS, un fichier de session ICA divulgue 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`

## Dépannage

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

August 20, 2024

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"
```

**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"
```

**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).

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\
  Citrix\XTEConfig" -t "REG_DWORD" -v "CgpClientToServerKeepAlive"
  -d "10" --force
```

## Dépannage

### 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 (utilisez le port 2598 à titre d'exemple).

```
1 netstat -an | grep 2598
```

S'il n'y a pas d'écouteur TCP sur le port de fiabilité de session, activez l'écouteur en exécutant la commande suivante.

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\WinStations\cgp" -v "fEnableWinStation" -d "0x00000001"
```

## Enregistrement de session (version Technical Preview)

August 20, 2024

Vous pouvez enregistrer et relire des sessions hébergées sur un Linux VDA.

### Remarque :

Cette fonctionnalité est disponible dans la Tech Preview. Les fonctionnalités de la version Technical Preview peuvent ne pas être entièrement localisées et sont recommandées pour une utilisation dans des environnements hors production. Les problèmes identifiés avec les fonctionnalités Technical Preview ne sont pas pris en charge par le support technique Citrix.

### Activer ou désactiver l'enregistrement de session

Pour activer ou désactiver l'enregistrement de session pour un Linux VDA, définissez **SMAudAllowed** sur **1** ou **0**, respectivement. Vous pouvez utiliser les commandes suivantes :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD" -v "SmAudAllowed" -d "0x00000001" --force
```

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
  CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD" -v "
  SmAudAllowed" -d "0x00000000" --force
```

**Remarque :**

Une fois que vous avez activé l'enregistrement de session sur un Linux VDA, les utilisateurs sont informés de l'enregistrement de leurs sessions lorsqu'ils se connectent à leurs sessions.

## Spécifier la taille du fichier pour les enregistrements

À mesure que la taille des enregistrements augmente, les fichiers d'enregistrement prennent plus longtemps à se télécharger et réagissent plus lentement lorsque vous utilisez le curseur de recherche pour naviguer pendant la lecture. Pour contrôler la taille des fichiers, spécifiez un seuil limite. Lorsque l'enregistrement atteint cette limite, le fichier en cours est fermé et un fichier supplémentaire est créé pour poursuivre l'enregistrement. Cette action s'appelle une substitution.

À l'aide des commandes suivantes, vous pouvez préciser deux seuils pour une substitution :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
  CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD" -v "
  RolloverFileSizeInMB" -d "0x00000032" --force
2
3 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
  CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD" -v "
  RolloverTimeInHours" -d "0x0000000c" --force
```

- **RolloverFileSizeInMB.** Le fichier en cours se ferme lorsqu'il atteint cette taille et un nouveau fichier s'ouvre. Par défaut, la substitution se produit lorsque la taille dépasse 50 Mo. Valeurs prises en charge : 10 à 300.
- **RolloverTimeInHours.** Lorsque la durée est atteinte, le fichier en cours se ferme et un nouveau fichier s'ouvre. Par défaut, la substitution se produit lorsque la session enregistre pendant 12 heures. Valeurs prises en charge : 1 à 24.

Les substitutions se produisent lorsque la première des deux conditions ci-dessus est remplie. Par exemple, vous pouvez spécifier 17 Mo pour la taille du fichier et 6 heures pour la durée. Lorsque votre enregistrement atteint 17 Mo en 3 heures, l'enregistrement de session ferme le fichier et en ouvre un nouveau.

Pour éviter de créer trop de fichiers de petite taille, la substitution est effectuée avant qu'une heure au moins ne se soit écoulée, quelle que soit la valeur spécifiée pour la taille de fichier. L'exception à cette règle est si la taille du fichier dépasse 300 Mo.

## Spécifier l'emplacement du stockage des enregistrements

Les fichiers d'enregistrement sont stockés dans le répertoire `/var/xdl/session_recordings` par défaut. Pour spécifier un chemin différent, exécutez la commande suivante :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
  CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_SZ" -v "Path"
  -d "<your custom storage path>" --force
```

Vous pouvez stocker des enregistrements sur un lecteur local ou sur un point de montage pointant vers un chemin réseau. Configurez les autorisations d'accès appropriées au chemin de stockage que vous avez défini et accordez à l'utilisateur `ctxsrvr` l'autorisation d'écriture sur ce chemin.

## Afficher les enregistrements

Pour visionner les enregistrements, procédez comme suit pour installer le lecteur d'enregistrement de session ou le lecteur Web d'enregistrement de session :

1. Utilisez vos informations d'identification de compte Citrix pour accéder à la [page de téléchargement de Citrix Virtual Apps and Desktops](#) et télécharger le fichier du produit. Décompressez le fichier.
2. Cliquez deux fois sur `SessionRecordingPlayer.msi` et `SessionRecordingWebPlayer.msi`, puis suivez les invites pour terminer l'installation.

### Conseil :

Pour utiliser le lecteur Web d'enregistrement de session, installez-le uniquement sur le serveur d'enregistrement de session et assurez-vous que les enregistrements sont disponibles sur le serveur d'enregistrement de session. Pour plus d'informations, consultez la [documentation Enregistrement de session Citrix](#).

## Limitations

- Pour les sessions d'applications virtuelles, les notifications d'enregistrement peuvent ne pas être centrées.

## SDK du canal virtuel (version Technical Preview)

August 20, 2024

Avec le kit SDK du canal virtuel, vous pouvez écrire des applications côté serveur pour les exécuter sur le VDA. Pour en savoir plus, consultez la documentation du [SDK du canal virtuel Citrix pour Linux VDA](#).

Le SDK de 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.

**Remarque :**

Cette fonctionnalité est disponible dans la Tech Preview. Les fonctionnalités de la version Technical Preview peuvent ne pas être entièrement localisées et sont recommandées pour une utilisation dans des environnements hors production. Le support technique de Citrix ne traite pas les problèmes rencontrés avec les fonctionnalités Technical Preview.

## Wayland (version Technical Preview)

August 20, 2024

Le VDA Linux prend en charge Wayland dans GNOME sur RHEL 9.2/9.0, Rocky Linux 9.2/9.0 et Ubuntu 22.04. Les fonctionnalités suivantes ont été entièrement testées dans Wayland :

- Audio
- Presse-papiers
- Mappage des lecteurs clients (CDM)
- Impression
- Redirection de périphérique USB

**Remarque :**

- Cette fonctionnalité est disponible dans la Tech Preview. Les fonctionnalités de la version Technical Preview peuvent ne pas être entièrement localisées et sont recommandées pour une utilisation dans des environnements hors production. Les problèmes identifiés avec les fonctionnalités Technical Preview **ne sont pas pris en charge par** le support technique Citrix.
- HDX 3D Pro n'est pas pris en charge.
- Les sessions d'applications virtuelles Linux ne sont pas prises en charge.

## Activer Wayland

Pour utiliser Wayland, définissez la clé de registre **EnableWayland** sur **1** en exécutant la commande suivante :

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\Wayland" -t "REG_DWORD" -v "EnableWayland" -d "0x00000001" --force
```

Par défaut, la clé de registre **EnableWayland** est définie sur **0**, ce qui signifie que X11 est utilisé.

## Vérifier si Wayland est utilisé

1. Ouvrez une fenêtre de terminal sous Linux.
2. Exécutez la commande **echo \$XDG\_SESSION\_TYPE**.

Si Wayland est utilisé, vous obtenez '**wayland**' dans les résultats.

## Limitations

Lorsque Wayland est utilisé, les limites suivantes sont identifiées :

- La disposition du clavier de la machine cliente n'est pas synchronisée avec la disposition du clavier du VDA.
- Il faut environ 20 secondes pour fermer une session sur RHEL 9.1/9.0 ou Rocky Linux 9.1/9.0.

## Recommandations

August 20, 2024

Cette section vous guide tout au long des procédures suivantes :

- [Créer des Linux VDA sur Google Cloud Platform \(GCP\) à l'aide de Machine Creation Services \(MCS\)](#)

## Créer des Linux VDA sur Google Cloud Platform (GCP) à l'aide de Machine Creation Services (MCS)

August 21, 2024

Pour créer des Linux VDA sur GCP à l'aide de MCS, procédez comme suit :

Étape 1 : Créer une machine virtuelle (MV) Linux sur GCP

Étape 2 : Créer un compte de service GCP

Étape 3 : Créer une connexion hôte à GCP dans Citrix Studio

Étape 4 : Préparer une image principale du Linux VDA

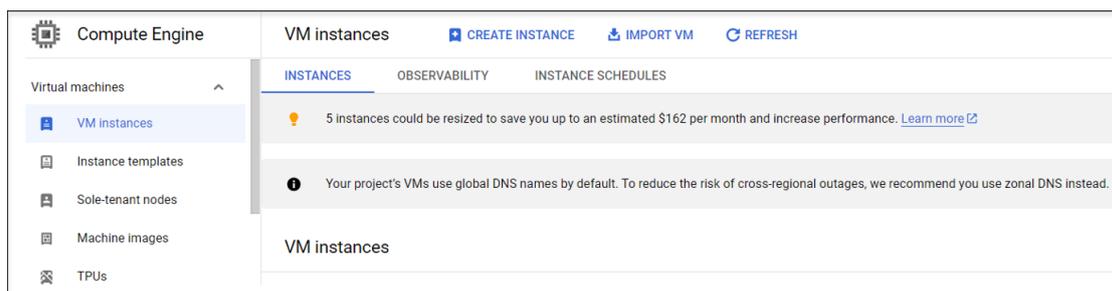
Étape 5 : créer un catalogue de machines

Étape 6 : créer un groupe de mise à disposition

## Étape 1 : Créer une machine virtuelle Linux sur GCP

**Étape 1a :** Dans la console Google Cloud, accédez à **Compute Engine > Instances de machine virtuelle**.

**Étape 1b :** Sur la page Instances de MV, cliquez sur **CRÉER UNE INSTANCE** pour créer une instance de machine virtuelle.



**Étape 1c :** Procédez aux configurations suivantes et conservez les autres configurations par défaut :

- Entrez un nom pour votre instance de machine virtuelle.
- Sélectionnez une région et une zone pour héberger votre machine virtuelle.
- (Facultatif) Ajoutez un unité de traitement graphique à votre machine virtuelle. Pour plus d'informations, consultez l'**Étape 4c** de cet article.
- Dans la section **Disque de démarrage**, sélectionnez le système d'exploitation et la taille du disque de votre machine virtuelle. Par exemple :

Boot disk

Select an image or snapshot to create a boot disk or attach an existing disk. Can't find what you're looking for? Explore hundreds of VM solutions in [Marketplace](#)

**PUBLIC IMAGES** CUSTOM IMAGES SNAPSHOTS ARCHIVE SNAPSHOTS EXISTING DISKS

Operating system  
Rocky Linux

Version \*  
Rocky Linux 8  
x86\_64, x86\_64 built on 20220920

Boot disk type \*  
Balanced persistent disk

**COMPARE DISK TYPES**

Size (GB) \*  
40

**SHOW ADVANCED CONFIGURATION**

**SELECT** CANCEL

- Accédez à **Options avancées > Réseau** et définissez le champ **Nom d'hôte** sur un nom de domaine complet.

Google Cloud linuxvda Search (/) for resources, docs, products, and more

← Create an instance

to create a VM instance, select one of the options:

- New VM instance**  
Create a single VM instance from scratch
- New VM instance from template  
Create a single VM instance from an existing template
- New VM instance from machine image  
Create a single VM instance from an existing machine image
- Marketplace  
Deploy a ready-to-go solution onto a VM instance

Monitor your system through collection of logs and key metrics.

Install Ops Agent for Monitoring and Logging

**Advanced options**

**Networking**  
Hostname and network interfaces

Network tags

**Hostname**  
instance-1.us-central1-a.c.linuxvda.internal  
Set a custom hostname for this instance or leave it default. Choice is permanent

**IP forwarding**  
 Enable

**Network performance configuration**

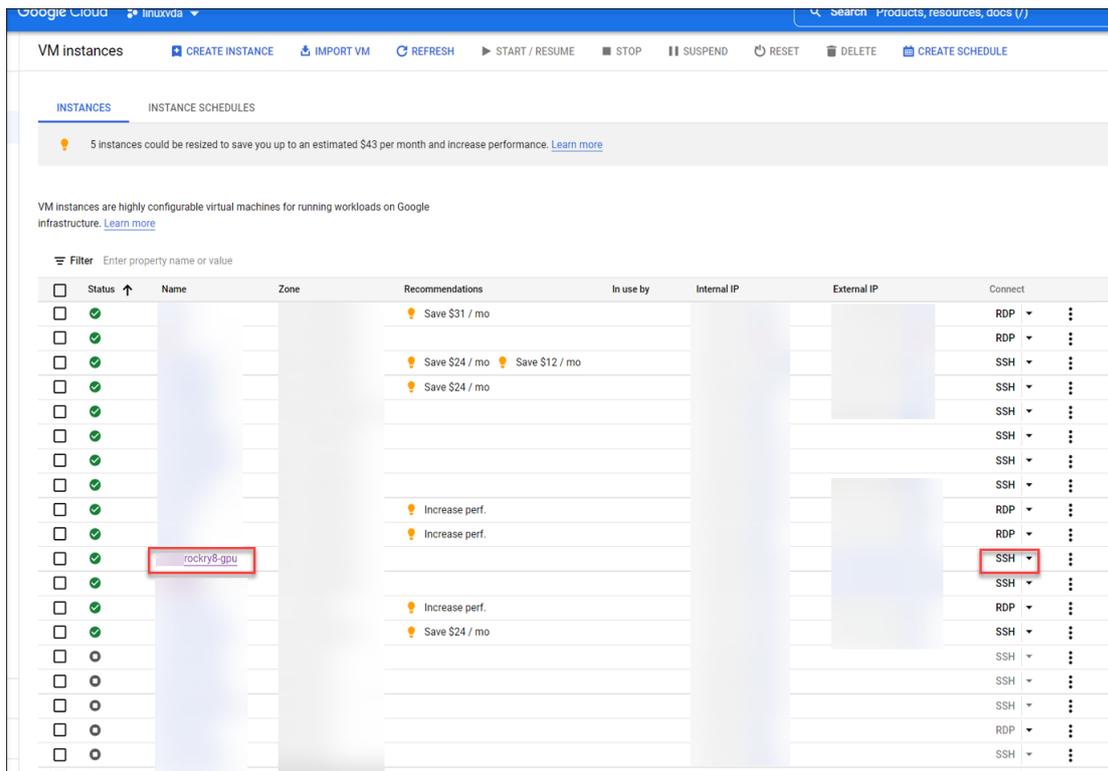
Network interface card

**Network bandwidth**  
 Enable per VM Tier\_1 networking performance  
Maximum outbound network bandwidth: 2Gbps  
VM to Public IP: 2Gbps

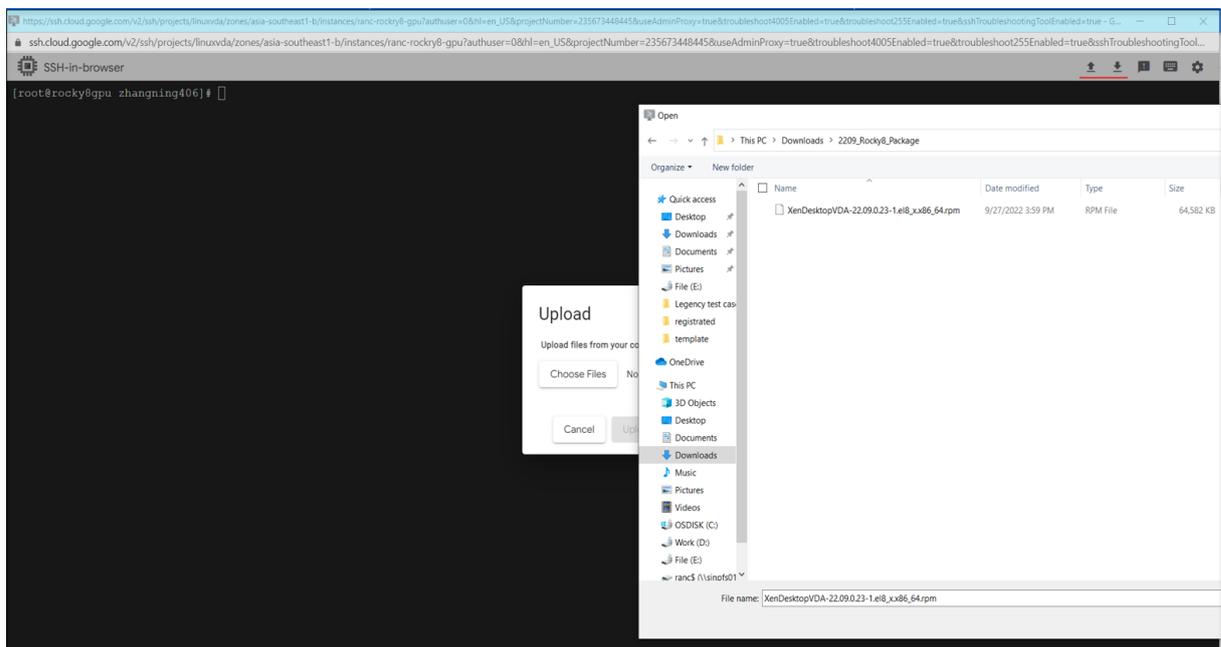
**CREATE** CANCEL **EQUIVALENT CODE**

**Étape 1d :** Cliquez sur **Créer** pour créer l'instance de MV.

**Étape 1e :** Une fois la machine virtuelle créée, revenez au tableau de bord **Compute Engine**, recherchez l'instance de votre machine virtuelle dans la liste, puis cliquez sur le bouton SSH pour vous connecter à votre machine virtuelle.



**Étape 1f :** Chargez le package Linux VDA sur votre machine virtuelle via le client SSH basé sur le Web.



**Étape 1g :** Évitez les échecs d'accès à la machine virtuelle via SSH.

La machine virtuelle peut être inaccessible après un redémarrage. Pour contourner ce problème, définissez un mot de passe racine lorsque vous vous connectez à la VM pour la première fois et assurez-vous que vous pouvez vous connecter à la VM en tant qu'utilisateur racine. Exécutez ensuite les com-

mandes suivantes dans la console après avoir redémarré la VM :

```
1 nmcli dev connect eth0
2 systemctl restart NetworkManager
```

The screenshot shows the Google Cloud console interface for virtual machines. On the left, there is a sidebar with 'Virtual machines' and 'VM instances' selected. The main content area has tabs for 'DETAILS', 'OBSERVABILITY', 'OS INFO', and 'SCREENSHOT'. Under 'DETAILS', there is an 'SSH' dropdown menu and a 'CONNECT TO SERIAL CONSOLE' dropdown menu, which is highlighted with a red box. Below these, there is a message: 'Connecting to serial ports is enabled in project-wide metadata'. To the right, there is a 'RED HAT KNOWLEDGEBASE' link. Below the message, there is a 'Logs' section with links for 'Logging' and 'Serial port 1 (console)', and a 'SHOW MORE' button.

## Étape 2 : Créer un compte de service GCP

Cette section vous explique comment créer un compte de service GCP, y compris comment créer une clé de compte de service et attribuer les rôles requis au compte de service.

### Remarque :

Pour créer un compte de service GCP, assurez-vous que le rôle IAM d'[administrateur du compte de service](#) (roles/iam.serviceAccountAdmin) vous est attribué.

**Étape 2a :** Dans la console Google Cloud, accédez à **IAM et administration > Comptes de service**, puis cliquez sur l'onglet **Créer un compte de service**.

The screenshot shows the Google Cloud IAM & Admin console. The left sidebar is expanded to 'IAM & Admin' > 'Service Accounts'. The main content area shows 'Service accounts for project "linuxvda"'. There is a search bar and a 'Filter' input. Below, there is a table of service accounts:

<input type="checkbox"/>	Email	Status	Name	Description	Key ID
<input type="checkbox"/>	[redacted]_t.serviceaccount.com	Enabled	App Engine default service account		No keys
<input type="checkbox"/>	[redacted]_t.serviceaccount.com	Enabled	binz-pvs		No keys
<input type="checkbox"/>	[redacted]_t.serviceaccount.com	Enabled	binzhou-mcs		
<input type="checkbox"/>	[redacted]_t.serviceaccount.com	Enabled	Compute Engine default service account		No keys
<input type="checkbox"/>	[redacted]_t.serviceaccount.com	Enabled	gcpldp	This account is used for Google IDP integration	

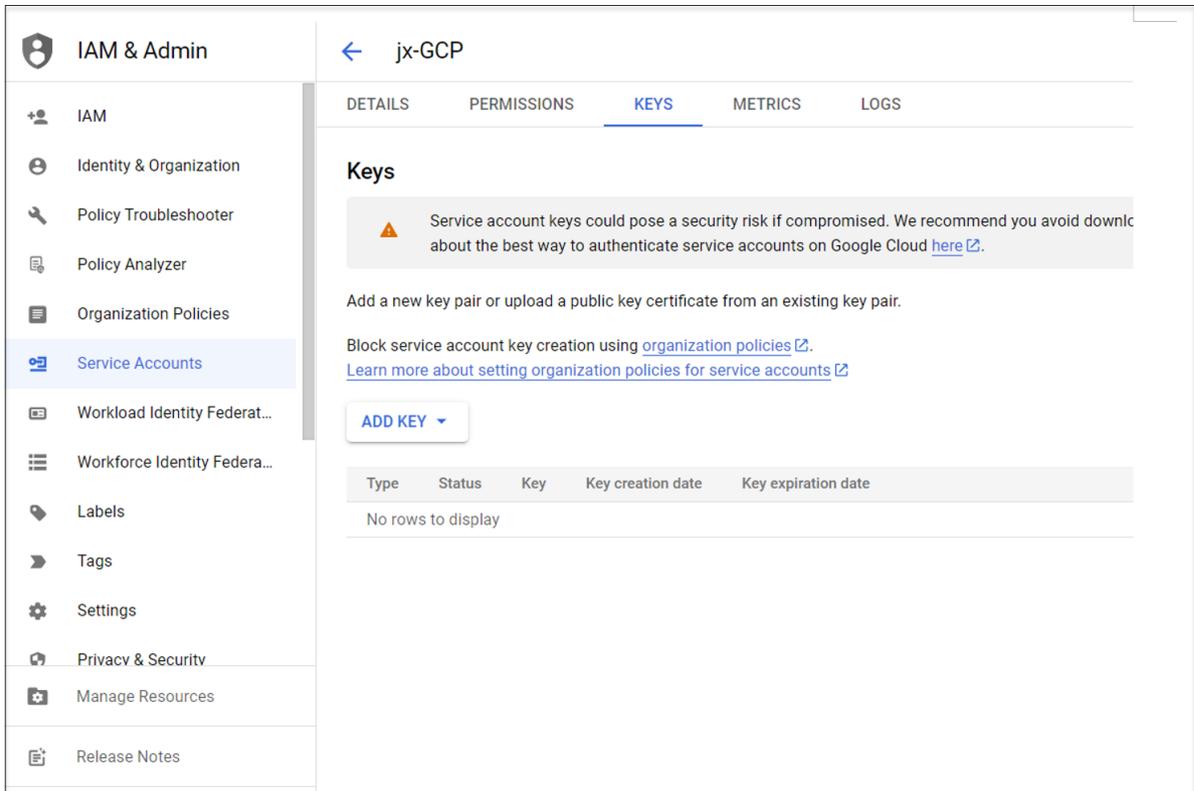
**Étape 2b :** À l'étape **Détails du compte de service**, saisissez les valeurs requises dans les champs, puis cliquez sur **Créer et continuer**.

The screenshot shows the Google Cloud IAM & Admin console. The left sidebar lists navigation options like IAM, Identity & Organization, and Service Accounts. The main content area is titled 'Create service account' and has three numbered steps. Step 1, 'Service account details', is the active step and contains four input fields: 'Service account name', 'Service account ID', 'Email address', and 'Service account description'. Below these fields is a 'CREATE AND CONTINUE' button. Step 2, 'Grant this service account access to project (optional)', and Step 3, 'Grant users access to this service account (optional)', are currently inactive. At the bottom of the page, there are 'DONE' and 'CANCEL' buttons.

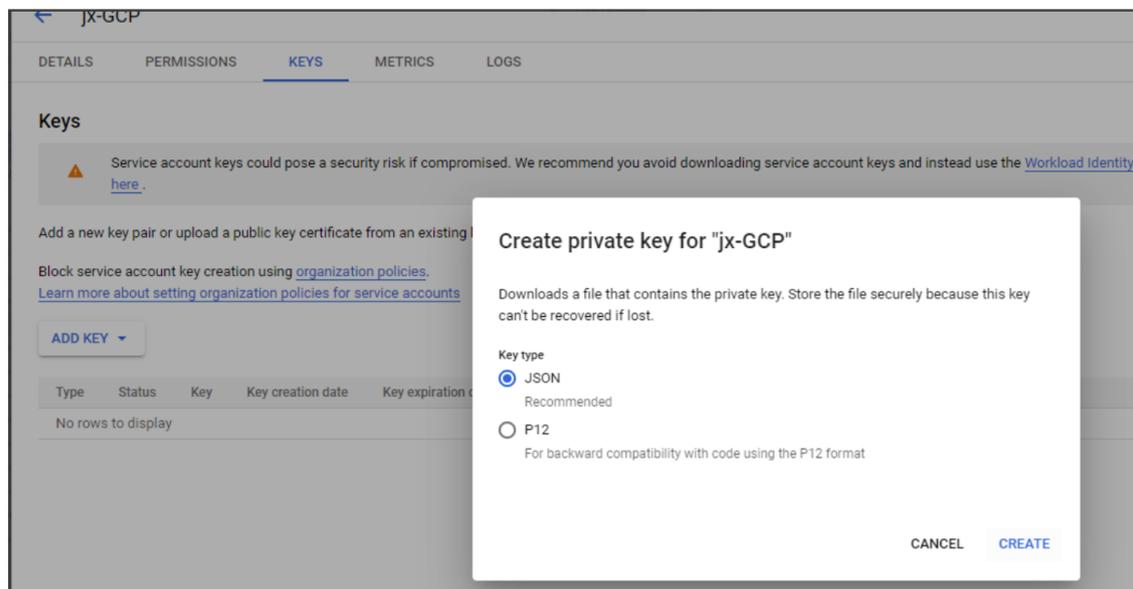
**Étape 2c :** Ignorez les étapes facultatives et cliquez sur **Terminé** en bas de la page.

This screenshot shows the same 'Create service account' page, but now Step 2, 'Grant this service account access to project (optional)', is the active step. Step 1 is marked as complete with a checkmark. Step 2 contains a text instruction, a 'Select a role' dropdown menu, an 'ADD IAM CONDITION' button, and an 'ADD ANOTHER ROLE' button. Step 3, 'Grant users access to this service account (optional)', remains inactive. The 'CONTINUE' button from the previous step is now disabled. The 'DONE' and 'CANCEL' buttons are still present at the bottom.

**Étape 2d:** Accédez à nouveau à **IAM et administration > Comptes de service**, puis cliquez sur l'onglet **Comptes de service**. Recherchez le compte de service que vous venez de créer, accédez à l'onglet **Clés**, puis cliquez sur **Ajouter une clé > Créer une nouvelle clé > JSON > Créer**.



The screenshot shows the IAM & Admin console for a service account named 'jx-GCP'. The left sidebar contains navigation options like IAM, Identity & Organization, and Service Accounts. The main content area is titled 'Keys' and includes a warning message, instructions to add a new key pair, and a table with columns for Type, Status, Key, Key creation date, and Key expiration date. The table currently shows 'No rows to display'.



The screenshot shows a dialog box titled 'Create private key for "jx-GCP"'. It contains a warning message and instructions to store the private key securely. The dialog offers two key types: JSON (Recommended) and P12 (For backward compatibility with code using the P12 format). The 'CREATE' button is highlighted.

### Remarque :

Une fois le fichier de clé téléchargé, vous ne pourrez plus le télécharger à nouveau.

**Étape 2e :** Dans la console Google Cloud, accédez à **IAM et administration > IAM**, puis cliquez sur **Ajouter**. Recherchez et sélectionnez le compte de service nouvellement créé dans le champ **Nouveaux membres**, puis sélectionnez un rôle pour le compte de service afin de lui accorder l'accès à vos ressources. Continuez à attribuer des rôles en cliquant sur **Ajouter un autre rôle** pour attribuer tous les rôles suivants au compte de service nouvellement créé.

- **Administrateur informatique**
- **Administrateur de l'espace de stockage**
- **Éditeur Cloud Build**
- **Utilisateur du compte de service**
- **Utilisateur de Cloud Datastore**
- **Administrateur d'instances Compute (version Bêta)**
- **Propriétaire**

Par exemple :



Cloud Build Editor	4/7 excess permissions
Cloud Datastore User	15/16 excess permissions
Compute Admin	524/576 excess permissions
Compute Instance Admin (beta)	121/162 excess permissions
Owner	4804/4871 excess permissions
Service Account User	3/5 excess permissions
Storage Admin	13/24 excess permissions

### Étape 3 : Créer une connexion hôte 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 hôte à GCP.

1. Pour les Delivery Controller locaux, choisissez **Configuration > Hébergement > Ajouter une connexion et des ressources** dans la configuration locale Citrix Studio pour créer une connexion hôte. 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 hôte.
2. Dans l'assistant **Ajouter une connexion et des ressources**, sélectionnez **Google Cloud Platform** comme type de connexion.

Par exemple, dans la console Studio Web sur Citrix Cloud :

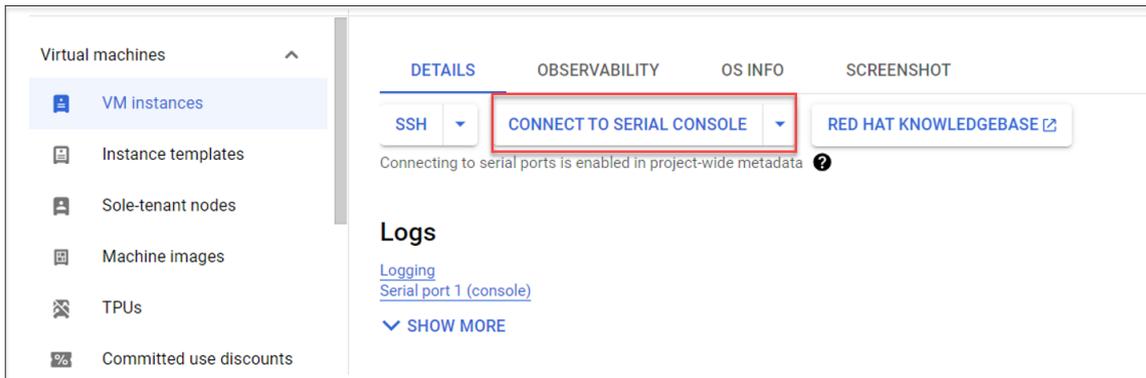
3. Importez la clé de compte de service de votre compte GCP et saisissez votre nom de connexion.
4. L'assistant vous guide à travers les pages. Le contenu de la page dépend du type de connexion sélectionné. Après avoir complété chaque page, sélectionnez **Suivant** jusqu'à la page **Résumé**. Pour plus d'informations, consultez [Étape 2 : créer une connexion hôte](#) dans l'article [Créer des VDA Linux non joints à un domaine à l'aide de MCS](#).

## Étape 4 : Préparer une image principale du Linux VDA

**Étape 4a :** (Pour RHEL 8.x/9.x et Rocky Linux 8.x/9.x) Configurez la connexion Ethernet.

Après avoir installé le Linux VDA sur RHEL 8.x/9.x et Rocky Linux 8.x/9.x hébergés sur GCP, la connexion Ethernet peut être perdue et le Linux VDA peut être inaccessible après le redémarrage d'une machine virtuelle. Pour contourner ce problème, définissez un mot de passe racine lorsque vous vous connectez à la VM pour la première fois et assurez-vous que vous pouvez vous connecter à la VM en tant qu'utilisateur racine. Exécutez ensuite les commandes suivantes dans la console après avoir redémarré la VM :

```
1 nmcli dev connect eth0
2 systemctl restart NetworkManager
```



**Étape 4b :** Installez le package du Linux VDA sur la VM modèle.

Sur la VM modèle, procédez comme suit pour installer le package du Linux VDA :

1. Installez .NET Runtime 6.0 :

```
1 sudo yum install dotnet-sdk-6.0
```

2. Installez le package du Linux VDA :

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

3. Activez le référentiel EPEL :

```
1 sudo rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

**Étape 4c :** Ajoutez une unité de traitement graphique à la VM modèle sur GCP (facultatif).

1. Dans la console Google Cloud, ajoutez une ou plusieurs unités de traitement graphique à la VM modèle. Pour plus d'informations sur l'ajout et la suppression d'unités de traitement graphique sur GCP, consultez <https://cloud.google.com/compute/docs/gpus/add-remove-gpus>.

← Create an instance

To create a VM instance, select one of the options:

- New VM instance**  
Create a single VM instance from scratch
- New VM instance from template  
Create a single VM instance from an existing template
- New VM instance from machine image  
Create a single VM instance from an existing machine image
- Marketplace  
Deploy a ready-to-go solution onto a VM instance

Name \*  
instance-1

MANAGE TAGS AND LABELS

Region \*  
us-central1 (Iowa)  
Region is permanent

Zone \*  
us-central1-a  
Zone is permanent

**Machine configuration**

General purpose | Compute optimized | Memory optimized | **GPUs**

Graphics processing units (GPUs) accelerate specific workloads on your instances such as machine learning and data processing. [Learn More](#)

GPU type  
NVIDIA T4

Number of GPUs  
1

Enable Virtual Workstation (NVIDIA GRID)

Series	Description	vCPUs	Memory	Platform
<b>N1</b>	Balanced price & performance	1 - 96	1.8 - 624 GB	Intel Skylake

**Machine type**  
Choose a machine type with preset amounts of vCPUs and memory that suit most workloads.

2. Installez le pilote d'unité de traitement graphique approprié sur la VM modèle. Pour plus d'informations, consultez <https://cloud.google.com/compute/docs/gpus/install-drivers-gpu>.

### Version des pilotes NVIDIA requise :

Les unités de traitement graphique NVIDIA exécutées sur Compute Engine doivent utiliser les versions de pilote NVIDIA suivantes :

- Pour les unités de traitement graphique L4 :
  - Linux : 525.60.13 ou version ultérieure
- Pour les unités de traitement graphique A100 :
  - Linux : 450.80.02 ou version ultérieure
- Pour les unités de traitement graphique T4, P4, P100 et V100 :
  - Linux : 410.79 ou version ultérieure
- Pour les unités de traitement graphique K80 (*fin de vie*) :
  - Linux : 410.79 - dernière version R470

Pour les unités de traitement graphique K80, NVIDIA a annoncé que la [version R470 des pilotes](#) est la dernière à bénéficier du support de débogage. Pour consulter cette mise à jour, consultez la matrice [NVIDIA Software Support Matrix](#).

### Script d'installation :

Vous pouvez utiliser le script suivant pour automatiser le processus d'installation :

```
1 https://raw.githubusercontent.com/GoogleCloudPlatform/compute-gpu-installation/main/linux/install_gpu_driver.py --output install_gpu_driver.py
```

### Systèmes d'exploitation pris en charge :

Le script d'installation a été testé sur les distributions Linux suivantes :

- CentOS 7/8
- Debian 10/11
- Red Hat Enterprise Linux (RHEL) 7/8
- Rocky Linux 8
- Ubuntu 18/20/22

Si vous utilisez ce script sur d'autres distributions Linux, l'installation échoue. Pour les machines virtuelles Linux, ce script installe uniquement le pilote NVIDIA.

a) Téléchargez le script d'installation.

```
1 curl https://raw.githubusercontent.com/GoogleCloudPlatform/compute-gpu-installation/main/linux/install_gpu_driver.py --output install_gpu_driver.py
```

b) Accordez un accès complet au script.

```
1 chmod 777 install_gpu_driver.py
```

c) Exécutez le script d'installation.

```
1 python3 install_gpu_driver.py
```

d) Désactivez Wayland dans gdm3.

- Localisez le fichier de configuration Wayland de votre distribution dans l'un des emplacements suivants :
  - /etc/gdm3/custom.conf (Ubuntu)
  - /etc/gdm/custom.conf (CentOS, RHEL, Rocky Linux)
- Ouvrez le fichier avec les privilèges sudo/root.
- Supprimez les marques de commentaire **WaylandEnable=False** en supprimant le # au début de la ligne.
- Redémarrez la machine virtuelle.

e) Si vous avez installé un pilote NVIDIA 510 ou version ultérieure, désactivez le microprogramme GSP.

Si le microprogramme GSP est activé, désactivez-le en réglant le paramètre du module NVIDIA **NVreg\_EnableGpuFirmware** sur 0.

Définissez ce paramètre en ajoutant l'entrée suivante au fichier /etc/modprobe.d/nvidia.conf :

- options nvidia NVreg\_EnableGpuFirmware=0
- Si le fichier /etc/modprobe.d/nvidia.conf n'existe pas, créez-le.

Lorsque vous effectuez cette étape, gardez les points suivants à l'esprit :

- Utilisez `sudo` pour exécuter les commandes permettant de créer et de mettre à jour le fichier de configuration.
- Pour redémarrer la machine virtuelle, vous pouvez utiliser le **redémarrage sudo** dans le terminal Linux ou arrêter et démarrer la machine virtuelle.

#### Étape 4d : Configurez les variables MCS.

Configurez les variables MCS en modifiant le fichier `/etc/xdl/mcs/mcs.conf`. Les variables MCS suivantes peuvent être configurées pour des scénarios de non-appartenance à un domaine et d'appartenance à un domaine :

- **Pour les scénarios de non-appartenance à un domaine**

Vous pouvez utiliser les valeurs des variables par défaut ou personnaliser les variables selon vos besoins (facultatif) :

```
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
```

```
#####Linux VDA Configuration#####
# Provide Linux VDA configuration information.
# Please refer to Linux VDA Documentation for these settings.
DOTNET_RUNTIME_PATH=/usr/bin
DESKTOP_ENVIRONMENT=gnome
SUPPORT_DDC_AS_CNAME=N
VDA_PORT=80
REGISTER_SERVICE=Y
ADD_FIREWALL_RULES=Y
HDX_3D_PRO=N
VDI_MODE=N
SITE_NAME='<none>'
LDAP_LIST='<none>'
SEARCH_BASE='<none>'
START_SERVICE=Y
```

- **Pour les scénarios avec appartenance à un domaine**

- `Use_AD_Configuration_Files_Of_Current_VDA` : détermine s'il faut utiliser les fichiers de configuration liés à AD existants (`/etc/krb5.conf`, `/etc/sss.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. Pour utiliser un VDA en cours d'exécution comme machine virtuelle modèle, définissez la valeur sur Y. Sinon, définissez-la sur N.

- `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 domaine 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](#).
- `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

```

#### Étape 4e : Créer une image principale

1. (Pour SSSD + RHEL 8.x/9.x ou Rocky Linux 8.x/9.x uniquement) Exécutez la commande `update-crypto-policies --set DEFAULT:AD-SUPPORT`, puis redémarrez la machine virtuelle modèle.
2. Exécutez `/opt/Citrix/VDA/sbin/deploymcs.sh`.

Pour les scénarios de non-appartenance à un domaine, l'erreur suivante est normale et ne vous empêche pas de continuer.

```

[root@localhost ~]#
[root@localhost ~]# /opt/Citrix/VDA/sbin/deploymcs.sh
Installing Linux VDA dependency packages ...
Installing package redhat-lsb-core
Installing package nautilus
Installing package totem-nautilus
Installing package brasero-nautilus
Installing package pulseaudio
Installing package pulseaudio-module-x11
Installing package pulseaudio-gdm-hooks
Installing package pulseaudio-module-bluetooth
Installing package alsa-plugins-pulseaudio
Installing package pciutils
Installing package openssh
Installing package openssh-clients
Installing package java-11-openjdk
Installing package chrony
Installing package krb5-workstation
Installing package oddjob-mkhomedir
Starting PostgreSQL database ...
Installing package tdb-tools
Installing package ntf3-3g
/opt/Citrix/VDA/lib64/mcs ~
installing mcs systemd unit file: ad_join.service ...
~
/opt/Citrix/VDA/lib64/mcs ~
~
Installing winbind dependency packages ...
Installing package samba-winbind
Installing package samba-winbind-clients
ERROR: Exit function conf_dns, dns not configured, please do it manually.
[root@localhost ~]#

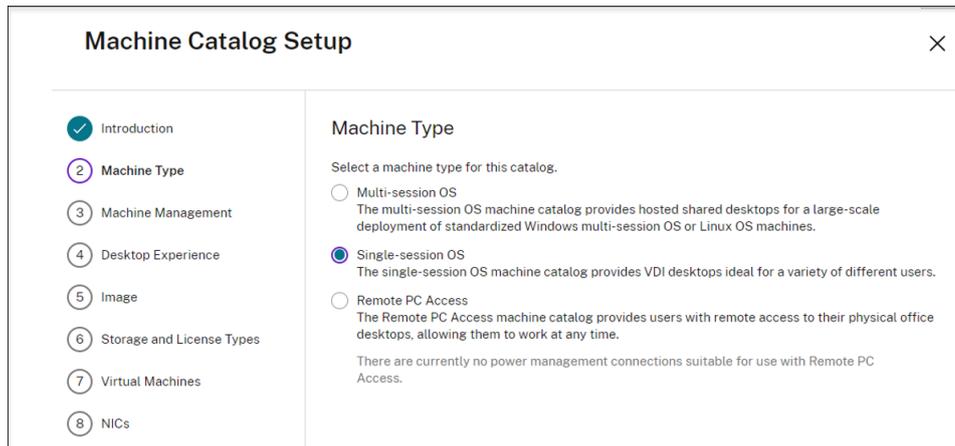
```

3. Installez les applications sur la VM modèle, puis arrêtez-la. Créez et nommez un instantané de l'image principale.

#### Étape 5 : créer un catalogue de machines

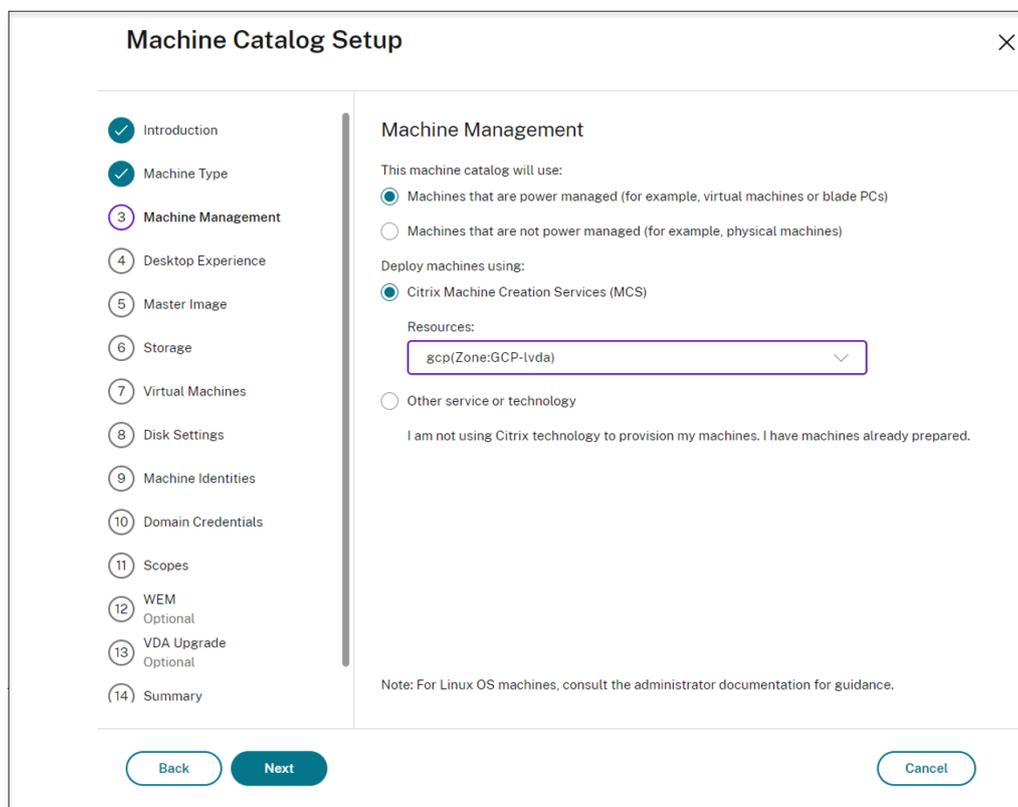
1. Connectez-vous à [Citrix Cloud](#). Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS**.

2. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet gauche.
3. Sélectionnez **Créer un catalogue de machines** dans la barre d'actions.
4. Sur la page **Type de machine**, sélectionnez **OS multi-session** ou **OS mono-session**, puis sélectionnez **Suivant**.



The screenshot shows the 'Machine Catalog Setup' dialog box with the 'Machine Type' step selected. The left sidebar lists steps 1 through 8, with 'Machine Type' (step 2) highlighted. The main content area is titled 'Machine Type' and contains the following text: 'Select a machine type for this catalog.' Below this are three radio button options: 'Multi-session OS' (with a description: 'The multi-session OS machine catalog provides hosted shared desktops for a large-scale deployment of standardized Windows multi-session OS or Linux OS machines.'), 'Single-session OS' (which is selected, with a description: 'The single-session OS machine catalog provides VDI desktops ideal for a variety of different users.'), and 'Remote PC Access' (with a description: 'The Remote PC Access machine catalog provides users with remote access to their physical office desktops, allowing them to work at any time. There are currently no power management connections suitable for use with Remote PC Access.').

5. Sur la page **Gestion des machines**, sélectionnez **des machines dont l'alimentation est gérée** et les options **Citrix Machine Creation Services**, puis sélectionnez **Suivant**. S'il existe plusieurs ressources, sélectionnez-en une dans le menu.



The screenshot shows the 'Machine Catalog Setup' dialog box with the 'Machine Management' step selected. The left sidebar lists steps 1 through 14, with 'Machine Management' (step 3) highlighted. The main content area is titled 'Machine Management' and contains the following text: 'This machine catalog will use:' followed by two radio button options: 'Machines that are power managed (for example, virtual machines or blade PCs)' (which is selected) and 'Machines that are not power managed (for example, physical machines)'. Below this is the text 'Deploy machines using:' followed by a radio button option 'Citrix Machine Creation Services (MCS)' (which is selected). Underneath is a 'Resources:' label and a dropdown menu showing 'gcp(Zone:GCP-lvda)'. There is also a radio button option 'Other service or technology'. At the bottom of the main content area, there is a note: 'I am not using Citrix technology to provision my machines. I have machines already prepared.' and a note: 'Note: For Linux OS machines, consult the administrator documentation for guidance.' At the bottom of the dialog box, there are three buttons: 'Back', 'Next', and 'Cancel'.

6. Sur la page **Image principale**, sélectionnez l'image principale créée précédemment.

The screenshot shows the 'Machine Catalog Setup' wizard at step 5, 'Master Image'. The left sidebar lists steps 1 through 14, with 'Master Image' highlighted. The main content area is titled 'Master Image' and contains the following elements:

- A heading 'Master Image' followed by a descriptive paragraph: 'The selected master image will be the template for all virtual machines in this catalog. (A master image is also known as a clone, golden image, or base image.)'
- A 'Master image' section with a '+ Select an image' button.
- A 'Note:' section with a text input field containing the placeholder 'Enter a note for the selected image' and a character count '0 / 500'.
- An unchecked checkbox labeled 'Use a machine profile' with a help icon.
- A dropdown menu for 'Select the minimum functional level for this catalog:' set to '1811 (or later)' with a help icon.
- A note at the bottom: 'To register with delivery groups that reference this catalog, machines require the selected version of the VDA or later. [Learn more](#)'

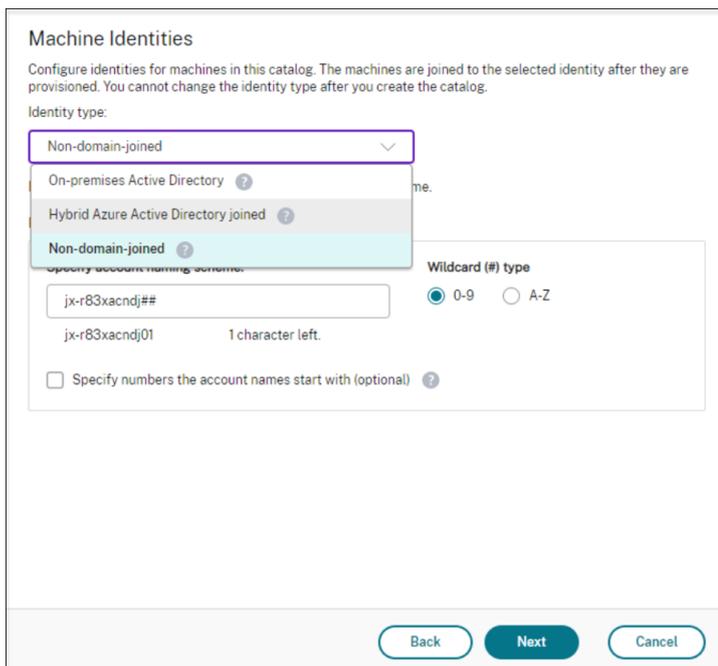
At the bottom of the wizard are three buttons: 'Back', 'Next', and 'Cancel'.

The screenshot shows the 'Machine Catalog Setup' wizard at step 5, 'Image'. The left sidebar lists steps 1 through 8, with 'Image' highlighted. The main content area is titled 'Image' and contains the following elements:

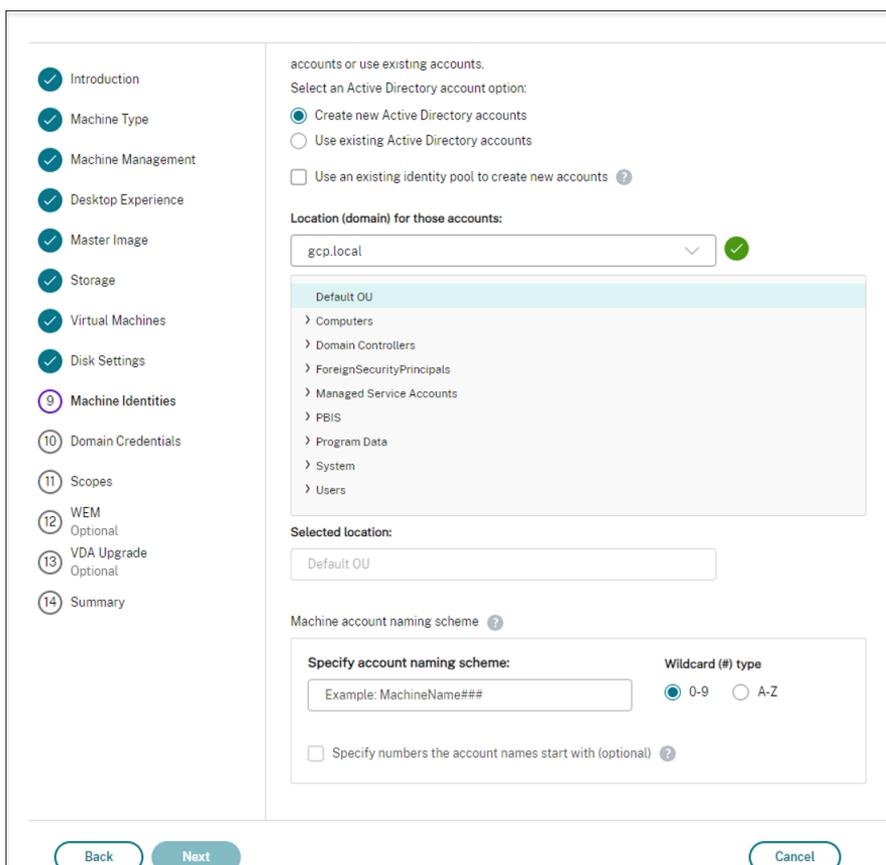
- A heading 'Image' followed by the text: 'Select the type of image for the machine catalog:'
- Two radio button options: 'Master image' (selected) and 'Prepared image'.
- A descriptive paragraph: 'The selected master image will be the template for all virtual machines in this catalog. (A master image is also known as a clone, golden image, or base image.)'
- A 'Master image' section showing a green checkmark, a computer icon, and the path 'XDHyp:\HostingUnits\gcplranc-rocky88-3d.vm' with an edit icon.
- A 'Note:' section with a text input field.

7. Sur la page **Identités des machines**, sélectionnez **Non joint au domaine** si l'image principale n'a été associée à aucun domaine ou sélectionnez un compte Active Directory si vous avez joint l'image principale à un domaine.

Pour les scénarios de non-appartenance à un domaine :



Pour les scénarios d'appartenance à un domaine :



- Si vous sélectionnez **Créer des nouveaux comptes Active Directory**, sélectionnez un domaine, puis entrez la séquence de caractères représentant le schéma de dénomination

pour les comptes d'ordinateurs machine virtuelle provisionnés créés dans Active Directory. Le schéma d'attribution de nom de compte peut contenir entre 1 et 64 caractères et ne peut pas contenir d'espaces vides, ni de caractères non ASCII ou spéciaux.

- Si vous sélectionnez **Utiliser des comptes Active Directory existants**, sélectionnez **Parcourir** pour accéder aux comptes d'ordinateur Active Directory existants pour les machines sélectionnées.
  - Sur la page **Informations d'identification du domaine**, sélectionnez **Entrer informations d'identification**, tapez le nom d'utilisateur et le mot de passe, sélectionnez **Enregistrer**, puis **Suivant**. Les informations d'identification que vous tapez doivent disposer de l'autorisation permettant d'effectuer des opérations de compte Active Directory.
8. Configurez des paramètres supplémentaires sur les autres pages. Pour plus d'informations, consultez la section [Créer un catalogue Google Cloud Platform](#).
  9. Sur la page **Résumé**, vérifiez les informations, spécifiez un nom pour le catalogue, puis sélectionnez **Terminer**.

**Machine Catalog Setup** [X]

- Introduction
- Machine Type
- Machine Management
- Desktop Experience
- Master Image
- Storage
- Virtual Machines
- Disk Settings
- Machine Identities
- Domain Credentials
- Scopes
- WEM Optional
- VDA Upgrade Optional
- 14 Summary**

### Summary

Machine type:	Single-session OS
Machine management:	Virtual
Provisioning method:	Machine creation services (MCS)
Desktop experience:	Users connect to the same desktop each time they log on Save changes on the local disk
Resources:	gcp
Master image:	-rocky88-3d
Storage:	Standard persistent disk
VDA version:	1811 (or later)
Number of VMs to create:	1
Virtual CPUs:	2
Memory (MB):	7680
Hard disk (GB):	40
Available zones:	asia-southeast1-a, asia-southeast1-b, asia-southeast1-c
Identity type:	On-premises AD
Computer accounts:	Create new accounts
New accounts location:	gcp.local (Domain)

Machine catalog name:

Machine catalog description for administrators (optional):

To complete the deployment, assign this machine catalog to a delivery group by selecting delivery groups and then create or edit a delivery group.

La création du catalogue de machines peut prendre du temps. Une fois terminé, le catalogue est répertorié. Vous pouvez vérifier que les machines sont créées sur les groupes de nœuds cibles dans la console Google Cloud.

## Étape 6 : 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 relative à la création de groupes de mise à disposition dans la documentation de [Citrix DaaS](#).

1. Connectez-vous à [Citrix Cloud](#). Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS**.
2. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
3. Sélectionnez **Créer un groupe de mise à disposition** dans la barre d'actions. L'assistant de création de groupes de mise à disposition s'ouvre.

Les pages de l'assistant qui s'affichent peuvent varier selon les sélections que vous effectuez.

4. Sur la page **Machines**, sélectionnez un catalogue et sélectionnez le nombre de machines que vous souhaitez utiliser dans ce catalogue.

Catalog	Type	Machines
ROCK8-MCS-3D	VDI MCS   Random   Discard	1
rocky88-gpu	VDI MCS   Random   Discard	1

5. Configurez des paramètres supplémentaires sur les autres pages. Pour plus d'informations, consultez la section [Créer des groupes de mise à disposition](#).
6. Sur la page **Résumé**, entrez le nom du groupe de mise à disposition. Vous pouvez également entrer une description (facultatif), qui s'affiche dans l'application Workspace et dans l'interface de gestion **Configuration complète**. Par exemple :

Entrez un nom pour le groupe de mise à disposition :

**Create Delivery Group**
✕

- ✔ Introduction
- ✔ Machines
- ✔ Users
- ✔ Applications
- ✔ Desktops
- ✔ App Protection
- ✔ Scopes
- ✔ License Assignment
- 9
Summary

### Summary

Machine catalog: rocky88-gpu

Machine type: Single-session OS

Allocation type: Random

Machines added: GCP-...-rock88-3d1  
1 unassigned

Users: Allow authenticated users

Desktops: Rocky8-gpu-mcs

Launch in user's home zone: No

Manage Autoscale ?: Disabled

License: DaaS Premium - Per User/Device

App Protection: -

Folder: -

**Delivery group name:**

**Delivery group description, used as label in Citrix Workspace app (optional):**

Liste des groupes de mise à disposition dans l'interface de gestion de la **configuration complète** :

Delivery Group	Delivering	Machine Count	Session in Use
GCP-...-rocky9-ndj Single-session OS	Desktops (Static machine assignment)	Total: 1 Unregistered: 0	Total: 0 Disconnected: 0
GCP-...-Rocky9-rdv2 Single-session OS	Desktops	Total: 1 Unregistered: 0	Total: 0 Disconnected: 0
GCP-...-rocky9-static Single-session OS	Desktops (Static machine assignment)	Total: 1 Unregistered: 0	Total: 0 Disconnected: 0
lp-rhe192-ndj Multi-session OS	Applications and Desktops	Total: 1 Unregistered: 1	Total: 0 Disconnected: 0
lp-sle155-chrome Multi-session OS	Desktops	Total: 1 Unregistered: 1	Total: 0 Disconnected: 0
lp-sle155-ndj Multi-session OS	Desktops	Total: 1 Unregistered: 0	Total: 0 Disconnected: 0

Machine mise à disposition dans l'application Citrix Workspace

- Home
- Apps
- Desktops

Apps

Recents Favorites

[View all applications](#)

Favorite apps will display here.  
[View all applications](#)

Desktops

Recents Favorites

[View all desktops](#)

★ Rocky8-gpu



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).