



Linux Virtual Delivery Agent 2103

Contents

Nouveautés	4
Problèmes résolus	6
Problèmes connus	6
Avis de tiers	9
Fin de prise en charge	9
Configuration système requise	10
Présentation de l'installation	15
Configurer Delivery Controller	16
Easy Install	18
Créer des Linux VDA dans Citrix Virtual Apps and Desktops Standard pour Azure	32
Utiliser Machine Creation Services (MCS) pour créer des machines virtuelles Linux	35
Installer Linux Virtual Delivery Agent pour RHEL/CentOS	72
Installer Linux Virtual Delivery Agent pour SUSE	105
Installer Linux Virtual Delivery Agent pour Ubuntu	132
Installer Linux Virtual Delivery Agent pour Debian	162
Configurer le Linux VDA	189
Intégrer NIS avec Active Directory	189
Publier des applications	195
Streaming Linux	196
Remote PC Access	203
Imprimer	216
Copier et coller des fichiers	223
Transfert de fichiers	224

Impression PDF	229
Configurer les graphiques	230
Affichage progressif Thinwire	239
Autres graphiques 3D	242
Configurer les stratégies	244
Liste des stratégies prises en charge	246
Configurer IPv6	257
Configurer le Programme d'amélioration de l'expérience utilisateur Citrix (CEIP)	258
Configurer la redirection USB	262
Configurer la fiabilité de session	273
Clavier logiciel	276
Éditeur IME	279
Prise en charge des entrées en plusieurs langues	280
Synchronisation dynamique de la disposition du clavier	282
Synchronisation de l'interface utilisateur de l'éditeur IME client	286
HDX Insight	290
Protocole Rendezvous	291
Transport adaptatif	293
Intégrer avec Citrix Telemetry Service	296
Traçage activé	300
Observer des sessions	303
Redirection du contenu du navigateur	309
Prise en charge de l'application Citrix Workspace pour HTML5	315
Surveiller les sessions Linux et les VM Linux dans Citrix Director	316

Démon du service de surveillance	319
Sécuriser les sessions utilisateur en utilisant TLS	322
Sécuriser les sessions utilisateur en utilisant DTLS	325
Filigrane de session textuel	326
Authentification unique avec des cartes à puce	327
Authentification Single Sign-On double-hop	337
Configurer des sessions non authentifiées	339
Configurer LDAPS	342
Créer un environnement virtuel Python3	346
XDPing	348
Configurer Xauthority	352
Configurer le service d'authentification fédérée	355

Nouveautés

November 5, 2021

Nouveautés dans la version 2103

La version 2103 du Linux VDA comprend les nouvelles fonctionnalités et améliorations suivantes :

Prise en charge de Debian 10.7 et CentOS 8.3

Debian 10.7 et CentOS 8.3 ont été ajoutées en tant que distributions prises en charge. Pour plus d'informations, consultez [Configuration système requise](#), [Installer Linux Virtual Delivery Agent pour Debian](#) et [Installer Linux Virtual Delivery Agent pour RHEL/CentOS](#).

Prise en charge SSSD pour joindre des machines SUSE aux domaines Windows

La prise en charge SSSD a été ajoutée pour joindre des machines SUSE aux domaines Windows.

Image Linux VDA unique pour les cas d'utilisation appartenant à un domaine ou non

Une image unique est désormais fournie pour créer des Linux VDA appartenant à un domaine ou non dans Citrix Virtual Apps and Desktops Standard pour Azure. Cette fonctionnalité simplifie la préparation et la maintenance de l'image. Pour plus d'informations, consultez [Créer des Linux VDA dans Citrix Virtual Apps and Desktops Standard pour Azure](#).

Amélioration du transfert de fichiers

La fonctionnalité de transfert de fichiers a été améliorée grâce à la nouvelle configuration de la barre de progression, ce qui a permis d'accélérer la vitesse de téléchargement et de résoudre certains bogues. Le nombre de fichiers que vous pouvez transférer simultanément a été augmenté de 10 à 100. Pour plus d'informations, consultez la section [Transfert de fichiers](#).

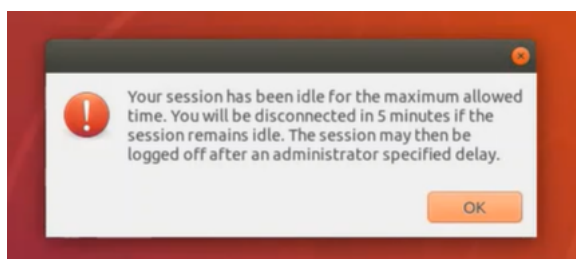
Prise en charge de la configuration des horloges de connexion de session dans Citrix Studio

Auparavant, vous pouviez configurer des délais pour les sessions inactives et déconnectées uniquement via `/opt/Citrix/VDA/bin/ctxcfg` séparément pour chaque VDA. Cette version ajoute les stratégies suivantes pour configurer les 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. Pour plus d'informations sur les stratégies, consultez la section [Liste des stratégies prises en charge](#).

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.



Disponibilité de nouvelles mesures pour les machines virtuelles Linux et les sessions Linux dans Citrix Director

Cette version ajoute de nouvelles mesures pour les machines virtuelles Linux et les sessions Linux dans Citrix Director.

Nouvelle mesure pour chaque machine virtuelle Linux :

- Nombre de cœurs de processeur
- Taille de la mémoire
- Capacité du disque dur
- Utilisation actuelle et historique du processeur et de la mémoire

Nouvelle mesure pour chaque session Linux :

- Délai d'inactivité

Pour plus d'informations, consultez la section [Surveiller les sessions Linux et les VM Linux dans Citrix Director](#).

Amélioration du FAS pour Linux VDA

Des sorties de journal plus pertinentes sont désormais disponibles et vous permettent de spécifier un chemin qui contient à la fois le certificat racine et tous les certificats intermédiaires lorsque vous exécutez le script `ctxfascfg.sh`. Pour plus d'informations sur la configuration, consultez la section [Configurer le service d'authentification fédérée](#).

Prise en charge du streaming Linux pour RHEL 8.3 et Ubuntu 18.04.5 (fonctionnalité expérimentale)

En utilisant la fonctionnalité de streaming Linux avec Citrix Provisioning, vous pouvez provisionner des bureaux virtuels Linux directement dans l'environnement Citrix Virtual Apps and Desktops. Pour plus d'informations, consultez la section [Streaming Linux](#).

Problèmes résolus

February 3, 2022

Les problèmes suivants ont été résolus depuis Linux Virtual Delivery Agent 2012 :

- Lorsque la liaison de canal est activée, les tentatives d'enregistrement d'un Linux VDA auprès du Delivery Controller peuvent échouer. Le problème se produit lorsque le ticket Kerberos utilisé pour l'authentification expire. [LNXVDA-9076]
- Les tentatives de sélection des options USB Picture Transfer Protocol (PTP) et Media Transfer Protocol (MTP) peuvent échouer sur un téléphone Xiaomi Mi 10. [CVADHELP-16188]
- Dans les Linux VDA, il est possible que certaines applications ne reconnaissent pas un périphérique webcam qui apparaît dans l'option **Appareil**. [CVADHELP-16247]
- Lorsque vous utilisez la redirection USB pour une webcam dans une session Linux VDA, le processus `ctxusbds` peut se fermer de façon inattendue avec une erreur `segfault`. [CVADHELP-16366]

Problèmes connus

July 13, 2023

Les problèmes suivants ont été identifiés dans cette version :

- Dans une session de bureau GNOME, les tentatives de modification de la disposition du clavier peuvent échouer. [CVADHELP-15639]
- Les applications publiées non transparentes peuvent se fermer peu de temps après leur lancement. Le problème se produit après une mise à niveau de Mutter vers une version supérieure à mutter-3.28.3-4. Pour contourner le problème, utilisez mutter-3.28.3-4 ou une version antérieure. [LNXVDA-6967]
- Le Linux VDA ne fonctionne pas comme prévu lorsque vous utilisez des cartes NVIDIA GRID 3D sans activer HDX 3D Pro. Le problème se produit sur RHEL 7.7 et versions antérieures, SUSE 12.5 et versions antérieures et Ubuntu 16.04. Ce problème se produit car plusieurs bibliothèques OpenGL ne peuvent pas coexister dans les systèmes graphiques de ces distributions Linux.
- Une fenêtre inattendue apparaît lors du téléchargement de fichier. La fenêtre n'affecte pas la fonctionnalité de téléchargement de fichier et disparaît automatiquement après un certain temps. [LNXVDA-5646]
- Les paramètres par défaut de PulseAudio provoquent la fermeture du programme du serveur audio après 20 secondes d'inactivité. Lorsque PulseAudio se termine, le son ne fonctionne pas. Pour contourner ce problème, définissez `exit-idle-time=-1` dans le fichier `/etc/pulse/daemon.conf`. [LNXVDA-5464]
- `libtcmalloc` 4.3.0 dans SUSE 12.5 peut provoquer la fermeture inattendue des processus.
- Le service `ctxhdx` peut se fermer de manière inattendue sur les VDA Ubuntu 16.04 et SUSE 12.5. Le problème se produit avec les versions 2.22 à 2.24 de la bibliothèque GNU C (`glibc`). Le problème est résolu dans `glibc` 2.25. Si vous utilisez la distribution SUSE 12.5, vous pouvez installer le correctif fourni par SUSE pour résoudre le problème. Aucun correctif n'est disponible pour Ubuntu 16.04 au moment de la publication de Linux VDA. [LNXVDA-4481]
- Les sessions ne peuvent pas être lancées dans l'application Citrix Workspace pour Linux lorsque le chiffrement SSL est activé et que la fiabilité de session est désactivée. [RFLNX-1557]
- Le processus `indicator-datetime-service` n'utilise pas la variable d'environnement `$TZ`. Lorsque le client et la session se trouvent dans des fuseaux horaires différents, le panneau Unity sur un bureau Unity Ubuntu 16.04 n'affiche pas l'heure du client. [LNXVDA-2128]
- 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

December 9, 2022

[Linux Virtual Delivery Agent version 2103](#) (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

November 5, 2021

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

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

Fins de prise en charge et retraits

Le tableau suivant indique les plates-formes, les produits Citrix et les fonctionnalités qui sont obsolètes ou ont été retirés. Les éléments

obsolètes ne sont pas retirés immédiatement. Citrix continue de les prendre en charge dans cette version, mais ils seront retirés dans une future version.

Les éléments retirés sont retirés, ou ne sont plus pris en charge, dans VDA Linux.

Élément	Abandon annoncé dans	Retrait dans
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

Élément	Abandon annoncé dans	Retrait dans
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

November 5, 2021

Distributions Linux

Remarque :

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

Avant d'installer Linux VDA, installez .NET Core Runtime 3.1 conformément aux instructions de l'article <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers>.

Pour plus d'informations sur l'utilisation de cette 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](#).

Linux VDA prend en charge les distributions Linux suivantes :

- SUSE Linux Enterprise :
 - Server 12 Service Pack 5 + SUSE Linux Enterprise Workstation Extension 12 SP5
 - Server 12 Service Pack 5
- Red Hat Enterprise Linux

- Workstation 8.3
 - Workstation 8.2
 - Workstation 8.1
 - Workstation 7.9
 - Workstation 7.8
 - Server 8.3
 - Server 8.2
 - Server 8.1
 - Server 7.9
 - Server 7.8
- CentOS Linux
 - CentOS 8.3
 - CentOS 8.2
 - CentOS 8.1
 - CentOS 7.9
 - CentOS 7.8
- Ubuntu Linux
 - Ubuntu Desktop 20.04
 - Ubuntu Server 20.04
 - Ubuntu Desktop 18.04
 - Ubuntu Server 18.04
 - Ubuntu Live Server 18.04
 - Ubuntu Desktop 16.04
 - Serveur Ubuntu 16.04
- Linux Debian
 - Debian 10.7

Remarque :

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

Le VDA Linux prend en charge plusieurs méthodes d'intégration des machines Linux avec Microsoft Active Directory (AD) :

	Winbind	SSSD	Centrify	PBIS	Quest
RHEL 8.3	Oui	Oui	Oui	Non	Non
CentOS 8.3	Oui	Oui	Oui	Non	Non
RHEL 8.2	Oui	Oui	Oui	Non	Non
CentOS 8.2	Oui	Oui	Oui	Non	Non
RHEL 8.1	Oui	Oui	Oui	Non	Non
CentOS 8.1	Oui	Oui	Oui	Non	Non
RHEL 7.9	Oui	Oui	Oui	Oui	Oui
CentOS 7.9	Oui	Oui	Oui	Oui	Oui
RHEL 7.8	Oui	Oui	Oui	Oui	Oui
CentOS 7.8	Oui	Oui	Oui	Oui	Oui
Ubuntu 20.04	Oui	Oui	Oui	Oui	Oui
Ubuntu 18.04	Oui	Oui	Oui	Oui	Oui
Ubuntu 16.04	Oui	Oui	Oui	Oui	Oui
Debian 10.7	Oui	Oui	Oui	Oui	Non
SUSE 12.5	Oui	Oui	Oui	Oui	Oui

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

Distribution Linux	Version Xorg
RHEL 8.3, CentOS 8.3	1.20.8
RHEL 8.2, CentOS 8.2	1.20.8
RHEL 8.1, CentOS 8.1	1.20.8
RHEL 7.9, CentOS 7.9	1.20
RHEL 7.8, CentOS 7.8	1.20
Ubuntu 20.04	1.20
Ubuntu 18.04	1.19
Ubuntu 16.04	1.18

Distribution Linux	Version Xorg
Debian 10.7	1.20
SUSE 12.5	1.19

N'utilisez pas le noyau HWE ou HWE Xorg sur Ubuntu.

Utilisez PulseAudio 13.99 sur RHEL 8.x et CentOS 8.x.

Dans tous les cas, l'architecture de processeur prise en charge est x86-64.

Remarque :

La prise en charge par Citrix d'une plate-forme et d'une version de système d'exploitation Linux expire lorsque le support du fournisseur du système d'exploitation expire.

Important :

Les bureaux GNOME et KDE sont pris en charge dans SUSE 12, RHEL 7, CentOS 7, RHEL 8 et CentOS 8. Le bureau Unity est pris en charge sur Ubuntu 16.04. Le bureau GNOME est pris en charge sur Ubuntu 20.04 et Ubuntu 18.04. Au moins un bureau doit être installé.

Citrix Virtual Desktops

Le Linux VDA est compatible avec toutes les versions actuellement prises en charge de Citrix Virtual Apps and Desktops. 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.

Environnements de virtualisation et plates-formes hôte pris en charge

- Serveurs bare metal
- Citrix Hypervisor
- VMware ESX et ESXi
- Microsoft Hyper-V
- Nutanix AHV
- Microsoft Azure Resource Manager
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

Conseil :

consultez la documentation du fournisseur pour obtenir la liste des plates-formes prises en charge.

Remarque :

Azure, AWS et GCP ne sont compatibles qu'avec le service Citrix Virtual Apps and Desktops. Les serveurs bare metal ne sont pas pris en charge lorsque MCS est utilisé pour créer des machines virtuelles.

Packages d'intégration d'Active Directory

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

- Samba Winbind
- Quest Authentication Services v4.1 ou version ultérieure
- Centrify DirectControl
- SSSD
- PBIS (compatible avec RHEL 7, Ubuntu et Debian)

Conseil :

pour obtenir la liste des plates-formes prises en charge, reportez-vous à la documentation des fournisseurs des packages d'intégration d'Active Directory.

HDX 3D Pro

Les hyperviseurs et processeurs graphiques NVIDIA GRID™ suivants sont requis pour la prise en charge de HDX 3D Pro.

Hyperviseurs

- Citrix Hypervisor
- VMware ESX et ESXi
- Nutanix AHV

Remarque les hyperviseurs sont compatibles avec certaines distributions Linux.

Processeur graphique

Le Linux VDA prend en charge les GPU suivants pour le GPU pass-through :

- NVIDIA GRID - Tesla T4
- NVIDIA GTX750Ti
- NVIDIA GRID - Tesla M60
- NVIDIA GRID - K2
- NVIDIA GRID - Tesla P40
- NVIDIA GRID - Tesla P4
- NVIDIA GRID - Tesla P100

Le Linux VDA prend en charge les GPU suivants pour vGPU :

- NVIDIA GRID - Tesla T4
- NVIDIA GRID - Tesla V100
- NVIDIA GRID - Tesla M60
- NVIDIA GRID - Tesla M10
- NVIDIA GRID - Tesla P40
- NVIDIA GRID - Tesla P4
- NVIDIA GRID - Tesla P100

Présentation de l'installation

November 5, 2021

Il existe plusieurs options pour installer l'agent Linux VDA. Vous pouvez effectuer une nouvelle installation ou effectuer une mise à niveau d'une installation existante à partir des deux versions précédentes et d'une version LTSR.

- Easy Install. Après l'installation du package Linux VDA sur une machine, vous pouvez configurer l'environnement d'exécution à l'aide du script `ctxinstall.sh`. Pour de plus amples informations, consultez la section [Easy Install](#).
- Créer des Linux VDA dans Citrix Virtual Apps and Desktops Standard pour Azure : vous pouvez créer des Linux VDA joints et non joints à un domaine dans Citrix Virtual Apps and Desktops Standard pour Azure pour fournir des applications et des bureaux virtuels sur n'importe quel appareil à partir de Microsoft Azure. Pour plus d'informations, consultez [Créer des Linux VDA dans Citrix Virtual Apps and Desktops Standard pour Azure](#).
- MCS. Vous pouvez utiliser MCS pour créer des machines virtuelles Linux par lots où le package Linux VDA est également installé. Pour plus d'informations, consultez la section [Utiliser MCS pour créer des machines virtuelles Linux](#).
- Installation manuelle. Vous pouvez suivre les étapes générales suivantes pour installer le Linux VDA. Les variantes et commandes spécifiques sont documentées par la distribution. Pour plus

d'informations, voir [Installer Virtual Delivery Agent Linux pour RHEL/CentOS](#), [Installer Virtual Delivery Agent Linux pour SUSE](#), [Installer Virtual Delivery Agent Linux pour Ubuntu](#) et [Installer Linux Virtual Delivery Agent pour Debian](#).

1. Préparez l'installation.
2. Préparez l'hyperviseur.
3. Ajoutez la machine virtuelle Linux au domaine Windows.
4. Installez le Linux VDA.
5. Configurez le Linux VDA.
6. Créez le catalogue de machines dans Citrix Virtual Apps ou Citrix Virtual Desktops.
7. Créez le groupe de mise à disposition dans Citrix Virtual Apps ou Citrix Virtual Desktops.

XDPing

Vous pouvez utiliser l'outil XDPing Linux pour vérifier les problèmes de configuration courants avec un environnement VDA Linux. Pour de plus amples informations, consultez la section [XDPing](#).

Installer .NET Core Runtime 3.1 en tant que condition préalable

Avant d'installer le VDA Linux, installez .NET Core Runtime 3.1 conformément aux instructions de l'article <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers>.

Après avoir installé .NET Core Runtime 3.1, exécutez la commande **which dotnet** pour trouver votre chemin d'exécution.

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

Configurer Delivery Controller

March 30, 2022

XenDesktop 7.6 et les versions antérieures requièrent des modifications pour prendre en charge le Linux VDA. Pour ces versions, un correctif ou un script de mise à jour est requis. Les instructions d'installation et de vérification sont décrites dans cet article.

Mettre à jour la configuration d'un Delivery Controller

Pour XenDesktop 7.6 SP2, appliquez le correctif Update 2 pour mettre à jour le broker pour Linux Virtual Desktop. Les correctifs Update 2 sont disponibles ici :

[CTX142438](#) : correctif Update 2 - pour Delivery Controller 7.6 (32 bits) –Anglais

Pour les versions antérieures à XenDesktop 7.6 SP2, vous pouvez utiliser le script PowerShell appelé **Update-BrokerServiceConfig.ps1** pour mettre à jour la configuration du Broker Service. Ce script est disponible dans le package suivant :

- citrix-linuxvda-scripts.zip

Répétez les étapes suivantes sur chaque Delivery Controller de la batterie de serveurs :

1. Copiez le script **Update-BrokerServiceConfig.ps1** sur la machine Delivery Controller.
2. Ouvrez une console Windows PowerShell dans le contexte de l'administrateur local.
3. Accédez au dossier contenant le script **Update-BrokerServiceConfig.ps1**.
4. Exécutez le script **Update-BrokerServiceConfig.ps1** :

```
1 .\Update-BrokerServiceConfig.ps1
```

Conseil :

Par défaut, PowerShell est configuré pour empêcher l'exécution des scripts PowerShell. Si le script ne réussit pas à s'exécuter, modifiez la stratégie d'exécution PowerShell avant d'essayer à nouveau :

```
1 Set-ExecutionPolicy Unrestricted
```

Le script **Update-BrokerServiceConfig.ps1** met à jour le fichier de configuration du Broker Service en utilisant de nouveaux points de terminaison WCF requis par le Linux VDA et redémarre le Broker Service. Le script détermine automatiquement l'emplacement du fichier de configuration du Broker Service. Une copie de sauvegarde du fichier de configuration d'origine est créée dans le même répertoire avec l'extension **.prelinux** ajoutée au nom du fichier.

Ces modifications n'ont pas d'impact sur la négociation des VDA Windows configurés pour utiliser la même batterie de Delivery Controller. Une seule batterie de Delivery Controller peut gérer et négocier les sessions pour les VDA Windows et Linux en toute facilité.

Remarque :

Le Linux VDA ne prend pas en charge Secure ICA pour le chiffrement. L'activation de Secure ICA sur le Linux VDA provoque l'échec du lancement de la session.

Vérifier la configuration d'un Delivery Controller

Lorsque les modifications de configuration requises ont été appliquées à un Delivery Controller, la chaîne **EndpointLinux** apparaît cinq fois dans le fichier **%PROGRAMFILES%\Citrix\Broker\Service\BrokerService**.

À partir de l'invite de commande de Windows, connectez-vous en tant qu'administrateur local pour vérifier les éléments suivants :

```
1 cd "%PROGRAMFILES%" \ Citrix \ Broker \ Service \
2 findstr EndpointLinux BrokerService.exe.config
```

Easy Install

June 17, 2022

Easy Install est pris en charge à partir de la version 7.13 de Linux VDA. Cette fonctionnalité vous permet de configurer un environnement d'exécution de Linux VDA en installant les packages nécessaires et en personnalisant automatiquement les fichiers de configuration.

Utiliser Easy Install

Pour utiliser cette fonctionnalité, procédez comme suit :

1. Préparez les informations de configuration et la machine Linux.
2. Installez 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. Définissez l'environnement d'exécution afin de terminer l'installation du Linux VDA.

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 : le nom NetBIOS du domaine
- Nom de zone : le nom de la zone Kerberos
- FQDN du domaine actif : nom de domaine complet

Important :

- Pour installer le Linux VDA, vérifiez que les référentiels sont ajoutés correctement sur la

machine Linux.

- Pour lancer une session, vérifiez que les environnements de bureau et du système X Windows sont installés.

Considérations

- Le nom du groupe de travail est le nom de domaine par défaut. Pour personnaliser le groupe de travail dans votre environnement, procédez comme suit :
 - a. Créez le fichier /tmp/ctxinstall.conf sur la machine Linux VDA.
 - b. Ajoutez la ligne « workgroup=<votre groupe de travail> » au fichier et enregistrez vos modifications.
- Centrify ne prend pas en charge la configuration DNS IPv6 pures. Au moins un serveur DNS utilisant IPv4 est requis dans /etc/resolv.conf pour que **adcli**ent puisse trouver les services AD correctement.

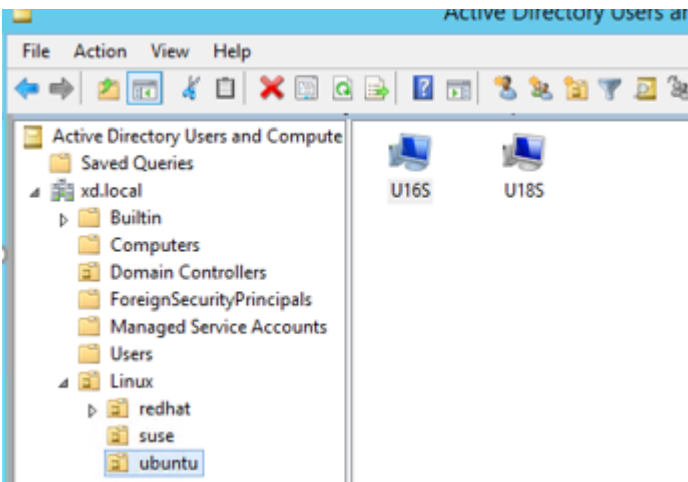
Journal :

```
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**.
- Pour joindre votre VDA à une unité d'organisation spécifique, procédez comme suit :
 1. Assurez-vous que l'unité d'organisation spécifique existe sur le contrôleur de domaine.

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



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

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

OS	Winbind	SSSD	Centrify	PBIS
RHEL 8	ou="" OU=redhat,OU=Linux	ou="" OU=redhat,OU=Linux	ou="" XD.LOCAL/Linux/redhat	NON PRIS EN CHARGE
RHEL 7	ou="" Linux/redhat"	ou="" Linux/redhat"	ou="" XD.LOCAL/Linux/redhat	ou="" Linux/redhat"
Ubuntu	ou="" Linux/ubuntu"	ou="" Linux/ubuntu"	ou="" XD.LOCAL/Linux/ubuntu	ou="" Linux/ubuntu"
SUSE 12.5	ou=""Linux/suse"	ou=""Linux/suse"	ou="" XD.LOCAL/Linux/suse	NON PRIS EN CHARGE
Debian	ou="" Linux/debian"	ou="" Linux/debian"	ou="" XD.LOCAL/Linux/debian	ou="" Linux/debian"

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

Remarque :

Si votre réseau est un réseau IPv6 pur et que toutes vos entrées sont au format IPv6 correct, le VDA s’enregistre auprès du Delivery Controller via IPv6. Si votre réseau dispose d’une

configuration hybride IPv4 et IPv6, le type de la première adresse IP du DNS détermine si IPv4 ou IPv6 est utilisé pour l'enregistrement.

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

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

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

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

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

- Récupérez le package Centrifry à partir d'un répertoire local. Procédez comme suit pour spécifier le répertoire du package Centrifry :
 - a. Créez le fichier `/tmp/ctxinstall.conf` sur le serveur Linux VDA, s'il n'existe pas.
 - b. Ajoutez la ligne « `centrifypkgpath=<nom du chemin d'accès>` » au fichier.

Par exemple :

```
1 cat /tmp/ctxinstall.conf
2 set "centrifypkgpath=/home/mydir"
3 ls -ls /home/mydir
4 9548 -r-xr-xr-x. 1 root root 9776688 May 13 2016
   adcheck-rhel4-x86_64
5 4140 -r--r--r--. 1 root root 4236714 Apr 21 2016
   centrifryda-3.3.1-rhel4-x86_64.rpm
6 33492 -r--r--r--. 1 root root 34292673 May 13 2016
   centrifrydc-5.3.1-rhel4-x86_64.rpm
7 4 -rw-rw-r--. 1 root root 1168 Dec 1 2015
   centrifrydc-install.cfg
8 756 -r--r--r--. 1 root root 770991 May 13 2016
   centrifrydc-ldaproxy-5.3.1-rhel4-x86_64.rpm
9 268 -r--r--r--. 1 root root 271296 May 13 2016
   centrifrydc-nis-5.3.1-rhel4-x86_64.rpm
10 1888 -r--r--r--. 1 root root 1930084 Apr 12 2016
   centrifrydc-openssh-7.2p2-5.3.1-rhel4-x86_64.rpm
11 124 -rw-rw-r--. 1 root root 124543 Apr 19 2016
   centrifry-suite.cfg
12 0 lrwxrwxrwx. 1 root root 10 Jul 9 2012 install-
   express.sh -> install.sh
```

13	332 -r-xr-xr--. 1 root root	338292 Apr 10 2016 install
	.sh	
14	12 -r--r--r--. 1 root root	11166 Apr 9 2015 release-
	notes-agent-rhel4-x86_64.txt	
15	4 -r--r--r--. 1 root root	3732 Aug 24 2015 release-
	notes-da-rhel4-x86_64.txt	
16	4 -r--r--r--. 1 root root	2749 Apr 7 2015 release-
	notes-nis-rhel4-x86_64.txt	
17	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. Le script ctxinstall.sh peut obtenir le package PBIS de deux façons :

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

RHEL 7/CentOS 7 : wget https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh

Ubuntu/Debian : wget https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh

- Le script peut également récupérer une version spécifique du package PBIS à partir d'Internet. Pour ce faire, modifiez la ligne « pbisDownloadPath » dans le fichier /opt/Citrix/VDA/sbin/ctxinstall.sh pour spécifier l'URL du package PBIS.

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"
```

Étape 2 : installer le package Linux VDA

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

Pour les distributions RHEL et CentOS :

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

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, ajoutez la ligne `deb http://deb.debian.org/debian/ oldstable main` au fichier /etc/apt/sources.list.

Pour les distributions SUSE :

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

Étape 3 : définir l'environnement d'exécution afin de terminer l'installation

Remarque :

Avant de configurer l'environnement d'exécution, assurez-vous que les paramètres régionaux `en_US.UTF-8` ont été 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`.

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

Remarque :

Easy install peut sembler ne pas répondre lorsqu'il télécharge .NET Core Runtime, qui fait plus de 27 Mo. Vérifiez le fichier `/var/log/ctxinstall.log` pour connaître la progression du téléchargement.

Mode interactif :

Pour effectuer une configuration manuelle, exécutez la commande suivante et entrez le paramètre approprié à chaque invite.

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

Mode silencieux :

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

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

- **CTX_EASYINSTALL_PASSWORD=password** : spécifie le mot de passe de l'utilisateur du domaine, utilisé pour rejoindre le domaine.

Le script ctxsetup.sh utilise les variables suivantes :

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N** : le Linux VDA prend en charge la spécification d'un nom de Delivery Controller à l'aide d'un enregistrement DNS CNAME.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** : le Linux VDA requiert une liste séparée par des espaces de noms de domaines complets de Delivery Controller. Cette dernière sera utilisée pour l'enregistrement auprès d'un Delivery Controller. Au moins un nom de domaine complet (FQDN) ou CNAME doit être spécifié.
- **CTX_XDL_VDA_PORT=port-number** : le Linux VDA communique avec les Delivery Controller via un port TCP/IP.
- **CTX_XDL_REGISTER_SERVICE = Y | N** : les services Linux VDA sont lancés après le démarrage de la machine.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** : les services Linux VDA requièrent que les connexions réseau entrantes soient autorisées via le pare-feu du système. Vous pouvez ouvrir automatiquement les ports requis (par défaut, les ports 80 et 1494) dans le pare-feu du système pour Linux Virtual Desktop.
- **CTX_XDL_HDX_3D_PRO = Y | N** : Linux VDA prend en charge HDX 3D Pro, un ensemble de technologies d'accélération GPU conçues pour optimiser la virtualisation des applications riches en graphiques. Si HDX 3D Pro est sélectionné, le Virtual Delivery Agent doit être configuré pour le mode Bureaux VDI (session unique), c'est-à-dire, CTX_XDL_VDI_MODE=Y.
- **CTX_XDL_VDI_MODE=Y | N** : indique si la machine est configurée comme modèle de mise à disposition de bureaux dédiés (VDI) ou comme modèle de mise à disposition de bureaux partagés hébergés. Pour les environnements HDX 3D Pro, définissez cette valeur sur Y.
- **CTX_XDL_SITE_NAME=dns-name** : le Linux VDA découvre les serveurs LDAP à l'aide de DNS. Pour limiter les résultats de recherche DNS à un site local, spécifiez un nom de site DNS. Si cela n'est pas nécessaire, définissez la valeur sur **<none>**.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** : le Linux VDA envoie une requête vers le DNS pour découvrir les serveurs LDAP. Si DNS ne peut pas fournir d'enregistrements de service LDAP, vous pouvez entrer une liste séparée par des espaces de noms de domaines complets LDAP avec ports LDAP. Par exemple, ad1.mycompany.com:389. Si cela n'est pas nécessaire, définissez la valeur sur **<none>**.
- **CTX_XDL_SEARCH_BASE=search-base-set** : le Linux VDA envoie une requête à LDAP via une base de recherche définie sur la racine du domaine Active Directory (par exemple, D, DC=mycompany,DC=com). Pour améliorer les performances de recherche, vous pouvez spécifier une base de recherche (par exemple, OU=VDI,DC=mycompany,DC=com). Si cela n'est pas nécessaire, définissez la valeur sur **<none>**.
- **CTX_XDL_FAS_LIST='list-fas-servers'** : les serveurs du service d'authentification fédérée (FAS) sont configurés via la stratégie de groupe AD. Le Linux VDA ne prend pas en charge la

stratégie de groupe AD mais vous pouvez fournir une liste de serveurs FAS séparés par des points-virgules. La séquence doit être la même que celle configurée dans la stratégie de groupe AD. Si une adresse de serveur est supprimée, remplissez son espace vide avec la chaîne de texte **<none>** et ne modifiez pas l'ordre des adresses de serveur.

- **CTX_XDL_DOTNET_RUNTIME_PATH=***path-to-install-dotnet-runtime* : chemin d'accès à l'installation de .NET Core Runtime 3.1 pour la prise en charge du nouveau Broker Agent Service (*ctxvda*). Le chemin par défaut est `/usr/bin`.
- **CTX_XDL_START_SERVICE=Y | N** : indique si les services Linux VDA sont démarrés lorsque la configuration est terminée.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** : port socket permettant d'écouter Citrix Scout. Le port par défaut est 7503.
- **CTX_XDL_TELEMETRY_PORT** : port de communication avec Citrix Scout. Le port par défaut est 7502.

Si aucun paramètre n'est défini, l'installation retourne en mode interactif et l'utilisateur est invité à intervenir. Lorsque tous les paramètres sont déjà définis via les variables d'environnement, le script `ctxinstall.sh` invite toujours l'utilisateur à entrer le chemin d'installation de .NET Core Runtime 3.1.

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

```
1 export CTX_EASYINSTALL_HOSTNAME=host-name
2
3 export CTX_EASYINSTALL_DNS=ip-address-of-dns
4
5 export CTX_EASYINSTALL_NTPS=address-of-ntps
6
7 export CTX_EASYINSTALL_DOMAIN=domain-name
8
9 export CTX_EASYINSTALL_REALM=realm-name
10
11 export CTX_EASYINSTALL_FQDN=ad-fqdn-name
12
13 export CTX_EASYINSTALL_ADINTEGRATIONWAY=winbind | sssd | centrify |
    pbis
14
15 export CTX_EASYINSTALL_USERNAME=domain-user-name
16
17 export CTX_EASYINSTALL_PASSWORD=password
18
19 export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N
20
21 export CTX_XDL_DDC_LIST= ' list-ddc-fqdns '
22
23 export CTX_XDL_VDA_PORT=port-number
24
25 export CTX_XDL_REGISTER_SERVICE=Y | N
26
```

```
27 export CTX_XDL_ADD_FIREWALL_RULES=Y | N
28
29 export CTX_XDL_HDX_3D_PRO=Y | N
30
31 export CTX_XDL_VDI_MODE=Y | N
32
33 export CTX_XDL_SITE_NAME=dns-site-name | '<none>'
34
35 export CTX_XDL_LDAP_LIST= ' list-ldap-servers ' | '<none>'
36
37 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
38
39 export CTX_XDL_FAS_LIST= ' list-fas-servers ' | '<none>'
40
41 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
42
43 export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number
44
45 export CTX_XDL_TELEMETRY_PORT=port-number
46
47 export CTX_XDL_START_SERVICE=Y | N
48
49 sudo -E /opt/Citrix/VDA/sbin/ctxinstall.sh
```

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

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

```
1 sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
2
3 CTX_XDL_DDC_LIST= ' list-ddc-fqdns ' \
4
5 CTX_XDL_VDA_PORT=port-number \
6
7 CTX_XDL_REGISTER_SERVICE=Y|N \
8
9 CTX_XDL_ADD_FIREWALL_RULES=Y|N \
10
11 CTX_XDL_AD_INTEGRATION=1|2|3|4 \
12
13 CTX_XDL_HDX_3D_PRO=Y|N \
14
15 CTX_XDL_VDI_MODE=Y|N \
16
17 CTX_XDL_SITE_NAME=dns-name \
18
19 CTX_XDL_LDAP_LIST= ' list-ldap-servers ' \
20
21 CTX_XDL_SEARCH_BASE=search-base-set \
22
23 CTX_XDL_FAS_LIST= ' list-fas-servers ' \
```

```
24
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
26
27 CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \
28
29 CTX_XDL_TELEMETRY_PORT=port-number \
30
31 CTX_XDL_START_SERVICE=Y|N \
32
33 /opt/Citrix/VDA/sbin/ctxsetup.sh
```

Résolution des problèmes

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

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:

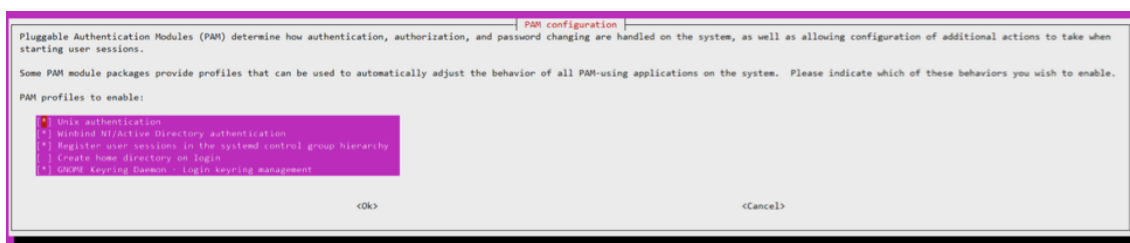
```
1 2016-11-02 13:21:19.015 <P22492:S1> citrix-ctxlogin: StartUserSession:
   failed to change to directory(/home/CITRIXLAB/ctxadmin) errno(2)
2
3 2016-11-02 13:21:19.017 <P22227> citrix-ctxhdx: logSessionEvent:
   Session started for user ctxadmin.
4
5 2016-11-02 13:21:19.023 <P22492:S1> citrix-ctxlogin: 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/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 Linux VDA dans Citrix Virtual Apps and Desktops Standard pour Azure

June 16, 2023

Vous pouvez créer des Linux VDA appartenant et n'appartenant pas à un domaine dans 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 Virtual Apps and Desktops Standard pour Azure](#).

Distributions Linux prises en charge

Les distributions Linux suivantes prennent en charge cette fonctionnalité :

- RHEL 8.3
- RHEL 8.2
- RHEL 7.8
- Ubuntu 20.04
- Ubuntu 18.04
- Ubuntu 16.04

Étapes

Pour créer des Linux VDA dans Citrix Virtual Apps and Desktops Standard pour Azure, procédez comme suit :

1. Préparez une image principale dans Azure :
 - a) Dans Azure, créez une machine virtuelle Linux d'une distribution prise en charge.
 - b) Installez un environnement de bureau sur la machine virtuelle Linux si nécessaire.
 - c) Sur la machine virtuelle, installez .NET Core Runtime 3.1 conformément aux instructions de <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers>.
 - d) (Pour Ubuntu uniquement) Ajoutez la ligne `source /etc/network/interfaces.d/*` dans le fichier `/etc/network/interfaces`.
 - e) (Pour Ubuntu uniquement) Pointez `/etc/resolv.conf` sur `/run/systemd/resolve/resolv.conf` au lieu de `/run/systemd/resolve/stub-resolv.conf`:

```

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

```

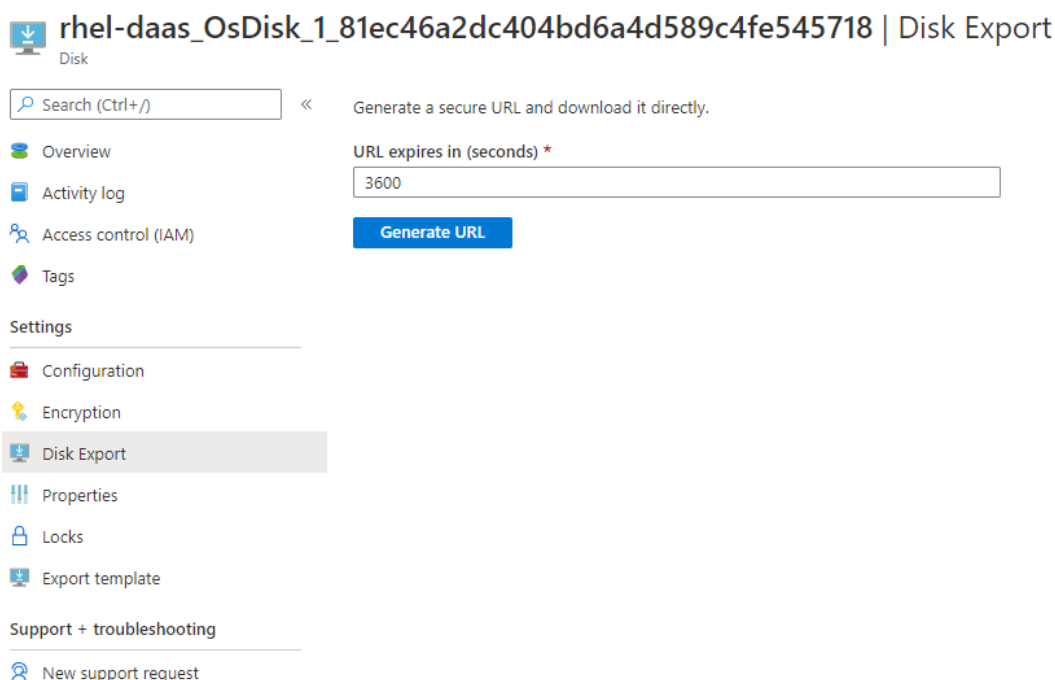
- f) Installez le package Linux VDA.
- g) Modifiez les variables dans `/etc/xdl/mcs/mcs.conf`. Le fichier de configuration `mcs.conf` contient des variables pour la configuration de MCS et du Linux VDA.

Remarque :

Laissez la variable `dns` non spécifiée.

Si vous sélectionnez le type **Statique** ou **Aléatoire** lors de la création d'un catalogue de machines, définissez `VDI_MODE=Y`.

- h) Exécutez `/opt/Citrix/VDA/sbin/deploymcs.sh`.
- i) Dans Azure, arrêtez (ou désallouez) la machine virtuelle. Cliquez sur **Exportation de disque** pour générer une URL SAS pour le fichier de disque dur virtuel (VHD) que vous pouvez utiliser comme image principale pour créer d'autres machines virtuelles.



- j) (Facultatif) Réglez des paramètres de stratégie de groupe sur l'image principale.

```

1 You can use the `ctxreg` tool to make group policy settings. For
  example, the following command enables the **Auto-create PDF
  Universal Printer** policy for PDF printing.
2
3

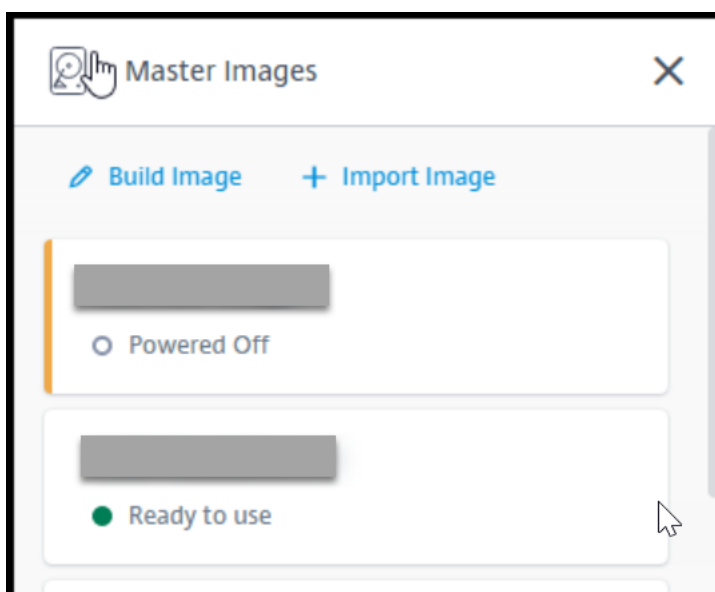
```

```
4 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\  
   GroupPolicy\Defaults\PrintingPolicies" -t "REG_DWORD" -v "  
5   AutoCreatePDFPrinter" -d "0x00000001" - force
```

2. Importez l'image principale à partir d'Azure.

- a) Dans le tableau de bord **Gérer**, développez **Images principales** sur la droite. L'affichage répertorie les images principales fournies par Citrix et les images que vous avez créées et importées.

Conseil : La plupart des activités d'administrateur de ce service sont gérées via les tableaux de bord **Gérer** et **Surveiller**. Après avoir créé votre premier catalogue, le tableau de bord **Gérer** se lance automatiquement après vous être connecté à Citrix Cloud et avoir sélectionné le service **Bureaux gérés**.



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

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"

- d) Suivez les instructions de l'assistant pour procéder à l'importation de l'image principale.
3. Créez un catalogue de machines.

Accédez au tableau de bord [Gérer](#) et cliquez sur **Créer un catalogue**. Lors de la création du catalogue de machines, choisissez l'image principale que vous avez créée précédemment.

Remarque : vous pouvez créer des catalogues de machines Linux qui n'appartiennent pas à un domaine uniquement dans un abonnement Azure géré par Citrix.

Utiliser Machine Creation Services (MCS) pour créer des machines virtuelles Linux

May 3, 2023

Pour utiliser MCS pour créer des machines virtuelles Linux, préparez une image principale sur votre hyperviseur. Ce processus implique l'installation du VDA sur la VM modèle, la création d'un catalogue de machines dans Citrix Studio, la création d'un groupe de mise à disposition et l'exécution de certaines tâches de configuration.

Remarque :

Des résultats inattendus peuvent se produire si vous essayez de préparer une image principale sur des hyperviseurs autres que Citrix Hypervisor, Microsoft Azure, VMware vSphere, AWS, GCP ou Nutanix AHV.

Microsoft Azure, AWS et GCP ne sont pas pris en charge à partir de Citrix Virtual Apps and Desktops

7 2003. Mais vous pouvez continuer à utiliser les hôtes dans Citrix Virtual Apps and Desktops Service.

Distributions prises en charge

	Winbind	SSSD	Centrify	PBIS
RHEL 8.3	Oui	Non	Non	Non
CentOS 8.3	Oui	Non	Non	Non
RHEL 8.2	Oui	Non	Non	Non
CentOS 8.2	Oui	Non	Non	Non
RHEL 8.1	Oui	Non	Non	Non
CentOS 8.1	Oui	Non	Non	Non
RHEL 7.9	Oui	Oui	Non	Non
CentOS 7.9	Oui	Oui	Non	Non
RHEL 7.8	Oui	Oui	Non	Non
CentOS 7.8	Oui	Oui	Non	Non
Ubuntu 20.04	Oui	Oui	Non	Non
Ubuntu 18.04	Oui	Oui	Non	Non
Ubuntu 16.04	Oui	Oui	Non	Non
Debian 10.7	Oui	Oui	Non	Non
SUSE 12.5	Oui	Oui	Non	Non

Utiliser MCS pour créer des machines virtuelles Linux sur Citrix Hypervisor

Étape 1 : préparer une image principale

Une image principale contient le système d’exploitation, les applications non virtualisées, le VDA, et d’autres logiciels. Pour préparer une image principale, procédez comme suit :

Étape 1a : installer Citrix VM Tools Le composant Citrix VM Tools doit être installé sur la VM modèle pour que chaque VM puisse utiliser l’interface de ligne de commande xe ou XenCenter. Les performances de la VM peuvent être lentes à moins que les outils ne soient installés. Sans les outils, vous ne pouvez pas effectuer les opérations suivantes :

- Arrêter, redémarrer ou suspendre une VM correctement
- Afficher les données de performances de la VM dans XenCenter
- Migrer une VM en cours d'exécution (via [XenMotion](#)).
- Créer des instantanés ou des instantanés avec de la mémoire (points de contrôle) et revenir aux instantanés
- Régler le nombre de vCPU sur une VM Linux en cours d'exécution

1. Exécutez la commande suivante pour monter le composant Citrix VM Tools nommé guest-tools.iso.

```
1 sudo mount /dev/cdrom /mnt
```

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

Pour RHEL/CentOS :

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

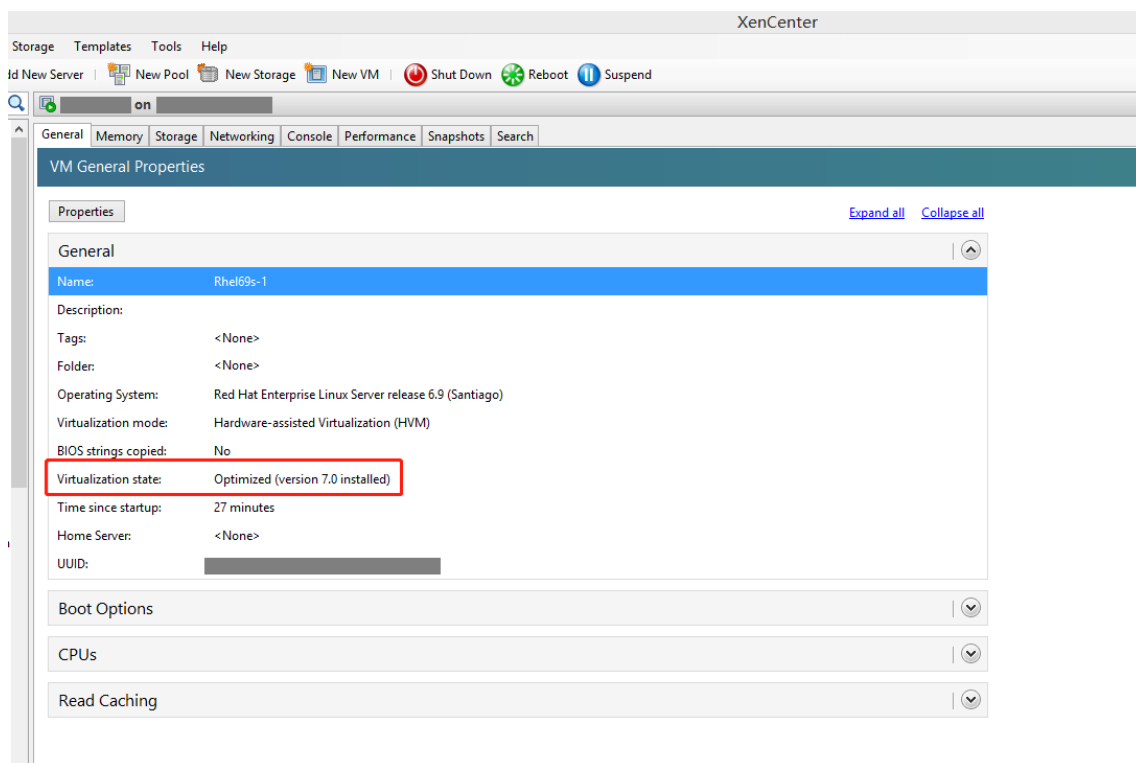
Pour Ubuntu/Debian :

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

Pour SUSE 12 :

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

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



Étape 1b : installer le package du Linux VDA sur la VM modèle

Remarque :

Pour utiliser un VDA en cours d'exécution comme VM modèle, omettez cette étape.

Avant d'installer le package VDA Linux sur la machine virtuelle modèle, installez .NET Core Runtime 3.1. Pour plus d'informations, consultez [Présentation de l'installation](#).

Selon votre distribution Linux, exécutez la commande suivante pour configurer l'environnement du Linux VDA :

Pour RHEL/CentOS :

```
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 12 :

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

Étape 1c : activer les référentiels pour installer le package `tdb-tools` 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 1d : installer le référentiel EPEL qui contient `ntfs-3g` Installez le référentiel EPEL sur RHEL 8/CentOS 8, RHEL 7/CentOS 7 afin que l'exécution de `deploymcs.sh` installe ultérieurement le package `ntfs-3g` qu'il contient.

Étape 1e : installer manuellement `ntfs-3g` sur SUSE 12 Sur la plate-forme SUSE 12, 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 1f : configurer l'environnement d'exécution Avant d'exécuter `deploymcs.sh`, procédez comme suit :

- Modifiez les variables dans `/etc/xdl/mcs/mcs.conf`. Le fichier de configuration `mcs.conf` contient des variables pour la configuration de MCS et du Linux VDA. Vous pouvez définir les variables suivantes si nécessaire :
 - `Use_Existing_Configurations_Of_Current_VDA` : détermine si les configurations existantes du VDA en cours d'exécution doivent être utilisées. 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 fichiers de configuration sur les machines créées avec MCS sont déterminés par des modèles de configuration sur l'image principale.

- `dns` : définit l'adresse IP du DNS.
 - `AD_INTEGRATION` : définit Winbind ou SSSD. 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.
 - `WORKGROUP` : définit le nom du groupe de travail (sensible à la casse) s'il est configuré dans AD.
- 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 "0x00000003" --force
```

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

Étape 1g : créer une image principale

1. Exécutez `/opt/Citrix/VDA/sbin/deploymcs.sh`.
2. (Facultatif) 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/mcs/winbind_krb5.conf.tpl` et `/etc/xdl/mcs/winbind_smb.conf.tpl`.

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

Remarque :

Conservez le format existant utilisé dans les fichiers de modèle et utilisez des variables telles que \$WORKGROUP, \$REALM, \$realm et \$AD_FQDN.

3. Sur Citrix Hypervisor, arrêtez la VM modèle. Créez et nommez un instantané de l'image principale.

Étape 2 : créer un catalogue de machines

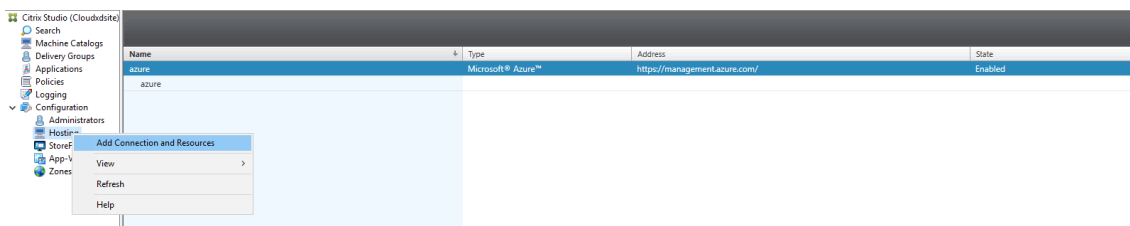
Dans Citrix Studio, créez un catalogue de machines et spécifiez le nombre de VM à créer dans le catalogue. Effectuez d'autres tâches de configuration si nécessaire. Pour plus d'informations, consultez l'article [Créer un catalogue de machines à l'aide de Studio](#).

Étape 3 : 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. Le groupe de mise à disposition spécifie quels utilisateurs peuvent utiliser ces machines, ainsi que les applications et bureaux disponibles auprès de ces utilisateurs. Pour plus d'informations, consultez la section [Créer des groupes de mise à disposition](#).

Utiliser MCS pour créer des machines virtuelles Linux sur Azure**Étape 1 : créer une connexion d'hébergement à Azure dans Citrix Studio**

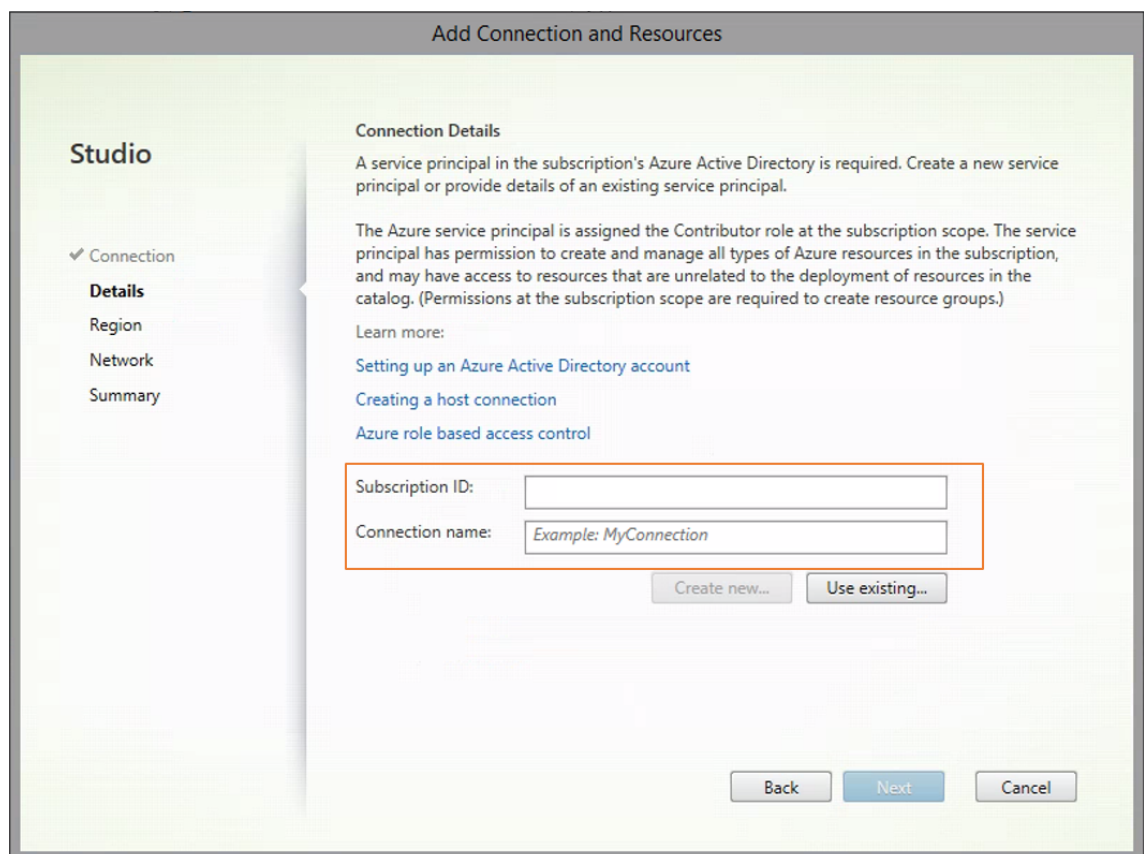
1. Dans Citrix Studio, sur Citrix Cloud, sélectionnez **Configuration > Hébergement > Ajouter une connexion et des ressources** pour créer une connexion à Azure.



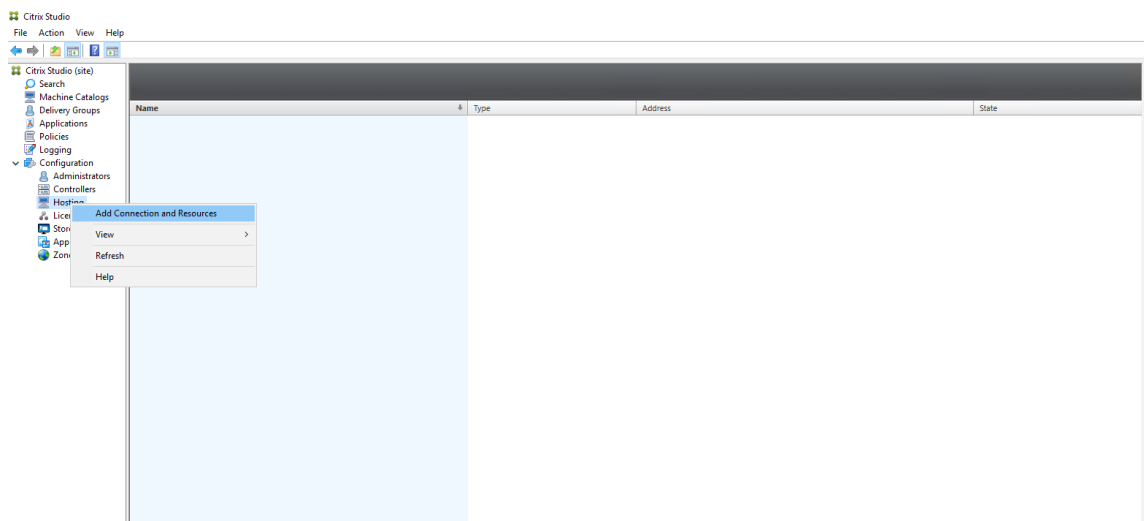
2. Sélectionnez le type de connexion Microsoft Azure.

The screenshot shows the 'Add Connection and Resources' dialog box in the Studio application. The 'Connection' tab is active in the left sidebar. The main area has two radio buttons: 'Use an existing Connection' (unselected) and 'Create a new Connection' (selected). Below 'Create a new Connection', there is a 'Connection type' dropdown menu with 'Microsoft® Azure™' selected, and an 'Azure environment' dropdown menu with 'Azure Global' selected. Below these, there is a section 'Create virtual machines using:' with two radio buttons: 'Studio tools (Machine Creation Services)' (selected) and 'Other tools' (unselected). A note below the first radio button says 'Select this option when using AppDisks, even if you are using Provisioning Services.' At the bottom right, there are three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

3. Entrez l’ID d’abonnement de votre compte Azure, ainsi que votre nom de connexion.



Une nouvelle connexion apparaît dans le panneau d'hébergement.



Étape 2 : préparer une image principale sur la VM modèle

Une image principale contient le système d'exploitation, les applications non virtualisées, le VDA, et d'autres logiciels. Pour préparer une image principale, procédez comme suit :

Étape 2a : configurer cloud-init pour Ubuntu 18.04 Pour vous assurer que le nom d'hôte du VDA soit préservé lorsqu'une VM est redémarrée ou arrêtée, exécutez la commande suivante.

```
1 echo "preserve_hostname: true" > /etc/cloud/cloud.cfg.d/99_hostname.cfg
```

Assurez-vous que les lignes suivantes sont présentes sous la section **system_info** du fichier `/etc/cloud/cloud.cfg` :

```
1 system_info:
2   network:
3     renderers: ['netplan', 'eni', 'sysconfig']
```

Étape 2b : installer le package du Linux VDA sur la VM modèle

Remarque :

Pour utiliser un VDA en cours d'exécution comme VM modèle, omettez cette étape.

Avant d'installer le package VDA Linux sur la machine virtuelle modèle, installez .NET Core Runtime 3.1. Pour plus d'informations, consultez [Présentation de l'installation](#).

Selon votre distribution Linux, exécutez la commande suivante pour configurer l'environnement du Linux VDA :

Pour RHEL/CentOS :

```
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 12 :

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

Étape 2c : installer le référentiel EPEL qui contient ntfs-3g Installez le référentiel EPEL sur RHEL 8/CentOS 8, RHEL 7/CentOS 7 afin que l'exécution de `deploymcs.sh` installe ultérieurement le package `ntfs-3g` qu'il contient.

Étape 2d : installer manuellement ntfs-3g sur SUSE 12 Sur la plate-forme SUSE 12, 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 2e : configurer l'environnement d'exécution Avant d'exécuter `deploymcs.sh`, procédez comme suit :

- Modifiez les variables dans `/etc/xdl/mcs/mcs.conf`. Le fichier de configuration `mcs.conf` contient des variables pour la configuration de MCS et du Linux VDA. Vous trouverez ci-dessous quelques variables, dont `dns` et `AD_INTEGRATION` qui doivent être définies :

Remarque : si une variable peut être définie avec plusieurs valeurs, placez les valeurs entre guillemets simples et séparez-les par des espaces. Par exemple, `LDAP_LIST='aaa.lab:389 bbb.lab:389.'`

- `Use_Existing_Configurations_Of_Current_VDA` : détermine si les configurations existantes du VDA en cours d'exécution doivent être utilisées. 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 fichiers de configuration sur les machines créées avec MCS sont déterminés par des modèles de configuration sur l'image principale.
 - `dns` : définit l'adresse IP du DNS.
 - `AD_INTEGRATION` : définit Winbind ou SSSD (SSSD n'est pas pris en charge sur SUSE).
 - `WORKGROUP` : définit le nom du groupe de travail (sensible à la casse) s'il est configuré dans AD.
- 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 "0x00000003" --force
```

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

Étape 2f : créer une image principale

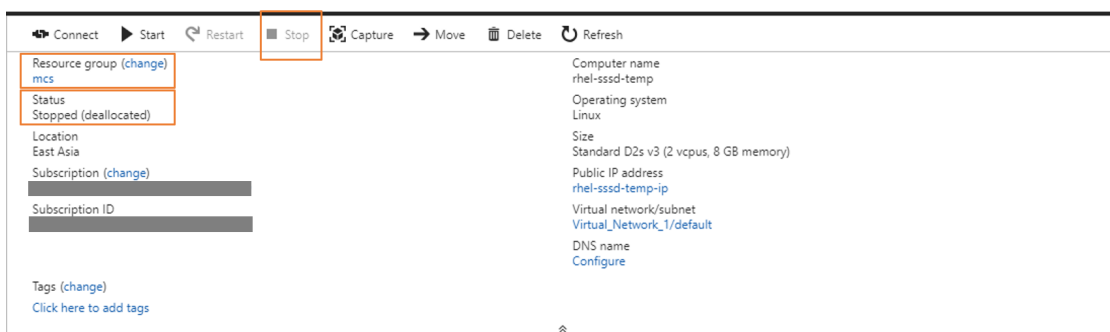
1. Exécutez `/opt/Citrix/VDA/sbin/deploymcs.sh`.
2. (Facultatif) Sur la VM modèle, mettez à jour les modèles de configuration pour personnaliser les fichiers `/etc/krb5.conf`, `/etc/samba/smb.conf` et `/etc/sss/sss.conf` sur toutes les VM créées.

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

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

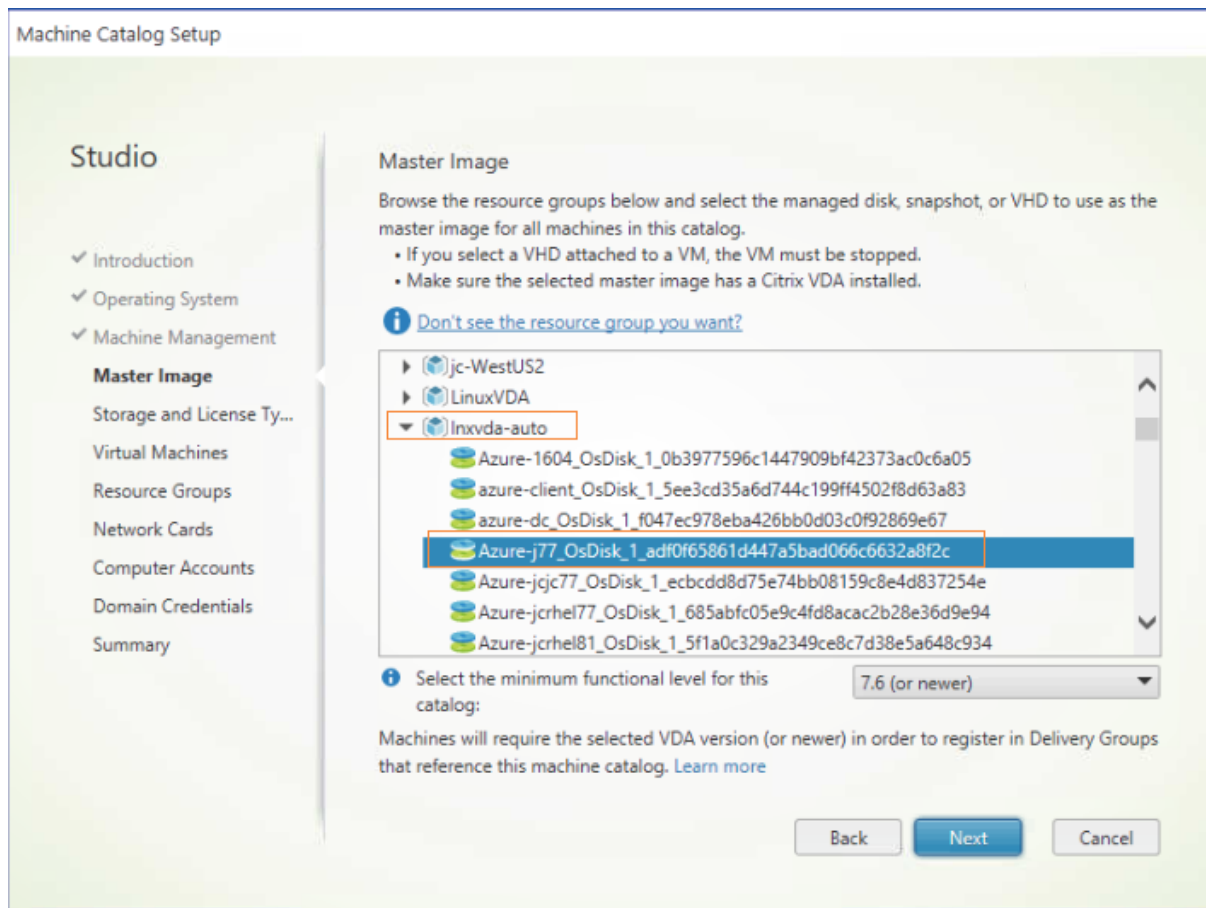
Remarque : conservez le format existant utilisé dans les fichiers de modèle et utilisez des variables telles que `$WORKGROUP`, `$REALM`, `$realm` et `$AD_FQDN`.

3. 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)**. Mémo-risez le nom du groupe de ressources. Vous avez besoin du nom pour localiser votre image principale sur Azure.



Étape 3 : créer un catalogue de machines

Dans Citrix Studio, créez un catalogue de machines et spécifiez le nombre de VM à créer dans le catalogue. Lors de la création du catalogue de machines, choisissez votre image principale dans le groupe de ressources auquel appartient la VM modèle et recherchez le disque dur virtuel de la VM modèle.



Effectuez d'autres tâches de configuration si nécessaire. Pour plus d'informations, consultez l'article [Créer un catalogue de machines à l'aide de Studio](#).

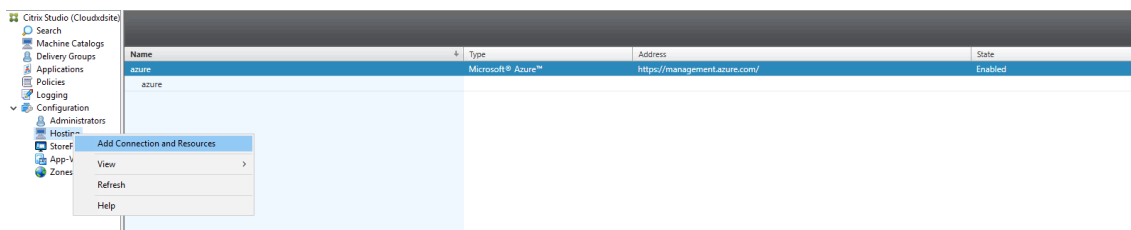
Étape 4 : créer un groupe de mise à disposition

Un groupe de mise à disposition est une collection de machines sélectionnées à partir d'un ou de plusieurs catalogues de machines. Le groupe de mise à disposition spécifie quels utilisateurs peuvent utiliser ces machines, ainsi que les applications et bureaux disponibles auprès de ces utilisateurs. Pour plus d'informations, consultez la section [Créer des groupes de mise à disposition](#).

Utiliser MCS pour créer des machines virtuelles Linux sur VMware vSphere

Étape 1 : créer une connexion d'hébergement vers VMware dans Citrix Studio

1. Installez vCenter Server dans l'environnement vSphere. Pour plus d'informations, consultez la section [VMware vSphere](#).
2. Dans Citrix Studio, sélectionnez **Configuration > Hébergement > Ajouter une connexion et des ressources** pour créer une connexion à VMware vSphere.



3. Sélectionnez le type de connexion VMware vSphere.

Add Connection and Resources

Studio

- Connection
- Storage Management
- Storage Selection
- Network
- Summary

Connection

☐ Use an existing Connection

RanConnection

☒ Create a new Connection

Connection type: VMware vSphere®

Connection address: Example: https://vmware.example.com/sdk

[Learn about user permissions](#)

User name: Example: domain\username

Password:

Connection name: Example: MyConnection

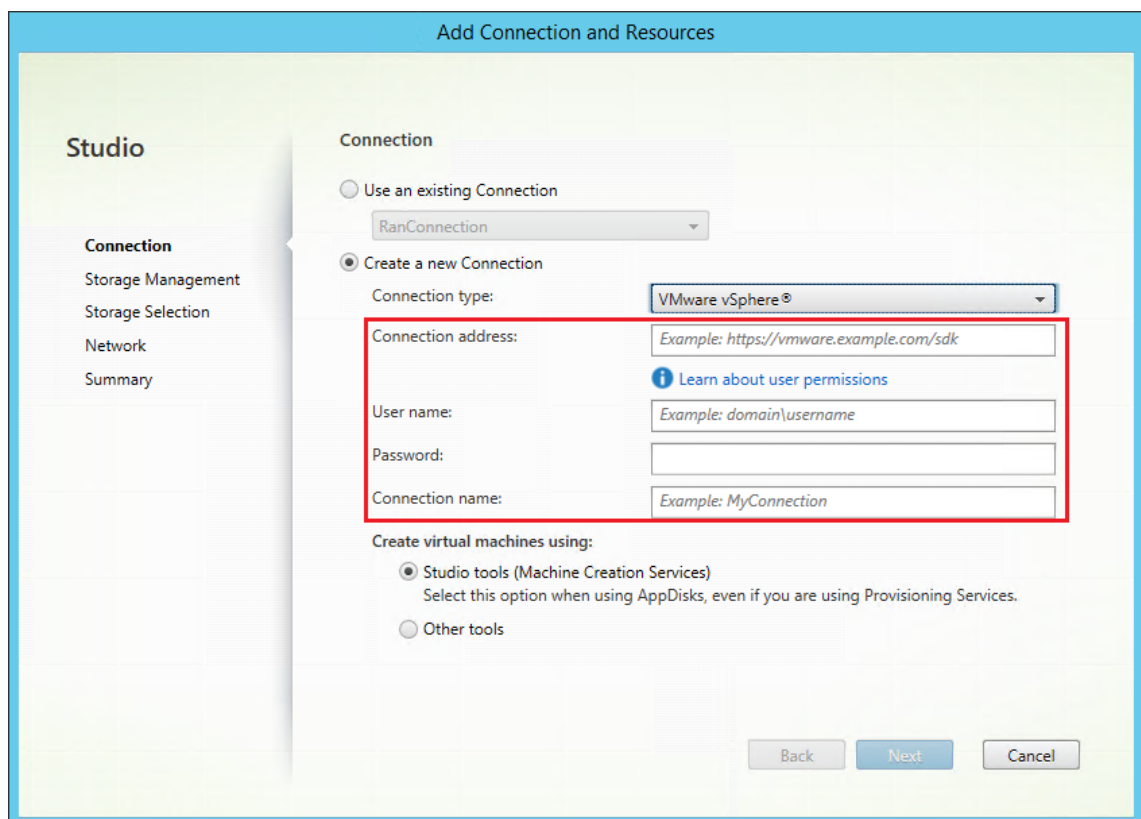
Create virtual machines using:

☒ Studio tools (Machine Creation Services)
Select this option when using AppDisks, even if you are using Provisioning Services.

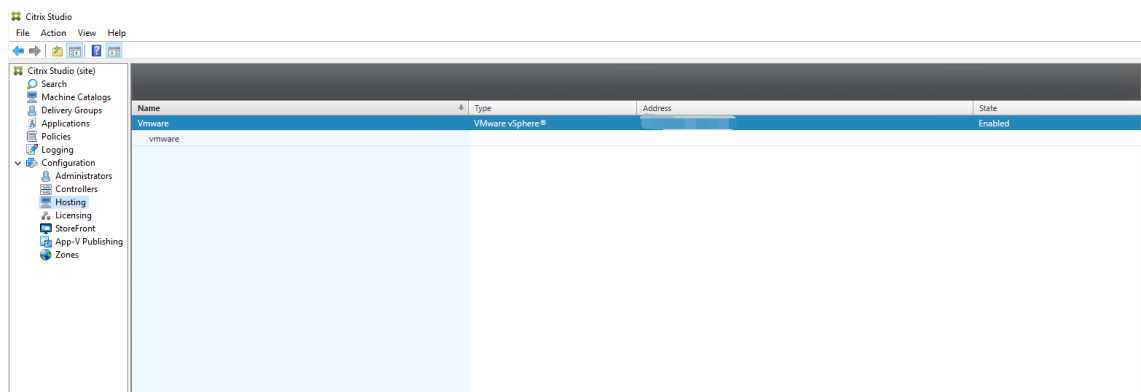
☐ Other tools

Back Next Cancel

4. Saisissez l'adresse de connexion (l'adresse URL du serveur vCenter) de votre compte VMware, votre nom d'utilisateur et votre mot de passe ainsi que votre nom de connexion.



Une nouvelle connexion apparaît dans le panneau d'hébergement.



Étape 2 : préparer une image principale

Une image principale contient le système d'exploitation, les applications non virtualisées, le VDA, et d'autres logiciels. Pour préparer une image principale, procédez comme suit :

Étape 2a : installer le package du Linux VDA sur la VM modèle

Remarque :

Pour utiliser un VDA en cours d'exécution comme VM modèle, omettez cette étape.

Avant d'installer le package VDA Linux sur la machine virtuelle modèle, installez .NET Core Runtime 3.1. Pour plus d'informations, consultez [Présentation de l'installation](#).

Selon votre distribution Linux, exécutez la commande suivante pour configurer l'environnement du Linux VDA :

Pour RHEL/CentOS :

```
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 12 :

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

Étape 2b : installer le référentiel EPEL qui contient ntfs-3g Installez le référentiel EPEL sur RHEL 8/CentOS 8, RHEL 7/CentOS 7 afin que l'exécution de `deploymcs.sh` installe ultérieurement le package `ntfs-3g` qu'il contient.

Étape 2c : installer manuellement ntfs-3g sur SUSE 12 Sur la plate-forme SUSE 12, 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 2d : configurer l'environnement d'exécution Avant d'exécuter `deploymcs.sh`, procédez comme suit :

- Modifiez les variables dans `/etc/xdl/mcs/mcs.conf`. Le fichier de configuration `mcs.conf` contient des variables pour la configuration de MCS et du Linux VDA. Vous trouverez ci-dessous quelques variables, dont `dns` et `AD_INTEGRATION` qui doivent être définies :

Remarque : si une variable peut être définie avec plusieurs valeurs, placez les valeurs entre guillemets simples et séparez-les par des espaces. Par exemple, `LDAP_LIST='aaa.lab:389 bbb.lab:389.'`

- `Use_Existing_Configurations_Of_Current_VDA` : détermine si les configurations existantes du VDA en cours d'exécution doivent être utilisées. 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 fichiers de configuration sur les machines créées avec MCS sont déterminés par des modèles de configuration sur l'image principale.
 - `dns` : définit l'adresse IP du DNS.
 - `AD_INTEGRATION` : définit Winbind ou SSSD (SSSD n'est pas pris en charge sur SUSE).
 - `WORKGROUP` : définit le nom du groupe de travail (sensible à la casse) s'il est configuré dans AD.
- 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 "0x00000003" --force
```

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

Étape 2e : créer une image principale

1. Exécutez `/opt/Citrix/VDA/sbin/deploymcs.sh`.
2. (Facultatif) 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/mcs/winbind_krb5.conf.tmpl` et `/etc/xdl/mcs/winbind_smb.conf.tmpl`.

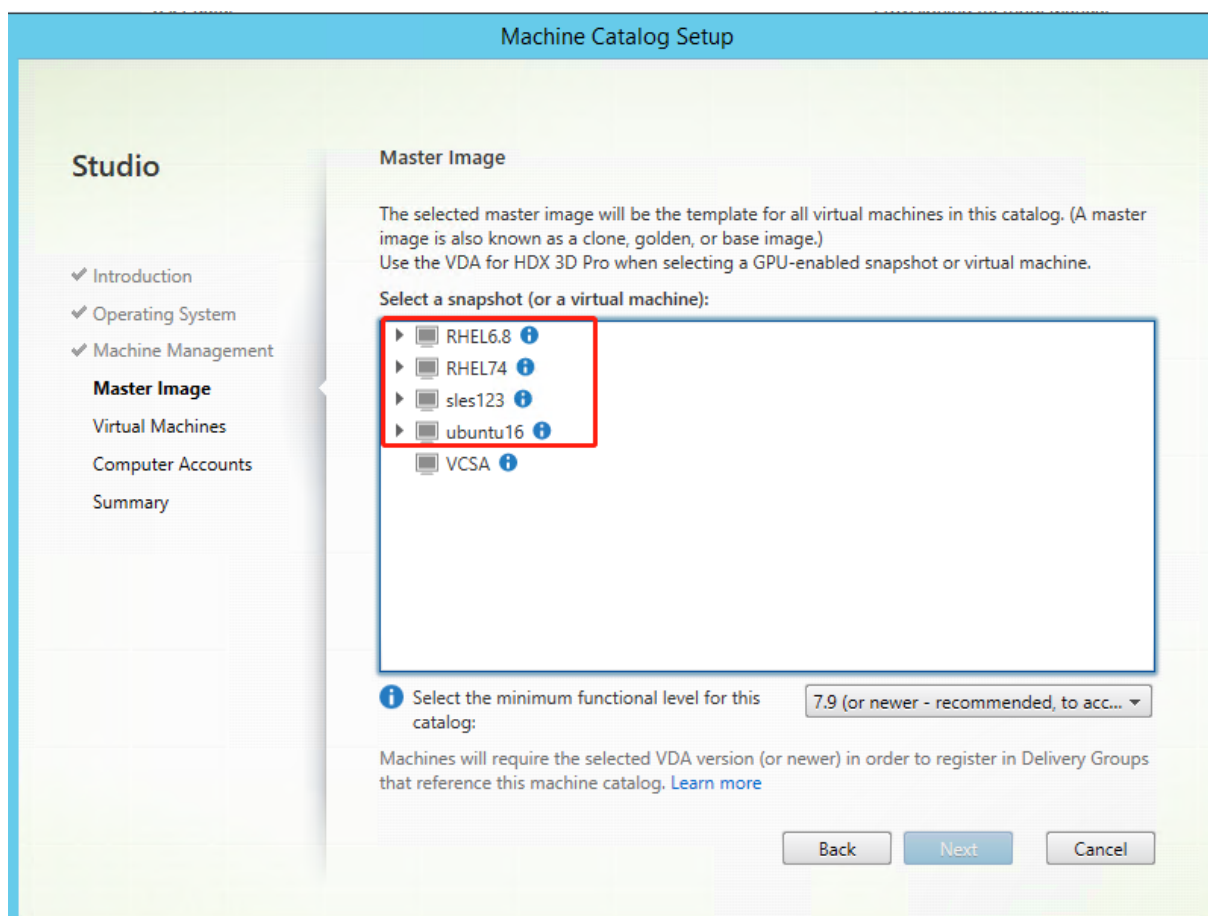
Pour les utilisateurs SSSD, mettez à jour les modèles `/etc/xdl/mcs/sss.conf.tmpl`, `/etc/xdl/mcs/sss_krb5.conf.tmpl` et `/etc/xdl/mcs/sss_smb.conf.tmpl`.

Remarque : conservez le format existant utilisé dans les fichiers de modèle et utilisez des variables telles que `$WORKGROUP`, `$REALM`, `$realm` et `$AD_FQDN`.

3. Après avoir installé les applications sur la VM modèle, fermez la VM modèle à partir du portail VMware. Prenez un instantané de la VM modèle.

Étape 3 : créer un catalogue de machines

Dans Citrix Studio, créez un catalogue de machines et spécifiez le nombre de VM à créer dans le catalogue. Lorsque vous créez le catalogue de machines, sélectionnez votre image principale dans la liste des instantanés.



Effectuez d'autres tâches de configuration si nécessaire. Pour plus d'informations, consultez l'article [Créer un catalogue de machines à l'aide de Studio](#).

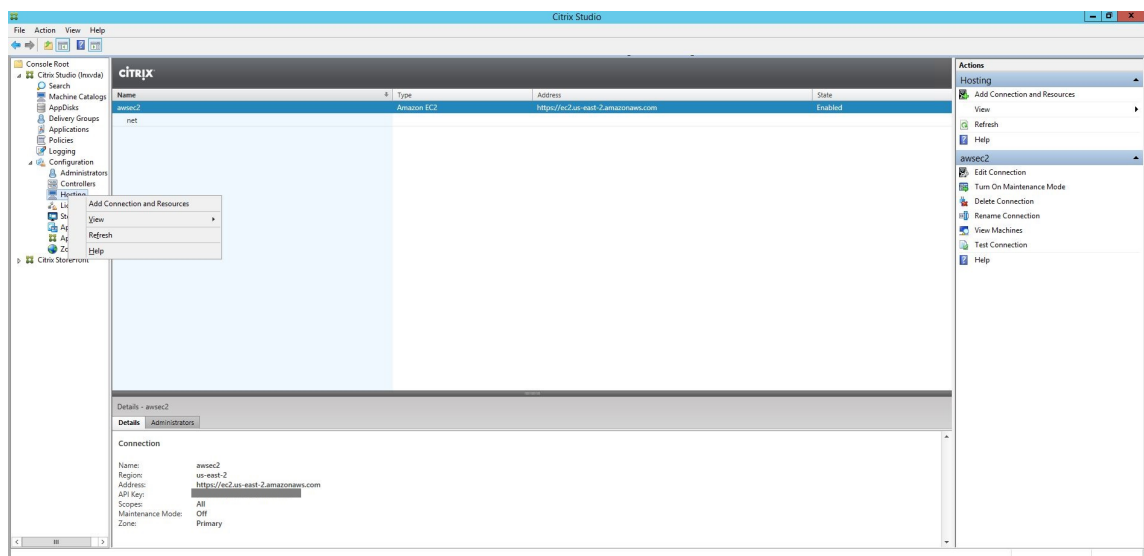
Étape 4 : créer un groupe de mise à disposition

Un groupe de mise à disposition est une collection de machines sélectionnées à partir d'un ou de plusieurs catalogues de machines. Le groupe de mise à disposition spécifie quels utilisateurs peuvent utiliser ces machines, ainsi que les applications et bureaux disponibles auprès de ces utilisateurs. Pour plus d'informations, consultez la section [Créer des groupes de mise à disposition](#).

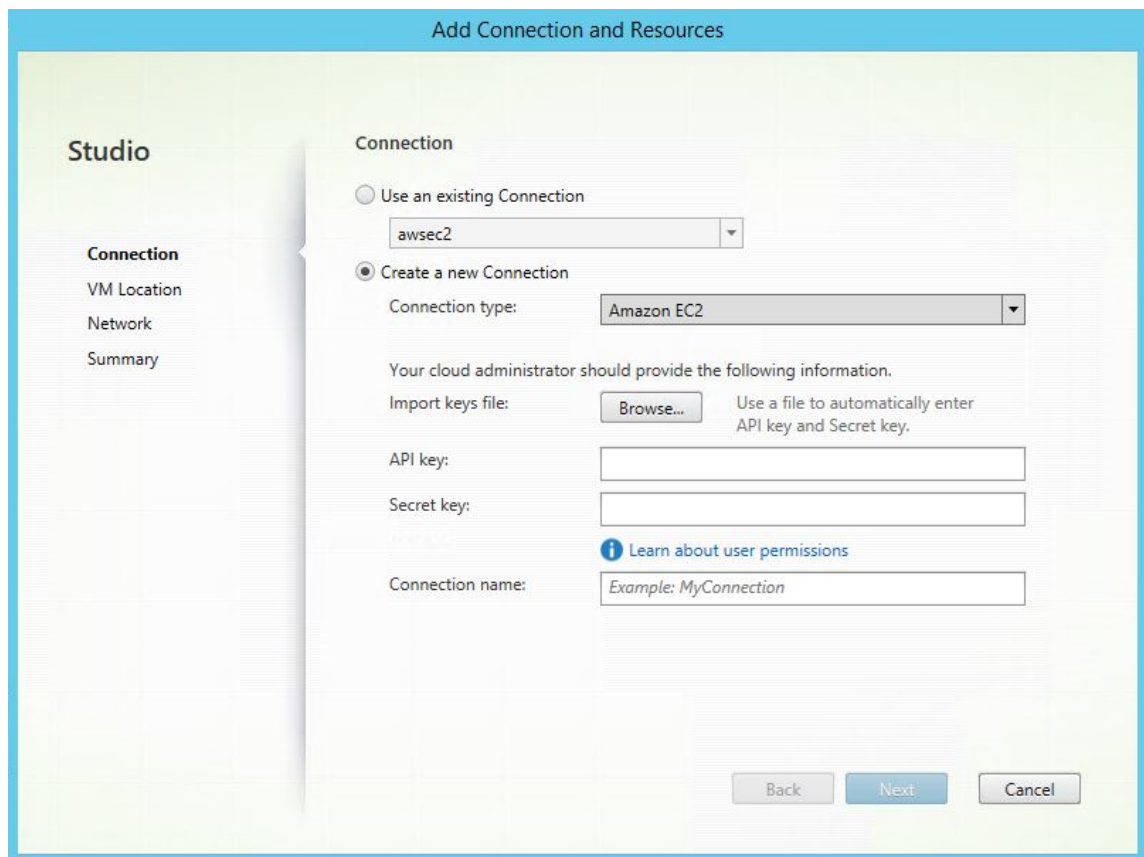
Utiliser MCS pour créer des machines virtuelles Linux sur AWS

Étape 1 : créer une connexion d'hébergement à AWS dans Citrix Studio

1. Dans Citrix Studio, sur Citrix Cloud, sélectionnez **Configuration > Hébergement > Ajouter une connexion et des ressources** pour créer une connexion à AWS.



2. Choisissez le type de connexion **Amazon EC2**.



3. Entrez la clé API et la clé secrète de votre compte AWS, puis entrez le nom de votre connexion.

Add Connection and Resources

Studio

- Connection
- VM Location
- Network
- Summary

Connection

☐ Use an existing Connection

awsec2

☒ Create a new Connection

Connection type: Amazon EC2

Your cloud administrator should provide the following information.

Import keys file: Use a file to automatically enter API key and Secret key.

API key:

Secret key:

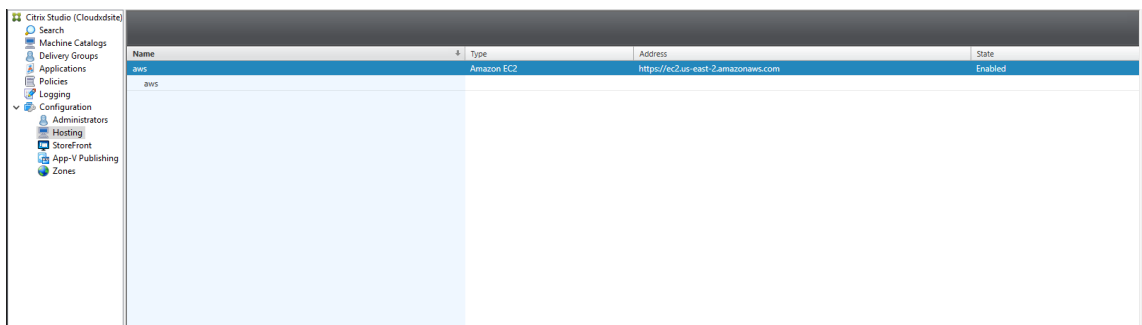
[Learn about user permissions](#)

Connection name:

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 :

- Connectez-vous aux services AWS.
- Accédez à la console Identity and Access Management (IAM).
- Dans le panneau de navigation de gauche, choisissez **Users**.
- Sélectionnez l’utilisateur cible et faites défiler vers le bas pour sélectionner l’onglet **Security credentials**.
- Faites défiler vers le bas et cliquez sur **Create access key**. Une nouvelle fenêtre apparaît.
- Cliquez sur **Download .csv file** et enregistrez la clé d’accès dans un emplacement sécurisé.

Une nouvelle connexion apparaît dans le panneau d’hébergement.



Étape 2 : préparer une image principale

Une image principale contient le système d'exploitation, les applications non virtualisées, le VDA, et d'autres logiciels. Pour préparer une image principale, procédez comme suit :

Étape 2a : Configurer cloud init

1. Pour vous assurer que le nom d'hôte du VDA soit préservé lorsqu'une instance EC2 est redémarrée ou arrêtée, exécutez la commande suivante.

```
1 echo "preserve_hostname: true" > /etc/cloud/cloud.cfg.d/99_hostname.cfg
```

Pour Ubuntu 18.04, assurez-vous que les lignes suivantes sont présentes sous la section `system_info` du fichier `/etc/cloud/cloud.cfg` :

```
1 system_info:
2   network:
3     renderers: ['netplan', 'eni', 'sysconfig']
```

2. Pour utiliser SSH pour accéder à distance aux machines virtuelles créées avec MCS sur AWS, activez l'authentification par mot de passe car aucun nom de clé n'est attaché à ces machines virtuelles. Au besoin, procédez comme suit.

- Modifiez le fichier de configuration `cloud-init`, `/etc/cloud/cloud.cfg`. Assurez-vous que la ligne **`ssh_pwauth: true`** est présente. Supprimez la ligne **`set-password`** et les lignes suivantes si elles existent ou ajoutez des commentaires.

```
1 users:
2   - default
```

- Si vous souhaitez utiliser l'utilisateur par défaut `ec2-user` ou `ubuntu` créé par `cloud-init`, vous pouvez modifier le mot de passe utilisateur à l'aide de la commande `passwd`. Conservez le nouveau mot de passe pour une utilisation ultérieure pour vous connecter aux machines virtuelles créées avec MCS.

- Modifiez le fichier `/etc/ssh/sshd_config` pour vous assurer que la ligne suivante est présente :

```
1 PasswordAuthentication yes
```

Enregistrez le fichier et exécutez la commande `sudo service sshd restart`.

Étape 2b : installer le package du Linux VDA sur la VM modèle

Remarque :

Pour utiliser un VDA en cours d'exécution comme VM modèle, omettez cette étape.

Avant d'installer le package VDA Linux sur la machine virtuelle modèle, installez .NET Core Runtime 3.1. Pour plus d'informations, consultez [Présentation de l'installation](#).

Selon votre distribution Linux, exécutez la commande suivante pour configurer l'environnement du Linux VDA :

Pour RHEL/CentOS :

```
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 12 :

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

Étape 2c : installer le référentiel EPEL qui contient ntfs-3g Installez le référentiel EPEL sur RHEL 8/CentOS 8, RHEL 7/CentOS 7 afin que l'exécution de `deploymcs.sh` installe ultérieurement le package `ntfs-3g` qu'il contient.

Étape 2d : installer manuellement ntfs-3g sur SUSE 12 Sur la plate-forme SUSE 12, 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 2e : configurer l'environnement d'exécution Avant d'exécuter `deploymcs.sh`, procédez comme suit :

- Modifiez les variables dans `/etc/xdl/mcs/mcs.conf`. Le fichier de configuration `mcs.conf` contient des variables pour la configuration de MCS et du Linux VDA. Vous trouverez ci-dessous quelques variables, dont `dns` et `AD_INTEGRATION` qui doivent être définies :

Remarque : si une variable peut être définie avec plusieurs valeurs, placez les valeurs entre guillemets simples et séparez-les par des espaces. Par exemple, `LDAP_LIST='aaa.lab:389 bbb.lab:389.'`

- `Use_Existing_Configurations_Of_Current_VDA` : détermine si les configurations existantes du VDA en cours d'exécution doivent être utilisées. 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 fichiers de configuration sur les machines créées avec MCS sont déterminés par des modèles de configuration sur l'image principale.
 - `dns` : définit l'adresse IP du DNS.
 - `AD_INTEGRATION` : définit Winbind ou SSSD (SSSD n'est pas pris en charge sur SUSE).
 - `WORKGROUP` : définit le nom du groupe de travail (sensible à la casse) s'il est configuré dans AD.
- 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 "0x00000003" --force
```

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

Étape 2f : créer une image principale

1. Exécutez `/opt/Citrix/VDA/sbin/deploymcs.sh`.
2. (Facultatif) 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/mcs/winbind_krb5.conf.tpl` et `/etc/xdl/mcs/winbind_smb.conf.tpl`.

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

Remarque : conservez le format existant utilisé dans les fichiers de modèle et utilisez des variables telles que `$WORKGROUP`, `$REALM`, `$realm` et `$AD_FQDN`.

3. 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**.
4. 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

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	40	General Purpose SSD (gp2)	120 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

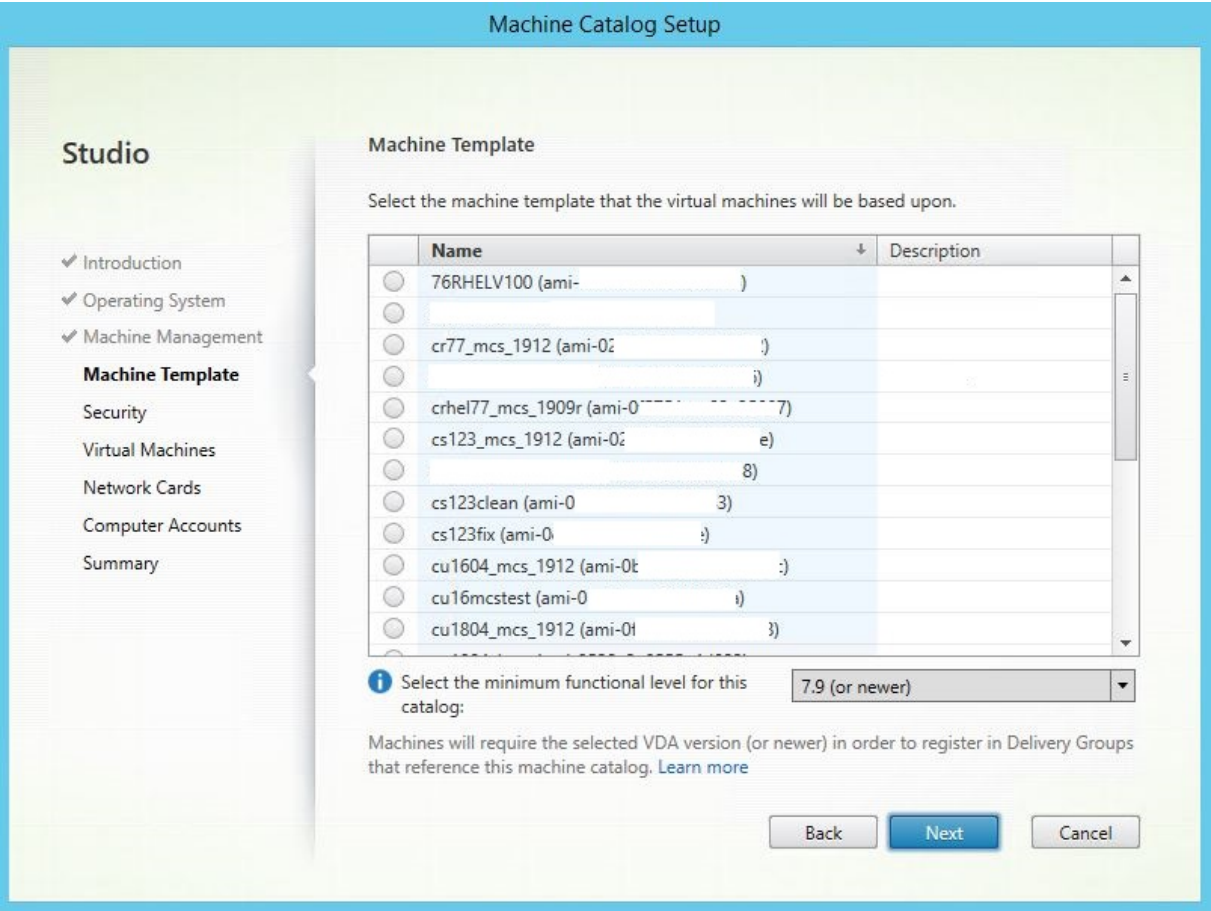
Total size of EBS Volumes: 40 GiB
When you create an EBS image, an EBS snapshot will also be created for each of the above volumes.

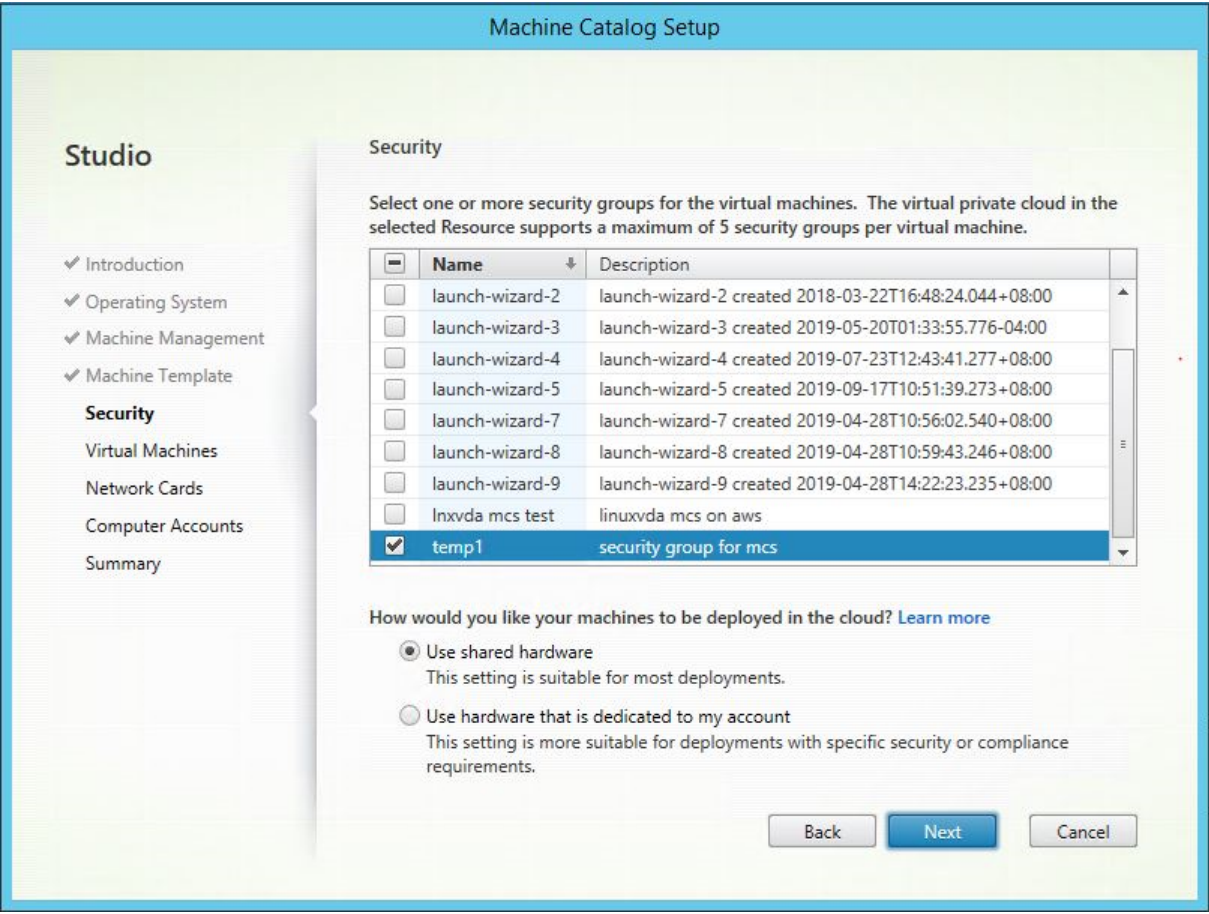
Cancel

Create Image

Étape 3 : créer un catalogue de machines

Dans Citrix Studio, créez un catalogue de machines et spécifiez le nombre de VM à créer dans le catalogue. Lors de la création du catalogue de machines, choisissez votre machine modèle (l’image principale que vous avez créée précédemment) et sélectionnez un ou plusieurs groupes de sécurité.





Effectuez d’autres tâches de configuration si nécessaire. Pour plus d’informations, consultez l’article [Créer un catalogue de machines à l’aide de Studio](#).

Étape 4 : 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. Le groupe de mise à disposition spécifie quels utilisateurs peuvent utiliser ces machines, ainsi que les applications et bureaux disponibles auprès de ces utilisateurs. Pour plus d’informations, consultez la section [Créer des groupes de mise à disposition](#).

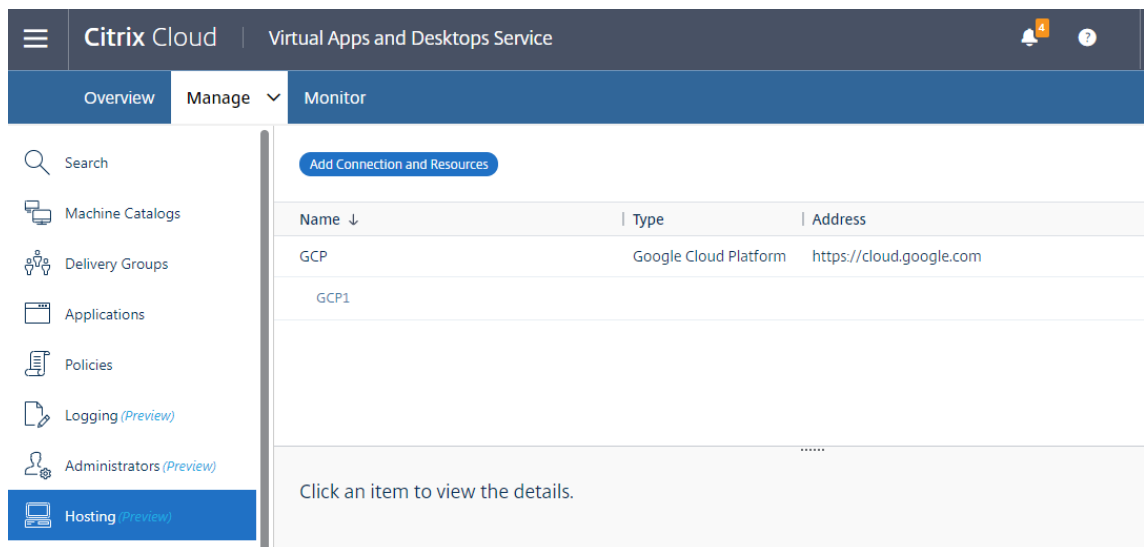
Utiliser MCS pour créer des machines virtuelles Linux sur GCP

Étape 1 : configurer votre environnement GCP

Pour plus d’informations, voir [Environnements de virtualisation Google Cloud Platform](#).

Étape 2 : créer une connexion d'hébergement à GCP dans Citrix Studio

1. Dans Citrix Studio, sur Citrix Cloud, sélectionnez **Configuration > Hébergement > Ajouter une connexion et des ressources** pour créer une connexion à GCP.



2. Sélectionnez **Google Cloud Platform** comme type de connexion.

Add Connection and Resources

1 Connection

2 Region

3 Network

4 Summary

Create a new Connection

Connection type: Google Cloud Platform

Service account key: Import key...

Service account ID:

Zone name: GCP

Connection name:

Create virtual machines using:
☒ Studio tools (Machine Creation Services)
☐ Other tools

Next

Cancel

3. Importez la clé de compte de service de votre compte GCP et saisissez votre nom de connexion.

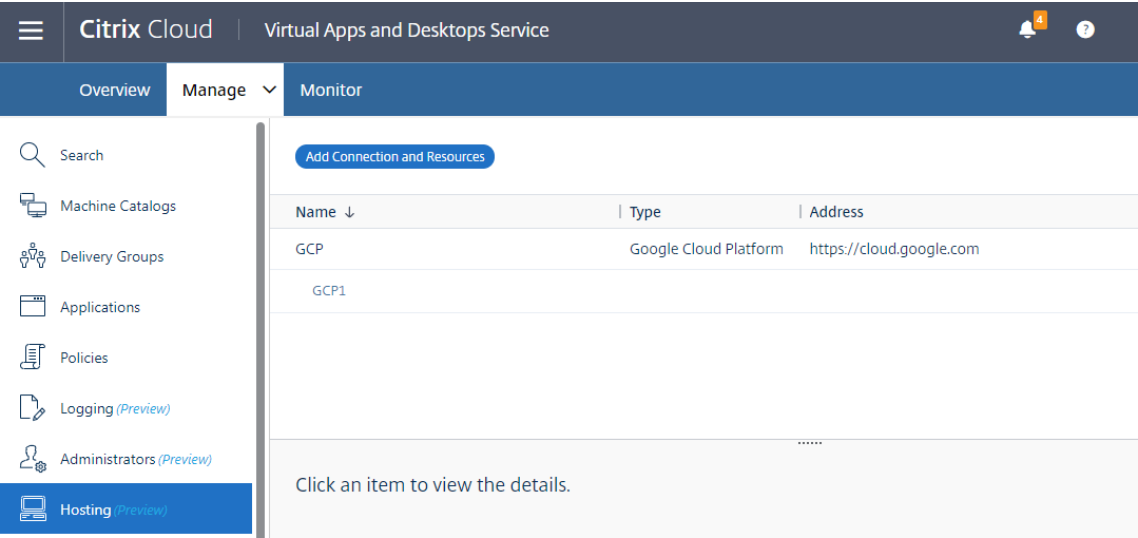
Google Cloud Platform Service Account Credentials

Paste the key contained in your Google service account credential file (.json).

Save

Cancel

Une nouvelle connexion apparaît dans le panneau d’hébergement.



Étape 3 : préparer une image principale

Une image principale contient le système d’exploitation, les applications non virtualisées, le VDA, et d’autres logiciels. Pour préparer une image principale, procédez comme suit :

Étape 3a : installer le package du Linux VDA sur la VM modèle

Remarque :

Pour utiliser un VDA en cours d'exécution comme VM modèle, omettez cette étape.

Avant d'installer le package VDA Linux sur la machine virtuelle modèle, installez .NET Core Runtime 3.1. Pour plus d'informations, consultez [Présentation de l'installation](#).

Selon votre distribution Linux, exécutez la commande suivante pour configurer l'environnement du Linux VDA :

Pour RHEL/CentOS :

```
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 12 :

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

Étape 3b : installer le référentiel EPEL qui contient ntfs-3g Installez le référentiel EPEL sur RHEL 8/CentOS 8, RHEL 7/CentOS 7 afin que l'exécution de `deploymcs.sh` installe ultérieurement le package `ntfs-3g` qu'il contient.

Étape 3c : installer manuellement ntfs-3g sur SUSE 12 Sur la plate-forme SUSE 12, 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 3d : configurer l'environnement d'exécution Avant d'exécuter `deploymcs.sh`, procédez comme suit :

- Modifiez les variables dans `/etc/xdl/mcs/mcs.conf`. Le fichier de configuration `mcs.conf` contient des variables pour la configuration de MCS et du Linux VDA. Vous trouverez ci-dessous quelques variables, dont `dns` et `AD_INTEGRATION` qui doivent être définies :

Remarque : si une variable peut être définie avec plusieurs valeurs, placez les valeurs entre guillemets simples et séparez-les par des espaces. Par exemple, `LDAP_LIST='aaa.lab:389 bbb.lab:389.'`

- `Use_Existing_Configurations_Of_Current_VDA` : détermine si les configurations existantes du VDA en cours d'exécution doivent être utilisées. 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 fichiers de configuration sur les machines créées avec MCS sont déterminés par des modèles de configuration sur l'image principale.
 - `dns` : définit l'adresse IP du DNS.
 - `AD_INTEGRATION` : définit Winbind ou SSSD (SSSD n'est pas pris en charge sur SUSE).
 - `WORKGROUP` : définit le nom du groupe de travail (sensible à la casse) s'il est configuré dans AD.
- 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 "0x00000003" --force
```



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

Étape 3e : créer une image principale

1. Exécutez `/opt/Citrix/VDA/sbin/deploymcs.sh`.
2. (Facultatif) 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/mcs/winbind_krb5.conf.tpl` et `/etc/xdl/mcs/winbind_smb.conf.tpl`.

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

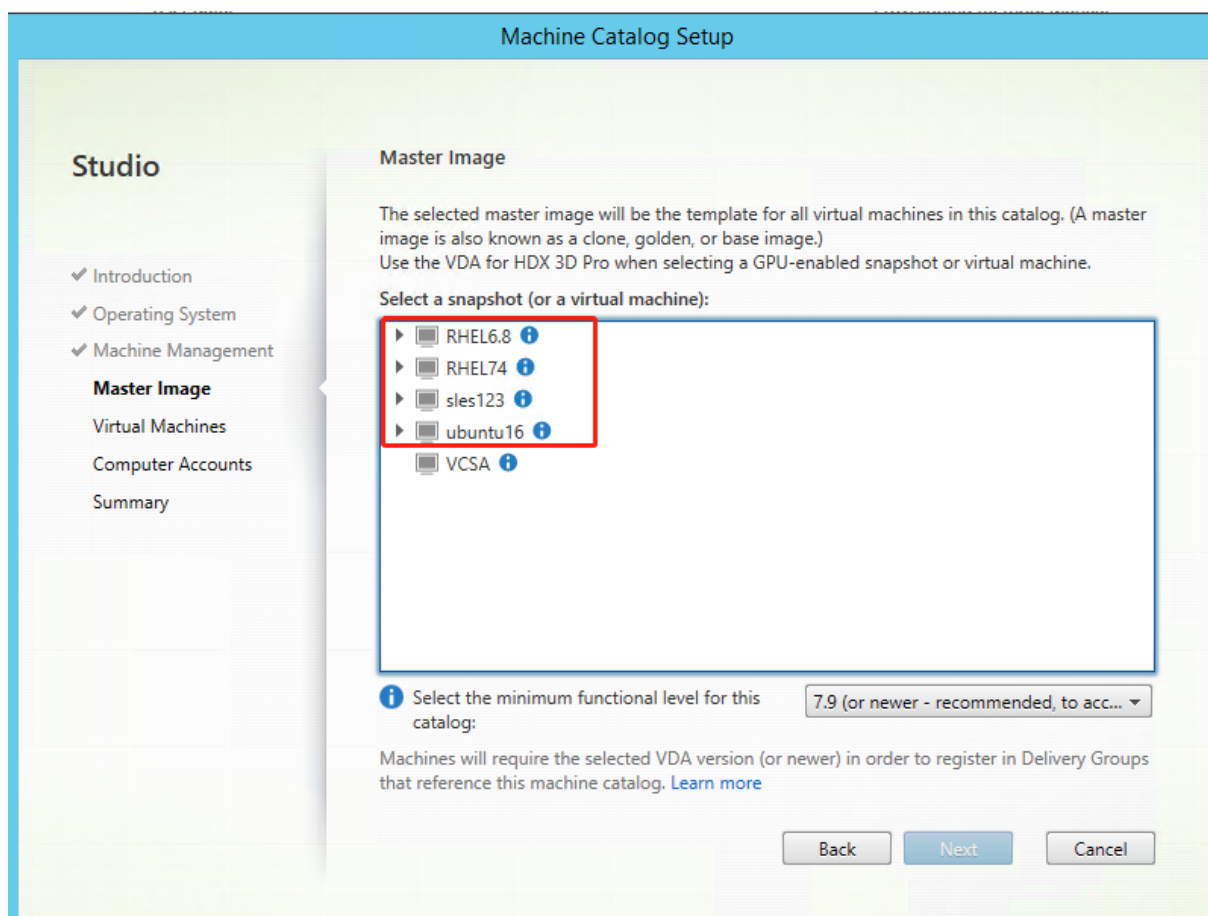
Remarque :

Conservez le format existant utilisé dans les fichiers de modèle et utilisez des variables telles que `$WORKGROUP`, `$REALM`, `$realm` et `$AD_FQDN`.

3. Après avoir installé les applications sur la VM modèle, fermez la VM modèle à partir du portail VMware. Prenez un instantané de la VM modèle.

Étape 4 : créer un catalogue de machines

Dans Citrix Studio, créez un catalogue de machines et spécifiez le nombre de VM à créer dans le catalogue. Lorsque vous créez le catalogue de machines, sélectionnez votre image principale dans la liste des instantanés.



Effectuez d'autres tâches de configuration si nécessaire. Pour plus d'informations, consultez l'article [Créer un catalogue de machines à l'aide de Studio](#).

Étape 5 : créer un groupe de mise à disposition

Un groupe de mise à disposition est une collection de machines sélectionnées à partir d'un ou de plusieurs catalogues de machines. Le groupe de mise à disposition spécifie quels utilisateurs peuvent utiliser ces machines, ainsi que les applications et bureaux disponibles auprès de ces utilisateurs. Pour plus d'informations, consultez la section [Créer des groupes de mise à disposition](#).

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

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

1. Vérifiez que vous avez installé .NET Core Runtime 3.1 avant de mettre à niveau votre VDA Linux vers la version actuelle.
2. Mettez à niveau votre Linux VDA sur la machine modèle :

Pour RHEL 7 et CentOS 7 :

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

Pour RHEL 8 et CentOS 8 :

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

Pour SUSE 12 :

```
1 sudo rpm -U XenDesktopVDA-<version>.sle12_x.x86_64.rpm
```

Pour Ubuntu 16.04 :

```
1 sudo dpkg -i xendesktopvda_<version>.ubuntu16.04_amd64.deb
```

Pour Ubuntu 18.04 :

```
1 sudo dpkg -i xendesktopvda_<version>.ubuntu18.04_amd64.deb
```

Pour Ubuntu 20.04 :

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

3. Modifiez `/etc/xdl/mcs/mcs.conf` et `/etc/xdl/mcs/mcs_local_setting.reg`.
4. Prenez un nouvel instantané.
5. Dans Citrix Studio, sélectionnez le nouvel instantané pour la mise à jour de votre catalogue de machines. Attendez avant que chaque machine redémarre. Ne redémarrez pas une machine manuellement.

Automatiser les mises à jour du mot de passe du compte de machine

Par défaut, les mots de passe du compte de machine expirent 30 jours après la création du catalogue de machines. Pour empêcher l'expiration du mot de passe et automatiser les mises à jour du mot de passe du compte de machine, procédez comme suit :

1. Ajoutez l'entrée suivante dans `/etc/xdl/mcs/mcs.conf` avant d'exécuter `/opt/Citrix/VDA/sbin/deploymcs.sh`.

```
UPDATE_MACHINE_PW="enabled"
```

2. Après avoir exécuté `/opt/Citrix/VDA/sbin/deploymcs.sh`, ouvrez `/etc/cron.d/mcs_update_password_cronjob` pour définir l'heure et la fréquence de mise à jour. Le paramètre par défaut met à jour les mots de passe du compte de machine chaque semaine à 2 h 30, le dimanche.

Après chaque mise à jour du mot de passe du compte de machine, le cache des tickets sur le Delivery Controller n'est plus valide et l'erreur suivante peut apparaître dans `/var/log/xdl/jproxy.log` :

[ERROR] - AgentKerberosServiceAction.Run: GSSException occurred.
Error: Failure unspecified at GSS-API level (Mechanism level:
Checksum failed)

Pour éliminer l'erreur, videz le cache des tickets régulièrement. Vous pouvez planifier une tâche de nettoyage du cache sur tous les Delivery Controller ou sur le contrôleur de domaine.

Activer FAS sur les VM créées par MCS

Vous pouvez activer FAS sur les VM créées par MCS qui s'exécutent sur les distributions suivantes :

	Winbind	SSSD	Centrify
RHEL 8, CentOS 8	Oui	Non	Non
RHEL 7, CentOS 7	Oui	Oui	Non
Ubuntu 20.04	Oui	Non	Non
Ubuntu 18.04	Oui	Non	Non
Ubuntu 16.04	Oui	Non	Non
Debian 10.7	Oui	Non	Non
SUSE 12.5	Oui	Non	Non

Activer FAS lorsque vous préparez une image principale sur la VM modèle

1. Exécutez le script `opt/Citrix/VDA/sbin/ctxinstall.sh` et définissez toutes les variables d'environnement conformément à la liste des serveurs FAS. Pour plus d'informations sur les variables d'environnement, consultez la section [Easy Install](#).

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

2. Importez le certificat d'autorité de certification racine.

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

3. Exécutez `ctxfascfg.sh`.

4. Définissez les variables dans `/etc/xdm/mcs/mcs.conf`.

- a) Définissez la valeur de `Use_Existing_Configurations_Of_Current_VDA` sur Y.
- b) Définissez la variable `FAS_LIST` sur votre adresse de serveur FAS ou sur plusieurs adresses de serveur FAS séparées par des points-virgules et entourées de guillemets, par exemple, `FAS_LIST="<FAS_SERVER_FQDN>;<FAS_SERVER_FQDN>"`.

- c) Définissez les autres variables selon vos besoins, par exemple `VDI_MODE`.
5. 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`.
 - a) Définissez la valeur de `Use_Existing_Configurations_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`.

Remarque :

vous devez définir toutes les variables nécessaires dans `/etc/xdl/mcs/mcs.conf` car ces variables sont appelées au démarrage de la VM.

Installer Linux Virtual Delivery Agent pour RHEL/CentOS

August 21, 2024

Vous pouvez choisir de suivre les étapes dans cet article pour l'installation manuelle ou [easy install](#) pour l'installation et la configuration automatiques. Easy Install permet des gains de temps et de main d'œuvre et il est plus fiable que l'installation manuelle.

Remarque :

Utilisez [Easy Install](#) uniquement pour les nouvelles installations. N'utilisez pas Easy Install pour mettre à jour une installation existante.

Étape 1 : préparer RHEL 8/CentOS 8, RHEL 7/CentOS 7 pour l'installation sur un VDA

Étape 1a : vérifier la configuration réseau

Nous vous recommandons de disposer d'un réseau connecté et correctement configuré avant de continuer.

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. 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 (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 peut entraîner des problèmes de décalage d'horloge. Pour cette raison, il est recommandé de synchroniser l'heure avec un service de temps à distance.

Un environnement par défaut RHEL 8/RHEL 7 utilise le démon Chrony ([chronyd](#)) pour la synchronisation de l'horloge.

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

```
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 /sbin/service chronyd restart
```

Étape 1g : installer OpenJDK

Le Linux VDA dépend de OpenJDK. L'environnement d'exécution est généralement installé dans le cadre de l'installation du système d'exploitation.

Vérifiez que la version est correcte :

```
1 sudo yum info java-1.8.0-openjdk
```

Le OpenJDK préconditionné peut être une version antérieure. Mettez à jour vers la dernière version :

```
1 sudo yum -y update java-1.8.0-openjdk
```

Ouvrez un nouveau shell et vérifiez la version de Java :

```
1 java -version
```

Conseil :

Pour éviter les échecs d'enregistrement auprès du Delivery Controller, assurez-vous d'avoir installé uniquement OpenJDK 1.8.0. Supprimez toutes les autres versions de Java de votre système.

Étape 1h : installer PostgreSQL

Linux VDA requiert PostgreSQL 10.5 ou version ultérieure sur RHEL 8 ou PostgreSQL 9.2 ou version ultérieure sur RHEL 7.

Installez les packages suivants :

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

L'étape de post-installation suivante est requise pour initialiser la base de données et s'assurer que le service est lancé au démarrage de la machine. Cette opération crée les fichiers de base de données sous **/var/lib/pgsql/data**. Cette commande diffère entre PostgreSQL 10 et 9 :

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


Étape 1i : démarrer PostgreSQL

Une fois la machine démarrée, démarrez le service immédiatement :

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

Vérifiez la version de PostgreSQL avec :

```
1 psql --version
```

(RHEL 7 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'
```

Étape 2 : préparer l'hyperviseur

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

Corriger la synchronisation de l'heure sur Citrix Hypervisor

Si la fonctionnalité de synchronisation de l'heure de Citrix Hypervisor est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée car NTP et Citrix Hypervisor tenteront de gérer l'horloge du 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.

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

```
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 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 car l'hyperviseur et NTP tenteront de synchroniser l'hor-

loge du système. Pour éviter que l'horloge ne soit plus synchronisée avec d'autres serveurs, assurez-vous l'horloge du système de chaque invité Linux est synchronisée avec NTP. Cela nécessite la désactivation de la synchronisation de l'heure de l'hôte.

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

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

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

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

- [Samba Winbind](#)
- [Quest Authentication Services](#)
- [Centrify DirectControl](#)
- [SSSD](#)
- [PBIS](#) (compatible avec RHEL 7 uniquement)

Suivez les instructions en fonction de la méthode choisie.

Remarque :

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

Samba Winbind

Installez ou mettez à jour les packages requis :

Pour RHEL 8/CentOS 8 :

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

Pour RHEL 7/CentOS 7 :

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

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 8 :

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

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

Dans la section [libdefaults] :

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

Dans la section [realms] :

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

Dans la section [domain_realm] :

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

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

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

RHEL 8 :

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

RHEL 7 :

```
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 /sbin/service winbind restart
```

Conseil :

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

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

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

Vérifier l'appartenance à un domaine Le 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 4 : 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'ou-

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.

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 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 4 : 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 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 4 : 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`.

Cette section décrit les approches `Samba` et `adcli` pour RHEL 7 et RHEL 8 respectivement. Pour `realmd`, reportez-vous à la documentation de RHEL ou CentOS. Ces étapes doivent être suivies avant la configuration de SSSD.

- **Samba (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 :

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

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

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

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

```
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 8) :**

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) :

```
1 [sssd]
2 config_file_version = 2
3 domains = ad.example.com
4 services = nss, pam
5
6 [domain/ad.example.com]
7 # Uncomment if you need offline logins
8 # cache_credentials = true
9
10 id_provider = ad
11 auth_provider = ad
12 access_provider = ad
13 ldap_id_mapping = true
14 ldap_schema = ad
15
16 # Should be specified as the lower-case version of the long version of
17   the Active Directory domain.
18 ad_domain = ad.example.com
19
20 # Kerberos settings
21 krb5_ccachedir = /tmp
22 krb5_ccname_template = FILE:%d/krb5cc_%U
23
24 # Uncomment if service discovery is not working
25 # ad_server = server.ad.example.com
26
27 # Comment out if the users have the shell and home dir set on the AD
28   side
29 default_shell = /bin/bash
30 fallback_homedir = /home/%d/%u
31
32 # Uncomment and adjust if the default principal SHORTNAME$@REALM is not
33   available
34 # ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
```

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

(RHEL 8 uniquement)

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

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

Définissez les autorisations et les propriétaires du fichier `sssd.conf` :

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

Activer SSSD RHEL 8 :

Exécutez les commandes suivantes pour activer SSSD :

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

RHEL 7/CentOS 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 service sssd start
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 4 : 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/8.8.0/
  pbis-open-8.8.0.506.linux.x86_64.rpm.sh
```

Rendre le script d'installation PBIS exécutable Par exemple :

```
1 chmod +x pbis-open-8.8.0.506.linux.x86_64.rpm.sh
```

Exécuter le script d'installation PBIS Par exemple :

```
1 sh pbis-open-8.8.0.506.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 4 : installer le Linux VDA](#) après vérification de la jonction du domaine.

Étape 4 : installer le Linux VDA

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

Pour effectuer une nouvelle installation

1. (Facultatif) Désinstaller l'ancienne version

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

a) Arrêtez les services Linux VDA :

```
1 sudo /sbin/service ctxvda stop
2
3 sudo /sbin/service ctxhdx stop
```

Remarque :

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

b) Désinstallez le package :

```
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

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

Pour RHEL 8/CentOS 8 :

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

Pour RHEL 7/CentOS 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 RHEL 8/CentOS 8 :

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

Pour RHEL 7/CentOS 7 :

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

Liste des dépendances RPM pour RHEL 8.2/CentOS 8.2 :

```
1 postgresql-jdbc >= 42.2.3
2
3 postgresql-server >= 10.6
4
5 java-1.8.0-openjdk >= 1.8.0
6
7 icoutils >= 0.32
8
9 firewallld >= 0.8.0
10
11 policycoreutils-python-utils >= 2.9
12
13 python3-policycoreutils >= 2.9
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 motif >= 2.3.4
36
37 pam >= 1.3.1
```

```
38
39  util-linux >= 2.32.1
40
41  util-linux-user >= 2.32.1
42
43  xorg-x11-utils >= 7.5
44
45  bash >= 4.4
46
47  findutils >= 4.6
48
49  gawk >= 4.2
50
51  sed >= 4.5
52
53  cups >= 2.2
54
55  foomatic-filters >= 4.0.9
56
57  cups-filters >= 1.20.0
58
59  ghostscript >= 9.25
60
61  libxml2 >= 2.9
62
63  libmspack >= 0.7
```

Liste des dépendances RPM pour RHEL 7/CentOS 7 :

```
1  postgresql-server >= 9.2
2
3  postgresql-jdbc >= 9.2
4
5  java-1.8.0-openjdk >= 1.8.0
6
7  ImageMagick >= 6.7.8.9
8
9  firewalld >= 0.3.9
10
11  polycoreutils-python >= 2.0.83
12
13  dbus >= 1.6.12
14
15  dbus-x11 >= 1.6.12
16
17  xorg-x11-server-utils >= 7.7
18
19  xorg-x11-xinit >= 1.3.2
20
21  libXpm >= 3.5.10
22
23  libXrandr >= 1.4.1
24
```

```
25  libXtst >= 1.2.2
26
27  motif >= 2.3.4
28
29  pam >= 1.1.8
30
31  util-linux >= 2.23.2
32
33  bash >= 4.2
34
35  findutils >= 4.5
36
37  gawk >= 4.0
38
39  sed >= 4.2
40
41  cups >= 1.6.0
42
43  foomatic-filters >= 4.0.9
44
45  openldap >= 2.4
46
47  cyrus-sasl >= 2.1
48
49  cyrus-sasl-gssapi >= 2.1
50
51  libxml2 >= 2.9
52
53  python-requests >= 2.6.0
54
55  gperftools-libs >= 2.4
56
57  rpmlib(FileDigests) <= 4.6.0-1
58
59  rpmlib(PayloadFilesHavePrefix) <= 4.0-1
60
61  pmlib(CompressedFileNames) <= 3.0.4-1
62
63  rpmlib(PayloadIsXz) <= 5.2-1
```

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](#).

Remarque :

Après avoir installé le Linux VDA sur RHEL 7.x, exécutez la commande `sudo yum install -y`

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

Pour effectuer une mise à niveau d'une installation existante

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

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

Pour RHEL 7/CentOS 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 RHEL 7/CentOS 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 5 : installer les pilotes NVIDIA GRID

Pour activer HDX 3D Pro, des étapes d'installation supplémentaires sont requises pour installer les pilotes graphiques nécessaires sur l'hyperviseur, ainsi que sur les machines VDA.

Configurez ce qui suit :

1. Citrix Hypervisor
2. VMware ESX

Suivez les instructions pour l'hyperviseur choisi.

Citrix Hypervisor:

Cette section détaillée décrit l'installation et la configuration des pilotes NVIDIA GRID sur [Citrix Hypervisor](#).

VMware ESX :

Suivez les informations contenues dans ce guide pour installer et configurer les pilotes NVIDIA GRID pour [VMware ESX](#).

Machines VDA :

Suivez ces étapes pour installer et configurer les pilotes pour chaque invité de VM Linux :

1. Avant de commencer, assurez-vous que la VM Linux est arrêtée.
2. Dans XenCenter, ajoutez un processeur graphique en mode GPU pass-through à la VM.
3. Démarrez la VM RHEL.

Pour préparer la machine pour les pilotes NVIDIA GRID, exécutez les commandes suivantes :

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

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.

Configuration automatique

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

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

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

- **CTX_XDL_SITE_NAME=dns-name** : le Linux VDA découvre les serveurs LDAP à l'aide de DNS. Pour limiter les résultats de recherche DNS à un site local, spécifiez un nom de site DNS. Cette variable est définie sur **<none>** par défaut.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** : le Linux VDA envoie une requête vers le DNS pour découvrir les serveurs LDAP. Si DNS ne peut pas fournir d'enregistrements de service LDAP, vous pouvez entrer une liste séparée par des espaces de noms de domaines complets LDAP avec ports LDAP. Par exemple, ad1.mycompany.com:389. Cette variable est définie sur **<none>** par défaut.
- **CTX_XDL_SEARCH_BASE=search-base-set** : le Linux VDA envoie une requête à LDAP via une base de recherche définie sur la racine du domaine Active Directory (par exemple, D, DC=mycompany,DC=com). Pour améliorer les performances de recherche, vous pouvez spécifier une base de recherche (par exemple, OU=VDI,DC=mycompany,DC=com). Cette variable est définie sur **<none>** par défaut.
- **CTX_XDL_FAS_LIST='list-fas-servers'** : les serveurs du service d'authentification fédérée (FAS) sont configurés via la stratégie de groupe AD. Le Linux VDA ne prend pas en charge la stratégie de groupe AD mais vous pouvez fournir une liste de serveurs FAS séparés par des points-virgules. La séquence doit être la même que celle configurée dans la stratégie de groupe AD. Si une adresse de serveur est supprimée, remplissez son espace vide avec la chaîne de texte **<none>** et ne modifiez pas l'ordre des adresses de serveur.
- **CTX_XDL_DOTNET_runtime_path=Path-to-install-dotnet-runtime** : chemin d'accès à l'installation de .NET Core Runtime 3.1 pour la prise en charge du nouveau Broker Agent Service ([ctxvda](#)). Le chemin par défaut est /usr/bin.
- **CTX_XDL_START_SERVICE = Y | N** : indique si les services Linux VDA sont lancés lorsque la configuration de Linux VDA est terminée. Valeur définie sur Y par défaut.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** : port socket permettant d'écouter Citrix Scout. Le port par défaut est 7503.
- **CTX_XDL_TELEMETRY_PORT** : port de communication avec Citrix Scout. Le port par défaut est 7502.

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

```
1 export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N
2
3 export CTX_XDL_DDC_LIST='list-ddc-fqdns'
4
5 export CTX_XDL_VDA_PORT=port-number
6
7 export CTX_XDL_REGISTER_SERVICE=Y|N
8
9 export CTX_XDL_ADD_FIREWALL_RULES=Y|N
10
11 export CTX_XDL_AD_INTEGRATION=1|2|3|4|5
12
13 export CTX_XDL_HDX_3D_PRO=Y|N
```

```
14
15 export CTX_XDL_VDI_MODE=Y|N
16
17 export CTX_XDL_SITE_NAME=dns-site-name | '<none>'
18
19 export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'
20
21 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
22
23 export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'
24
25 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
26
27 export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number
28
29 export CTX_XDL_TELEMETRY_PORT=port-number
30
31 export CTX_XDL_START_SERVICE=Y|N
32
33 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
```

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

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

```
1 sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
2
3 CTX_XDL_DDC_LIST='list-ddc-fqdns' \
4
5 CTX_XDL_VDA_PORT=port-number \
6
7 CTX_XDL_REGISTER_SERVICE=Y|N \
8
9 CTX_XDL_ADD_FIREWALL_RULES=Y|N \
10
11 CTX_XDL_AD_INTEGRATION=1|2|3|4|5 \
12
13 CTX_XDL_HDX_3D_PRO=Y|N \
14
15 CTX_XDL_VDI_MODE=Y|N \
16
17 CTX_XDL_SITE_NAME=dns-name \
18
19 CTX_XDL_LDAP_LIST='list-ldap-servers' \
20
21 CTX_XDL_SEARCH_BASE=search-base-set \
22
23 CTX_XDL_FAS_LIST='list-fas-servers' \
24
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
26
```

```
27 CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \  
28 \  
29 CTX_XDL_TELEMETRY_PORT=port-number \  
30 \  
31 CTX_XDL_START_SERVICE=Y|N \  
32 \  
33 /opt/Citrix/VDA/sbin/ctxsetup.sh
```

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 7 : 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 /sbin/service ctxhdx start  
2  
3 sudo /sbin/service ctxvda start
```

Arrêter Linux VDA :

Pour arrêter les services Linux VDA :

```
1 sudo /sbin/service ctxvda stop
2
3 sudo /sbin/service ctxhdx stop
```

Remarque :

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

Redémarrer Linux VDA :

Pour redémarrer les services Linux VDA :

```
1 sudo /sbin/service ctxvda stop
2
3 sudo /sbin/service ctxhdx restart
4
5 sudo /sbin/service ctxvda start
```

Vérifier l'état de Linux VDA :

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

```
1 sudo /sbin/service ctxvda status
2
3 sudo /sbin/service ctxhdx status
```

Étape 8 : créer le catalogue de machines dans Citrix Virtual Apps ou Citrix Virtual Desktops

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

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

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

- l’option **OS mono-session** pour un modèle de mise à disposition de bureaux dédiés VDI.
- Ne combinez pas de machines Linux VDA et Windows dans le même catalogue de machines.

Remarque :

Les versions antérieures de Citrix Studio ne prenaient pas en charge la notion de « système d’exploitation Linux. » Toutefois, la sélection de l’option **OS de serveur Windows** ou **OS de serveur** implique un modèle de mise à disposition équivalent de bureaux partagés hébergés. La sélection de l’option **OS de bureau Windows** ou **OS de bureau** implique un modèle de mise à disposition d’un utilisateur unique par machine.

Conseil :

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

Étape 9 : créer le groupe de mise à disposition dans Citrix Virtual Apps ou Citrix Virtual Desktops

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

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

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

Important :

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

Pour plus d’informations sur la création de catalogues de machines et de groupes de mise à disposition, consultez [Citrix Virtual Apps and Desktops 7 2103](#).

Installer Linux Virtual Delivery Agent pour SUSE

June 17, 2022

Vous pouvez choisir de suivre les étapes dans cet article pour l'installation manuelle ou [easy install](#) pour l'installation et la configuration automatiques. Easy Install permet des gains de temps et de main d'œuvre et il est plus fiable que l'installation manuelle.

Remarque :

utilisez Easy Install uniquement pour les nouvelles installations. N'utilisez pas Easy Install pour mettre à jour une installation existante.

Étape 1 : préparer l'installation

Étape 1 a : démarrer l'outil YaST

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

Pour démarrer l'outil YaST basé sur texte :

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

Vous pouvez également démarrer l'outil YaST basé sur 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

1. Ouvrez YaST Network Settings (Paramètres réseau).

2. SLED 12 uniquement : dans l'onglet **Global Options**, définissez **Network Setup Method** (Méthode de configuration réseau) sur **Wicked Service** (Service Wicked).
3. Ouvrez l'onglet **Hostname/DNS** (Nom d'hôte/DNS).
4. Désélectionnez **Change hostname via DHCP** (Changer le nom d'hôte via DHCP).
5. Sélectionnez **Assign Hostname to Loopback IP** (Attribuer le nom d'hôte à l'adresse IP de bouclage).
6. Modifiez les options suivantes pour refléter votre configuration réseau :
 - Host Name (Nom d'hôte) : ajoutez le nom d'hôte DNS de la machine.
 - Domain Name (Nom de domaine) : ajoutez le nom de domaine 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.

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.

Désactiver DNS multidiffusion Sur SLED uniquement, les paramètres par défaut activent DNS multidiffusion (mDNS), ce qui peut entraîner des résultats incohérents de résolution de nom. Par défaut, mDNS n'est pas activé sur SLES, aucune action n'est donc requise.

Pour désactiver mDNS, modifiez **/etc/nsswitch.conf** et dans la ligne suivante remplacez :

```
hosts: files mdns_minimal [NOTFOUND=return] dns
```

par :

```
hosts: files dns
```

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 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 :

1. Ouvrez YaST NTP Configuration et sélectionnez l'onglet **General Settings** (Paramètres généraux).
2. Dans la section Start NTP Daemon (Lancer le démon NTP), sélectionnez **Now and on Boot** (Maintenant et au démarrage).
3. Le cas échéant, sélectionnez l'élément **Undisciplined Local Clock (LOCAL)** et cliquez sur **Delete** (Supprimer).
4. Ajoutez une entrée pour un serveur NTP en cliquant sur **Add** (Ajouter).
5. Sélectionnez le type de serveur **Server Type**, et cliquez sur **Next** (Suivant).
6. Entrez le nom DNS du serveur NTP dans le champ Address (Adresse). Ce service est généralement hébergé sur le contrôleur de domaine Active Directory.
7. Ne modifiez pas le champ Options.
8. Cliquez sur **Test** pour vérifier si le service NTP est accessible.
9. Cliquez sur **OK** dans la série de fenêtres pour enregistrer les modifications.

Remarque :

Pour les installations SLES 12, le démon NTP peut ne pas démarrer à cause d'un problème SUSE connu avec les stratégies AppArmor. Suivez la [résolution](#) fournie pour obtenir des informations supplémentaires.

Étape 1d : installer les packages dépendants de Linux VDA

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

- PostgreSQL10-server 10.12 ou version ultérieure
- OpenJDK 1.8.0
- OpenMotif Runtime Environment 2.3.1 ou version ultérieure
- Cups 1.6.0 ou version ultérieure
- Filtres Foomatic 3.0.0 ou version ultérieure
- ImageMagick 6.8 ou version ultérieure

Ajouter des référentiels Vous pouvez obtenir certains packages requis, tels que PostgreSQL et ImageMagick, à partir du kit de développement logiciel (SDK) SUSE Linux Enterprise Software Development Kit (SDK). Pour obtenir les packages, ajoutez le référentiel SDK à l'aide de YaST ou téléchargez le fichier image SDK, puis montez-le localement à l'aide des commandes suivantes :

```
1 sudo mkdir -p /mnt/sdk
2
3 sudo mount -t iso9660 path-to-iso/SLE-12-SP5-SDK-DVD-x86_64-GM-DVD1.iso
  /mnt/sdk
4
5 sudo zypper ar -f /mnt/sdk sdk
```

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 Le Linux VDA est dépendant de OpenJDK 1.8.0.

Conseil :

Pour éviter les échecs d'enregistrement auprès du Delivery Controller, assurez-vous d'avoir in-

stallé uniquement OpenJDK 1.8.0. Supprimez toutes les autres versions de Java de votre système.

- **SLED :**

1. Sur SLED, Java Runtime Environment est généralement installé avec le système d'exploitation. Vérifiez que celui-ci a été installé :

```
1 sudo zypper info java-1_8_0-openjdk
```

2. Mettez-le à jour vers la version la plus récente si l'état est signalé comme obsolète :

```
1 sudo zypper update java-1_8_0-openjdk
```

3. Vérifiez la version Java :

```
1 java -version
```

- **SLES :**

1. Sur SLES, installez Java Runtime Environment :

```
1 sudo zypper install java-1_8_0-openjdk
```

2. Vérifiez la version Java :

```
1 java -version
```

Installer PostgreSQL Sur SLED/SLES 12, installez les packages :

```
1 sudo zypper install postgresql-init
2
3 sudo zypper install postgresql10-server
4
5 sudo zypper install postgresql-jdbc
```

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

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

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

Supprimer les référentiels Une fois les packages dépendants installés, exécutez les commandes suivantes pour supprimer le référentiel SDK configuré précédemment et le support monté :

```
1 sudo zypper rr sdk
2
3 sudo umount /mnt/sdk
4
5 sudo rmdir /mnt/sdk
```

Étape 2 : préparer une VM Linux pour l'hyperviseur

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

Corriger la synchronisation de l'heure sur Citrix Hypervisor

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

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

```
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 activée, 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 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 car l'hyperviseur et NTP tenteront de gérer l'horloge du système. Pour éviter que l'horloge ne soit plus synchronisée avec d'autres serveurs, synchronisez l'horloge du système de chaque invité Linux avec NTP. Cela nécessite la désactivation de la synchronisation de l'heure de l'hôte.

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

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

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

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

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

- [Samba Winbind](#)
- [Quest Authentication Service](#)
- [Centrify DirectControl](#)
- [SSSD](#)

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. Ouvrez YaST Windows Domain Membership.
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 **Also Use SMB information for Linux Authentication** (Utiliser aussi 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 **Yes**.
5. Lorsque vous y êtes invité(e), saisissez les informations d'identification d'un utilisateur de domaine avec les autorisations nécessaires pour ajouter des ordinateurs au domaine, et cliquez sur **OK**.
6. Un message indiquant si le processus a réussi s'affiche.
7. Si vous êtes invité(e) à installer des packages samba et krb5, cliquez sur **Install**.

YaST peut avoir indiqué que ces modifications nécessitent le redémarrage de certains services ou de la machine. Nous vous recommandons de redémarrer la machine :

```
1 su -
2
3 reboot
```

SUSE 12 uniquement : correctif du nom du fichier cache d'identification Kerberos SUSE 12 a remplacé la configuration du nom du fichier cache d'identification Kerberos habituelle **FILE:/tmp/krb5cc_%{uid}** par **DIR:/run/user/%{uid}/krb5cc**. Cette nouvelle méthode de mise en cache DIR n'est pas compatible avec le Linux VDA et doit être modifiée manuellement. En tant qu'utilisateur racine, modifiez **/etc/krb5.conf** en ajoutant le paramètre suivant dans la section **[libdefaults]** s'il n'est pas défini :

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

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

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

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

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

```
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 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 4 : 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 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

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 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
```

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

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

```
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 4 : 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 (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  
3 adinfo
```

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

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

```
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 4 : 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
3 sudo systemctl disable nscd
```

2. Installez ou mettez à jour les packages requis :

```
1 sudo zypper install krb5-client
2
3 sudo zypper install samba-client
```

3. 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 ````
2 [libdefaults]
3
4     dns_canonicalize_hostname = false
5
```

```
6     rdns = false
7
8     default_realm = REALM
9
10    forwardable = true
11
12    [realms]
13
14    REALM = {
15
16        kdc = fqdn-of-domain-controller
17
18        default_domain = realm
19
20        admin_server =      fqdn-of-domain-controller
21    }
22
23
24    [domain_realm]
25
26    .realm = REALM
27
28    realm = REALM
29    ...
30
31    **realm** is the Kerberos realm name, such as example.com. **REALM** is
    the Kerberos realm name in uppercase, such as EXAMPLE.COM. **fqdn-
    of-domain-controller** is the FQDN of the domain controller.
```

1. Modifiez /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      realm = REALM
5
6      security = ADS
7
8      kerberos method = secrets and keytab
9
10     client signing = yes
11
12     client use spnego = yes
```

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

2. 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
```

3. 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
```

L'élément **user** est un utilisateur du domaine autorisé à ajouter des machines au domaine.

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 sssd.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
    AD side
20
21    fallback_homedir = /home/%d/%u
```

```
22     default_shell = /bin/bash
23
24     # Uncomment and adjust if the default principal SHORTNAME$@REALM
      is not available
25
26     # ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
27
28     ad_gpo_access_control = permissive
```

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

Remarque :

ldap_id_mapping est défini sur `true` de façon à ce que SSSD se charge de mapper les SID Windows avec les UID Unix. Sinon, Active Directory doit être en mesure de fournir des extensions POSIX. L'élément **ad_gpo_access_control** est défini sur **permissive** pour éviter une erreur d'ouverture de session non valide pour les sessions Linux. Pour en savoir plus, consultez les pages `man` 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 Pour vérifier que Kerberos est correctement configuré pour être utilisé avec le Linux VDA, vérifiez que le fichier `keytab` système a été créé et contient des clés valides :

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

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

```
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 4 : installer le Linux VDA](#) après vérification de la jonction du domaine.

Étape 4 : installer le Linux VDA

Étape 4a : 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 /sbin/service ctxvda stop
2
3 sudo /sbin/service ctxhdx stop
```

Remarque :

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

2. Désinstallez le package :

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

Important :

La mise à niveau à partir des deux dernières versions est prise en charge.

Remarque :

Les composants d'installation se trouvent dans `/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 4b : 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.

Étape 4c : installer le Linux VDA

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

Pour SUSE 12 :


```
1 sudo zypper install XenDesktopVDA-<version>.sle12_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 SUSE 12 :

```
1 sudo rpm -i XenDesktopVDA-<version>.sle12_x.x86_64.rpm
```

Étape 4d : mettre à niveau le Linux VDA (facultatif)

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

Pour SUSE 12 :

```
1 sudo rpm -U XenDesktopVDA-<version>.sle12_x.x86_64.rpm
```

Liste des dépendances RPM pour SUSE 12 :

```
1 postgresql-server >= 9.3
2
3 postgresql-jdbc >= 9.2
4
5 java-1.8.0-openjdk >= 1.8.0
6
7 ImageMagick >= 6.8
8
9 dbus-1 >= 1.8.8
10
11 dbus-1-x11 >= 1.8.8
12
13 libXpm4 >= 3.5.11
14
15 libXrandr2 >= 1.4.2
16
17 libXtst6 >= 1.2.2
18
19 motif >= 2.3
20
21 pam >= 1.1.8
22
23 bash >= 4.2
24
25 findutils >= 4.5
26
27 gawk >= 4.1
28
29 sed >= 4.2
30
```

```
31 cups >= 1.6.0
32
33 cups-filters-foomatic-rip >= 1.0.0
34
35 openldap2 >= 2.4
36
37 cyrus-sasl >= 2.1
38
39 cyrus-sasl-gssapi >= 2.1
40
41 libxml2 >= 2.9
42
43 python-requests >= 2.8.1
44
45 rpmlib(PayloadFilesHavePrefix) <= 4.0-1
46
47 rpmlib(CompressedFileNames) <= 3.0.4-1
48
49 rpmlib(PayloadIsLzma) <= 4.4.6-1
50
51 libtcmalloc4 >= 2.5
52
53 libcap-progs >= 2.22
54
55 xorg-x11-server >= 7.6_1.18.3-76.15
56
57 ibus >= 1.5
58
59 xorg- x11-server = 7.6_1.19.6
60
61 xorg-x11 = 7.6_1
62
63 postgresql10-server >= 10.12
64
65 libgtk-2_0-0 >= 2.24
66
67 libgthread-2_0-0 >= 2.48
68
69 pulseaudio-utils >= 5.0
70
71 lsb-release >= 2.0
```

Important :

Redémarrez la machine Linux VDA après la mise à niveau.

Étape 5 : configurer le Linux VDA

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

paramètres.

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

- 1 –Samba Winbind

- 2 –Service d’authentification Quest
 - 3 –Centrify DirectControl
 - 4 –SSSD
- **CTX_XDL_HDX_3D_PRO = Y | N** : Linux VDA prend en charge HDX 3D Pro, un ensemble de technologies d’accélération GPU conçues pour optimiser la virtualisation des applications riches en graphiques. Si HDX 3D Pro est sélectionné, le Virtual Delivery Agent doit être configuré pour le mode Bureaux VDI (session unique), c’est-à-dire, CTX_XDL_VDI_MODE=Y.
 - **CTX_XDL_VDI_MODE=Y | N** : indique si la machine est configurée comme modèle de mise à disposition de bureaux dédiés (VDI) ou comme modèle de mise à disposition de bureaux partagés hébergés. Pour les environnements HDX 3D Pro, définissez cette variable sur Y. Elle est définie par défaut sur N.
 - **CTX_XDL_SITE_NAME=dns-name** : le Linux VDA découvre les serveurs LDAP à l’aide de DNS. Pour limiter les résultats de recherche DNS à un site local, spécifiez un nom de site DNS. Cette variable est définie sur **<none>** par défaut.
 - **CTX_XDL_LDAP_LIST='list-ldap-servers'** : le Linux VDA envoie une requête vers le DNS pour découvrir les serveurs LDAP. Si DNS ne peut pas fournir d’enregistrements de service LDAP, vous pouvez entrer une liste séparée par des espaces de noms de domaines complets LDAP avec ports LDAP. Par exemple, ad1.mycompany.com:389. Cette variable est définie sur **<none>** par défaut.
 - **CTX_XDL_SEARCH_BASE=search-base-set** : le Linux VDA envoie une requête à LDAP via une base de recherche définie sur la racine du domaine Active Directory (par exemple, D, DC=mycompany,DC=com). Pour améliorer les performances de recherche, vous pouvez spécifier une base de recherche (par exemple, OU=VDI,DC=mycompany,DC=com). Cette variable est définie sur **<none>** par défaut.
 - **CTX_XDL_FAS_LIST='list-fas-servers'** : les serveurs du service d’authentification fédérée (FAS) sont configurés via la stratégie de groupe AD. Le Linux VDA ne prend pas en charge la stratégie de groupe AD mais vous pouvez fournir une liste de serveurs FAS séparés par des points-virgules. La séquence doit être la même que celle configurée dans la stratégie de groupe AD. Si une adresse de serveur est supprimée, remplissez son espace vide avec la chaîne de texte **<none>** et ne modifiez pas l’ordre des adresses de serveur.
 - **CTX_XDL_DOTNET_runtime_path=Path-to-install-dotnet-runtime** : chemin d’accès à l’installation de .NET Core Runtime 3.1 pour la prise en charge du nouveau Broker Agent Service ([ctxvda](#)). Le chemin par défaut est /usr/bin.
 - **CTX_XDL_START_SERVICE = Y | N** : indique si les services Linux VDA sont lancés lorsque la configuration de Linux VDA est terminée. Valeur définie sur Y par défaut.
 - **CTX_XDL_TELEMETRY_SOCKET_PORT** : port socket permettant d’écouter Citrix Scout. Le port par défaut est 7503.
 - **CTX_XDL_TELEMETRY_PORT** : port de communication avec Citrix Scout. Le port par défaut est 7502.

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

```
1 export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N
2
3 export CTX_XDL_DDC_LIST= ' list-ddc-fqdns '
4
5 export CTX_XDL_VDA_PORT=port-number
6
7 export CTX_XDL_REGISTER_SERVICE=Y|N
8
9 export CTX_XDL_ADD_FIREWALL_RULES=Y|N
10
11 export CTX_XDL_AD_INTEGRATION=1|2|3|4
12
13 export CTX_XDL_HDX_3D_PRO=Y|N
14
15 export CTX_XDL_VDI_MODE=Y|N
16
17 export CTX_XDL_SITE_NAME=dns-site-name | '<none>'
18
19 export CTX_XDL_LDAP_LIST= ' list-ldap-servers ' | '<none>'
20
21 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
22
23 export CTX_XDL_FAS_LIST= ' list-fas-servers ' | '<none>'
24
25 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
26
27 export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number
28
29 export CTX_XDL_TELEMETRY_PORT=port-number
30
31 export CTX_XDL_START_SERVICE=Y|N
32
33 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
```

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

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

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

```
12
13 CTX_XDL_HDX_3D_PRO=Y|N \
14
15 CTX_XDL_VDI_MODE=Y|N \
16
17 CTX_XDL_SITE_NAME=dns-name \
18
19 CTX_XDL_LDAP_LIST= ' list-ldap-servers ' \
20
21 CTX_XDL_SEARCH_BASE=search-base-set \
22
23 CTX_XDL_FAS_LIST= ' list-fas-servers ' \
24
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
26
27 CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \
28
29 CTX_XDL_TELEMETRY_PORT=port-number \
30
31 CTX_XDL_START_SERVICE=Y|N \
32
33 /opt/Citrix/VDA/sbin/ctxsetup.sh
```

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 6 : 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 /sbin/service ctxhdx start
2
3 sudo /sbin/service ctxvda start
```

Arrêter Linux VDA :

Pour arrêter les services Linux VDA :

```
1 sudo /sbin/service ctxvda stop
2
3 sudo /sbin/service ctxhdx stop
```

Remarque :

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

Redémarrer Linux VDA :

Pour redémarrer les services Linux VDA :

```
1 sudo /sbin/service ctxvda stop
2
3 sudo /sbin/service ctxhdx restart
4
5 sudo /sbin/service ctxvda start
```

Vérifier l'état de Linux VDA :

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

```
1 sudo /sbin/service ctxvda status
2
3 sudo /sbin/service ctxhdx status
```

Étape 7 : créer le catalogue de machines dans Citrix Virtual Apps ou Citrix Virtual Desktops

Le processus de création de catalogues de machines et d'ajout de machines Linux VDA est similaire à l'approche traditionnelle avec les VDA Windows. Pour obtenir une description plus détaillée de la

méthode à utiliser pour effectuer ces tâches, consultez les sections [Créer des catalogues de machines](#) et [Gérer des catalogues de machines](#).

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

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

Remarque :

Les versions antérieures de Citrix Studio ne prenaient pas en charge la notion de « système d'exploitation Linux. » Toutefois, la sélection de l'option **OS de serveur Windows** ou **OS de serveur** implique un modèle de mise à disposition équivalent de bureaux partagés hébergés. La sélection de l'option **OS de bureau Windows** ou **OS de bureau** implique un modèle de mise à disposition d'un utilisateur unique par machine.

Conseil :

Si 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 8 : créer le groupe de mise à disposition dans Citrix Virtual Apps ou Citrix Virtual Desktops

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

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

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

Important :

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

Pour plus d'informations sur la création de catalogues de machines et de groupes de mise à disposition, consultez [Citrix Virtual Apps and Desktops 7 2103](#).

Installer Linux Virtual Delivery Agent pour Ubuntu

June 17, 2022

Vous pouvez choisir de suivre les étapes dans cet article pour l'installation manuelle ou [easy install](#) pour l'installation et la configuration automatiques. Easy Install permet des gains de temps et de main d'œuvre et il est plus fiable que l'installation manuelle.

Remarque :

utilisez Easy Install uniquement pour les nouvelles installations. N'utilisez pas Easy Install pour mettre à jour une installation existante.

Étape 1 : préparer Ubuntu pour l'installation du VDA

Étape 1a : vérifier la configuration réseau

Nous vous recommandons de disposer d'un réseau connecté et correctement configuré avant de continuer.

Si vous utilisez un serveur Ubuntu 18.04 Live Server, effectuez la modification suivante dans le fichier de configuration `/etc/cloud/cloud.cfg` avant de définir le nom d'hôte :

```
preserve_hostname: true
```

Étape 1b : définir le nom d'hôte

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

```
hostname
```

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

Assurez-vous que le nom de domaine DNS et le nom de domaine complet (FQDN) de la machine sont signalés correctement. Pour ce faire, modifiez la ligne suivante du fichier **/etc/hosts** pour inclure le nom de domaine complet et le nom d'hôte en tant que deux premières entrées :

```
127.0.0.1 hostname-fqdn hostname localhost
```

Par exemple :

```
127.0.0.1 vda01.example.com vda01 localhost
```

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

Remarque :

Le Linux VDA ne prend actuellement pas en charge la troncation de noms NetBIOS. Par conséquent, le nom d'hôte ne doit pas comporter plus de 15 caractères.

Conseil :

Utilisez uniquement les caractères a–z, A–Z, 0–9 et tiret (-). Évitez les caractères de soulignement (_), les espaces et autres symboles. Ne démarrez pas un nom d'hôte par un chiffre et ne le terminez pas par un tiret. Cette règle s'applique également aux noms d'hôte Delivery Controller.

Étape 1d : vérifier le nom d'hôte

Vérifiez que le nom d'hôte est correctement configuré :

```
1 hostname
```

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 **/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 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

Le Linux VDA dépend de OpenJDK. L'environnement d'exécution est généralement installé dans le cadre de l'installation du système d'exploitation.

Sur Ubuntu 16.04, installez OpenJDK à l'aide de :

```
1 sudo apt-get install -y default-jdk
```

Sur Ubuntu 18.04, installez OpenJDK à l'aide de :

```
1 sudo apt-get install -y openjdk-8-jdk
```

Étape 1i : installer PostgreSQL

Le Linux VDA requiert PostgreSQL version 9.x sur Ubuntu :

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

Étape 1j : installer Motif

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

Étape 1k : installer les autres packages

```
1 sudo apt-get install -y libsasl2-2
2
3 sudo apt-get install -y libsasl2-modules-gssapi-mit
4
5 sudo apt-get install -y libldap-2.4-2
6
7 sudo apt-get install -y krb5-user
8
9 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 machine virtuelle sur un hyperviseur pris en charge. Apportez les modifications suivantes en fonction de la plateforme d'hyperviseur utilisée. Aucune modification n'est requise si vous utilisez la machine Linux sur un matériel bare metal.

Corriger la synchronisation de l'heure sur Citrix Hypervisor

Si la fonctionnalité de synchronisation de l'heure de Citrix Hypervisor est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée car NTP et Citrix Hypervisor tenteront de gérer l'horloge du 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.

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

```
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 activée, 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 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 car l'hyperviseur et NTP tenteront de synchroniser l'horloge du système. Pour éviter que l'horloge ne soit plus synchronisée avec d'autres serveurs, assurez-vous l'horloge du système de chaque invité Linux est synchronisée avec NTP. Cela nécessite la désactivation de la synchronisation de l'heure de l'hôte.

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

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

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

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

- [Samba Winbind](#)
- [Quest Authentication Service](#)
- [Centrify DirectControl](#)
- [SSSD](#)
- [PBIS](#)

Suivez les instructions en fonction de la méthode choisie.

Remarque :

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

Samba Winbind**Installer ou mettre à jour les packages requis**

```
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
```

Le paramètre **domain-dns-name** dans ce contexte est le nom de domaine DNS, tel que **example.com**. L'élément **REALM** est le nom du domaine Kerberos en majuscules, tel que **EXAMPLE.COM**.

Configurer l'authentification Winbind Vous devez configurer Winbind manuellement car Ubuntu ne possède pas d'outil tel que `authconfig` dans RHEL et `yast2` dans SUSE.

Ouvrez **/etc/samba/smb.conf** et configurez les paramètres suivants :

```
[global]
workgroup = WORKGROUP
security = ADS
realm = REALM
encrypt passwords = yes
idmap config *:range = 16777216-33554431
winbind trusted domains only = no
kerberos method = secrets and keytab
winbind refresh tickets = yes
template shell = /bin/bash
```

WORKGROUP est le premier champ dans **REALM**, et **REALM** est le nom de domaine Kerberos en majuscules.

Configurer nsswitch Ouvrez **/etc/nsswitch.conf** et ajoutez `winbind` aux lignes suivantes :

```
passwd: compat winbind
group: compat winbind
```

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

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

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

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

```
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 4 : 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 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
```

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

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

```
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 4 : 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 **CentrifyDC mode** renvoie **connected**. Si le mode reste bloqué à l'état de démarrage, le client Centrify rencontre des problèmes de connexion au serveur ou d'authentification.

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

```
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 4 : 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 domaine Kerberos en majuscules, tel que `EXAMPLE.COM`.

Joindre le domaine SSSD doit être configuré pour pouvoir utiliser Active Directory en tant que fournisseur d'identité et Kerberos pour l'authentification. Toutefois, SSSD ne fournit pas de fonctions de client Active Directory pour rejoindre le domaine et gérer le fichier keytab du système. Vous pouvez utiliser `adcli`, `realmd` ou `Samba`.

Remarque :

Cette section fournit uniquement des informations pour `adcli` et `Samba`.

Utilisez adcli pour rejoindre le domaine :

Installer adcli :

Installez les packages requis :

```
1 sudo apt-get install adcli
```

Rejoindre 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.

Vérifier le fichier keytab système :

Pour une machine Ubuntu 20.04, exécutez la commande `adcli testjoin` pour tester si elle est jointe au domaine.

Pour une machine Ubuntu 18.04 ou Ubuntu 16.04, 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.

Utiliser Samba pour rejoindre le domaine :

Installer le package :

```
1 sudo apt-get install samba krb5-user
```

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.

Rejoindre 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 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.

Le paramètre **domain-dns-name** dans ce contexte est le nom de domaine DNS, tel que example.com. L'élément **REALM** est le nom du domaine Kerberos en majuscules, tel que EXAMPLE.COM. Il n'est pas nécessaire de configurer le nom de domaine NetBIOS.

Pour de plus amples informations sur les paramètres de configuration, consultez les pages man pour sssd.conf et sssd-ad.

Le démon SSSD nécessite que le fichier de configuration dispose uniquement de l'autorisation d'accès en lecture de propriétaire :

```
1 sudo chmod 0600 /etc/sss/sss.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.

Utiliser addi pour vérifier l'appartenance à un domaine :

Affichez les informations de domaine en exécutant la commande suivante :

```
1 sudo adcli info domain-dns-name
```

Utiliser Samba pour vérifier l'appartenance à un domaine :

Exécutez la commande **net ads** de Samba pour vérifier que 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 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 inverse (\) pour empêcher le remplacement shell. Dans certains environnements, le nom de domaine DNS est différent du nom de domaine Kerberos. Assurez-vous que le nom de domaine est utilisé. Si cette commande réussit, aucun résultat n'est affiché.

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

```
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 4 : installer le Linux VDA](#) après vérification de la jonction du domaine.

PBIS

Télécharger le package PBIS requis Par exemple :

```
1 sudo wget https://github.com/BeyondTrust/pbis-open/releases/download
  /8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh
```

Rendre le script d'installation PBIS exécutable Par exemple :

```
1 sudo chmod +x pbis-open-8.8.0.506.linux.x86_64.deb.sh
```

Exécuter le script d'installation PBIS Par exemple :

```
1 sudo sh pbis-open-8.8.0.506.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 4 : installer le Linux VDA](#) après vérification de la jonction du domaine.

Étape 4 : installer le Linux VDA

Étape 4a : 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.

Étape 4b : installer le Linux VDA

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

Pour Ubuntu 20.04 :

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

Pour Ubuntu 18.04 :

```
1 sudo dpkg -i xendesktopvda_<version>.ubuntu18.04_amd64.deb
```

Pour Ubuntu 16.04 :

```
1 sudo dpkg -i xendesktopvda_<version>.ubuntu16.04_amd64.deb
```

Liste des dépendances Debian pour Ubuntu 20.04 :

```
1 postgresql >= 12
2
3 libpostgresql-jdbc-java >= 42.2
4
5 openjdk-8-jdk >= 8u252
6
7 imagemagick >= 8:6.9.10
8
9 ufw >= 0.36
10
11 ubuntu-desktop >= 1.450
12
13 libxrandr2 >= 2:1.5.2
14
15 libxtst6 >= 2:1.2.3
16
17 libxm4 >= 2.3.8
```

```
18
19 util-linux >= 2.34
20
21 gtk3-nocsd >= 3
22
23 bash >= 5.0
24
25 findutils >= 4.7.0
26
27 sed >= 4.7
28
29 cups >= 2.3
30
31 libmspack0 >= 0.10
32
33 libgoogle-perftools4 >= 2.7~
34
35 libpython2.7 >= 2.7~
```

Liste des dépendances Debian pour Ubuntu 18.04 :

```
1 postgresql >= 9.5
2
3 libpostgresql-jdbc-java >= 9.2
4
5 openjdk-8-jdk >= 1.8.0
6
7 gtk3-nocsd >=3
8
9 imagemagick >= 8:6.8.9.9
10
11 ufw >= 0.35
12
13 ubuntu-desktop >= 1.361
14
15 libxrandr2 >= 2:1.5.0
16
17 libxtst6 >= 2:1.2.2
18
19 libxm4 >= 2.3.4
20
21 util-linux >= 2.27.1
22
23 bash >= 4.3
24
25 findutils >= 4.6.0
26
27 sed >= 4.2.2
28
29 cups >= 2.1
30
31 libldap-2.4-2 >= 2.4.42
32
```

```
33 libsassl2-modules-gssapi-mit >= 2.1.~
34
35 python-requests >= 2.9.1
36
37 libgoogle-perftools4 >= 2.4~
38
39 xserver-xorg-core >= 2:1.18
40
41 xserver-xorg-core << 2:1.19
42
43 x11vnc>=0.9.13
44
45 python-websocketify >= 0.6.1
```

Liste des dépendances Debian pour Ubuntu 16.04 :

```
1 postgresql >= 9.5
2
3 libpostgresql-jdbc-java >= 9.2
4
5 default-jdk >= 2:1.8
6
7 imagemagick >= 8:6.8.9.9
8
9 ufw >= 0.35
10
11 ubuntu-desktop >= 1.361
12
13 libxrandr2 >= 2:1.5.0
14
15 libxtst6 >= 2:1.2.2
16
17 libxm4 >= 2.3.4
18
19 util-linux >= 2.27.1
20
21 bash >= 4.3
22
23 findutils >= 4.6.0
24
25 sed >= 4.2.2
26
27 cups >= 2.1
28
29 libldap-2.4-2 >= 2.4.42
30
31 libsassl2-modules-gssapi-mit >= 2.1.~
32
33 python-requests >= 2.9.1
34
35 libgoogle-perftools4 >= 2.4~
36
37 xserver-xorg-core >= 2:1.18
```

```
38
39 xserver-xorg-core << 2:1.19
40
41 x11vnc>=0.9.13
42
43 python-websocketify >= 0.6.1
```

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 4c : mettre à niveau le Linux VDA (facultatif)

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

```
1 sudo dpkg -i <PATH>/<Linux VDA deb>
```

Étape 4d : configurer le Linux VDA

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

Vous pouvez exécuter le script manuellement avec `invite`, ou automatiquement avec réponses 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_SUPPORT_DDC_AS_CNAME=Y | N** : le Linux VDA prend en charge la spécification d'un nom de Delivery Controller à l'aide d'un enregistrement DNS CNAME. La valeur est définie par défaut sur N.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** : le Linux VDA requiert une liste séparée par des espaces de noms de domaines complets de Delivery Controller. Cette dernière sera utilisée pour l'enregistrement auprès d'un Delivery Controller. Au moins un alias de nom de domaine complet (FQDN) ou CNAME doit être spécifié.
- **CTX_XDL_VDA_PORT = port-number** : le Linux VDA communique avec les Delivery Controller à l'aide d'un port (80 par défaut) TCP/IP.
- **CTX_XDL_REGISTER_SERVICE=Y | N** : les services Linux Virtual Desktop sont lancés après le démarrage de la machine. Valeur définie sur Y par défaut.
- **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 (ports 80 et 1494 par défaut) dans le pare-feu du système pour Linux Virtual Desktop. Valeur définie sur Y par défaut.
- **CTX_XDL_AD_INTEGRATION = 1 | 2 | 3 | 4 | 5** : le Linux VDA requiert que les paramètres de configuration Kerberos s'authentifient auprès des Delivery Controller. La configuration de Kerberos est déterminée depuis l'outil d'intégration d'Active Directory installé et configuré sur le système. Spécifiez la méthode d'intégration d'Active Directory prise en charge à utiliser :
 - 1 –Samba Winbind
 - 2 –Service d'authentification Quest
 - 3 –Centrify DirectControl
 - 4 –SSSD
 - 5 –PBIS
- **CTX_XDL_HDX_3D_PRO = Y | N** : Linux VDA prend en charge HDX 3D Pro, un ensemble de technologies d'accélération GPU conçues pour optimiser la virtualisation des applications riches en graphiques. Si HDX 3D Pro est sélectionné, le Virtual Delivery Agent doit être configuré pour le mode Bureaux VDI (session unique), c'est-à-dire, CTX_XDL_VDI_MODE=Y.
- **CTX_XDL_VDI_MODE=Y | N** : indique si la machine est configurée comme modèle de mise à disposition de bureaux dédiés (VDI) ou comme modèle de mise à disposition de bureaux partagés hébergés. Pour les environnements HDX 3D Pro, définissez cette variable sur Y. Elle est définie par défaut sur N.
- **CTX_XDL_SITE_NAME=dns-name** : le Linux VDA découvre les serveurs LDAP à l'aide de DNS. Pour limiter les résultats de recherche DNS à un site local, spécifiez un nom de site DNS. Cette variable est définie sur **<none>** par défaut.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** : le Linux VDA envoie une requête vers le DNS pour découvrir les serveurs LDAP. Si DNS ne peut pas fournir d'enregistrements de service LDAP, vous pouvez entrer une liste séparée par des espaces de noms de domaines complets LDAP avec ports LDAP. Par exemple, ad1.mycompany.com:389. Cette variable est définie sur **<none>** par

défaut.

- **CTX_XDL_SEARCH_BASE=search-base-set** : le Linux VDA envoie une requête à LDAP via une base de recherche définie sur la racine du domaine Active Directory (par exemple, D, DC=mycompany,DC=com). Toutefois, pour améliorer les performances de recherche, vous pouvez spécifier une base de recherche (par exemple, OU=VDI,DC=mycompany,DC=com). Cette variable est définie sur **<none>** par défaut.
- **CTX_XDL_FAS_LIST='list-fas-servers'** : les serveurs du service d'authentification fédérée (FAS) sont configurés via la stratégie de groupe AD. Le Linux VDA ne prend pas en charge la stratégie de groupe AD mais vous pouvez fournir une liste de serveurs FAS séparés par des points-virgules. La séquence doit être la même que celle configurée dans la stratégie de groupe AD. Si une adresse de serveur est supprimée, remplissez son espace vide avec la chaîne de texte **<none>** et ne modifiez pas l'ordre des adresses de serveur.
- **CTX_XDL_DOTNET_runtime_path=Path-to-install-dotnet-runtime** : chemin d'accès à l'installation de .NET Core Runtime 3.1 pour la prise en charge du nouveau Broker Agent Service (`ctxvda`). Le chemin par défaut est `/usr/bin`.
- **CTX_XDL_START_SERVICE = Y | N** : indique si les services Linux VDA sont lancés lorsque la configuration de Linux VDA est terminée. Valeur définie sur Y par défaut.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** : port socket permettant d'écouter Citrix Scout. Le port par défaut est 7503.
- **CTX_XDL_TELEMETRY_PORT** : port de communication avec Citrix Scout. Le port par défaut est 7502.

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

```
1 export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N
2
3 export CTX_XDL_DDC_LIST= ' list-ddc-fqdns '
4
5 export CTX_XDL_VDA_PORT=port-number
6
7 export CTX_XDL_REGISTER_SERVICE=Y|N
8
9 export CTX_XDL_ADD_FIREWALL_RULES=Y|N
10
11 export CTX_XDL_AD_INTEGRATION=1|2|3|4|5
12
13 export CTX_XDL_HDX_3D_PRO=Y|N
14
15 export CTX_XDL_VDI_MODE=Y|N
16
17 export CTX_XDL_SITE_NAME=dns-site-name | '<none>'
18
19 export CTX_XDL_LDAP_LIST= ' list-ldap-servers ' | '<none>'
20
21 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
22
```

```
23 export CTX_XDL_FAS_LIST= ' list-fas-servers ' | '<none>'
24
25 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
26
27 export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number
28
29 export CTX_XDL_TELEMETRY_PORT=port-number
30
31 export CTX_XDL_START_SERVICE=Y|N
32
33 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
```

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

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

```
1 sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
2
3 CTX_XDL_DDC_LIST= ' list-ddc-fqdns ' \
4
5 CTX_XDL_VDA_PORT=port-number \
6
7 CTX_XDL_REGISTER_SERVICE=Y|N \
8
9 CTX_XDL_ADD_FIREWALL_RULES=Y|N \
10
11 CTX_XDL_AD_INTEGRATION=1|2|3|4|5 \
12
13 CTX_XDL_HDX_3D_PRO=Y|N \
14
15 CTX_XDL_VDI_MODE=Y|N \
16
17 CTX_XDL_SITE_NAME=dns-name \
18
19 CTX_XDL_LDAP_LIST= ' list-ldap-servers ' \
20
21 CTX_XDL_SEARCH_BASE=search-base-set \
22
23 CTX_XDL_FAS_LIST= ' list-fas-servers ' \
24
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
26
27 CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \
28
29 CTX_XDL_TELEMETRY_PORT=port-number \
30
31 CTX_XDL_START_SERVICE=Y|N \
32
33 /opt/Citrix/VDA/sbin/ctxsetup.sh
```

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

Redémarrer Linux VDA :

Pour redémarrer les services Linux VDA :

```
1 sudo 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 6 : créer le catalogue de machines dans Citrix Virtual Apps ou Citrix Virtual Desktops

Le processus de création de catalogues de machines et d'ajout de machines Linux VDA est similaire à l'approche traditionnelle avec les VDA Windows. Pour obtenir une description plus détaillée de la

méthode à utiliser pour effectuer ces tâches, consultez les sections [Créer des catalogues de machines](#) et [Gérer des catalogues de machines](#).

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

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

Remarque :

Les versions antérieures de Citrix Studio ne prenaient pas en charge la notion de « système d'exploitation Linux. » Toutefois, la sélection de l'option **OS de serveur Windows** ou **OS de serveur** implique un modèle de mise à disposition équivalent de bureaux partagés hébergés. La sélection de l'option **OS de bureau Windows** ou **OS de bureau** implique un modèle de mise à disposition d'un utilisateur unique par machine.

Conseil :

Si 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 7 : créer le groupe de mise à disposition dans Citrix Virtual Apps ou Citrix Virtual Desktops

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

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

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

Pour plus d'informations sur la création de catalogues de machines et de groupes de mise à disposition, consultez [Citrix Virtual Apps and Desktops 7 2103](#).

Installer Linux Virtual Delivery Agent pour Debian

June 17, 2022

Vous pouvez choisir de suivre les étapes dans cet article pour l'installation manuelle ou [easy install](#) pour l'installation et la configuration automatiques. Easy Install permet des gains de temps et de main d'œuvre et il est plus fiable que l'installation manuelle.

Remarque :

utilisez Easy Install uniquement pour les nouvelles installations. N'utilisez pas Easy Install pour mettre à jour une installation existante.

Étape 1 : préparer Debian pour l'installation du VDA

Étape 1a : vérifier la configuration réseau

Nous vous recommandons de disposer d'un réseau connecté et correctement configuré avant de continuer.

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 **/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 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 les packages

```
1 sudo apt-get install -y libsasl2-2
2
3 sudo apt-get install -y libgtk2.0-0
```

Étape 1i : ajouter le référentiel oldstable

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

Étape 2 : préparer l'hyperviseur

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

Corriger la synchronisation de l'heure sur Citrix Hypervisor

Si la fonctionnalité de synchronisation de l'heure de Citrix Hypervisor est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée car NTP et Citrix Hypervisor tenteront de gérer l'horloge du 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.

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

```
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 activée, 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 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 car l'hyperviseur et NTP tenteront de synchroniser l'horloge du système. Pour éviter que l'horloge ne soit plus synchronisée avec d'autres serveurs, assurez-vous l'horloge du système de chaque invité Linux est synchronisée avec NTP. Cela nécessite la désactivation de la synchronisation de l'heure de l'hôte.

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

1. Ouvrez vSphere Client.
2. Modifiez les paramètres pour la VM Linux.
3. Dans la boîte de dialogue **Virtual Machine Properties** (Propriétés de la machine virtuelle), ouvrez l'onglet **Options**.
4. Sélectionnez **VMware Tools**.

5. Dans la zone **Advanced** (Avancé), désélectionnez **Synchronize guest time with host** (Synchroniser l'heure de l'invité avec l'hôte).

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

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

- [Samba Winbind](#)
- [Quest Authentication Service](#)
- [Centrify DirectControl](#)
- [SSSD](#)
- [PBIS](#)

Suivez les instructions en fonction de la méthode choisie.

Remarque :

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

Samba Winbind

Installer ou mettre à jour les packages requis

```
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
```

Le paramètre **domain-dns-name** dans ce contexte est le nom de domaine DNS, tel que **example.com**. L'élément **REALM** est le nom du domaine Kerberos en majuscules, tel que **EXAMPLE.COM**.

Configurer l'authentification Winbind Ouvrez **/etc/samba/smb.conf** et configurez les paramètres suivants :

```
[global]
workgroup = WORKGROUP
security = ADS
realm = REALM
encrypt passwords = yes
idmap config *:range = 16777216-33554431
winbind trusted domains only = no
kerberos method = secrets and keytab
winbind refresh tickets = yes
template shell = /bin/bash
```

WORKGROUP est le premier champ dans **REALM**, et **REALM** est le nom de domaine Kerberos en majuscules.

Configurer nsswitch Ouvrez **/etc/nsswitch.conf** et ajoutez **winbind** aux lignes suivantes :

```
passwd: systemd winbind
group: systemd winbind
```

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

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

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

```
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 4 : 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 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
```

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

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

```
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 4 : 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 **CentrifyDC mode** renvoie **connected**. Si le mode reste bloqué à l'état de démarrage, le client Centrify rencontre des problèmes de connexion au serveur ou d'authentification.

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

```
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 4 : 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 domaine Kerberos en majuscules, tel que `EXAMPLE.COM`.

Joindre le domaine SSSD doit être configuré pour pouvoir utiliser Active Directory en tant que fournisseur d'identité et Kerberos pour l'authentification. Toutefois, SSSD ne fournit pas de fonctions de client Active Directory pour rejoindre le domaine et gérer le fichier keytab du système. Vous pouvez utiliser `adcli`, `realmd` ou `Samba`.

Remarque :

Cette section fournit uniquement des informations pour `adcli` et `Samba`.

Utilisez `adcli` pour rejoindre le domaine :

Installer `adcli` :

Installez les packages requis :

```
1 sudo apt-get install adcli
```

Rejoindre 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.

Vérifier 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.

Utiliser Samba pour rejoindre le domaine :

Installer le package :

```
1 sudo apt-get install samba krb5-user
```

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.

Rejoindre 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 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`.

Le paramètre **domain-dns-name** dans ce contexte est le nom de domaine DNS, tel que `example.com`. L'élément **REALM** est le nom du domaine Kerberos en majuscules, tel que `EXAMPLE.COM`. Il n'est pas nécessaire de configurer le nom de domaine NetBIOS.

Pour de plus amples informations sur les paramètres de configuration, consultez les pages man pour `sssd.conf` et `sssd-ad`.

Le démon SSSD nécessite que le fichier de configuration dispose uniquement de l'autorisation d'accès en lecture de propriétaire :

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

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.

Utiliser addi pour vérifier l'appartenance à un domaine :

Affichez les informations de domaine en exécutant la commande suivante :

```
1 sudo adcli info domain-dns-name
```

Utiliser Samba pour vérifier l'appartenance à un domaine :

Exécutez la commande **net ads** de Samba pour vérifier que 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 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 inverse (\) pour empêcher le remplacement shell. Dans certains environnements, le nom de domaine DNS est différent du nom de domaine Kerberos. Assurez-vous que le nom de domaine est utilisé. Si cette commande réussit, aucun résultat n'est affiché.

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

```
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 4 : installer le Linux VDA](#) après vérification de la jonction du domaine.

PBIS

Télécharger le package PBIS requis Par exemple :

```
1 sudo wget https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh
```

Rendre le script d'installation PBIS exécutable Par exemple :

```
1 sudo chmod +x pbis-open-8.8.0.506.linux.x86_64.deb.sh
```

Exécuter le script d'installation PBIS Par exemple :

```
1 sudo sh pbis-open-8.8.0.506.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 4 : installer le Linux VDA](#) après vérification de la jonction du domaine.

Étape 4 : installer le Linux VDA

Étape 4a : 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.

Étape 4b : installer le Linux VDA

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

```
1 sudo dpkg -i xendesktopvda_<version>.debian10_amd64.deb
```

Liste des dépendances Debian pour Debian 10.7 :

```
1 postgresql           >= 11
2 libpostgresql-jdbc-java >= 42.2
3 openjdk-8-jdk        >= 8u252
4 imagemagick          >= 8:6.9.10
5 ufw                  >= 0.36
6 desktop-base         >= 10.0.2
7 libxrandr2           >= 2:1.5.1
8 libxtst6             >= 2:1.2.3
9 libxm4               >= 2.3.8
10 util-linux           >= 2.33
11 gtk3-nocsd           >= 3
12 bash                 >= 5.0
```

```
13 findutils          >= 4.6.0
14 sed                >= 4.7
15 cups               >= 2.2
16 ghostscript        >= 9.27~
17 libmspack0         >= 0.10
18 libgoogle-perftools4 >= 2.7~
19 libpython2.7        >= 2.7~
20 libsasl2-modules-gssapi-mit >= 2.1.~
```

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 4c : mettre à niveau le Linux VDA (facultatif)

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

```
1 sudo dpkg -i <PATH>/<Linux VDA deb>
```

Étape 4d : configurer le Linux VDA

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

Vous pouvez exécuter le script manuellement avec `invite`, ou automatiquement avec réponses 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_SUPPORT_DDC_AS_CNAME=Y | N** : le Linux VDA prend en charge la spécification d'un nom de Delivery Controller à l'aide d'un enregistrement DNS CNAME. La valeur est définie par défaut sur N.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** : le Linux VDA requiert une liste séparée par des espaces de noms de domaines complets de Delivery Controller. Cette dernière sera utilisée pour l'enregistrement auprès d'un Delivery Controller. Au moins un alias de nom de domaine complet (FQDN) ou CNAME doit être spécifié.
- **CTX_XDL_VDA_PORT = port-number** : le Linux VDA communique avec les Delivery Controller à l'aide d'un port (80 par défaut) TCP/IP.
- **CTX_XDL_REGISTER_SERVICE=Y | N** : les services Linux Virtual Desktop sont lancés après le démarrage de la machine. Valeur définie sur Y par défaut.
- **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 (ports 80 et 1494 par défaut) dans le pare-feu du système pour Linux Virtual Desktop. Valeur définie sur Y par défaut.
- **CTX_XDL_AD_INTEGRATION = 1 | 2 | 3 | 4 | 5** : le Linux VDA requiert que les paramètres de configuration Kerberos s'authentifient auprès des Delivery Controller. La configuration de Kerberos est déterminée depuis l'outil d'intégration d'Active Directory installé et configuré sur le système. Spécifiez la méthode d'intégration d'Active Directory prise en charge à utiliser :
 - 1 –Samba Winbind
 - 2 –Service d'authentification Quest
 - 3 –Centrify DirectControl
 - 4 –SSSD
 - 5 –PBIS
- **CTX_XDL_HDX_3D_PRO = Y | N** : Linux VDA prend en charge HDX 3D Pro, un ensemble de technologies d'accélération GPU conçues pour optimiser la virtualisation des applications riches en graphiques. Si HDX 3D Pro est sélectionné, le Virtual Delivery Agent doit être configuré pour le mode Bureaux VDI (session unique), c'est-à-dire, CTX_XDL_VDI_MODE=Y.
- **CTX_XDL_VDI_MODE=Y | N** : indique si la machine est configurée comme modèle de mise à disposition de bureaux dédiés (VDI) ou comme modèle de mise à disposition de bureaux partagés hébergés. Pour les environnements HDX 3D Pro, définissez cette variable sur Y. Elle est définie par défaut sur N.
- **CTX_XDL_SITE_NAME=dns-name** : le Linux VDA découvre les serveurs LDAP à l'aide de DNS. Pour limiter les résultats de recherche DNS à un site local, spécifiez un nom de site DNS. Cette variable est définie sur **<none>** par défaut.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** : le Linux VDA envoie une requête vers le DNS pour découvrir les serveurs LDAP. Si DNS ne peut pas fournir d'enregistrements de service LDAP, vous pouvez entrer une liste séparée par des espaces de noms de domaines complets LDAP avec ports LDAP. Par exemple, ad1.mycompany.com:389. Cette variable est définie sur **<none>** par

défaut.

- **CTX_XDL_SEARCH_BASE=search-base-set** : le Linux VDA envoie une requête à LDAP via une base de recherche définie sur la racine du domaine Active Directory (par exemple, D, DC=mycompany,DC=com). Toutefois, pour améliorer les performances de recherche, vous pouvez spécifier une base de recherche (par exemple, OU=VDI,DC=mycompany,DC=com). Cette variable est définie sur **<none>** par défaut.
- **CTX_XDL_FAS_LIST='list-fas-servers'** : les serveurs du service d'authentification fédérée (FAS) sont configurés via la stratégie de groupe AD. Le Linux VDA ne prend pas en charge la stratégie de groupe AD mais vous pouvez fournir une liste de serveurs FAS séparés par des points-virgules. La séquence doit être la même que celle configurée dans la stratégie de groupe AD. Si une adresse de serveur est supprimée, remplissez son espace vide avec la chaîne de texte **<none>** et ne modifiez pas l'ordre des adresses de serveur.
- **CTX_XDL_DOTNET_runtime_path=Path-to-install-dotnet-runtime** : chemin d'accès à l'installation de .NET Core Runtime 3.1 pour la prise en charge du nouveau Broker Agent Service (*ctxvda*). Le chemin par défaut est /usr/bin.
- **CTX_XDL_START_SERVICE = Y | N** : indique si les services Linux VDA sont lancés lorsque la configuration de Linux VDA est terminée. Valeur définie sur Y par défaut.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** : port socket permettant d'écouter Citrix Scout. Le port par défaut est 7503.
- **CTX_XDL_TELEMETRY_PORT** : port de communication avec Citrix Scout. Le port par défaut est 7502.

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

```

1 export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N
2
3 export CTX_XDL_DDC_LIST= ' list-ddc-fqdns '
4
5 export CTX_XDL_VDA_PORT=port-number
6
7 export CTX_XDL_REGISTER_SERVICE=Y|N
8
9 export CTX_XDL_ADD_FIREWALL_RULES=Y|N
10
11 export CTX_XDL_AD_INTEGRATION=1|2|3|4|5
12
13 export CTX_XDL_HDX_3D_PRO=Y|N
14
15 export CTX_XDL_VDI_MODE=Y|N
16
17 export CTX_XDL_SITE_NAME=dns-site-name | '<none>'
18
19 export CTX_XDL_LDAP_LIST= ' list-ldap-servers ' | '<none>'
20
21 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
22
```

```
23 export CTX_XDL_FAS_LIST= ' list-fas-servers ' | '<none>'
24
25 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
26
27 export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number
28
29 export CTX_XDL_TELEMETRY_PORT=port-number
30
31 export CTX_XDL_START_SERVICE=Y|N
32
33 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
```

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

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

```
1 sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
2
3 CTX_XDL_DDC_LIST= ' list-ddc-fqdns ' \
4
5 CTX_XDL_VDA_PORT=port-number \
6
7 CTX_XDL_REGISTER_SERVICE=Y|N \
8
9 CTX_XDL_ADD_FIREWALL_RULES=Y|N \
10
11 CTX_XDL_AD_INTEGRATION=1|2|3|4|5 \
12
13 CTX_XDL_HDX_3D_PRO=Y|N \
14
15 CTX_XDL_VDI_MODE=Y|N \
16
17 CTX_XDL_SITE_NAME=dns-name \
18
19 CTX_XDL_LDAP_LIST= ' list-ldap-servers ' \
20
21 CTX_XDL_SEARCH_BASE=search-base-set \
22
23 CTX_XDL_FAS_LIST= ' list-fas-servers ' \
24
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
26
27 CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \
28
29 CTX_XDL_TELEMETRY_PORT=port-number \
30
31 CTX_XDL_START_SERVICE=Y|N \
32
33 /opt/Citrix/VDA/sbin/ctxsetup.sh
```

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

Redémarrer Linux VDA :

Pour redémarrer les services Linux VDA :

```
1 sudo 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 6 : créer le catalogue de machines dans Citrix Virtual Apps ou Citrix Virtual Desktops

Le processus de création de catalogues de machines et d'ajout de machines Linux VDA est similaire à l'approche traditionnelle avec les VDA Windows. Pour obtenir une description plus détaillée de la

méthode à utiliser pour effectuer ces tâches, consultez les sections [Créer des catalogues de machines](#) et [Gérer des catalogues de machines](#).

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

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

Remarque :

Les versions antérieures de Citrix Studio ne prenaient pas en charge la notion de « système d'exploitation Linux. » Toutefois, la sélection de l'option **OS de serveur Windows** ou **OS de serveur** implique un modèle de mise à disposition équivalent de bureaux partagés hébergés. La sélection de l'option **OS de bureau Windows** ou **OS de bureau** implique un modèle de mise à disposition d'un utilisateur unique par machine.

Conseil :

Si 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 7 : créer le groupe de mise à disposition dans Citrix Virtual Apps ou Citrix Virtual Desktops

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

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

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

Pour plus d'informations sur la création de catalogues de machines et de groupes de mise à disposition, consultez [Citrix Virtual Apps and Desktops 7 2103](#).

Configurer le Linux VDA

April 19, 2021

Cette section détaille les fonctionnalités du Linux VDA, notamment la description des fonctionnalités, la configuration et le dépannage.

Conseil :

le script Bash `xdlcollect` utilisé pour collecter les journaux est intégré dans le logiciel Linux VDA et se trouve dans `/opt/Citrix/VDA/bin`. Après avoir installé Linux VDA, vous pouvez exécuter la commande `bash /opt/Citrix/VDA/bin/xdlcollect.sh` pour collecter les journaux.

Une fois la collecte de journaux terminée, un fichier journal compressé est généré dans le même dossier que le script. `xdlcollect` peut vous demander s'il faut ou non charger le fichier journal compressé dans Citrix Insight Services (CIS). Si vous acceptez, `xdlcollect` renvoie `upload_ID` une fois le chargement terminé. Le téléchargement ne supprime pas le fichier journal compressé de votre machine locale. Les autres utilisateurs peuvent utiliser `upload_ID` pour accéder au fichier journal dans CIS.

Intégrer NIS avec Active Directory

November 5, 2021

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 comme fournisseur d'UID et de GID au lieu d'AD requiert que les informations de compte (nom d'utilisateur et mot de passe) soient les mêmes dans AD et NIS.

Remarque :

L'authentification est toujours effectuée par le serveur Active Directory. NIS+ n'est pas pris en charge. Si vous utilisez NIS comme fournisseur d'UID et de GID, les attributs POSIX du serveur Windows ne sont plus utilisés.

Conseil :

Cette méthode de déploiement de Linux VDA est obsolète et n'est utilisée que pour des scénarios particuliers. Pour une distribution RHEL/CentOS, suivez les instructions indiquées dans la section [Installer Linux Virtual Delivery Agent pour RHEL/CentOS](#). Pour une distribution Ubuntu, suivez les instructions indiquées dans la section [Installer Linux Virtual Delivery Agent pour Ubuntu](#).

Présentation de SSSD

SSSD est un démon système. Sa fonction principale consiste à offrir un accès pour l'identification et l'authentification de ressources distantes par le biais d'une infrastructure commune qui peut fournir une mise en cache et un accès en mode déconnecté au système. Il propose des modules PAM et NSS et prendra en charge à l'avenir les interfaces D-BUS qui permettront d'obtenir davantage d'informations utilisateur. Il offre également une meilleure base de données pour stocker les comptes utilisateur locaux ainsi que les données utilisateur supplémentaires.

Intégrer NIS à Active Directory

Pour intégrer NIS à AD, suivez la procédure suivante :

1. [Ajouter l'agent Linux VDA en tant que client NIS](#)
2. [Rejoindre le domaine et créer un fichier keytab hôte avec Samba](#)
3. [Configurer SSSD](#)
4. [Configurer NSS/PAM](#)
5. [Vérifier la configuration de Kerberos](#)
6. [Vérifier l'authentification utilisateur](#)

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 ybind
2
3 sudo systemctl enable rpcbind ybind
```

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.

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 :

```
--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
```

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.

Configurer SSSD

La configuration de SSSD comprend les étapes suivantes :

- Installez les packages **sssd-ad** et **sssd-proxy** sur la machine cliente Linux.
- Apportez des modifications de configuration à plusieurs fichiers (par exemple, **sssd.conf**).
- Démarrez le service **sssd**.

/etc/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>[^\w]+)\w(?P<name>.+)) | (((?P<name>[^\w]+)@
    (?P<domain>.+)) | (^(?P<name>[^\w]+)$))
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 de fichier sur **sssd.conf** :

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

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.

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

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

```
1 sudo klist -ke
```

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
```

Publier des applications

July 8, 2022

Avec la version 7.13 de Linux VDA, Citrix a ajouté la fonctionnalité d'applications transparentes à toutes les plates-formes Linux prises en charge. Aucune procédure d'installation spécifique n'est requise pour utiliser cette fonctionnalité.

Conseil :

Citrix a ajouté la prise en charge des applications publiées non transparentes et du partage de session dans la version 1.4 du Linux VDA.

Publier des applications à l'aide de Citrix Studio

Vous pouvez publier des applications installées sur un Linux VDA lorsque vous créez un groupe de mise à disposition ou ajoutez des applications à un groupe de mise à disposition. Ce processus est similaire à la publication d'applications installées sur un VDA Windows. Pour de plus amples informations, consultez la [documentation de Citrix Virtual Apps and Desktops](#) (en fonction de la version de Citrix Virtual Apps and Desktops utilisée).

Conseil :

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**.

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 résoudre ce problème, nous vous recommandons de créer des groupes de mise à disposition distincts pour la mise à disposition d'applications et de

bureaux.

Remarque :

Pour utiliser les applications transparentes, ne désactivez pas le mode transparent sur Store-Front. 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.

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.
- Actuellement, le mode transparent prend en charge les gestionnaires de fenêtres suivants : Mutter, Metacity et Compiz (Ubuntu 16.04). Kwin et les autres gestionnaires de fenêtres ne sont pas pris en charge. Assurez-vous que votre gestionnaire de fenêtres est 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>.
- Tous les boutons de barre des tâches des applications publiées exécutées dans la même session ICA sont combinés dans le même groupe. Pour résoudre ce problème, définissez la propriété de barre des tâches de façon à ne pas combiner les boutons de barre des tâches.

Streaming Linux

June 16, 2023

Cet article fournit des informations sur la fonctionnalité de streaming Linux Citrix Provisioning. 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 16.04
- Ubuntu 18.04.5 (version Technical Preview)
- RHEL 8.3 (version Technical Preview)

Important :

- Pour utiliser cette fonctionnalité pour Ubuntu 18.04.5 et RHEL 8.3, utilisez le package **VS Linux Streaming Agent (Ubuntu 18.04)-Experimental** et le package **PVS Linux Streaming Agent (RHEL8.3)-Experimental**, respectivement. Les packages d'installation sont disponibles sur la [page de téléchargement Linux VDA](#).
- Pour utiliser cette fonctionnalité pour Ubuntu 16.04, téléchargez l'image ISO de Citrix Provisioning la plus récente et localisez le logiciel cible pour Ubuntu 16.04. Pour plus d'informations, consultez la section [Configuration du streaming Linux](#) dans la documentation de Citrix Provisioning.

Lorsque vous provisionnez des machines cibles Linux, tenez compte de ce qui suit :

- Dans certains cas, le lecteur client ne peut pas être mappé à une session de machine virtuelle Linux provisionnée. Pour résoudre ce problème, arrêtez le service CDM avec `service ctxcdm stop` avant d'installer la machine cible Citrix Provisioning, puis exécutez la commande `pvs-imager` pour la convertir.
- Le streaming Linux prend uniquement en charge Winbind en tant qu'outil de jonction à un domaine Windows.
- Si vous activez le cache RAM pour la machine Linux, définissez la taille du cache sur 8 Mo (valeur minimum). Linux utilise autant de RAM que nécessaire, y compris toute la mémoire disponible, pour le cache en écriture. La quantité spécifiée dans la console correspond à la quantité réservée d'avance. Citrix vous recommande de réserver le moins de mémoire possible, ce qui permet à Linux de gérer l'utilisation de la mémoire.
- Le nom de la machine cible dans l'interface utilisateur de l'imager Citrix Provisioning est généralement défini par défaut sur `im_localhost`. Cette valeur doit être modifiée lorsque vous créez plusieurs vDisk. L'utilisation du même nom de machine cible entraîne l'échec de la commande imager.
- L'installation (et les mises à jour ultérieures) doivent être effectuées en mode super utilisateur. Il y a deux façons d'installer en tant que super utilisateur :
 - Entrez le mode utilisateur dans un terminal à l'aide de la commande `su`.
 - Entrez `sudo` avant la commande. Par exemple, `sudo yum install tdb-tools` ; entrez `sudo` pour chaque commande.
- L'horloge système du client Linux doit être synchronisée à l'aide du contrôleur Active Directory.
- UEFI n'est pas prise en charge.

- VMM n'est pas pris en charge.
- Le lecteur cache en écriture doit avoir le libellé `PVS_Cache` pour pouvoir être utilisé en tant que cache en écriture. La partition entière est utilisée.
- La localisation en anglais est affichée sur les installations autres que l'anglais.
- SE Linux n'est pas pris en charge.
- Les cibles exécutées sur XenServer doivent tourner en mode HVM.
- Après le démarrage d'une machine cible Linux, un message d'avertissement peut s'afficher dans le navigateur d'alerte SELinux.
- Deux machines virtuelles Ubuntu 18.04 en streaming hébergées sur ESXi obtiennent la même adresse IP via DHCP. Pour résoudre ce problème, configurez la machine virtuelle pour qu'elle utilise l'adresse MAC comme ID unique pour récupérer une adresse IP via DHCP.
- Pour Ubuntu 18.04.5 et RHEL 8.3, les mots de passe des comptes de machine ne se mettent pas automatiquement à jour dans Active Directory. Lorsqu'un mot de passe expire et que la machine virtuelle en streaming ne parvient pas à joindre le domaine, essayez de réinitialiser le mot de passe via Citrix Provisioning Console.
- Pour Ubuntu 16.04, seul Winbind fourni par Samba 4.4 et versions antérieures est pris en charge lors du provisionnement de machines cibles Linux à l'aide de Citrix Provisioning.

Options d'installation

Pour installer le composant de streaming Linux, vous devez avoir ouvert une session en tant qu'administrateur. Lors de l'installation, n'oubliez pas que les commandes suivantes doivent être émises dans un shell root ou avec des privilèges `sudo`.

Remarque :

Un certificat auto-signé doit être créé si des machines cibles Linux Citrix Provisioning sont streamées. Le serveur SOAP utilise une connexion SSL qui requiert que vous configuriez un certificat X.509 sur le serveur SOAP.

L'autorité de certification du certificat doit également être présente sur le serveur Provisioning Server et la machine cible Linux. Pour plus d'informations sur la création d'un certificat auto-signé, consultez la section [Création de certificats auto-signés pour le streaming Linux](#).

Pour les distributions Ubuntu 16.04 :

```
1 sudo dpkg -i pvs-<version>.deb
2
3 sudo apt-get -yf install
```

Pour les distributions Ubuntu 18.04 :

```
1 sudo apt-get -y install dracut dracut-network tdb-tools python3 python3
  -distutils
```

```
2 sudo dpkg -i pvs_<version>_ubuntu18.04_amd64.deb
```

Pour les distributions RHEL 8.3 :

```
1 yum -nogpgcheck localinstall pvs_<version>_rhel8.3_x86_64.deb
```

Utilisation de l'interface utilisateur pour créer une image principale de Linux

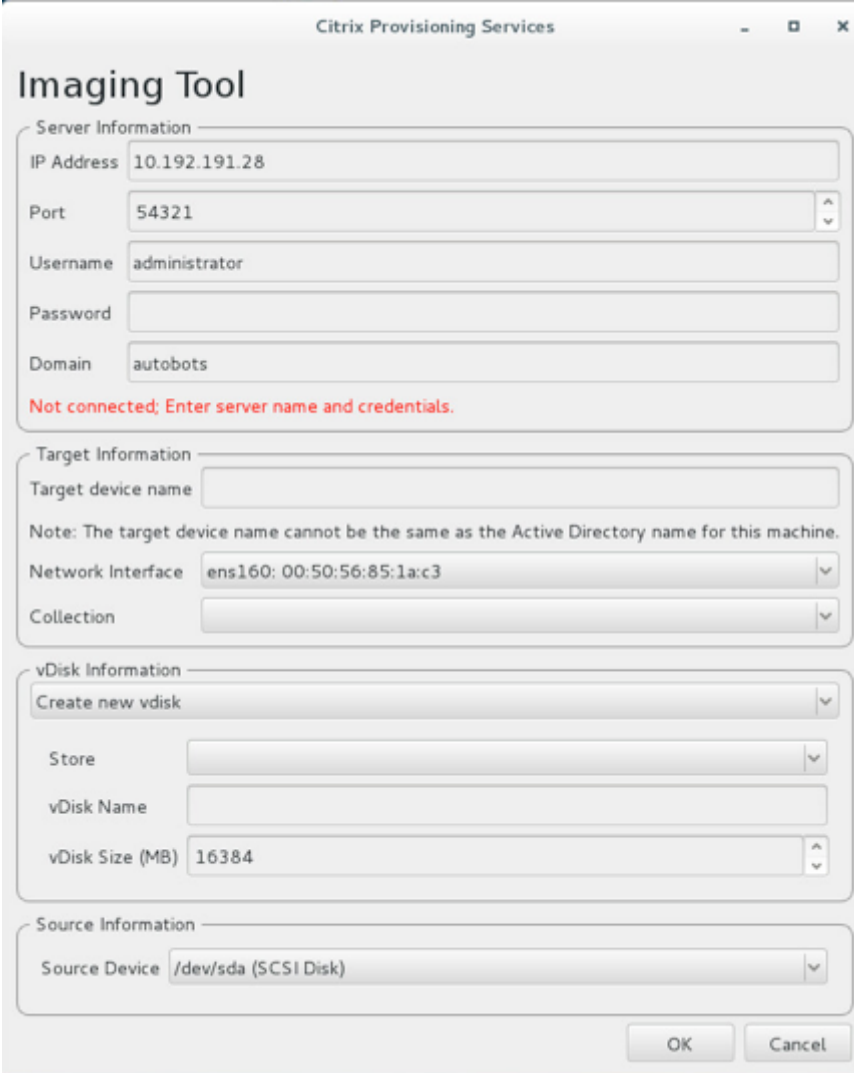
Pour appeler l'interface utilisateur de manière à installer cette fonctionnalité :

1. Ouvrez une session en tant qu'administrateur.
2. Exécutez la commande `pvs-imager` :

Conseil :

Si la commande `pvs-imager` échoue en raison d'un problème avec le nom d'hôte, vérifiez que votre configuration réseau est correcte. Ne définissez pas le nom d'hôte du système sur `localhost`. Sur RHEL8.3, ouvrez une session avec un serveur d'affichage X11 au lieu de Wayland pour utiliser l'interface graphique.

Après l'exécution de la commande, l'interface utilisateur s'affiche :



The image shows the 'Citrix Provisioning Services Imaging Tool' window. It has a title bar with 'Citrix Provisioning Services' and standard window controls. The main area is divided into four sections: 'Server Information', 'Target Information', 'vDisk Information', and 'Source Information'. The 'Server Information' section includes fields for IP Address (10.192.191.28), Port (54321), Username (administrator), Password, and Domain (autobots). A red message below says 'Not connected; Enter server name and credentials.' The 'Target Information' section has a 'Target device name' field, a note about Active Directory names, a 'Network Interface' dropdown (ens160: 00:50:56:85:1a:c3), and a 'Collection' dropdown. The 'vDisk Information' section has a 'Create new vdisk' dropdown, a 'Store' dropdown, a 'vDisk Name' field, and a 'vDisk Size (MB)' dropdown (16384). The 'Source Information' section has a 'Source Device' dropdown (/dev/sda (SCSI Disk)). At the bottom right are 'OK' and 'Cancel' buttons.

Citrix Provisioning Services

Imaging Tool

Server Information

IP Address: 10.192.191.28

Port: 54321

Username: administrator

Password:

Domain: autobots

Not connected; Enter server name and credentials.

Target Information

Target device name:

Note: The target device name cannot be the same as the Active Directory name for this machine.

Network Interface: ens160: 00:50:56:85:1a:c3

Collection:

vDisk Information

Create new vdisk

Store:

vDisk Name:

vDisk Size (MB): 16384

Source Information

Source Device: /dev/sda (SCSI Disk)

OK Cancel

Utiliser l'interface de ligne de commande pour installer la fonctionnalité de streaming Linux

Pour appeler la ligne de commande pour installer cette fonctionnalité :

1. Ouvrez une session en tant qu'administrateur.
2. Exécutez la commande suivante :

```
pvs-imager -C
```

L'installation par ligne de commande comprend deux options :

- \-C vous permet de créer un vDisk
- \-U vous permet de mettre à jour un vDisk existant

Les informations suivantes ci-dessous illustrent des options d'installation non GUI pour la fonctionnalité de streaming Linux :

```

1  Usage: ./pvs-imager \[-hCU\] \[-a|--address=<IPAddr>\] \[-u|--username=<
    username>\] \[-p|--password=<password>\] \[-P|--port=<port>\] \[-d|--
    domain=<domain>\] \[-S|--store=<store>\] \[-v|--vdisk=<vdisk name>\] \[-
    s|--size=<vdisk size>\] \[-D|--device=<sourceDevice>\] \[-c|--
    collection=<collection>\] \[-n|--name=<name>\]
2  Non-GUI Modes:
3  -C          - Create a new vDisk
4  ---OR---
5  -U          - Update an existing vDisk
6
7  General Options:
8  -a <server IP> - Address or hostname of PVS server
9  -u <username>  - Username for API login
10 -p <password>  - Password for API login
11 -d <domain>    - AD domain for API login
12 -P <port>      - Base port for API login (default: 54321)
13 -S <store>     - Store containing vDisk
14 -c <collection> - Collection to store imaging device in
15 -n <name>      - Device name for imaging device
16 -v <name>      - vDisk name
17 -s <size>      - vDisk size (Create Mode only, default: sourceDevice
    size)
18 -D <sourceDev> - devnode to clone
19 -V            - increment debug verbosity (up to 5 times)
20 -g <grubMode> - Supported Grub settings ( 'debug' )

```

Les systèmes de fichiers pris en charge pour la création d'images sont **ext4**, **xfs** ou **btrfs**.

Conseil :

Les journaux de débogage de **pvs-imager**, créés à l'aide du commutateur **-VVVVV**, sont créés dans le dossier qui a exécuté l'outil **pvs-imager**. Le nom du fichier journal est **pvs-imager.log**.

À propos de la mise en cache du disque

Pour la mise en cache sur disque dur ou la mise en cache du dépassement sur disque dur sans l'Assistant d'installation Citrix Virtual Apps and Desktops, formatez le disque de la machine cible avec une partition formatée. Incluez le libellé **PVS_Cache**. Cet objet peut être créé avec la commande **mkfs -L PVS_Cache** sur la machine cible. Tout système de fichiers sensible à la casse peut être utilisé pour le cache, mais XFS est recommandé.

Conseil :

Un administrateur peut créer une logique de sélection de disque cache pour son environnement

en écrivant un script bash qui s'exécute au démarrage. Le script recherche un périphérique cache à l'aide du mécanisme le plus adapté à l'environnement, en exécutant `mkfs` sur ce dernier et en redémarrant.

Lors de la configuration de la mise en cache de disque :

- Citrix recommande d'utiliser l'assistant d'installation de Citrix Virtual Apps and Desktops pour créer la machine cible Linux.
- La création manuelle de l'étiquette nécessite le respect de la casse pour éviter les conflits de configuration.
- Vous pouvez également utiliser la méthode manuelle pour créer le cache d'écriture.

Création manuelle du cache d'écriture pour une machine cible

Par défaut, l'assistant d'installation de Citrix Virtual Apps and Desktops ignore les lecteurs attachés au modèle actuel. L'assistant crée un cache d'écriture en fonction des paramètres que vous fournissez. Parfois, le lecteur de cache d'écriture rencontre des problèmes lors de la création automatique à l'aide de l'assistant ou lorsque la machine cible revient continuellement au cache côté serveur à la suite d'un problème avec le lecteur créé. Pour résoudre ces problèmes, créez manuellement l'objet à l'aide de la commande `mkfs -L PVS_Cache` sur la machine cible.

L'assistant d'installation de Citrix Virtual Apps and Desktops reconnaît par défaut les modifications apportées au cache d'écriture créé manuellement pour la machine cible lorsque vous utilisez le paramètre `UseTemplateCache`. Sur le serveur de provisioning exécutant l'assistant d'installation de Citrix Virtual Apps and Desktops ou sur l'emplacement sur lequel pointe la console de provisioning distante, modifiez le paramètre de registre :

Créez la clé de registre suivante sur la machine de console de provisioning pour désactiver le cache de modèle :

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ProvisioningServices`

Name: `UseTemplateCache`

Type: `DWORD`

Value: `0`

Exécutez l'assistant de configuration de Citrix Virtual Apps and Desktops. Sur la page **Machines virtuelles**, modifiez la taille du disque de cache d'écriture local à 0 Go (la valeur par défaut est 6 Go).

Remote PC Access

July 15, 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 pour la mise à disposition de ressources virtuelles. Cette uniformité offre une expérience administrative cohérente et unifiée. Les utilisateurs bénéficient d'une meilleure expérience utilisateur lorsque Citrix HDX est utilisé pour fournir 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 et affiche les activités de la session 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 exécutée sur la machine cliente 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

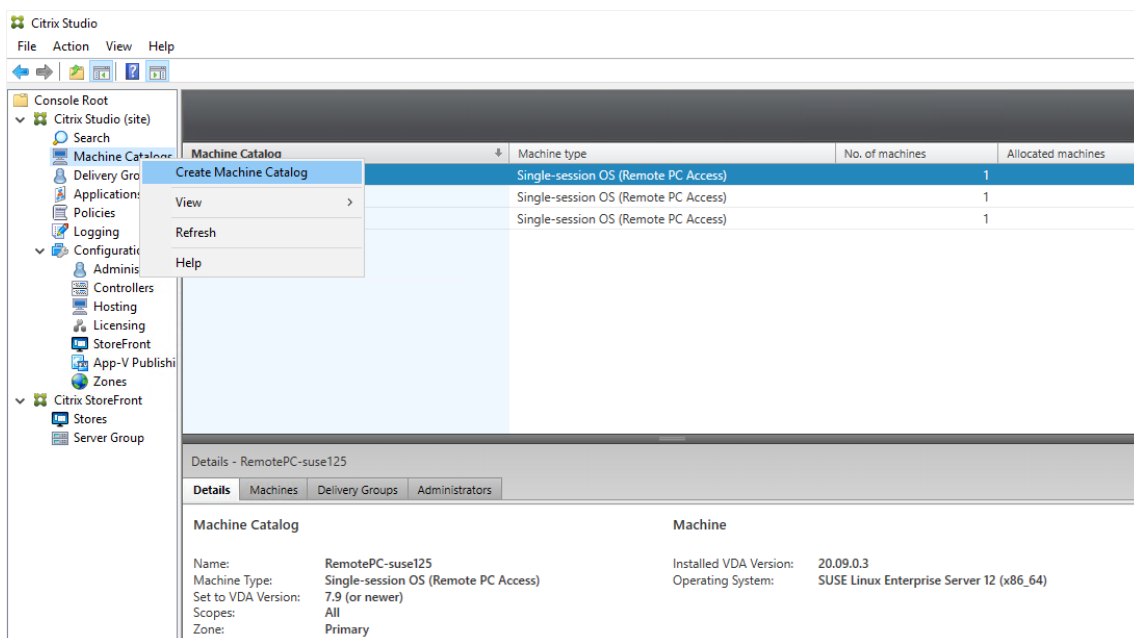
Pour fournir des sessions PC Linux, installez le Linux VDA sur les PC cibles, créez un catalogue de machines du type **Remote PC Access** et créez un groupe de mise à disposition pour rendre les PC du catalogue de machines disponibles pour les utilisateurs qui en demandent l'accès. La section suivante 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`.

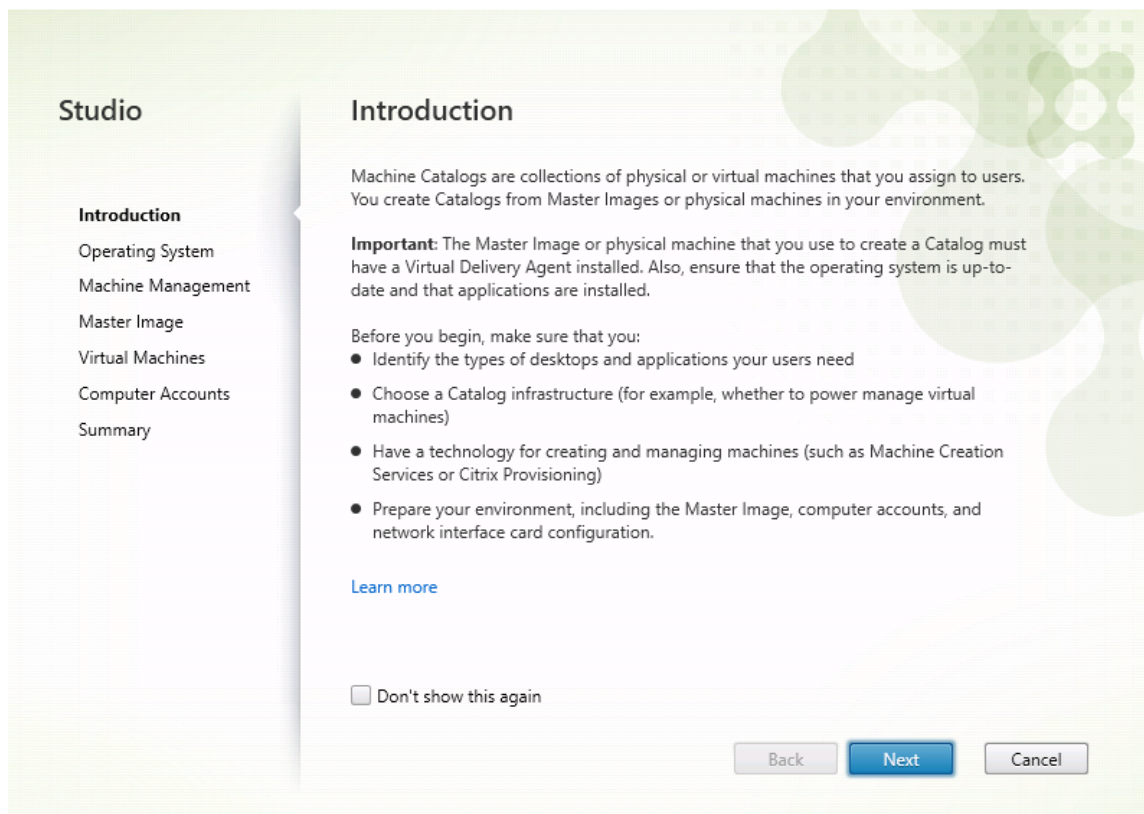
Étape 2 : créer un catalogue de machines du type Remote PC Access

1. Dans Citrix Studio, cliquez avec le bouton droit sur **Catalogues de machines** et sélectionnez **Créer un catalogue de machines** dans le menu contextuel.

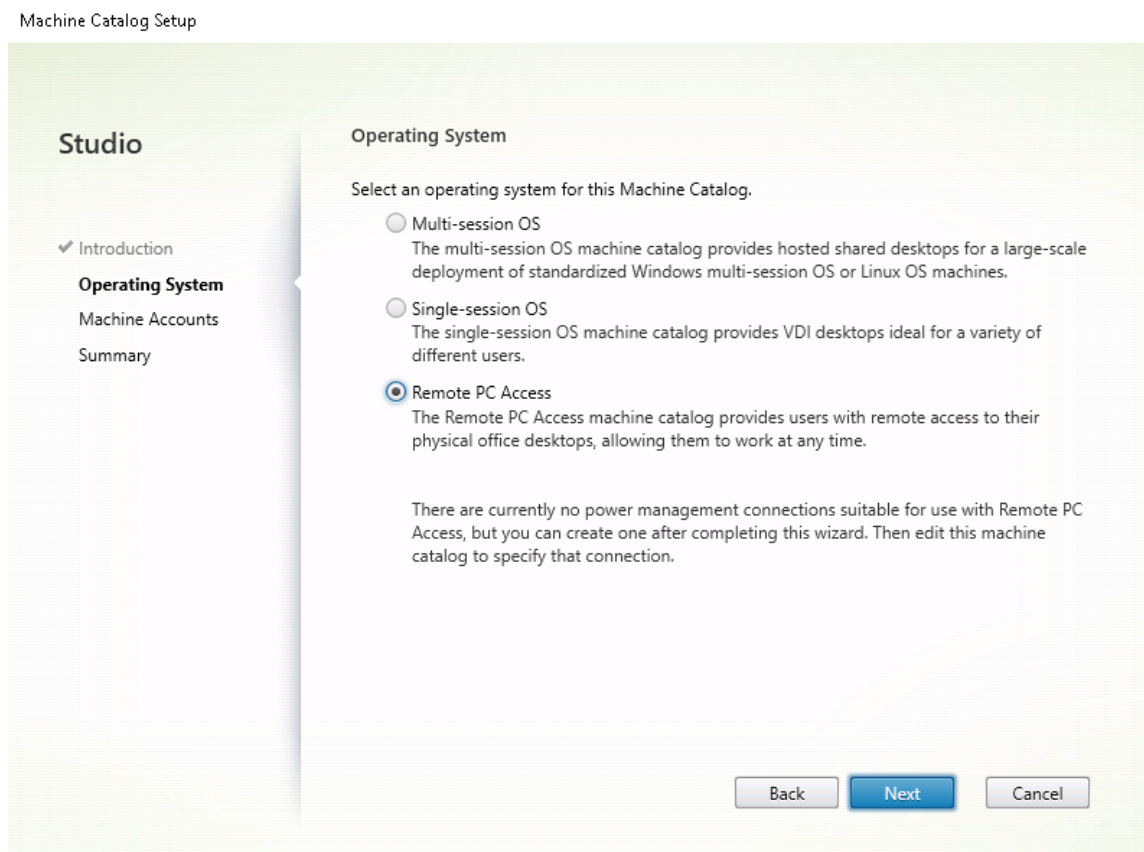


2. Cliquez sur **Suivant** sur la page **Introduction**.

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

The screenshot shows the 'Machine Accounts' step of the 'Machine Catalog Setup' wizard. On the left, a 'Studio' sidebar contains a list of steps: 'Introduction', 'Operating System', 'Machine Accounts' (which is highlighted), and 'Summary'. The main area is titled 'Machine Accounts' and contains the following text: 'Machines in your network domain have an associated machine account. The machine account name is usually the same name as the machine. The machine accounts you choose must match the machines that users use for remote access. To add groups of machines by Organizational Units (OUs), select Add OUs.' Below this text, it says 'Select the machine accounts and/or OUs associated with your users:'. A large rectangular box with a light green background and a grid pattern contains the text 'To get started, add a machine account or OU.' and a blue link 'Learn more'. Below this box are three buttons: 'Add machine accounts...', 'Add OUs...' (which is highlighted with a blue border), and 'Remove'. Below the buttons is an information icon (i) followed by the text 'Select the minimum functional level for this catalog:' and a dropdown menu showing '7.9 (or newer)'. Below this is a note: 'Machines will require the selected VDA version (or newer) in order to register in Delivery Groups that reference this machine catalog.' with a blue link 'Learn more'. At the bottom right are three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

Studio

- ✓ Introduction
- ✓ Operating System
- Machine Accounts**
- Summary

Machine Accounts

Machines in your network domain have an associated machine account. The machine account name is usually the same name as the machine. The machine accounts you choose must match the machines that users use for remote access. To add groups of machines by Organizational Units (OUs), select Add OUs.

Select the machine accounts and/or OUs associated with your users:

To get started, add a machine account or OU.
[Learn more](#)

Add machine accounts... Add OUs... Remove

i Select the minimum functional level for this catalog: 7.9 (or newer) ▾

Machines will require the selected VDA version (or newer) in order to register in Delivery Groups that reference this machine catalog. [Learn more](#)

Back Next Cancel

5. Nommez le catalogue de machines.

Machine Catalog Setup

Studio

- ✓ Introduction
- ✓ Operating System
- ✓ Machine Accounts
- Summary**

Summary

Machine type:Remote PC Access

Machines added:1 organizational unit (OU)

VDA version:7.9 (or newer)

Scopes:-

Zone:Primary

Machine Catalog name:

RemotePC_RHEL81

Machine Catalog description for administrators: (Optional)

Example: Windows 7 SP1 desktops for the London Sales office

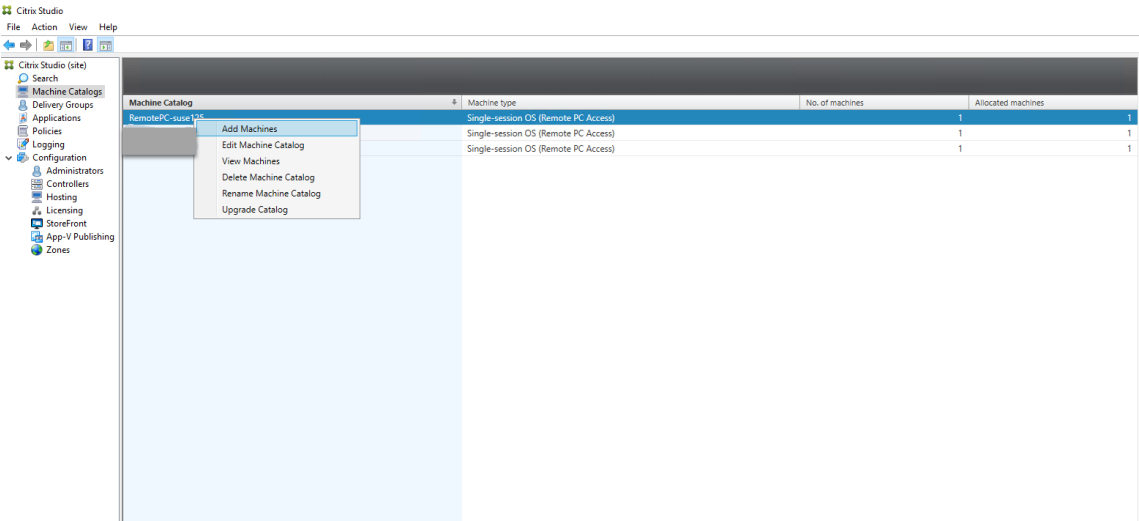
To complete the deployment, assign this Machine Catalog to a Delivery Group by selecting Delivery Groups and then Create or Edit a Delivery Group.

Back

Finish

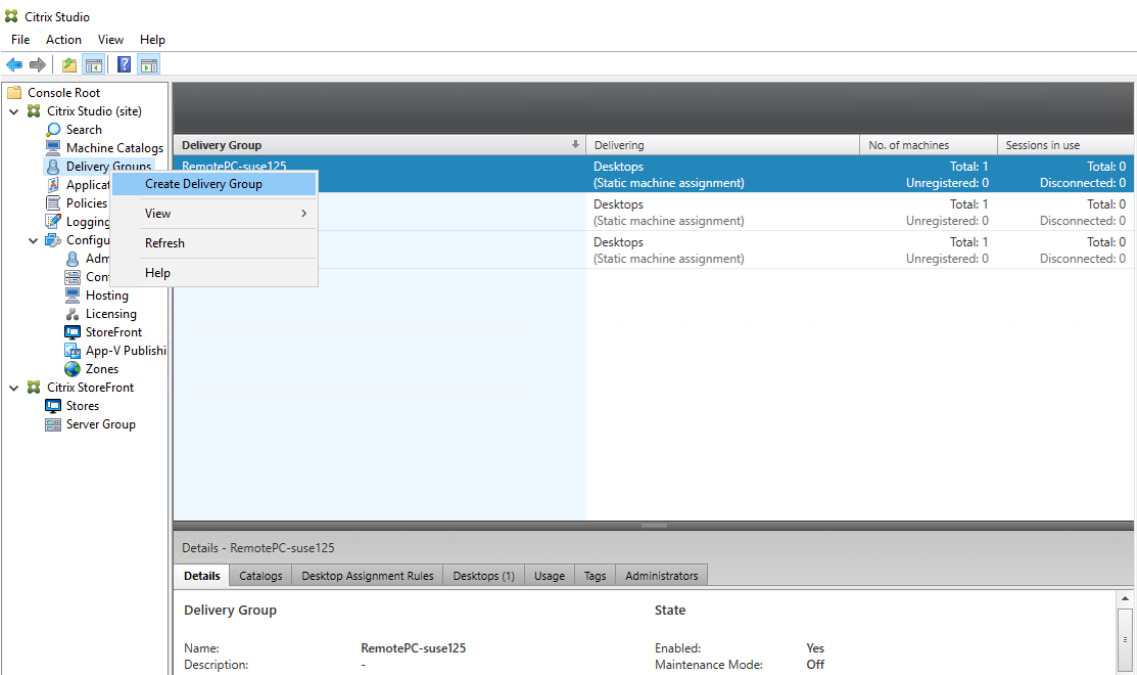
Cancel

6. (Facultatif) Cliquez avec le bouton droit sur le catalogue de machines pour effectuer des opérations pertinentes.

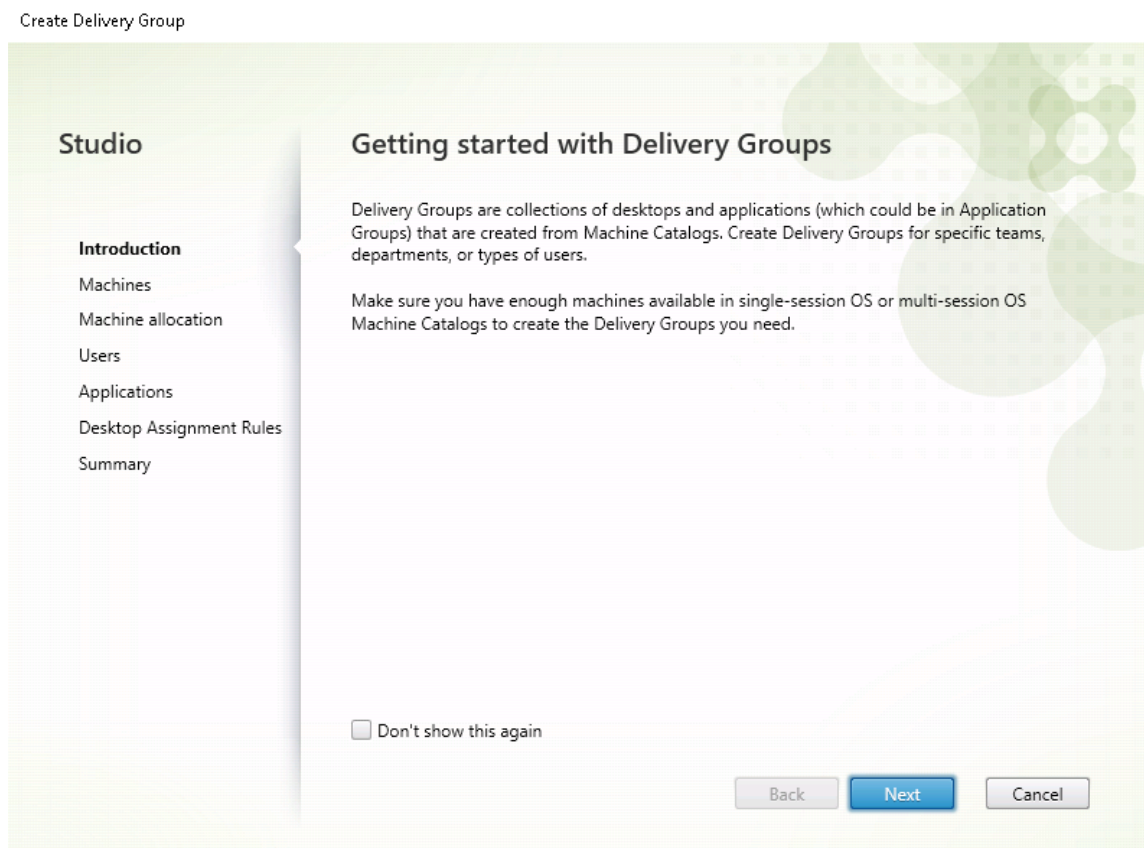


Étape 3 : créer un groupe de mise à disposition pour rendre les PC du catalogue de machines disponibles auprès des utilisateurs qui demandent l'accès

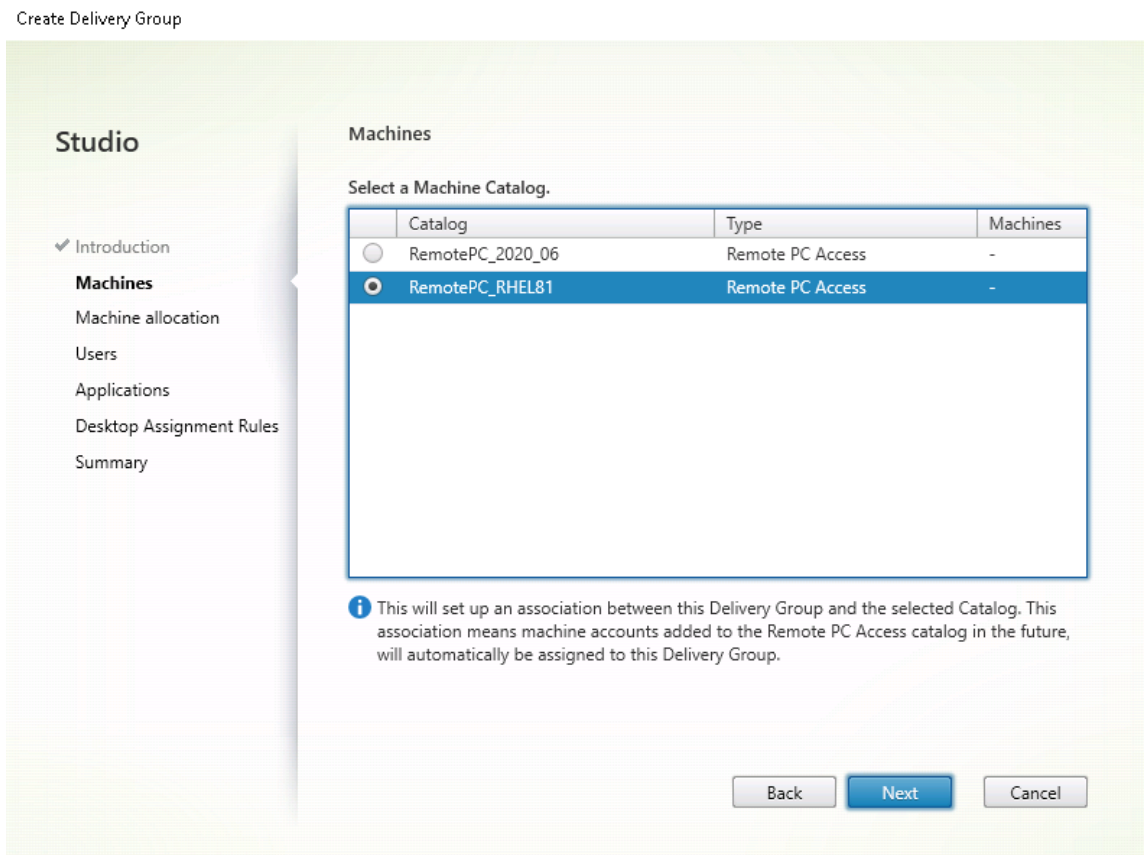
1. Dans Citrix Studio, cliquez avec le bouton droit sur **Groupe de mise à disposition** et sélectionnez **Créer un groupe de mise à disposition** dans le menu contextuel.



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.

Create Delivery Group

The screenshot shows the 'Create Delivery Group' wizard in the 'Studio' application. The left sidebar contains a navigation pane with the following items: 'Introduction' (checked), 'Machines' (checked), 'Users' (selected), 'Desktop Assignment Rules', and 'Summary'. The main area is titled 'Users' and contains the following text: 'Specify who can use the applications and desktops in this Delivery Group. You can assign users and user groups who log on with valid credentials.' Below this text are two radio buttons: 'Allow any authenticated users to use this Delivery Group.' (selected) and 'Restrict use of this Delivery Group to the following users:'. Below the radio buttons is a large empty rectangular box with the text 'Add users and groups' inside. At the bottom of this box are two buttons: 'Add...' and 'Remove'. At the bottom right of the main area are three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

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 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 Wake on LAN dans BIOS et sur la carte d'interface réseau sur chaque machine virtuelle du catalogue de machines.

Remarque : la méthode d'activation de Wake on LAN varie selon les configurations de machine.

- Pour activer Wake on LAN dans BIOS :
 - a) Entrez le BIOS et activez la fonction Wake on LAN.
La méthode d'accès au BIOS dépend du fabricant de votre carte mère et du fournisseur BIOS sélectionné par le fabricant.
 - b) Enregistrez vos paramètres et redémarrez la machine.
- Pour activer Wake on LAN sur la carte d'interface réseau :
 - a) Exécutez la commande `sudo ethtool <NIC>` pour vérifier si votre carte d'interface réseau prend en charge les paquets magiques.
<NIC> est le nom de l'appareil de votre carte d'interface réseau, par exemple, `eth0`. La commande `sudo ethtool <NIC>` fournit une sortie sur les capacités de votre carte d'interface réseau :
 - Si la sortie contient une ligne similaire à `Supports Wake-on: <letters>` où <letters> contient la lettre `g`, votre carte d'interface réseau prend en

charge la méthode de paquet magique Wake on LAN.

- Si la sortie contient une ligne similaire à `Wake-on: <letters>` où `<letters>` contient la lettre `g` et ne contient pas la lettre `d`, la méthode de paquet magique LAN est activée. Toutefois, si la chaîne `<letters>` contient la lettre `d`, elle indique que la fonction Wake on LAN est désactivée. Dans ce cas, activez Wake on LAN en exécutant la commande `sudo ethtool -s <NIC> wol g`.

- b) Sur la plupart des distributions, la commande `sudo ethtool -s <NIC> wol g` est requise après chaque démarrage. Pour définir cette option de manière persistante, procédez comme suit en fonction de vos distributions :

Ubuntu :

Ajoutez la ligne `up ethtool -s <NIC> wol g` au fichier de configuration de l'interface `/etc/network/interfaces`. Par exemple :

```
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](#).

Imprimer

September 5, 2022

Cet article contient des informations sur les meilleures pratiques de l'impression.

Installation

Linux VDA requiert les filtres **cups** et **foomatic**. Les filtres sont installés lorsque vous installez le VDA. Vous pouvez également installer les filtres manuellement en fonction de la distribution. Par exemple :

Sur RHEL 7 :

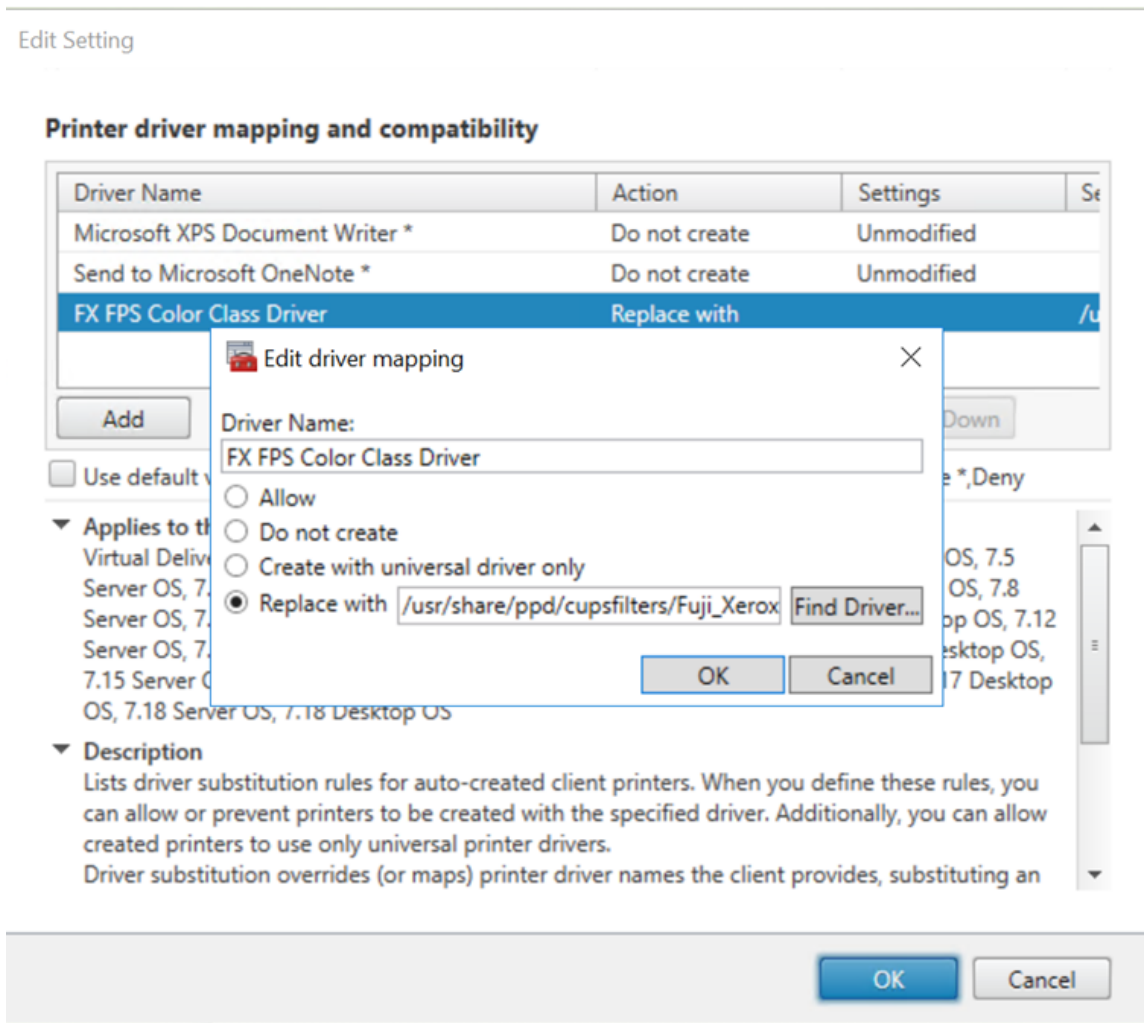
```
1 sudo yum -y install cups
2
3 sudo yum -y install foomatic-filters
```

Configuration

Il existe trois types de pilote d'imprimante universel fournis par Citrix (postscript, pcl5 et pcl6). Toutefois, le pilote d'imprimante universel peut ne pas être compatible avec votre imprimante cliente. Dans ce cas, la seule option dans les versions précédentes était de modifier le fichier de configuration `~/.CtxlpProfile$CLIENT_NAME`. À partir de la version 1906, vous pouvez choisir de configurer la stratégie **Mappage et compatibilité du pilote d'imprimante** dans Citrix Studio.

Pour configurer la stratégie **Mappage et compatibilité du pilote d'imprimante** dans Citrix Studio, procédez comme suit :

1. Sélectionnez la stratégie **Mappage et compatibilité du pilote d'imprimante**.
2. Cliquez sur **Ajouter**.
3. Dans le champ **Nom du pilote**, spécifiez le nom du pilote de l'imprimante cliente. Si vous utilisez l'application Citrix Workspace pour Linux, spécifiez plutôt le nom de l'imprimante.
4. Choisissez **Remplacer par** et entrez le chemin d'accès absolu du fichier du pilote sur le VDA.



Remarque :

- Seuls les fichiers de pilote PPD sont pris en charge.
- Les autres options de la stratégie **Mappage et compatibilité du pilote d'imprimante** ne sont pas prises en charge. Seule l'option **Remplacer par** prend effet.

Utilisation

Vous pouvez imprimer à partir d'applications et de bureaux publiés. Seule l'imprimante par défaut côté client est mappée vers une session Linux VDA. Les noms d'imprimante doivent être différents pour les bureaux et les applications.

- Pour les bureaux publiés :
`CitrixUniversalPrinter:$CLIENT_NAME:dsk$SESSION_ID`
- Pour les applications publiées :
`CitrixUniversalPrinter:$CLIENT_NAME:app$SESSION_ID`

Remarque :

Si le même utilisateur ouvre un bureau publié et une application publiée, les deux imprimantes sont disponibles pour la session. L'impression vers une imprimante de bureau dans une session d'application publiée ou l'impression vers une imprimante d'application dans un bureau publié échoue.

Résolution des problèmes

Impossible d'imprimer

Lorsque l'impression ne fonctionne pas correctement, vérifiez le démon d'impression, **ctxlpmngt** et l'infrastructure CUPS.

Le démon d'impression, **ctxlpmngt**, est un processus par session et doit être en cours d'exécution pour la durée de la session. Exécutez la commande suivante pour vérifier que le démon d'impression est en cours d'exécution. Si le processus **ctxlpmngt** n'est pas exécuté, démarrez manuellement **ctxlpmngt** à partir d'une ligne de commande.

```
1 ps -ef | grep ctxlpmngt
```

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 service ctxcups status
```

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 service cups stop
2
3 sudo vi /etc/systemd/system/printer.target.wants/cups.service
4
5 PrivateTmp=false
6
7 sudo service cups start
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 de spouleur est enregistré sous **/var/spool/cups-ctx/\$logon_user/\$spool_file**.
6. Vérifiez si le fichier de spouleur est vide. Si la taille du fichier de spouleur est zéro, ceci indique un problème. Contactez le support Citrix (et fournissez le journal d'impression) pour une assistance supplémentaire.
7. Si la taille du fichier de spouleur n'est pas zéro, copiez le fichier sur le client. Le contenu du fichier de spouleur dépend du type de pilote de l'imprimante par défaut du client. Si le pilote (natif) de l'imprimante mappée est postscript, le fichier de spouleur peut être ouvert directement dans le système d'exploitation Linux. Vérifiez si le contenu est correct.

Si le fichier de spouleur est PCL ou si le système d'exploitation client est Windows, copiez le fichier de spouleur sur le client et imprimez-le à l'aide de l'imprimante côté client en utilisant un autre pilote d'imprimante.

8. Modifiez l'imprimante mappée pour utiliser un autre pilote d'imprimante. L'exemple suivant utilise l'imprimante client postscript :

- a) Connectez-vous à une session active et ouvrez un navigateur sur le bureau client.
- b) Ouvrez le portail de gestion de l'impression :

```
1 localhost:631
```

- c) Sélectionnez l'imprimante mappée **CitrixUniversalPrinter:\$ClientName:app/dsk\$SESSION_ID** et **Modify Printer**. Cette opération requiert des privilèges d'administrateur.
- d) Conservez la connexion cups-ctx, puis cliquez sur Continue pour modifier le pilote d'imprimante.
- e) Dans les champs **Make** et **Model**, choisissez un pilote d'imprimante autre que le pilote UPD Citrix. Par exemple, si l'imprimante virtuelle CUPS-PDF est installée, sélectionnez le pilote Generic CUPS-PDF Printer. Enregistrez la modification.
- f) Si ce processus réussit, configurez le chemin d'accès au fichier PPD du pilote dans **.Ctxlp-Profile\$CLIENT_NAME** pour autoriser l'imprimante mappée à utiliser le nouveau pilote sélectionné.

Problèmes connus

Les problèmes suivants ont été identifiés lors de l'impression sur le Linux VDA :

Le pilote CTXPS n'est pas compatible avec certaines imprimantes PLC

Si l'impression présente des anomalies, définissez le pilote d'imprimante sur le pilote d'imprimante natif fourni par le fabricant.

Impression lente avec les documents volumineux

Lorsque vous imprimez un document volumineux sur une imprimante cliente locale, le document est transféré sur une connexion serveur. Si la connexion est lente, le transfert risque de durer longtemps.

Notifications d'imprimante et de travaux d'impression d'autres sessions

Le concept de session de Linux n'est pas le même que celui du système d'exploitation Windows. Par conséquent, tous les utilisateurs reçoivent les notifications de l'ensemble du système. Vous pouvez désactiver ces notifications en modifiant le fichier de configuration CUPS : **/etc/cups/cupsd.conf**.

Recherchez le nom de stratégie configuré dans le fichier.

DefaultPolicy **default**

Si le nom de la stratégie est *default*, ajoutez les lignes suivantes dans le bloc XML de la stratégie par défaut :

```
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>
```

Copier et coller des fichiers

November 5, 2021

En utilisant Citrix Virtual Apps and Desktops 2006 et de l'application Citrix Workspace 1903 ou version ultérieure pour Windows, les utilisateurs peuvent désormais copier et coller des fichiers entre une session et un client local. Les fonctions de copier-coller utilisent le menu contextuel ou les raccourcis clavier.

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.

Plates-formes prises en charge

La fonction de copier-coller des fichiers est disponible pour :

- RHEL 7.8
- SLES 12.5
- Ubuntu 16.04
- Ubuntu 18.04
- Debian 10

Stratégies pertinentes

Les stratégies de presse-papiers suivantes sont pertinentes pour la configuration de la fonctionnalité. Pour plus d'informations sur les stratégies de presse-papiers, consultez la section [Liste des stratégies prises en charge](#).

- Redirection de Presse-papiers client
- Mode de mise à jour de la sélection du Presse-papiers
- Mode de mise à jour de la sélection principale

Limitations

- La fonction Couper n'est pas prise en charge. Les opérations Couper d'un fichier sont traitées comme une opération de copie.
- La fonction Glisser-déposer n'est pas prise en charge.
- La copie des répertoires n'est pas prise en charge.

Transfert de fichiers

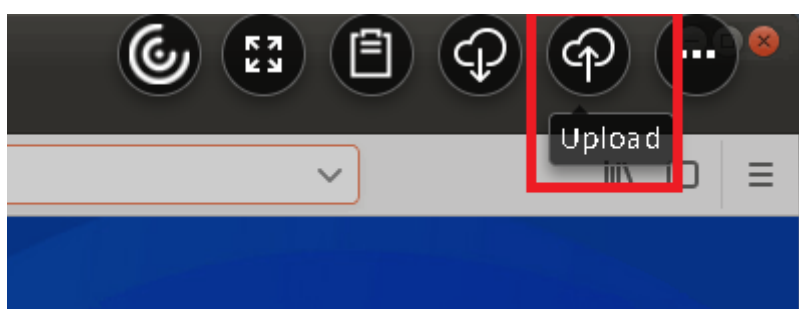
November 5, 2021

Le transfert de fichiers est pris en charge entre le Linux VDA et le périphérique client. Cette fonctionnalité est disponible lorsque le périphérique client exécute un navigateur Web qui prend en charge l'attribut sandbox HTML5. L'attribut sandbox HTML5 permet aux utilisateurs d'accéder à des applications et des bureaux virtuels à l'aide de l'application Citrix Workspace pour HTML5 ou pour Chrome.

Remarque :

le transfert de fichiers est disponible pour l'application Citrix Workspace pour HTML5 et Chrome.

Dans les sessions d'application et de bureau publiées, le transfert de fichiers permet le chargement et le téléchargement de fichiers entre le VDA Linux et la machine cliente. Pour télécharger des fichiers depuis la machine cliente vers le VDA Linux, cliquez sur l'icône **Charger** dans la barre d'outils de l'application Citrix Workspace et sélectionnez le fichier souhaité dans les boîtes de dialogue de fichiers. Pour télécharger des fichiers à partir du VDA Linux sur la machine cliente, cliquez sur l'icône **Télécharger**. Vous pouvez ajouter des fichiers lors du chargement ou du téléchargement. Vous pouvez transférer jusqu'à 100 fichiers en même temps.

**Remarque :**

pour charger et télécharger des fichiers entre le VDA Linux et la machine cliente, assurez-vous que la barre d'outils de l'application Citrix Workspace est activée.

Vous pouvez utiliser une version de l'application Citrix Workspace qui vous permet de glisser-déposer des fichiers.

Le téléchargement automatique est une amélioration du transfert de fichiers. Les fichiers que vous téléchargez ou déplacez vers le répertoire **Enregistrer sur mon appareil** sur le VDA sont automatiquement transférés sur la machine cliente.

Remarque :

Le téléchargement automatique nécessite que les stratégies **Autoriser le transfert de fichiers entre le bureau et le client** et **Télécharger des fichiers depuis le bureau** soient définies sur **Autorisé**.

Voici quelques cas d'utilisation pour le téléchargement automatique :

- Télécharger des fichiers vers le répertoire **Enregistrer sur mon appareil**

Dans les sessions d'applications de bureau et de navigateur Web publiées, les fichiers que vous téléchargez à partir de sites Web peuvent être enregistrés dans le répertoire **Enregistrer sur mon appareil** du VDA pour un transfert automatique vers la machine cliente. Pour effectuer le

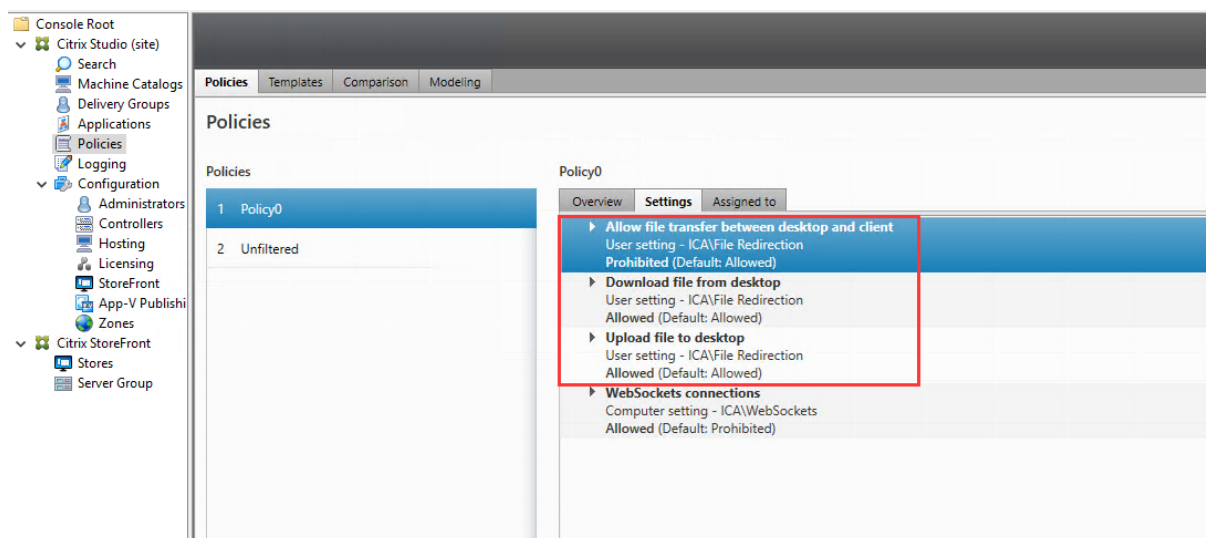
téléchargement automatique, définissez le répertoire de téléchargement par défaut du navigateur Web en session sur **Enregistrer sur mon appareil** et définissez un répertoire de téléchargement local dans le navigateur Web qui exécute votre application Citrix Workspace pour HTML5 ou Chrome.

- Déplacer ou copier des fichiers vers **Enregistrer sur mon appareil**

Dans les sessions de bureau publiées, choisissez les fichiers cibles et déplacez-les ou copiez-les dans le répertoire **Enregistrer sur mon appareil** pour qu'ils soient disponibles sur la machine cliente.

Stratégies de transfert de fichiers

Vous pouvez utiliser Citrix Studio pour définir les stratégies de transfert de fichiers. Par défaut, le transfert de fichiers est activé.



Descriptions des stratégies :

- **Autoriser le transfert de fichiers entre le bureau et le client.** Autorise ou empêche les utilisateurs de transférer des fichiers entre une session Citrix Virtual Apps and Desktops et leurs appareils.
- **Télécharger des fichiers depuis le bureau.** Autorise ou empêche les utilisateurs de télécharger des fichiers depuis une session Citrix Virtual Apps and Desktops vers leurs appareils.
- **Charger des fichiers sur le bureau.** Autorise ou empêche les utilisateurs de charger des fichiers depuis leurs appareils sur une session Citrix Virtual Apps and Desktops.

Remarque :

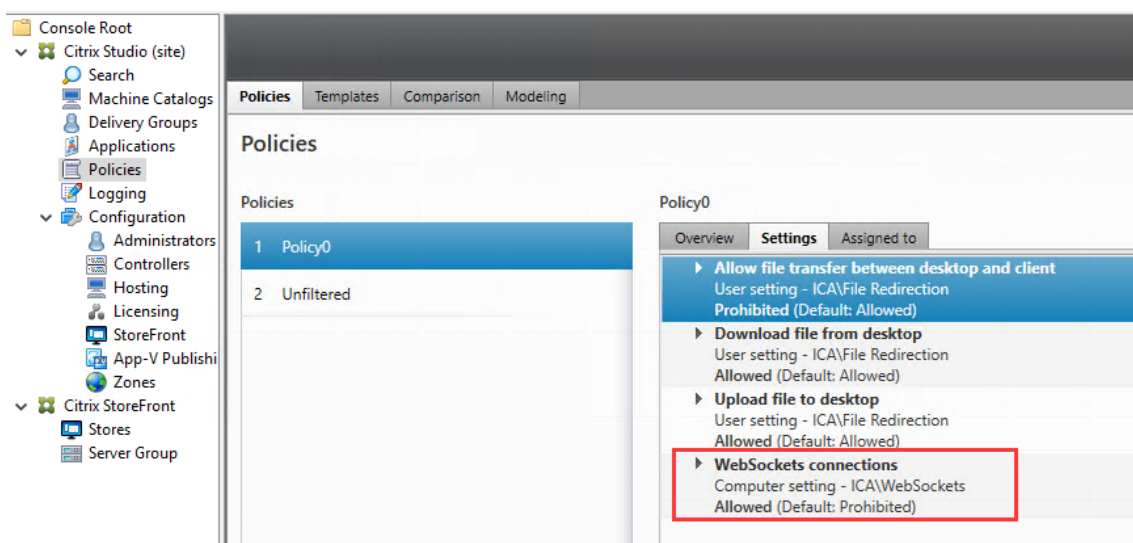
pour vous assurer que les stratégies **Télécharger des fichiers depuis le bureau** et **Charger des**

fichiers sur le bureau prennent effet, définissez l'option **Autoriser le transfert de fichiers entre le bureau et le client** sur **Autorisé**.

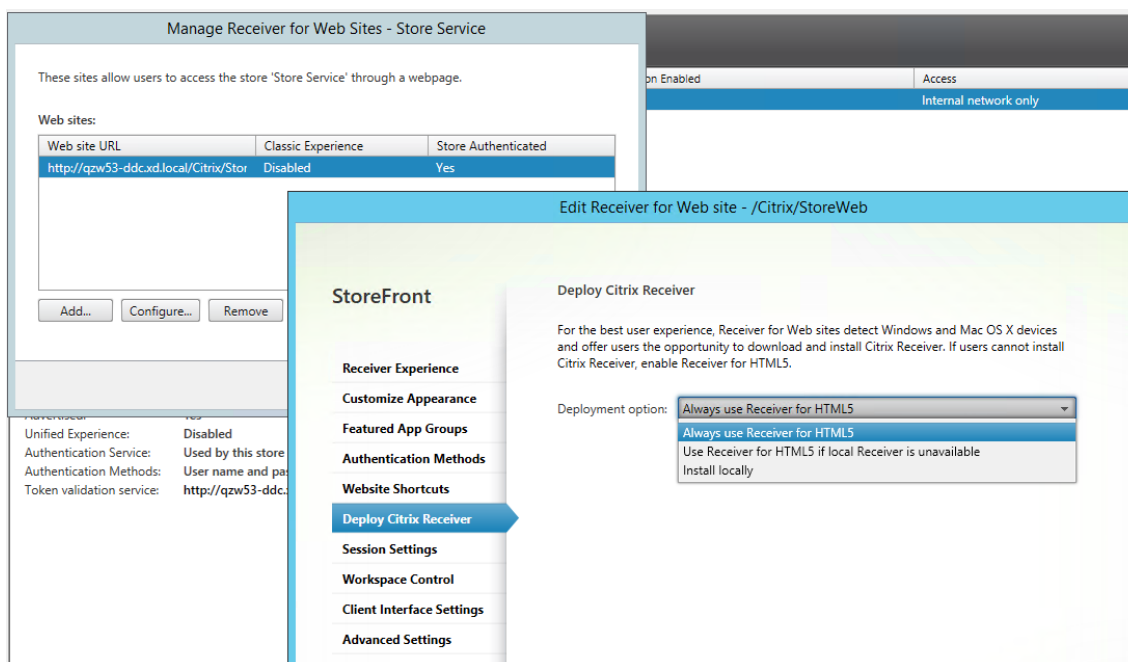
Utilisation

Pour utiliser la fonctionnalité de transfert de fichiers via l'application Citrix Workspace pour HTML5 :

1. Dans Citrix Studio, définissez la stratégie **Connexions WebSockets** sur **Autorisé**.



2. Dans Citrix Studio, activez le transfert de fichiers via les stratégies de transfert de fichiers décrites précédemment.
3. Dans la console de gestion Citrix StoreFront, cliquez sur **Magasins**, sélectionnez le nœud **Gérer les sites Receiver pour Web** et activez Citrix Receiver pour HTML5 en sélectionnant l'option **Toujours utiliser Receiver pour HTML5**.



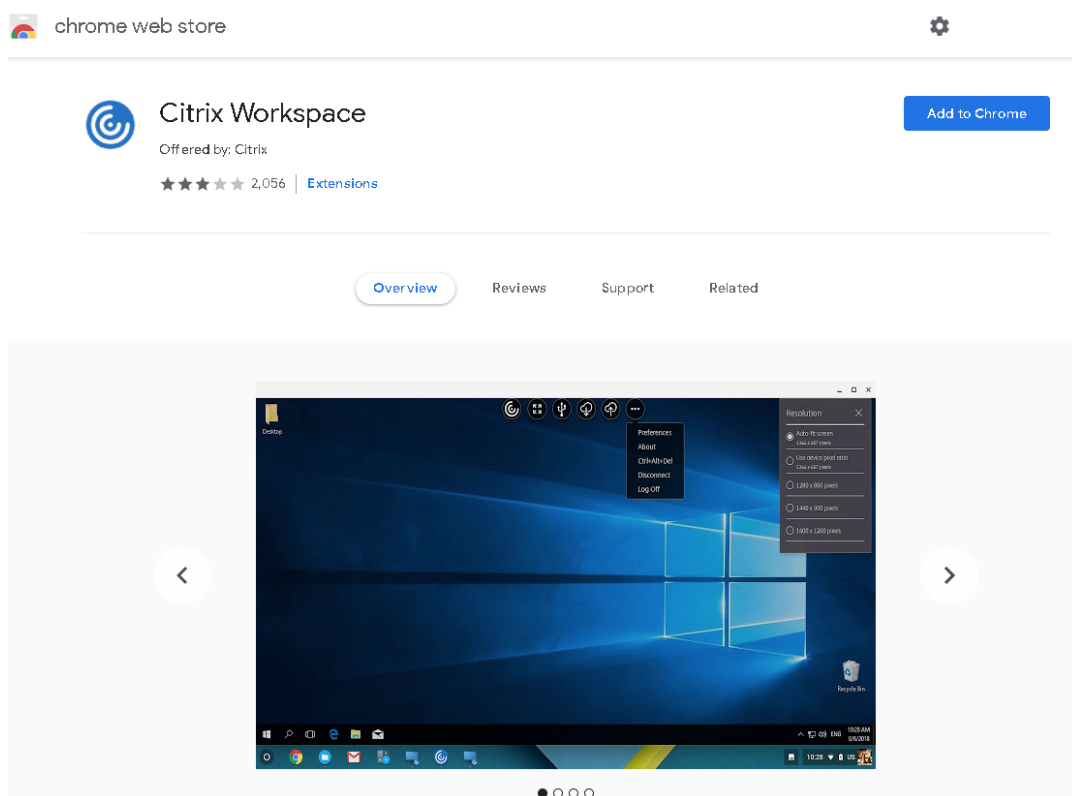
4. Lancez une session de bureau virtuel ou d'application de navigateur Web. Effectuez un ou plusieurs transferts de fichiers entre le VDA Linux et votre machine cliente.

Pour utiliser la fonctionnalité de transfert de fichiers via l'application Citrix Workspace pour Chrome :

1. Activez le transfert de fichiers via les stratégies de transfert de fichiers décrites précédemment.
2. Obtenez l'application Citrix Workspace à partir de Chrome Web Store.

Ignorez cette étape si vous avez déjà ajouté l'application Citrix Workspace pour Chrome à la page des applications Chrome.

- a) Tapez **Citrix Workspace for Chrome** dans la zone de recherche de Google Chrome. Cliquez sur l'icône de recherche.
- b) Parmi les résultats de la recherche, cliquez sur l'URL du Chrome Web Store où l'application Citrix Workspace est disponible.



- c) Cliquez sur **Ajouter à Chrome** pour ajouter l'application Citrix Workspace à Google Chrome.
3. Cliquez sur l'application Citrix Workspace pour Chrome sur la page des applications Chrome.
4. Tapez l'URL de votre magasin StoreFront pour la connexion.
Ignorez cette étape si vous avez déjà saisi l'URL.
5. Lancez une session de bureau virtuel ou d'application. Effectuez un ou plusieurs transferts de fichiers entre le VDA Linux et votre machine cliente.

Impression PDF

November 5, 2021

Si vous utilisez une version de l'application Citrix Workspace qui prend en charge l'impression PDF, vous pouvez imprimer des PDF convertis depuis les sessions Linux VDA. Les tâches d'impression de session sont envoyées à la machine locale sur laquelle l'application Citrix Workspace est installée. Sur la machine locale, vous pouvez ouvrir les fichiers PDF en utilisant la visionneuse PDF de votre choix et les imprimer sur l'imprimante de votre choix.

Le Linux VDA prend en charge l'impression PDF sur les versions suivantes de l'application Citrix Workspace :

- Citrix Receiver pour HTML5 versions 2.4 à 2.6.9, application Citrix Workspace 1808 pour HTML5 et versions ultérieures
- Citrix Receiver pour Chrome versions 2.4 à 2.6.9, application Citrix Workspace 1808 pour Chrome et versions ultérieures
- Application Citrix Workspace 1905 pour Windows et versions ultérieures

Configuration

En plus d'utiliser l'une des versions de l'application Citrix Workspace prenant en charge l'impression PDF, vous devez également activer les stratégies suivantes dans Citrix Studio :

- **Redirection d'imprimante cliente** (activée par défaut)
- **Créer automatiquement l'imprimante universelle PDF** (désactivée par défaut)

Lorsque ces stratégies sont activées, un aperçu d'impression s'affiche sur la machine locale, ce qui vous permet de sélectionner une imprimante lorsque vous cliquez sur **Imprimer** dans votre session. Consultez la [documentation de l'application Citrix Workspace](#) pour plus d'informations sur la configuration d'imprimantes par défaut.

Configurer les graphiques

April 18, 2024

Cet article fournit des instructions pour configurer et ajuster les graphiques du Linux VDA.

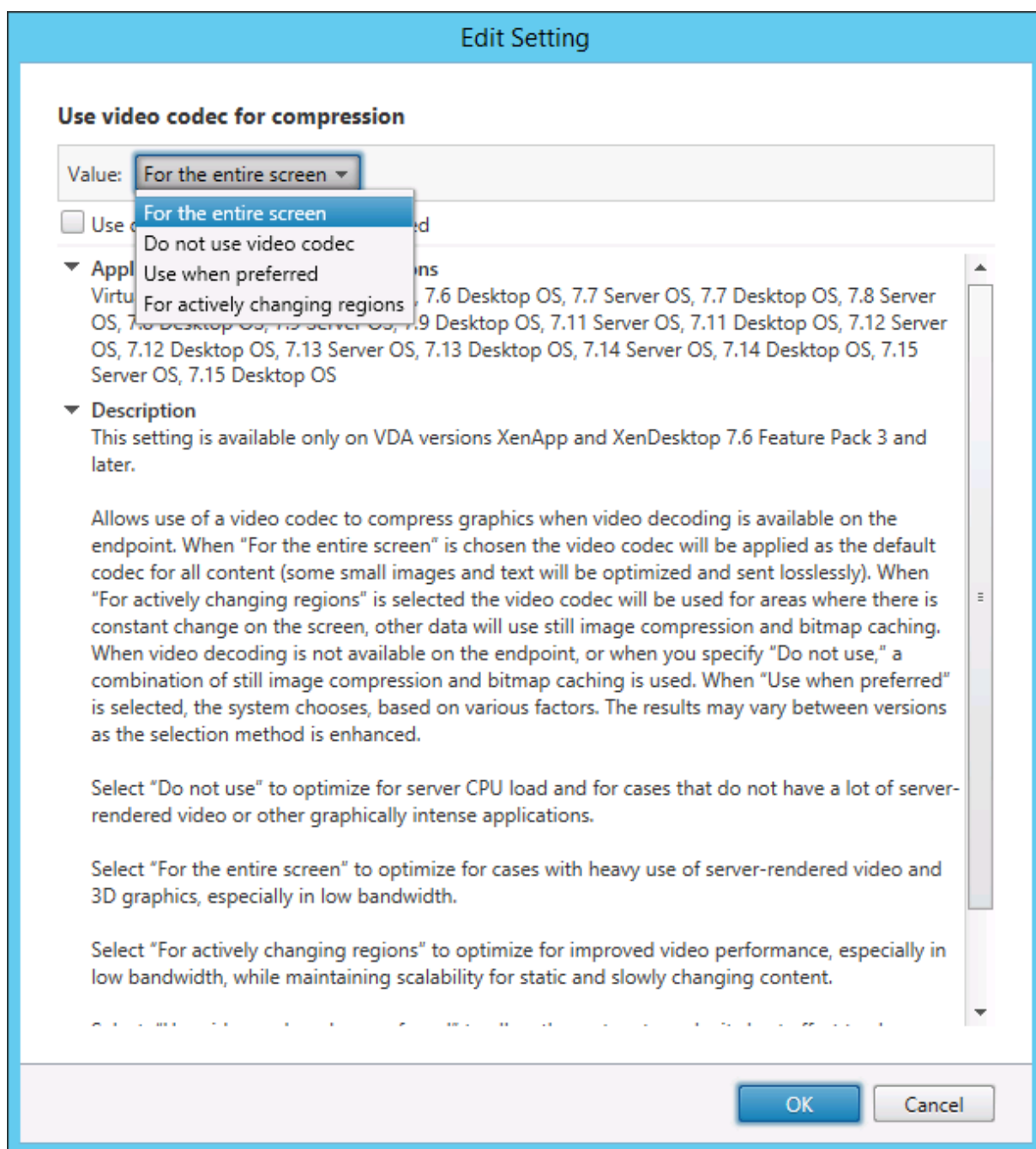
Pour de plus amples informations, consultez les sections [Configuration système requise](#) et [Présentation de l'installation](#).

Configuration

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. Le maintien de 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.
- **Pour les zones changeant constamment.** La technologie d'affichage adaptatif dans Thinwire identifie les images en mouvement (vidéo, 3D en mouvement) et utilise H.264 uniquement dans la partie de l'écran sur laquelle l'image est en mouvement. L'**utilisation sélective du codec vidéo H.264** permet à HDX Thinwire de détecter et de coder des parties de l'écran qui sont fréquemment mises à jour à l'aide du codec vidéo H.264, par exemple du contenu vidéo. La compression d'images immobiles (JPEG, RLE) et la mise en cache de bitmaps continuent à être utilisées pour le reste de l'écran, y compris le texte et l'imagerie photographique. Les utilisateurs bénéficient d'une bande passante plus faible et d'une meilleure qualité pour le contenu vidéo, conjointement avec du texte sans perte ou à des images de haute qualité. Pour activer cette fonctionnalité, remplacez le paramètre de stratégie **Utiliser codec vidéo pour la compression** par **Utiliser au choix** (valeur par défaut) ou **Pour les zones changeant constamment**. Pour plus d'informations, veuillez consulter la section [Paramètres de stratégie des graphiques](#).



D'autres paramètres de stratégie, y compris les paramètres de stratégie Affichage visuel suivants, peuvent être utilisés pour optimiser les performances de la communication à distance d'écran :

- **Nombre de couleurs préféré pour les graphiques simples**
- **Taux de trames cible**
- **Qualité visuelle**

Utilisation de H.264 pour l'option Sans perte si possible dans Thinwire

Par défaut, la préférence **Sans perte si possible** du paramètre de stratégie **Qualité visuelle** est désormais H.264 au lieu de JPEG pour les images en mouvement.

Le codage H.264 offre une qualité d'image supérieure. La stratégie **Utiliser codec vidéo pour la compression** contrôle cette préférence avec la valeur par défaut **Utiliser au choix**. Pour forcer l'option **Sans perte si possible** à utiliser JPEG, définissez la stratégie **Utiliser codec vidéo pour la compression** sur **Ne pas utiliser de codec vidéo**. Si votre client ne prend pas en charge le mode sélectif H.264, l'option **Sans perte si possible** revient au format JPEG, quels que soient les paramètres de stratégie. Citrix Receiver pour Windows 4.9 à 4.12, Citrix Receiver pour Linux 13.5 à 13.10, l'application Citrix Workspace 1808 pour Windows et versions ultérieures, et Citrix Workspace application 1808 pour Linux et versions ultérieures prennent en charge Sélectif 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](#).

Prise en charge du codec vidéo H.265

À compter de la version 7.18, le Linux VDA prend en charge le codec vidéo H.265 pour l'accélération matérielle des graphiques et vidéos distants. Vous pouvez utiliser cette fonctionnalité sur Citrix Receiver pour Windows 4.10 à 4.12 et sur l'application Citrix Workspace 1808 pour Windows et versions ultérieures. Pour bénéficier de cette fonctionnalité, activez-la à la fois sur le Linux VDA et sur votre client. Si le GPU de votre client ne prend pas en charge le décodage H.265 à l'aide de l'interface DXVA, le paramètre de stratégie de décodage H.265 pour les graphiques est ignoré et la session utilise le codec vidéo H.264. Pour plus d'informations, consultez la section [Codage vidéo H.265](#).

Pour activer le codage matériel H.265 sur le VDA :

1. Activez la stratégie **Utiliser le codage matériel pour le codec vidéo**.
2. Activez la stratégie **Optimiser pour la charge des graphiques 3D**.
3. Assurez-vous que la stratégie **Utiliser codec vidéo pour la compression** est définie par défaut ou définie sur **Pour l'écran entier**.
4. Assurez-vous que la stratégie **Qualité visuelle** n'est **PAS** définie sur **Sans perte si possible** ni sur **Toujours sans perte**.

Pour activer le codage matériel H.265 sur votre client, consultez la section [Codage vidéo H.265](#).

Prise en charge du codage logiciel YUV444

Le Linux VDA prend en charge le codage logiciel YUV444. Le schéma de codage YUV attribue à chaque pixel des valeurs de luminosité et de couleur. En YUV, **Y** représente la luminosité ou les valeurs « luma

» et **UV** représentent la couleur ou les valeurs « chroma ». Vous pouvez utiliser cette fonctionnalité du Linux VDA sur Citrix Receiver pour Windows 4.10 à 4.12 et sur l'application Citrix Workspace 1808 pour Windows et versions ultérieures.

Chaque valeur unique Y, U et V comprend 8 bits, ou un octet, de données. Le format de données YUV444 transmet 24 bits par pixel. Le format de données YUV422 partage les valeurs U et V entre deux pixels, ce qui permet un taux de transmission moyen de 16 bits par pixel. Le tableau suivant contient une comparaison intuitive entre YUV444 et YUV420.

YUV444				YUV420			
	A	B	C		A	B	C
1	Citrix	Citrix	Citrix	1	Citrix	Citrix	Citrix
2	Citrix	Citrix	Citrix	2	Citrix	Citrix	Citrix
3	Citrix	Citrix	Citrix	3	Citrix	Citrix	Citrix
4	Citrix	Citrix	Citrix	4	Citrix	Citrix	Citrix
5	Citrix	Citrix	Citrix	5	Citrix	Citrix	Citrix
6	Citrix	Citrix	Citrix	6	Citrix	Citrix	Citrix

Pour activer le codage logiciel YUV444 sur le VDA :

1. Assurez-vous que la stratégie **Utiliser codec vidéo pour la compression** est définie sur **Pour l'écran entier**.
2. Assurez-vous que la stratégie **Qualité visuelle** est définie sur **Toujours sans perte** ou **Sans perte si possible**

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 fonction des estimations de bande passante. Cette nouvelle fonctionnalité fournit un mécanisme pour équilibrer la netteté et la fluidité.

Par défaut, cette fonction est activée. Pour le désactiver, exécutez la commande suivante :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "DisableReconfigureEncoder" -d "0x00000001" --force
```

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](#).

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 si H.264 est utilisé

Exécutez la commande suivante pour vérifier si H.264 est en cours d'utilisation (**0** signifie pas en cours d'utilisation ; **1** signifie en cours d'utilisation) :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H264
```

Le résultat se présente comme suit :


```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"  
-v "H264"-d "0x00000000"--force
```

Vérifier si H.265 est utilisé

Exécutez la commande suivante pour vérifier si H.265 plein écran est en cours d'utilisation (**0** signifie pas en cours d'utilisation ; **1** signifie en cours d'utilisation) :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H265
```

Le résultat se présente comme suit :

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"  
-v "H265"-d "0x00000000"--force
```

Vérifier quel schéma de codage YUV est utilisé

Exécutez la commande suivante pour vérifier quel schéma de codage YUV est utilisé (**0** signifie YUV420. **1** signifie YUV422. **2** signifie YUV444) :

Remarque : la valeur de YuvFormat n'a de sens que lorsqu'un codec vidéo est utilisé.

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep YUVFormat
```

Le résultat se présente comme suit :

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"  
-v "YUVFormat"-d "0x00000000"--force
```

Vérifier si le codage logiciel YUV444 est utilisé

Exécutez la commande suivante pour vérifier si le codage logiciel YUV444 est utilisé :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep Graphics
```

Lorsque YUV444 est utilisé, le résultat se présente comme suit :

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"  
-v "GraphicsMode"-d "0x00000001"--force  
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"  
-v "H264"-d "0x00000001"--force  
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"  
-v "HardwareEncoding"-d "0x00000000"--force  
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"  
-v "YUVFormat"-d "0x00000002"--force
```

Vérifier si le codage matériel est utilisé pour 3D Pro

Exécutez la commande suivante (0 signifie qu'il n'est pas utilisé ; 1 signifie qu'il est utilisé) :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep HardwareEncoding
```

Le résultat se présente comme suit :

```
create -k "HKLM\Software\Citrix\Ica\Session\1\Graphics"-t "REG_DWORD"
-v "HardwareEncoding"-d "0x00000001"--force
```

Une autre méthode consiste à utiliser la commande **nvidia-smi**. Les résultats se présentent comme suit lorsque le codage matériel est utilisé :

```
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      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 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 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 xe vm-param-set uuid=<vm-uuid> platform:vgpu_extra_args="disable_vnc=1"
```

Les cartes graphiques NVIDIA K2 ne prennent pas en charge le codage matériel YUV444 en mode passthrough

Si le paramètre de stratégie **Sans perte si possible** est activé, un écran noir ou gris apparaît lorsque les utilisateurs lancent une application ou une session de bureau avec une carte graphique NVIDIA K2. Ce problème se produit car les cartes graphiques NVIDIA K2 ne prennent pas en charge le codage matériel YUV444 en mode passthrough. Pour plus d'informations, consultez la page [Video Encode and Decode GPU Support Matrix](#).

Les fenêtres contextuelles du bureau Gnome 3 sont lentes lors de l'ouverture de session

Il s'agit d'une limitation du démarrage de session de bureau Gnome 3.

Certaines applications OpenGL/WebGL ne s'affichent pas correctement après le redimensionnement de l'application Citrix Workspace

Si vous redimensionnez la fenêtre de l'application Citrix Workspace, la résolution de l'écran est modifiée. Le pilote propriétaire NVIDIA modifie certains états internes et peut attendre des applications une réponse adaptée. Par exemple, l'élément de bibliothèque WebGL **lightgl.js** peut générer une erreur « `Rendering to this texture is not supported (incomplete frame buffer)` ».

Affichage progressif Thinwire

November 5, 2021

L'interactivité de session peut se dégrader sur des connections à faible bande passante ou à latence élevée. Par exemple, sur les connexions avec une bande passante inférieure à 2 Mbits/s ou une latence

de plus de 200 ms, le défilement sur 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 compter de la version 7.18, HDX Thinwire bascule par défaut en mode de mise à jour progressive lorsque la bande passante disponible tombe en dessous de 2 Mbits/s, ou que la latence du réseau dépasse 200 ms. Dans ce mode :

- Toutes les images statiques sont fortement compressées.
- La qualité du texte est réduite.

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.

Autres graphiques 3D

March 11, 2024

Vue d'ensemble

Grâce à l'amélioration de cette fonctionnalité, Linux VDA prend non seulement en charge les cartes NVIDIA GRID 3D, mais également les cartes 3D non-GRID.

Installation

Pour utiliser la fonctionnalité de graphiques 3D non-GRID, vous devez :

- Installer XDamage avant de commencer. En règle générale, XDamage existe sous forme d'extension de XServer.
- Définissez `CTX_XDL_HDX_3D_PRO` sur `Y` lors de l'installation de Linux VDA. Pour plus d'informations sur les variables d'environnement, consultez [Étape 3 : définir l'environnement d'exécution afin de terminer l'installation](#).

Configuration

Fichiers de configuration Xorg

Si votre pilote de carte 3D est NVIDIA, les fichiers de configuration sont installés et définis automatiquement.

Autres types de cartes 3D

Si votre pilote de carte 3D n'est pas NVIDIA, vous devez modifier les quatre fichiers de configuration de modèle installés sous `/etc/X11/`:

- `ctx-driver_name-1.conf`
- `ctx-driver_name-2.conf`
- `ctx-driver_name-3.conf`
- `ctx-driver_name-4.conf`

En utilisant **`ctx-driver_name-1.conf`** en tant qu'exemple, suivez la procédure suivante pour modifier les fichiers de configuration de modèle :

1. Remplacez **`driver_name`** par le nom de votre pilote.

Par exemple, si votre nom de pilote est `intel`, vous pouvez modifier le nom du fichier de configuration pour `ctx-intel-1.conf`.

2. Ajoutez les informations du pilote vidéo.

Chaque fichier de configuration de modèle contient une section appelée « Machine », à laquelle un commentaire est ajouté. Cette section décrit les informations du pilote vidéo. Activez cette section avant d'ajouter les informations de votre pilote vidéo. Pour activer cette section :

- a) Consultez le guide de la carte 3D fourni par le fabricant pour obtenir des informations sur la configuration. Un fichier de configuration natif peut être généré. Vérifiez que votre carte 3D fonctionne dans un environnement local avec le fichier de configuration natif lorsque vous n'utilisez pas une session ICA de Linux VDA.
 - b) Copiez la section « Device » du fichier de configuration natif vers **`ctx-driver_name-1.conf`**.
3. Exécutez la commande suivante pour définir la clé de registre de façon à permettre au Linux VDA de reconnaître le nom du fichier de configuration défini à l'étape 1.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\System\
  CurrentControlSet\Control\Citrix\XDamage" -t "REG_SZ" -v "
  DriverName" -d "intel" --force
```

Activer la fonctionnalité de graphiques 3D non-GRID

Cette fonctionnalité est désactivée par défaut. Vous pouvez exécuter la commande suivante pour l'activer en définissant `XDamageEnabled` sur 1.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\System\
  CurrentControlSet\Control\Citrix\XDamage" -t "REG_DWORD" -v "
  XDamageEnabled" -d "0x00000001" --force
```


Dépannage

Pas de sortie graphique ou sortie illisible

Si vous pouvez exécuter des applications 3D localement et que toutes les configurations sont correctes, une sortie graphique manquante ou illisible est due à un bogue. Utilisez `/opt/Citrix/VDA/bing/setlog` et définissez `GFX_X11` sur `Détaillé` afin de collecter les informations de trace à des fins de débogage.

Le codage matériel ne fonctionne pas

Cette fonctionnalité prend uniquement en charge le codage logiciel.

Configurer les stratégies

November 5, 2021

Installation

Consultez les articles relatifs à l'installation pour préparer l'agent Linux VDA.

Dépendances

Assurez-vous que vous installez ces dépendances avant d'installer le package Linux VDA.

RHEL/CentOS :

```
1 sudo yum -y install openldap
2
3 sudo yum -y install libxml2
4
5 sudo yum -y install cyrus-sasl
6
7 sudo yum -y install cyrus-sasl-gssapi
```

SLES/SELD :

```
1 sudo zypper install openldap2
2
3 sudo zypper install libxml2
4
5 sudo zypper install cyrus-sasl
```

```
6
7 sudo zypper install cyrus-sasl-gssapi
```

Ubuntu :

```
1 sudo apt-get install -y libldap-2.4-2
2
3 sudo apt-get install -y libsasl2-2
4
5 sudo apt-get install -y libsasl2-modules-gssapi-mit
```

Configuration

Paramètres de stratégie dans Citrix Studio

Pour configurer des stratégies dans Citrix Studio, procédez comme suit :

1. Ouvrez **Citrix Studio**.
2. Sélectionnez le panneau **Stratégies**.
3. Cliquez sur **Créer une stratégie**.
4. Définissez la stratégie en fonction de la [liste de stratégies prises en charge](#).

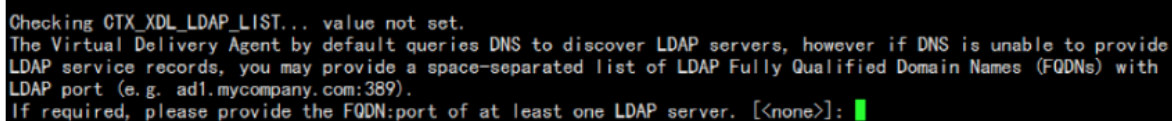
Paramètre du serveur LDAP sur le VDA

Le paramètre du serveur LDAP sur le Linux VDA est facultatif pour les environnements à domaine unique, mais obligatoire pour les environnements comportant plusieurs domaines et forêts. Le paramètre est requis par le service de stratégie pour effectuer une recherche LDAP dans ces environnements.

Après l'installation du package Linux VDA, exécutez la commande suivante :

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

Saisissez tous les serveurs LDAP dans le format recommandé : liste de noms de domaines complets (FQDN) séparés par des espaces avec le port LDAP (par exemple, ad1.mycompany.com:389 ad2.mycompany.com:389).



```
Checking CTX_XDL_LDAP_LIST... value not set.
The Virtual Delivery Agent by default queries DNS to discover LDAP servers, however if DNS is unable to provide
LDAP service records, you may provide a space-separated list of LDAP Fully Qualified Domain Names (FQDNs) with
LDAP port (e.g. ad1.mycompany.com:389).
If required, please provide the FQDN:port of at least one LDAP server. [<none>]: █
```

Vous pouvez également exécuter la commande **ctxreg** pour écrire ce paramètre directement sur le registre :

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent" -t "REG_SZ" -v "ListOfLDAPServers" -d "ad1.mycompany.com:389 ad2.mycomany.com:389" --force
```

Liste des stratégies prises en charge

November 5, 2021

Liste des stratégies prises en charge avec le Linux VDA

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Utilisation de l'heure locale du client	UseLocalTimeOfClient	Utilisateur	ICA\Contrôle de fuseau horaire	Utiliser le fuseau horaire du serveur
Calcul des boucles ICA	IcaroundTripCheckEnabled	Ordinateur	ICA\Contrôle de l'utilisateur final	Activé (1)
Intervalle de calcul des boucles ICA	IcaroundTripCheckPeriod	Ordinateur	ICA\Contrôle de l'utilisateur final	15
Calcul des boucles ICA pour les connexions inactives	IcaroundTripCheckWindow	Ordinateur	ICA\Contrôle de l'utilisateur final	Désactivé (0)
Limite de bande passante globale de session	LimitOverallBw	Utilisateur	ICA\Bande passante	0
Limite de bande passante de redirection audio	LimitAudioBw	Utilisateur	ICA\Bande passante	0
Pourcentage de limite de bande passante de la redirection audio	LimitAudioBwPercentage	Utilisateur	ICA\Bande passante	0

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Limite de bande passante de redirection du périphérique USB client	LimitUSBBw	Utilisateur	ICA\Bande passante	0
Pourcentage de bande passante de redirection du périphérique USB client	LimitUSBBwPercent	Utilisateur	ICA\Bande passante	0
Limite de bande passante de redirection du Presse-papiers	LimitClipbdBW	Utilisateur	ICA\Bande passante	0
Pourcentage de la limite de la bande passante de redirection du Presse-papiers	LimitClipbdBWPercent	Utilisateur	ICA\Bande passante	0
Limite de bande passante de redirection de fichier	LimitCdmBw	Utilisateur	ICA\Bande passante	0
Pourcentage de limite de bande passante de redirection de fichier	LimitCdmBwPercent	Utilisateur	ICA\Bande passante	0
Limite de bande passante de redirection d'imprimante	LimitPrinterBw	Utilisateur	ICA\Bande passante	0
Pourcentage de limite de bande passante de redirection de l'imprimante	LimitPrinterBwPercent	Utilisateur	ICA\Bande passante	0

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Connexions WebSockets	AcceptWebSocketsConnections	Ordinateur	ICA\WebSockets	Interdit
Numéro de port WebSockets	WebSocketsPort	Ordinateur	ICA\WebSockets	8008
Liste de serveurs d'origine WebSockets approuvés	WSTrustedOriginServers	Ordinateur	ICA\WebSockets	*
Persistances ICA	SendICAKeepAlives	Ordinateur	Persistence ICA	Ne pas envoyer de messages de persistance ICA (0)
Délai d'expiration de persistance ICA	ICAKeepAliveTimeout	Ordinateur	Persistence ICA	60 secondes
Numéro de port de l'écouteur ICA	IcaListenerPortNumber	Ordinateur	ICA	1494
Transport adaptatif HDX	HDXoverUDP	Ordinateur	ICA	Préfér�� (2)
Connexions de fiabilité de session	AcceptSessionReliability	Ordinateur	ICA\Fiabilité de session	Autorisé (1)
Niveau de transparence de l'interface durant la reconnexion	ReconnectionUiTransparencyLevel	Ordinateur	ICA\Reconnexion automatique des clients	80 %
Numéro de port de la fiabilité de session	SessionReliabilityPort	Ordinateur	ICA\Fiabilité de session	2598
Expiration de délai de la fiabilité de session	SessionReliabilityTimeout	Ordinateur	ICA\Fiabilité de session	180 s
Reconnexion automatique des clients	AllowAutoClientReconnection	Ordinateur	ICA\Reconnexion automatique des clients	Autorisé (1)
Redirection audio cliente	AllowAudioRedirection	Utilisateur	Audio	Autorisé (1)

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Redirection d'imprimante cliente	AllowPrinterRedir	Utilisateur	Impression	Autorisé (1)
Créer automatiquement l'imprimante universelle PDF	AutoCreatePDFPrinter	Utilisateur	Impression	Désactivé (0)
Mappage et compatibilité du pilote d'imprimante	DriverMappingList	Utilisateur	Impression	"Microsoft XPS Document Writer *, Deny;Send to Microsoft OneNote *, Deny"
Redirection de Presse-papiers client	AllowClipboardRedir	Utilisateur	Presse-papiers	Autorisé (1)
Redirection de périphérique USB client	AllowUSBRedir	Utilisateur	USB	Interdit (0)
Règles de redirection des périphériques USB clients	USBDeviceRules	Utilisateur	USB	"\0"
Compression d'images en mouvement	MovingImageCompression	Utilisateur	Configuration Thinwire	Activé (1)
Compression couleur supplémentaire	ExtraColorCompression	Utilisateur	Thinwire	Désactivé (0)
Taux de trame minimum cible	TargetedMinimumFramesPerSecond	Utilisateur	Thinwire	10 fps
Taux de trames cible	FramesPerSecond	Utilisateur	Thinwire	30 fps
Qualité visuelle	VisualQuality	Utilisateur	Thinwire	Moyenne (3)

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Utiliser codec vidéo pour la compression	VideoCodec	Utilisateur	Thinwire	Utiliser au choix (3)
Utiliser le codage matériel pour le codec vidéo	UseHardwareEncodingForVideoCodec	Utilisateur	Thinwire	Activé (1)
Autoriser la compression visuelle sans perte	AllowVisuallyLosslessCompression	Utilisateur	Thinwire	Désactivé (0)
Optimiser pour la charge des graphiques 3D	OptimizeFor3dWorkload	Utilisateur	Thinwire	Désactivé (0)
Nombre de couleurs préféré pour les graphiques simples	PreferredColorDepth	Utilisateur	Thinwire	24 bits par pixel (1)
Qualité audio	SoundQuality	Utilisateur	Audio	Élevée : audio à définition élevée (2)
Redirection du microphone client	AllowMicrophoneRedirection	Utilisateur	Audio	Autorisé (1)
Nombre maximum de sessions	MaximumNumberOfSessions	Administrateur	Gestion de la charge	250
Tolérance d'ouvertures de session simultanées	ConcurrentLogonsToTerminal	Administrateur	Gestion de la charge	2
Activer la mise à jour automatique des contrôleurs	EnableAutoUpdateOfControllers	Administrateur	Paramètres Virtual Delivery Agent	Autorisé (1)
Mode de mise à jour de la sélection du Presse-papiers	ClipboardSelectionUpdateMode	Utilisateur	Presse-papiers	3

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Mode de mise à jour de la sélection principale	PrimarySelectionUpdateMode	Utilisateur	Presse-papiers	3
Qualité speex maximale	MaxSpeexQuality	Utilisateur	Audio	5
Connecter automatiquement les lecteurs clients	AutoConnectDrives	Utilisateur	Redirection de fichier/CDM	Activé (1)
Lecteurs optiques clients	AllowCdromDrives	Utilisateur	Redirection de fichier/CDM	Autorisé (1)
Lecteurs fixes clients	AllowFixedDrives	Utilisateur	Redirection de fichier/CDM	Autorisé (1)
Lecteurs de disquette clients	AllowFloppyDrives	Utilisateur	Redirection de fichier/CDM	Autorisé (1)
Lecteurs réseau clients	AllowNetworkDrives	Utilisateur	Redirection de fichier/CDM	Autorisé (1)
Redirection de lecteur client	AllowDriveRedir	Utilisateur	Redirection de fichier/CDM	Autorisé (1)
Accès en lecture unique sur le lecteur client	ReadOnlyMappedDrives	Utilisateur	Redirection de fichier/CDM	Désactivé (0)
Affichage de clavier automatique	AllowAutoKeyboardRepeat	Utilisateur	MRVC	Désactivé (0)
Autoriser le transfert de fichiers entre le bureau et le client	AllowFileTransfer	Utilisateur	Transfert de fichiers	Autorisé
Télécharger des fichiers depuis le bureau	AllowFileDownload	Utilisateur	Transfert de fichiers	Autorisé
Charger des fichiers sur le bureau	AllowFileUpload	Utilisateur	Transfert de fichiers	Autorisé
Horloge inactive de session	EnableSessionIdleTime	Utilisateur	Horloges de session	Activé (1)

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Intervalle d'horloge inactive de session	SessionIdleTimerInterval	Utilisateur	Horloges de session	1440 minutes
Horloge de session déconnectée	EnableSessionDisconnectTimer	Utilisateur	Horloges de session	Désactivé (0)
Intervalle d'horloge de session déconnectée	SessionDisconnectTimerPeriod	Utilisateur	Horloges de session	1440 minutes

Remarque :

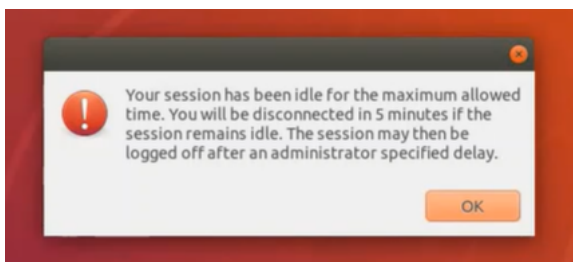
Seul le Virtual Delivery Agent (VDA) pour Windows prend en charge l'audio via UDP (User Datagram Protocol). Le VDA Linux ne prend pas en charge cette fonctionnalité. Pour de plus amples informations, consultez la section [Transport en temps réel audio via UDP \(User Datagram Protocol\)](#).

Vous pouvez utiliser les paramètres de stratégie Citrix suivants pour configurer des horloges de connexion de session dans Citrix Studio :

- **Horloge inactive de session** : détermine s'il faut appliquer un délai pour les sessions inactives.
- **Intervalle d'horloge inactive de session** : définit un délai pour les sessions inactives. Si l'option Horloge inactive de session est **Activé** et qu'une session active n'a pas reçu d'entrée utilisateur pendant la durée définie, la session se déconnecte.
- **Horloge de session déconnectée** : détermine s'il faut appliquer un délai pour les sessions déconnectées.
- **Intervalle d'horloge de session déconnectée** : définit un intervalle avant la déconnexion d'une session déconnectée.

Lorsque vous mettez à jour l'un de ces paramètres de stratégie, vous devez vous assurer qu'ils sont cohérents sur votre déploiement.

Un message d'avertissement s'affiche lorsque votre délai pour les sessions inactives expire. Pour obtenir un exemple, consultez la capture d'écran suivante. Lorsque vous sélectionnez **OK**, le message d'avertissement se ferme mais ne permet pas maintenir votre session active. Pour maintenir votre session active, fournissez une entrée utilisateur pour réinitialiser l'horloge inactive.



Les stratégies suivantes peuvent être configurées dans Citrix Studio 7.12 et versions ultérieures.

- MaxSpeexQuality

Valeur (entier) : [0-10]

Valeur par défaut : 5

Détails :

La redirection audio encode les données audio avec le codec Speex lorsque la qualité audio est moyenne voire faible (voir la stratégie Qualité audio). Speex est un codec avec perte, ce qui signifie qu'il atteint de meilleurs taux de compression au détriment de la fidélité du signal de la parole. Contrairement à d'autres codecs dédiés à la parole, il est possible de contrôler le compromis entre qualité et débit. Le processus d'encodage 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 d'encodage 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

▼ **Applicable OS versions**

Client selection changes are not updated to host

Selection changes are updated on both client and host

S, 7.1 Desktop OS, 7.5 Server OS, 7.2 Desktop OS, 7.6 Server OS, 7.3 Desktop OS, 7.7 Server OS, 7.4 Desktop OS, 7.8 Server OS, 7.9 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

- ClipboardSelectionUpdateMode

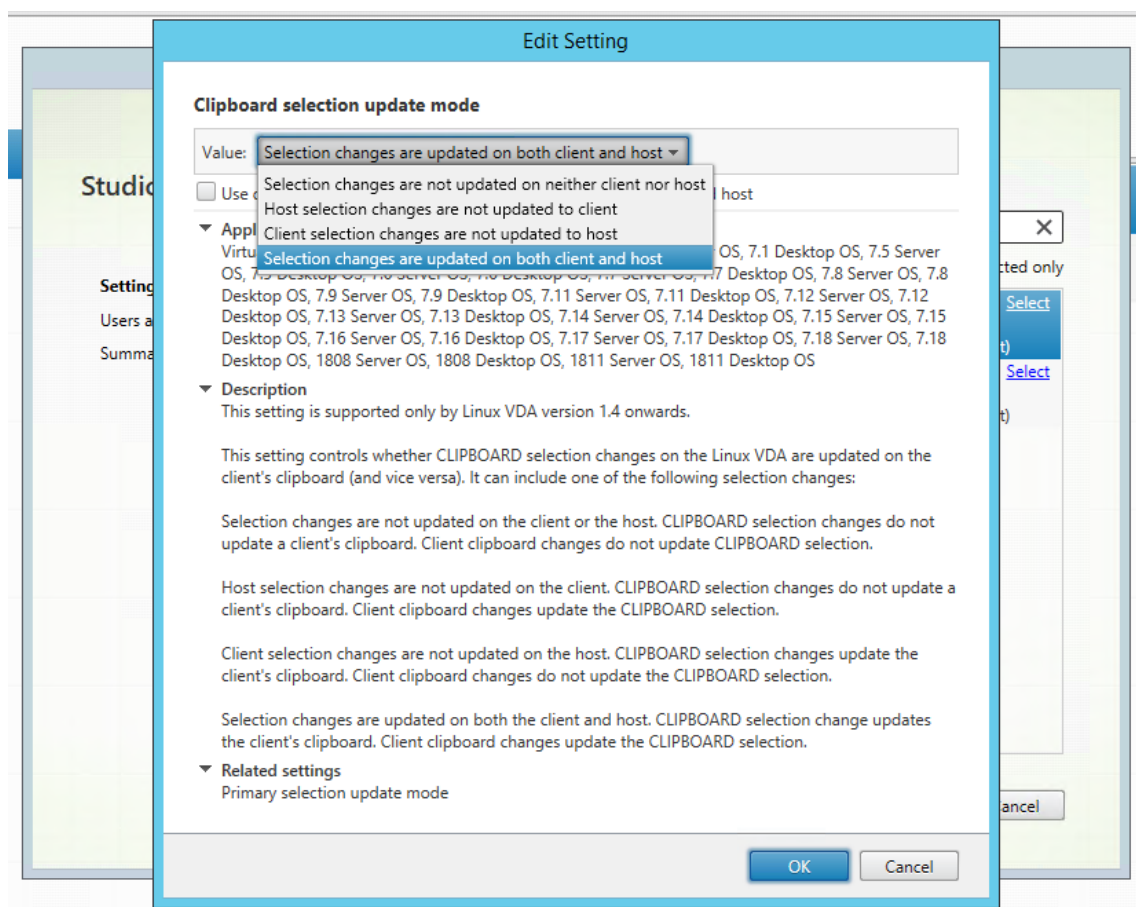
Valeur (énumération) : [0, 1, 2, 3]

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.

Configurer IPv6

November 5, 2021

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.
- Centrif 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"
```

OnlyUseIPv6ControllerRegistration doit être défini sur 1 pour activer IPv6 sur Linux VDA :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Policies\
   Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "
   OnlyUseIPv6ControllerRegistration" -d "0x00000001" --force
```

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](#).

Résolution des problèmes

Vérifiez l'environnement réseau IPv6 de base et utilisez ping6 pour vérifier si AD et Delivery Controller sont accessibles.

Configurer le Programme d'amélioration de l'expérience utilisateur Citrix (CEIP)

April 19, 2021

Si vous participez au programme CEIP, des informations d'utilisation et des statistiques anonymes sont envoyées à Citrix pour améliorer la qualité et les performances des produits Citrix. En outre, une copie des données anonymes est envoyée à Google Analytics (GA) pour une analyse rapide et efficace.

Paramètres de registre

Par défaut, vous participez automatiquement au programme CEIP lorsque vous installez le Linux VDA. Le premier chargement de données se produit approximativement sept jours après l'installation du Linux VDA. Vous pouvez modifier ce paramètre par défaut dans le registre.

- **CEIPSwitch**

Paramètre de Registre qui active ou désactive le programme CEIP (valeur par défaut = 0) :

Emplacement : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Nom : CEIPSwitch

Valeur : 1 = désactivé, 0 = activé

Si elle n'est pas spécifiée, le programme CEIP est activé.

Vous pouvez exécuter la commande suivante sur un client pour désactiver le programme CEIP.

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
  Citrix\CEIP" -v "CEIPSwitch" -d "1"
```

• **GASwitch**

Paramètre de Registre qui active ou désactive GA (valeur par défaut = 0) :

Emplacement : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Nom : GASwitch

Valeur : 1 = désactivé, 0 = activé

Si elle n'est pas spécifiée, GA est activé.

Vous pouvez exécuter la commande suivante sur un client pour désactiver GA :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
  Citrix\CEIP" -v "GASwitch" -d "1"
```

• **DataPersistPath**

Paramètre de Registre qui contrôle le chemin d'accès des données persistantes (défaut = /var/xdl/-ceip) :

Emplacement : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Nom : DataPersistPath

Valeur : chaîne

Vous pouvez exécuter la commande suivante pour définir ce chemin d'accès :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
  Citrix\CEIP" -v "DataPersistPath" -d "your_path"
```

Si le chemin d'accès configuré n'existe pas ou n'est pas accessible, les données sont enregistrées dans le chemin d'accès par défaut.

Données CEIP collectées depuis le Linux VDA

Le tableau suivant présente un exemple de types d'informations anonymes collectées. Les données ne contiennent aucun détail permettant d'identifier le client.

Point de données	Nom de la clé	Description
GUID de machine	machine_guid	Identification de la machine d'où les données proviennent
Solution Active Directory	ad_solution	Chaîne de texte indiquant la méthode de jonction du domaine de la machine
Version du noyau Linux	kernel_version	Chaîne de texte indiquant la version du noyau de la machine
Version LVDA	vda_version	Chaîne de texte indiquant la version installée du Linux VDA
Mise à jour LVDA ou nouvelle installation	update_or_fresh_install	Chaîne de texte indiquant que le package Linux VDA actuel est en cours de mise à jour ou d'installation
Méthode d'installation de LVDA	install_method	Chaîne de texte indiquant que le package Linux VDA actuel est installé à l'aide de MCS, PVS, Easy Install ou d'une installation manuelle.
HDX 3D pro activé ou non	hdx_3d_pro	Chaîne de texte indiquant si HDX 3D Pro est activé sur la machine
Mode VDI activé ou non	vdi_mode	Chaîne de texte indiquant si le mode VDI est activé
Paramètres régionaux système	system_locale	Chaîne de texte indiquant les paramètres régionaux de cette machine
Dernière heure de redémarrage des services LVDA principaux	ctxhdx ctxvda	Dernière heure de redémarrage des services <code>ctxhdx</code> et <code>ctxvda</code> , au format <code>jj-hh:mm:ss</code> , par exemple, 10-17:22:19
Type de GPU	gpu_type	Indique le type de processeur graphique de la machine

Point de données	Nom de la clé	Description
Cœurs d'UC	cpu_cores	Entier indiquant le nombre de cœurs d'UC de la machine
Fréquence du processeur	cpu_frequency	Nombre flottant indiquant la fréquence du processeur en MHz
Taille de la mémoire physique	memory_size	Entier indiquant la taille de la mémoire physique en Ko
Nombre de sessions lancées	session_launch	Entier indiquant le nombre de sessions lancées (connexions ou reconnexions) sur la machine au moment où ce point de données est collecté
Version et nom du système d'exploitation Linux	os_name_version	Chaîne de texte indiquant le nom et la version du système d'exploitation Linux de la machine
Clé de session	session_key	Identification de la session d'où les données proviennent
Type de ressource	resource_type	Chaîne de texte indiquant le type de ressource de la session lancée : bureau ou <appname>
Période active de session	active_session_time	Utilisé pour enregistrer les périodes actives de la session. Une session peut contenir plusieurs périodes actives car la session peut se déconnecter/se reconnecter.
Durée de session	session_duration_time	Utilisé pour enregistrer la durée de la session de l'ouverture à la fermeture de session
Type de client Receiver	receiver_type	Entier indiquant le type d'application Citrix Workspace utilisé pour lancer la session
Version du client Receiver	receiver_version	Chaîne de texte indiquant la version de l'application Citrix Workspace utilisée pour lancer la session

Point de données	Nom de la clé	Description
Nombre d'impressions	printing_count	Entier indiquant le nombre de fois que la session utilise la fonction d'impression
Nombre de redirections USB	usb_redirecting_count	Entier indiquant le nombre de fois que la session utilise un périphérique USB
Type de fournisseur Gfx	gfx_provider_type	Chaîne de texte indiquant le type de fournisseur de graphiques de la session
Nombre d'observations	shadow_count	Entier indiquant le nombre de fois que la session a été observée
Langue sélectionnée par l'utilisateur	ctxism_select	Chaîne longue composée qui contient toutes les langues sélectionnées par les utilisateurs
Nombre de redirections de carte à puce	scard_redirecting_count	Entier indiquant le nombre de fois que la redirection de carte à puce est utilisée pour les ouvertures de session et l'authentification utilisateur pour les applications de session

Configurer la redirection USB

September 23, 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, l'utilisateur peut utiliser le périphérique USB comme s'il était connecté localement.

Conseil :

Nous vous recommandons d'utiliser la redirection USB lorsque la latence réseau est inférieure à 100 millisecondes. N'utilisez pas la redirection USB lorsque la latence réseau est supérieure à

200 millisecondes.

La redirection USB contient trois domaines de fonctionnalité :

- Open Source Project Implementation (VHCI)
- Service VHCI
- Service USB

Open-source VHCI :

Cette partie de la fonctionnalité de redirection USB développe un système de partage de périphérique USB général sur un réseau IP. Elle comprend un pilote noyau Linux et des bibliothèques en mode utilisateur, ce qui vous permet de communiquer avec le pilote noyau pour obtenir toutes les données USB. Dans la mise en œuvre du Linux VDA, Citrix réutilise le pilote noyau de VHCI. Toutefois tous les transferts de données USB entre le Linux VDA et l'application Citrix Workspace sont encapsulés dans le protocole ICA de Citrix.

Service VHCI :

Le service VHCI est un service open source fourni par Citrix pour communiquer avec le module noyau VHCI. Ce service fonctionne en tant que passerelle entre VHCI et le service USB Citrix.

Service USB :

Le service USB représente un module Citrix qui gère tous les transferts de données et de virtualisation sur le périphérique USB.

Fonctionnement de la redirection USB

En général, si un périphérique USB n'est pas redirigé correctement vers Linux VDA, un ou plusieurs nœuds de périphérique sont créés dans le chemin d'accès `system/dev`. Parfois, cependant, le périphérique redirigé ne peut pas être utilisé par une session Linux VDA active. Les périphériques USB s'appuient sur les pilotes pour fonctionner correctement et certains périphériques nécessitent des pilotes spéciaux. Si les pilotes ne sont pas fournis, les périphériques USB redirigés sont inaccessibles à la session Linux VDA active. Pour assurer la connectivité du périphérique USB, installez les pilotes et configurez le système correctement.

Le Linux VDA prend en charge une liste de périphériques USB qui peuvent être redirigés vers et depuis le client. En outre, le périphérique est correctement monté, notamment le disque USB, ce qui permet à l'utilisateur d'accéder au disque sans aucune configuration supplémentaire.

Périphériques USB pris en charge

Les périphériques suivants ont été testés pour prendre en charge cette version de Linux VDA. D'autres périphériques peuvent être utilisés, avec des résultats imprévisibles :

Remarque :

le VDA Linux ne prend en charge que les protocoles USB 2.0.

Périphérique de stockage de masse USB	VID:PID	Système de fichiers
Netac Technology Co., Ltd	0dd8:173c	FAT32
Kingston Datatraveler 101 II	0951:1625	FAT32
Kingston Datatraveler GT101 G2	1567:8902	FAT32
Lecteur Flash SanDisk SDCZ80	0781:5580	FAT32
Disque dur HDD WD	1058:10B8	FAT32

Souris 3D USB	VID:PID
3DConnexion SpaceMouse Pro	046d: c62b

Scanner USB	VID:PID
Photo Epson Perfection V330	04B8: 0142

Configurer la redirection USB

Une stratégie Citrix détermine si la redirection de périphérique USB est activée ou désactivée. En outre, le type de périphérique peut également être spécifié à l'aide d'une stratégie Delivery Controller. Lors de la configuration de la redirection USB pour les Linux VDA, configurez les stratégies et règles suivantes :

- Stratégie de redirection de périphérique USB client
- Règles de redirection de périphérique USB client

Activer la stratégie de redirection USB

Dans Citrix Studio, activez (ou désactivez) la redirection de périphérique USB vers et depuis le client (hôtes de station de travail uniquement).

Dans la boîte de dialogue **Modifier le paramètre** :

1. Sélectionnez **Autorisé**.
2. Cliquez sur **OK**.

Edit Setting

Client USB device redirection

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

☒ **Allowed**
Client USB devices can be mapped, if specified elsewhere

☐ **Prohibited**
No client USB devices will be mapped

▼ **Details and related settings**

Enables or disables redirection of USB devices to and from the client (workstation hosts only).

Related Settings: Client USB device redirection rules

OK **Cancel**

Définir des règles de redirection USB

Après activation de la stratégie de redirection USB, définissez les règles de redirection à l'aide de Citrix Studio en spécifiant les périphériques qui sont autorisés (ou interdits) sur le Linux VDA.

Dans la boîte de dialogue Règles de redirection de périphérique USB client :

1. Cliquez sur **Nouveau** pour ajouter une règle de redirection, ou cliquez sur **Modifier** pour vérifier une règle existante.
2. Après avoir créé (ou modifié) une règle, cliquez sur **OK**.

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

New

Edit

Delete

Move Up

Move Down

☐ Use default value:

▼ Details and related settings

Lists redirection rules for USB devices.

Pour de plus amples informations sur la configuration de la redirection USB générique, reportez-vous au [Guide de configuration de la redirection USB générique Citrix](#).

Créer le module noyau VHCI

La redirection USB dépend des modules du noyau VHCI (`usb-vhci-hcd.ko` et `usb-vhci-iocif.ko`). Ces modules font partie de la distribution de Linux VDA (inclus dans le package RPM). Ils sont compilés selon les noyaux de distribution Linux officiels et sont indiqués dans le tableau suivant :

Distribution Linux prise en charge	Version du noyau
RHEL 8.3	4.18.0-240.10.1
RHEL 8.2	4.18.0-240.10.1
RHEL 8.1	4.18.0-240.10.1
RHEL 7.9	3.10.0-1160.11.1
RHEL 7.8	3.10.0-1160.11.1

Distribution Linux prise en charge	Version du noyau
SUSE 12.5	4.12.14-122.57.1
Ubuntu 20.04	5.4.0-58
Ubuntu 18.04	4.15.0-128
Ubuntu 16.04	4.4.0-197
Debian 10	4.19.0-13

Important :

Si le noyau de votre machine n'est pas compatible avec le pilote créé pour les Linux VDA, le service USB peut ne pas parvenir à démarrer. Dans ce cas, vous pouvez utiliser la fonctionnalité de redirection USB uniquement si vous créez vos propres modules noyau VHCI.

Vérifier que votre noyau est cohérent avec les modules créés par Citrix

Sur la ligne de commande, exécutez la commande suivante pour vérifier si le noyau est cohérent :

```
1 insmod /opt/Citrix/VDA/lib64/usb-vhci-hcd.ko
```

Si la commande s'exécute correctement, le module noyau a été chargé avec succès et la version est cohérente avec celle installée par Citrix.

Si la commande s'exécute avec des erreurs, le noyau n'est pas cohérent avec le module Citrix et doit être recréé.

Recréer le module noyau VHCI

Si votre module noyau n'est pas cohérent avec la version Citrix, procédez comme suit :

1. Téléchargez le code source LVDA depuis le [site de téléchargement de Citrix](#). Sélectionnez le fichier de la section « **Linux Virtual Delivery Agent (sources)** ».
2. Décompressez le fichier **citrix-linux-vda-sources.zip**. Accédez à **linux-vda-souces/vhci-hcd-1.15.tar.bz2** et décompressez les fichiers source VHCI à l'aide de **tar xvf vhci-hcd-1.15.tar.bz2**.
3. Créez le module noyau selon les fichiers d'en-tête et le fichier **Module.symvers**. Suivez la procédure suivante pour installer les fichiers d'en-tête du noyau et créez le fichier **Module.symvers** selon la distribution Linux appropriée :

RHEL/CentOS :


```
1 yum install kernel-devel
```

SUSE 12 :

```
1 zypper install kernel-devel
2
3 zypper install kernel-source
```

Ubuntu :

```
1 apt-get install linux-headers
```

Conseil :

Si l'installation réussit, un dossier de noyau similaire au suivant est créé :

```
/usr/src/kernels/3.10.0-327.10.1.el7.x86_64
```

4. Dans le dossier `/usr/src/kernels/3.10.0-327.10.1.el7.x86_64`, vérifiez que le fichier **Module.symvers** est présent. Si le fichier ne se trouve pas dans le dossier, créez le noyau pour obtenir ce fichier (en exécutant les commandes suivantes dans l'ordre : `make oldconfig`; `make prepare`; `make modules`; `make`) ou copiez-le depuis `/usr/src/kernels/3.10.0-327.10.1.el7.x86_64-obj/x86_64/defaults/module.*`
5. Exécutez les commandes suivantes pour installer les outils de développement.

RHEL 8, CentOS 8 :

```
1 yum groupinstall 'Development Tools'
2
3 yum install elfutils-libelf-devel
```

RHEL 7, CentOS 7 :

```
1 yum groupinstall 'Development Tools'
```

Ubuntu 20.04, Ubuntu 18.04, Debian 10 :

```
1 apt install build-essential flex bison libelf-dev
```

Ubuntu 16.04 :

```
1 apt install build-essential flex bison
```

6. Dans le fichier `vhci-hcd-1.15/Makefile`, modifiez le fichier Makefile de VCHI et définissez KDIR sur le répertoire du noyau :

```
1 #KDIR = $(BUILD_PREFIX)/lib/modules/$(KVERSION)/build
2
3 KDIR = /usr/src/kernels/3.10.0-327.10.1.el7.x86_64
```

7. Dans le dossier `vhci-hcd-1.15/`, exécutez `make` pour créer le noyau VHCI.

Remarque :

Si la création a réussi, les modules `usb-vhci-hcd.ko` et `usb-vhci-iocifc.ko` sont créés dans le dossier `vhci-hcd-1.15/`.

8. Remplacez le module du noyau par celui qui vient d'être créé : `cp -f usb-vhci-*.ko /opt/Citrix/VDA/lib64/`
9. Redémarrez le service USB :

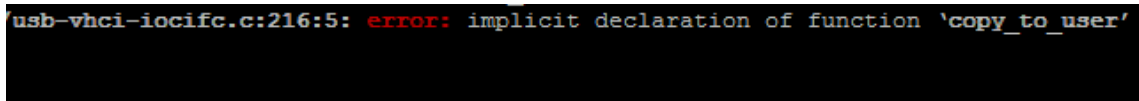
```
1 service ctxusbsd restart
```

10. Fermez, puis rouvrez la session. Vérifiez si la redirection USB fonctionne.

Résoudre les problèmes de compilation du noyau

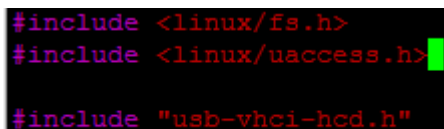
Les erreurs suivantes peuvent se produire lorsque vous créez le module VHCI avec des noyaux spécifiques :

- L'erreur `implicit declaration of function 'copy_to_user'` peut se produire, voir la capture d'écran suivante :



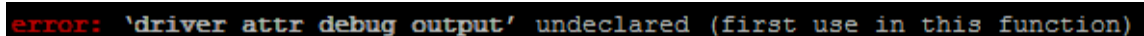
```
usb-vhci-iocifc.c:216:5: error: implicit declaration of function 'copy_to_user'
```

L'erreur se produit en raison des modifications du fichier d'en-tête dans les noyaux. Pour résoudre ce problème, ajoutez la ligne `#include <linux/uaccess.h>` au fichier `vhci-hcd-1.15/usb-vhci-iocifc.c`.



```
#include <linux/fs.h>
#include <linux/uaccess.h>
#include "usb-vhci-hcd.h"
```

- L'erreur `'driver_attr_debug_output' undeclared` peut se produire, voir la capture d'écran suivante :



```
error: 'driver_attr_debug_output' undeclared (first use in this function)
```

L'erreur se produit lorsque des symboles sont manquants sur le noyau. Pour contourner le problème, désactivez la définition de macro pour DEBUG dans les fichiers `vhci-hcd-1.15/usb-vhci-iocifc.c` et `vhci-hcd-1.15/usb-vhci-hcd.c`.

```

22
23 // #define DEBUG
24
25 #include <linux/module.h>

```

- L'erreur `'make[3]: *** No rule to make target 'arch/x86/tools/relocs_32.c', needed by 'arch/x86/tools/relocs_32.o'. Stop.` peut se produire, voir la capture d'écran suivante :

```

scripts/kconfig/conf --syncconfig Kconfig
make[3]: *** No rule to make target 'arch/x86/tools/relocs_32.c', needed by 'arch/x86/tools/relocs_32.o'. Stop.
arch/x86/Makefile:232: recipe for target 'archscripts' failed
make[2]: *** [archscripts] Error 2
make[2]: Leaving directory '/usr/src/linux-headers-5.4.0-1031-azure'
Makefile:102: recipe for target 'testcc' failed
make[1]: *** [testcc] Error 2
make[1]: Leaving directory '/home/administrator1/linuxvda-vhci'
Makefile:97: recipe for target 'conf/usb-vhci.config.h' failed
make: *** [conf/usb-vhci.config.h] Error 2

```

Pour contourner le problème, remplacez `SUBDIRS=$(PWD)` par `M=$(shell pwd)` en utilisant les commandes suivantes sous le chemin `vhci-hcd-1.15/` :

```

1 sed -i 's/SUBDIRS=$(PWD)/M=$(shell pwd)/g' Makefile
2
3 sed -i 's/SUBDIRS=$(PWD)/M=$(shell pwd)/g' test/Makefile

```

- L'erreur `./include/uapi/linux/stat.h:30:17: error: expected ')' before numeric constant`
`#define S_IRUSR 00400` peut se produire, voir la capture d'écran suivante :

```

In file included from ./include/linux/stat.h:7:0,
                 from ./include/linux/module.h:10,
                 from /home/administrator1/vhci-hcd-1.15/usb-vhci-hcd.c:24:
./include/uapi/linux/stat.h:30:17: error: expected ')' before numeric constant
#define S_IRUSR 00400
                  ^
/home/administrator1/vhci-hcd-1.15/usb-vhci-hcd.c:1312:34: note: in expansion of macro 'S_IRUSR'
static DRIVER_ATTR(debug_output, S_IRUSR | S_IWUSR, show_debug_output, store_debug_output);
                                   ^~~~~~

```

Run the following commands to work around the issue:

```

1 sed -i 's/show_debug_output/debug_output_show/g' usb-vhci-iocifc.c usb-vhci-hcd.c
2
3 sed -i 's/store_debug_output/debug_output_store/g' usb-vhci-iocifc.c usb-vhci-hcd.c
4
5 sed -i 's/static DRIVER_ATTR(debug_output, S_IRUSR | S_IWUSR, debug_output_show, debug_output_store);/static DRIVER_ATTR_RW(debug_output);/g' usb-vhci-iocifc.c usb-vhci-hcd.c

```

- L'erreur `./arch/x86/include/asm/uaccess.h:433:29: error: invalid initializer`
`__typeof__(ptr) __pu_ptr = (ptr); \` peut se produire, voir la capture d'écran suivante :

```

/home/administrator1/vhci-hcd-1.15/usb-vhci-iocifc.c: In function 'ioc_register':
./arch/x86/include/asm/uaccess.h:433:29: error: invalid initializer
  __typeof__(ptr) __pu_ptr = (ptr); \
                              ^
./arch/x86/include/asm/uaccess.h:553:2: note: in expansion of macro '__put_user_nocheck'
  __put_user_nocheck((__typeof__(*ptr))(x), (ptr), sizeof(*ptr))
  ^
/home/administrator1/vhci-hcd-1.15/usb-vhci-iocifc.c:219:3: note: in expansion of macro '__put_user'
  __put_user('\0', arg->bus_id);
  ^

```

As a workaround, change the 219 line of the `usb-vhci-iocifc.c` file from `__put_user('\0', arg->bus_id);` to `__put_user('\0', arg->bus_id + 0);`.

- L'erreur `error: 'access_ok' undeclared (first use in this function)` `if(unlikely((_IOC_DIR(cmd) & _IOC_READ) && !access_ok(VERIFY_WRITE, arg, _IOC_SIZE(cmd))))` peut se produire, voir la capture d'écran suivante :

```

/root/linuxvda-vhci/usb-vhci-iocifc.c:963:46: error: 'access_ok' undeclared (first use in this function)
  if(unlikely((_IOC_DIR(cmd) & _IOC_READ) && !access_ok(VERIFY_WRITE, arg, _IOC_SIZE(cmd))))
                                              ^
./include/linux/compiler.h:77:42: note: in definition of macro 'unlikely'
  # define unlikely(x) __builtin_expect(!(x), 0)
                                ^

```

Run the following commands to work around the issue:

```

1 sed -i 's/VERIFY_READ, //g' usb-vhci-iocifc.c
2 sed -i 's/VERIFY_WRITE, //g' usb-vhci-iocifc.c

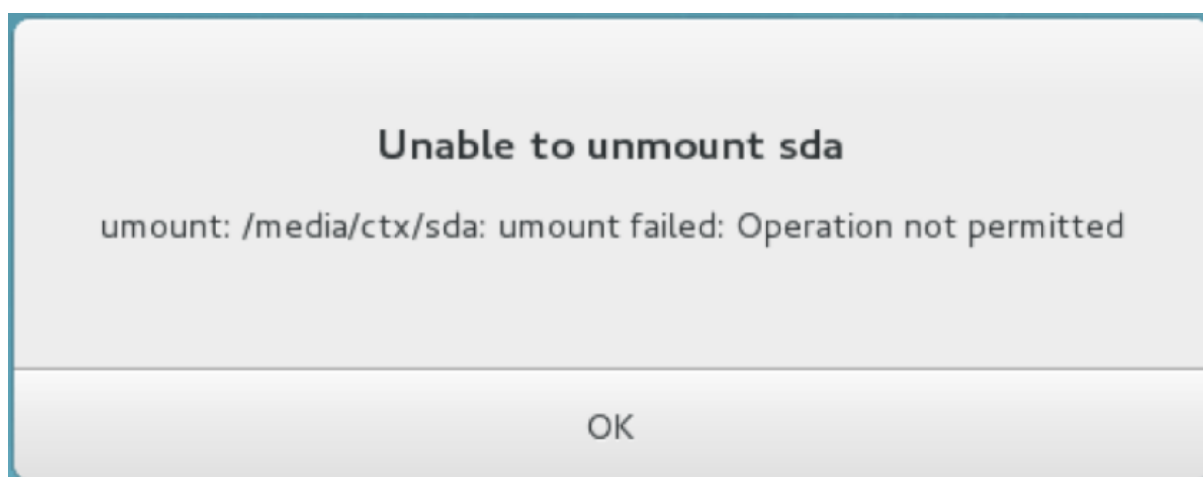
```

Résolution des problèmes de redirection USB

Utilisez les informations de cette section pour résoudre les problèmes que vous pourriez rencontrer lors de l'utilisation du Linux VDA.

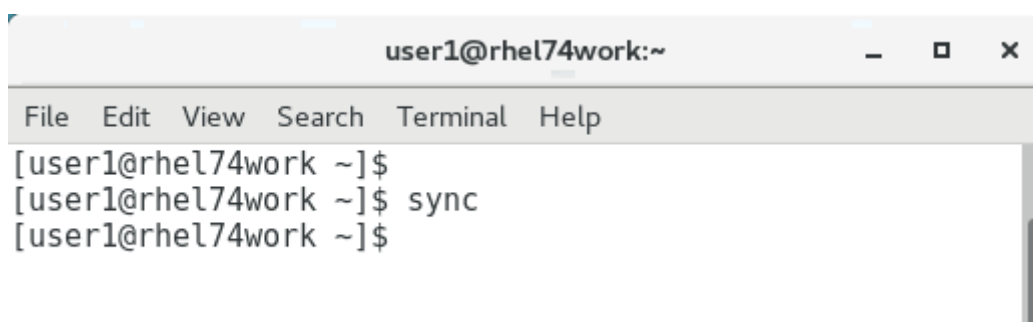
Impossible de démonter le disque USB redirigé

Pour le contrôle d'accès de tous les disques USB redirigés à partir de l'application Citrix Workspace, le Linux VDA gère tous ces périphériques sous privilèges d'administrateur afin de garantir que seul le propriétaire peut accéder au périphérique redirigé. Par conséquent, l'utilisateur ne peut pas démonter le périphérique sans privilèges d'administrateur.



Le fichier est perdu lorsque vous arrêtez la redirection d'un disque USB

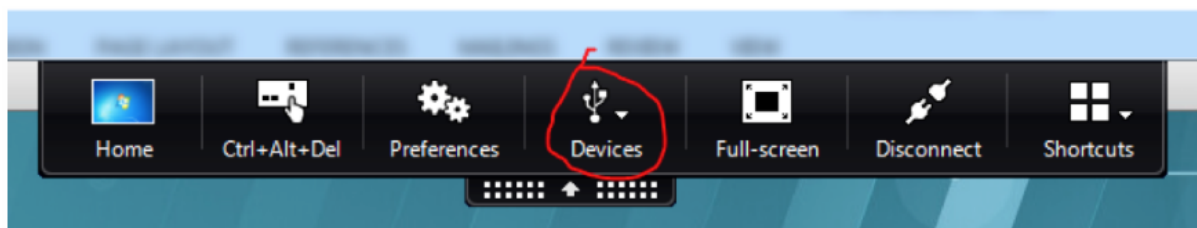
Si vous redirigez un disque USB dans une session, essayez de le modifier (par exemple, en créant des fichiers sur le disque), puis arrêtez de le rediriger immédiatement à l'aide de la barre d'outils de l'application Citrix Workspace, le fichier que vous avez modifié ou créé peut être perdu. Ce problème 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 éléments suivants :

- La stratégie est configurée pour permettre la redirection USB.
- Le module du noyau est compatible avec votre noyau

**Remarque :**

L'onglet **Périphériques** n'est pas disponible dans l'application Citrix Workspace pour Linux.

Affichage des périphériques USB dans la barre d'outils de l'application Citrix Workspace, mais avec la mention *Limité par une stratégie*, ce qui entraîne l'échec de la redirection

Lorsque le problème se produit, procédez comme suit :

- Configurez la stratégie du Linux VDA pour activer la redirection.
- Vérifiez si des restrictions de stratégie supplémentaires sont configurées dans le registre de l'application Citrix Workspace. Vérifiez **DeviceRules** dans le chemin d'accès du registre pour vous assurer que ce paramètre n'interdit pas l'accès au périphérique :

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB

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 :

Dans le cas des lecteurs USB, le VDA Linux 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.

Configurer la fiabilité de session

November 5, 2021

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 de fiabilité de session sont envoyés entre le Linux VDA et le client ICA 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
```

Résolution des problèmes

Impossible de lancer des sessions après avoir activé la fiabilité de session via le paramètre de stratégie.

Pour contourner ce problème, procédez comme suit :

1. Assurez-vous que le service VDA et le service HDX sont redémarrés, dans cet ordre, après avoir activé la fiabilité de session via le paramètre de stratégie dans Citrix Studio.

2. Sur le VDA, utilisez la commande suivante pour vérifier que l'écouteur TCP de fiabilité de session est en cours d'exécution (utilisez le port 2598 à titre d'exemple).

```
1 netstat -an | grep 2598
```

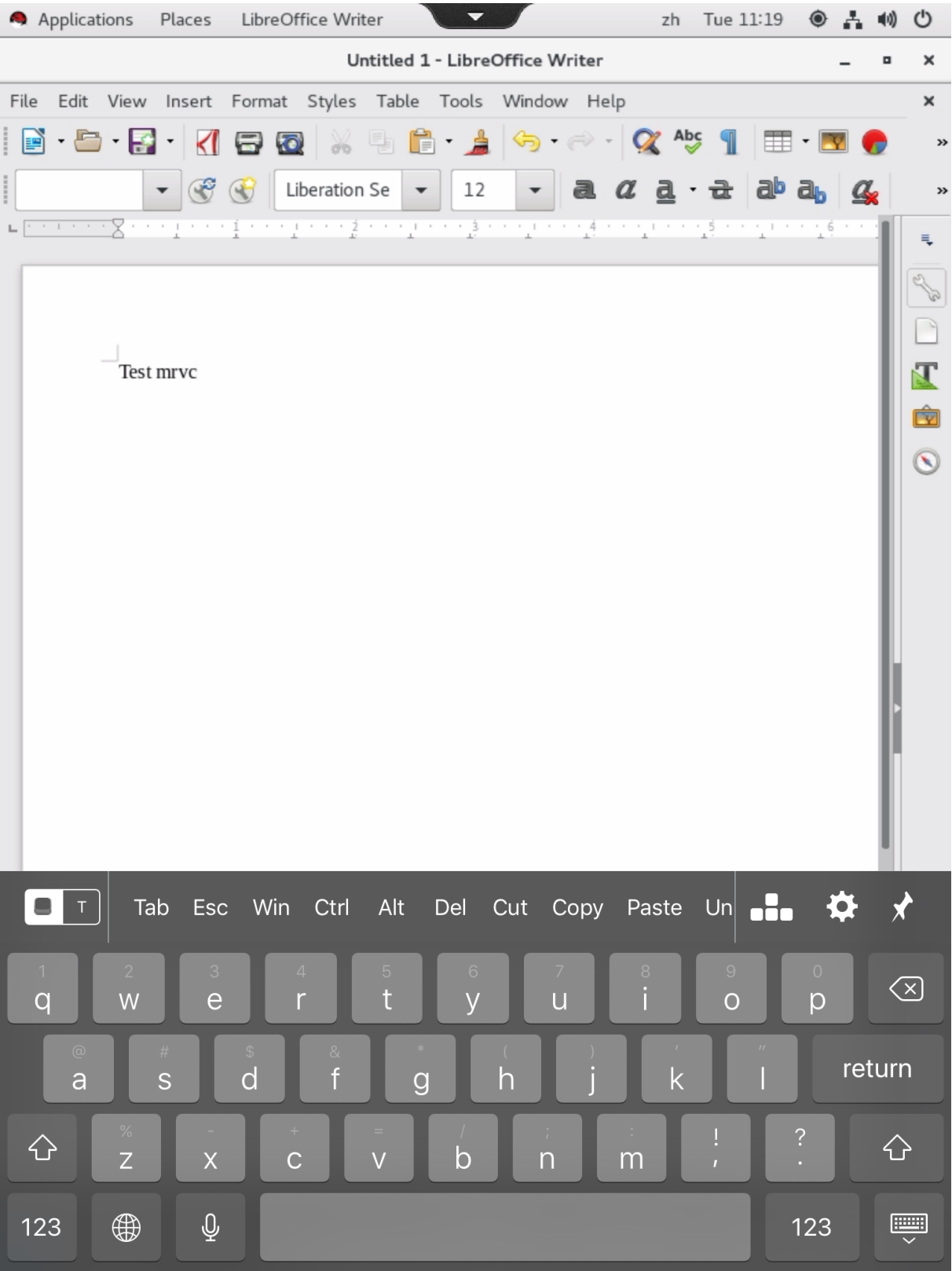
S'il n'y a pas d'écouteur TCP sur le port de fiabilité de session, activez l'écouteur en exécutant la commande suivante.

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
  CurrentControlSet\Control\Citrix\WinStations\cgp" -v "
  fEnableWinStation" -d "0x00000001"
```

Clavier logiciel

September 5, 2022

La fonctionnalité de clavier logiciel est disponible dans une session d'application ou de bureau virtuel Linux. Le clavier logiciel s'affiche ou se masque automatiquement lorsque vous accédez à un champ de saisie ou le quittez.



Remarque :

La fonctionnalité est disponible pour RHEL 7.8, RHEL 7.9, RHEL 8.1, RHEL 8.2, RHEL 8.3, SUSE 12.5, Ubuntu 16.04, Ubuntu 18.04 et Ubuntu 20.04. Elle est prise en charge sur l'application Citrix Workspace pour iOS et Android.

Activer et désactiver la fonctionnalité

Cette fonction est désactivée par défaut. Utilisez l'utilitaire **ctxreg** pour activer ou désactiver cette fonctionnalité. La configuration de la fonctionnalité sur un Linux VDA donné s'applique à toutes les sessions sur ce VDA.

Pour activer la fonctionnalité :

1. Exécutez la commande :

```
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.

Éditeur IME

November 5, 2021

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.

Prise en charge des entrées en plusieurs langues

November 5, 2021

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"
```

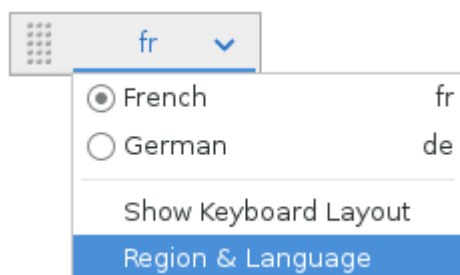
Pour désactiver cette fonctionnalité, exécutez la commande :

```
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.

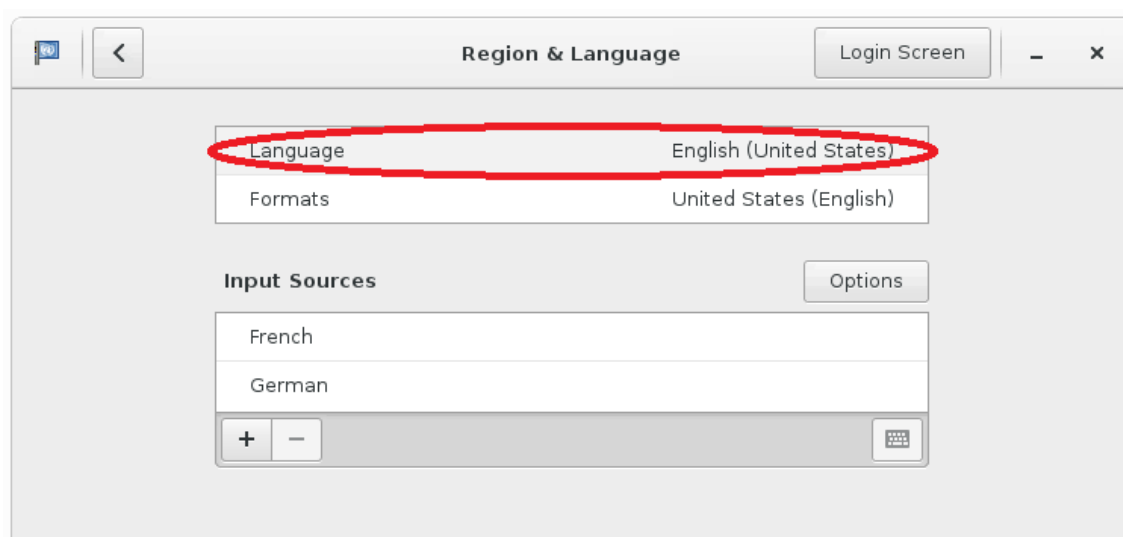
1. Activez la fonctionnalité.
2. Accédez à une application publiée pouvant accepter la saisie de texte. Une barre de langue s'affiche dans la session, à côté de l'application.
3. Dans le menu déroulant, sélectionnez **Région et langue** pour ajouter la langue souhaitée (source d'entrée).



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**.



Synchronisation dynamique de la disposition du clavier

November 5, 2021

Auparavant, les dispositions de clavier sur le Linux VDA et sur la machine cliente devaient être les mêmes. Par exemple, lorsque la disposition du clavier passait de l'anglais au français sur la machine cliente mais pas sur le VDA, des problèmes de mappage de touches pouvaient se produire et persister jusqu'à ce que le VDA passe également au français.

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.

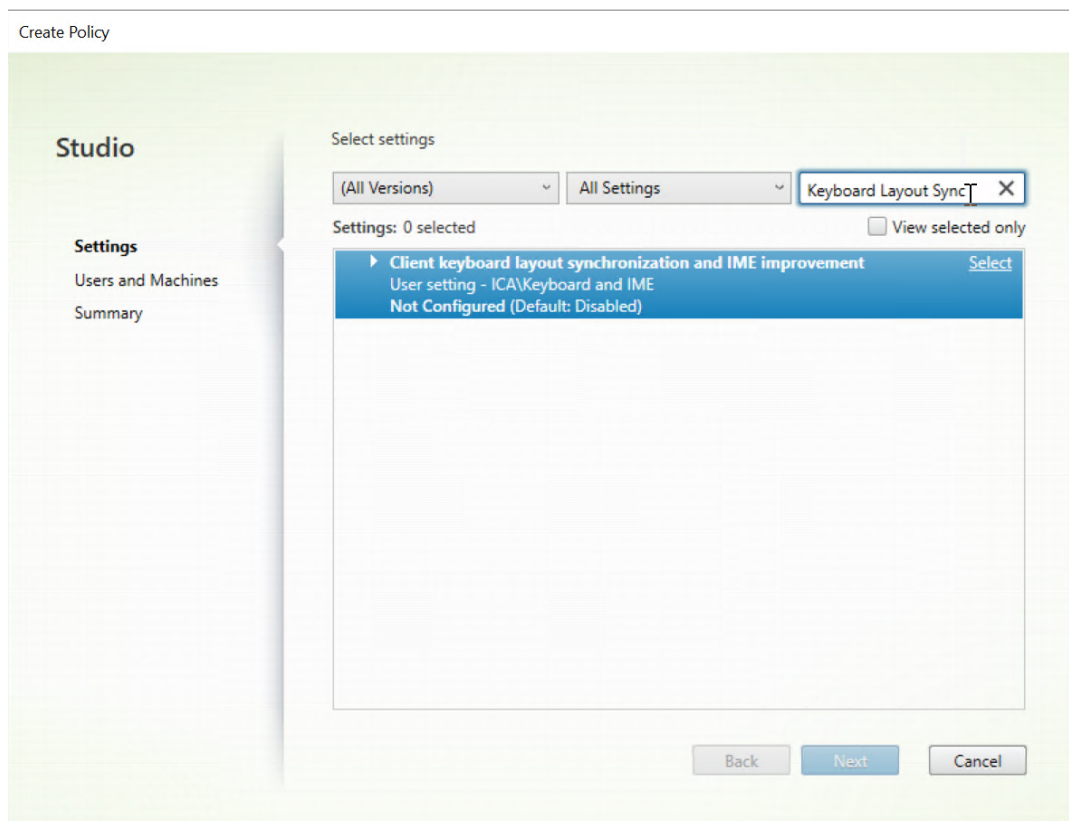
Configuration

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](#).

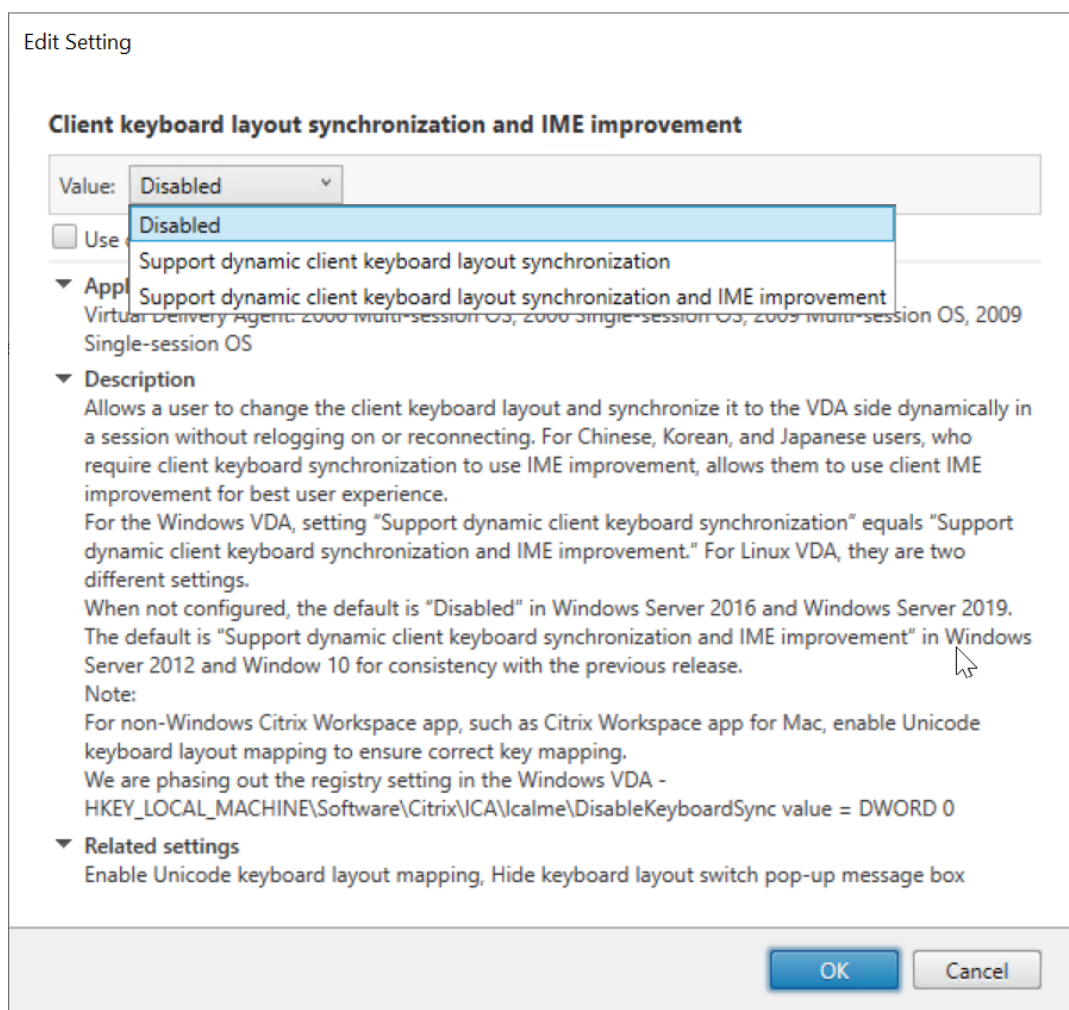
Remarque :

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

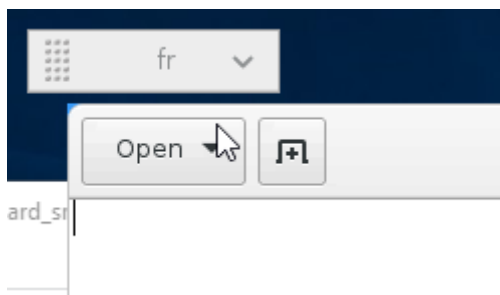
Lorsque cette fonctionnalité est activée, si la disposition du clavier change sur la machine cliente pendant une session, la disposition du clavier de la session change en conséquence.

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 :

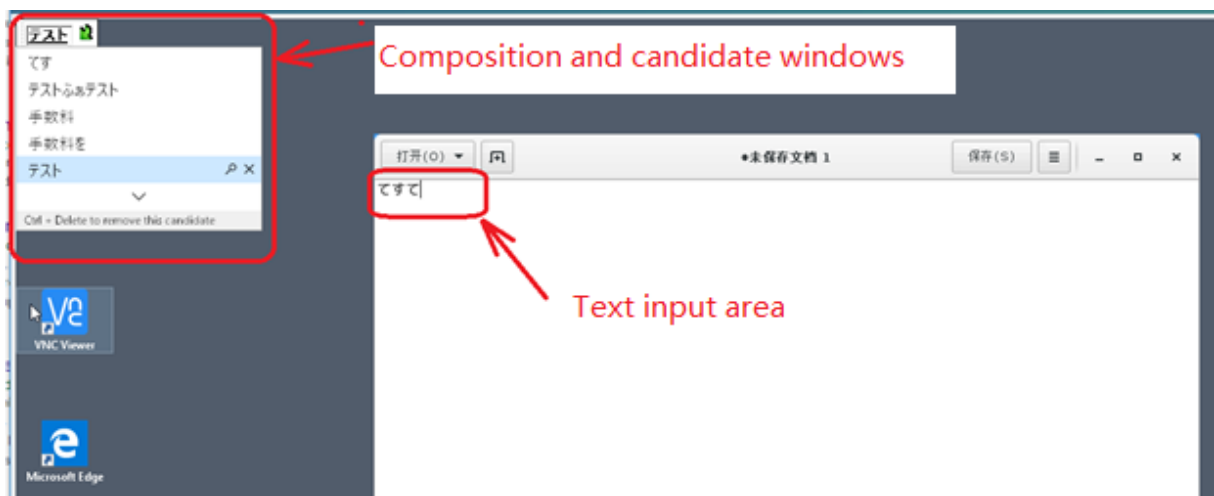


Synchronisation de l'interface utilisateur de l'éditeur IME client

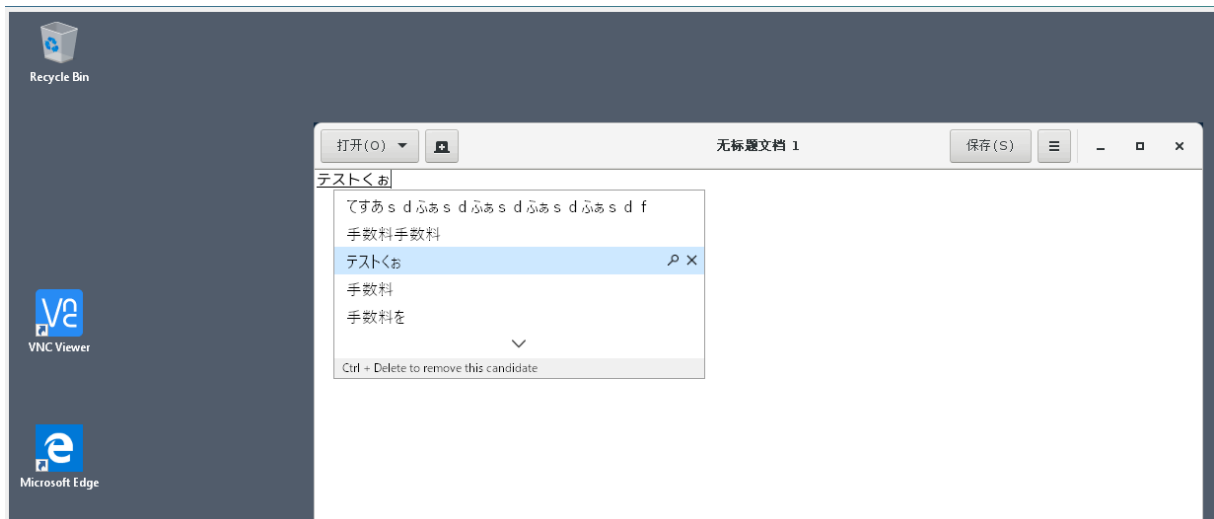
March 3, 2022

Vue d'ensemble

Jusqu'à présent, l'interface utilisateur de l'éditeur IME client (y compris la fenêtre de composition et la fenêtre candidate) était positionnée dans le coin supérieur gauche de l'écran. Celle-ci ne suivait pas le curseur et était parfois située loin du curseur dans la zone de saisie de texte.



Citrix améliore la convivialité et optimise davantage l'expérience avec l'éditeur IME client comme suit :



Remarque :

La fonctionnalité est disponible pour RHEL 7.x, CentOS 7.x, Ubuntu 16.04, Ubuntu 18.04 et SUSE 12.x. Elle est prise en charge sur l'application Citrix Workspace pour Windows et pour Mac.

Pour utiliser la fonctionnalité dans les sessions de bureau RHEL 7.x, vous devez activer **IBus**. Par exemple, définissez la langue de l'interface utilisateur sur une langue qui nécessite un éditeur IME, ou ajoutez **GTK_IM_MODULE=ibus** au fichier **\${HOME}/.config/ibussettings/xinputrc**.

La fonctionnalité s'installe automatiquement, mais vous devez l'activer avant de pouvoir l'utiliser.

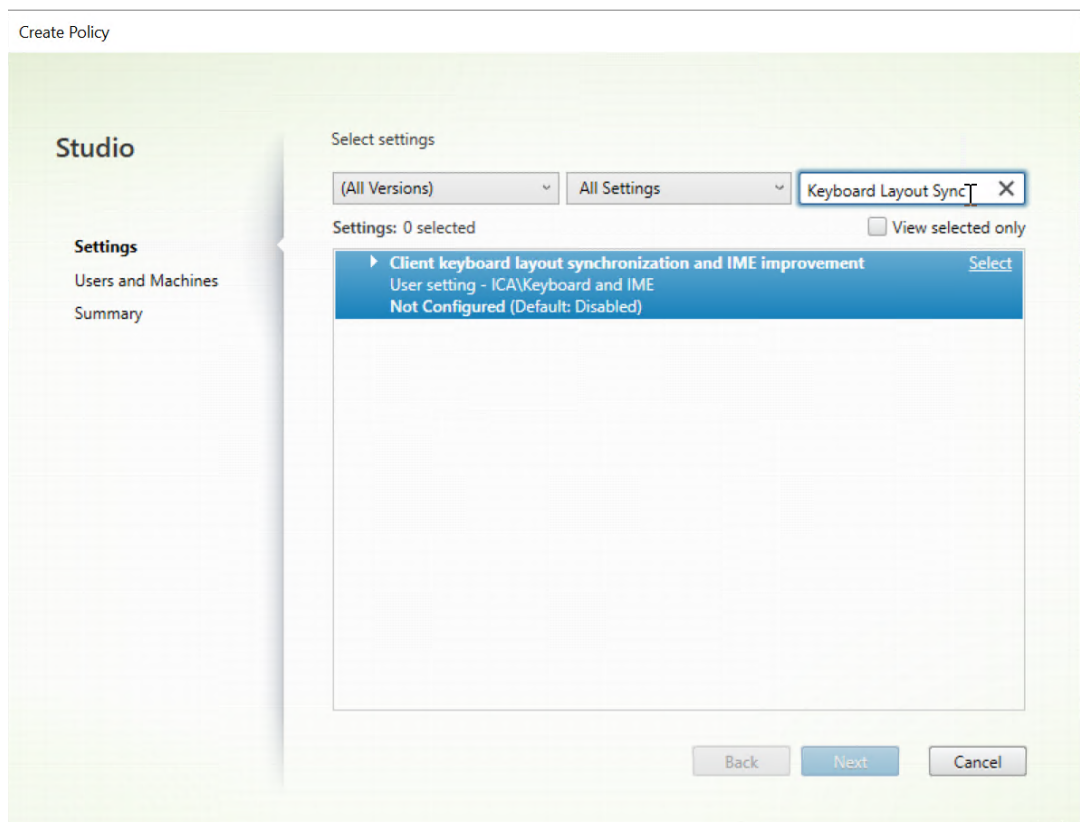
Activer et désactiver la fonctionnalité

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**.

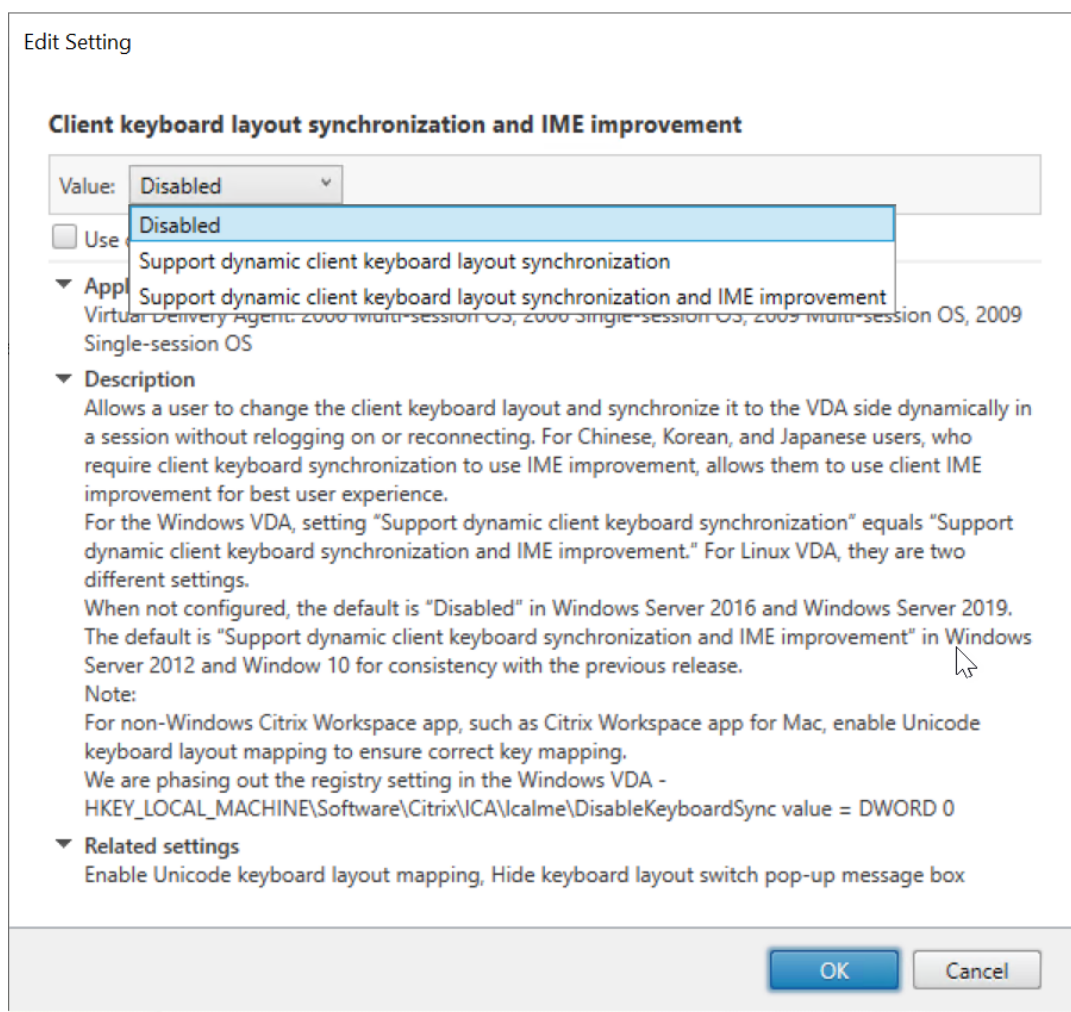
Remarque :

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"
```

HDX Insight

August 20, 2024

Vue d'ensemble

Le Linux VDA prend en charge partiellement la fonctionnalité HDX Insight. HDX Insight fait partie intégrante de Citrix Application Delivery Management (ADM) et est basé sur la norme industrielle AppFlow très répandue. Il permet au département informatique d'offrir une expérience utilisateur exceptionnelle en fournissant une visibilité inégalée de bout en bout du trafic ICA de Citrix qui transite via le tissu réseau de l'application Citrix ADC ou Citrix SD-WAN. Pour plus d'informations, consultez [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
```

Résolution des problèmes

Aucun point de données n'est affiché

Deux causes peuvent être à l'origine du problème :

- HDX Insight n'est pas configuré correctement.

Par exemple, AppFlow n'est pas activé sur le Citrix ADC ou une instance incorrecte de Citrix ADC est configurée sur Citrix ADM.

- Le canal virtuel de contrôle ICA n'est pas démarré sur le Linux VDA.

```
ps aux | grep -i ctxctl
```

Si `ctxctl` n'est pas exécuté, contactez votre administrateur pour signaler un bogue à Citrix.

Aucun point de données d'application n'est affiché

Vérifiez que le canal virtuel transparent est activé et qu'une application transparente est démarrée depuis un certain temps.

Protocole Rendezvous

November 5, 2021

Dans les environnements qui utilisent le service Citrix Gateway, le protocole Rendezvous permet aux sessions HDX de contourner Citrix Cloud Connector et de se connecter directement et en toute sécurité au service Citrix Gateway.

Exigences :

- Accès à l'environnement à l'aide du service Citrix Workspace et Citrix Gateway.
- Plan de contrôle : Citrix Virtual Apps and Desktops Service (Citrix Cloud).
- VDA Linux version 2012 ou ultérieure.
- Activez le protocole Rendezvous dans la stratégie Citrix. Pour plus d'informations, consultez la section [Paramètre de stratégie de protocole Rendezvous](#).

- Les VDA doivent avoir accès à https://*.nssvc.net, y compris tous les sous-domaines. Si vous ne pouvez pas mettre en liste blanche tous les sous-domaines de cette manière, utilisez plutôt https://*.c.nssvc.net et https://*.g.nssvc.net. Pour plus d'informations, reportez-vous à la section [Exigences en termes de connexion Internet](#) de la documentation Citrix Cloud (sous Virtual Apps and Desktop service) et à l'article du centre de connaissances [CTX270584](#).
- Les Cloud Connector doivent obtenir les noms de domaine complets des VDA lors de la négociation d'une session. Pour atteindre cet objectif, activez la résolution DNS pour le site : à l'aide du kit SDK Citrix Virtual Apps and Desktops Remote PowerShell, exécutez la commande `Set-BrokerSite -DnsResolutionEnabled $true`. Pour plus d'informations sur le SDK Remote PowerShell Citrix Virtual Apps and Desktops, consultez [SDK et API](#).

Important :

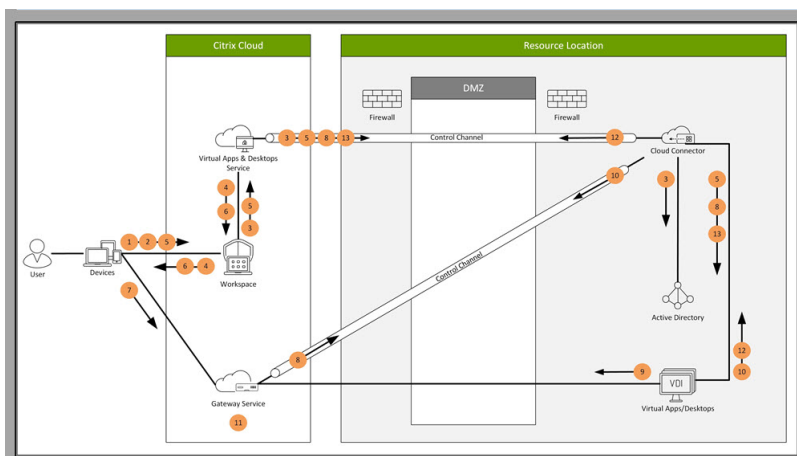
Le protocole Rendezvous ne prend pas en charge les proxy transparents ou explicites. Pour utiliser des proxy, continuez à utiliser Cloud Connector pour le trafic ICA.

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.

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 `su root -c "/opt/Citrix/VDA/bin/ctxquery -f iuStdP"`.
3. Les protocoles de transport utilisés indiqueront le type de connexion :
 - TCP Rendezvous : TCP - SSL - CGP - ICA
 - EDT Rendezvous : UDP - DTLS - CGP - ICA
 - Proxy via Cloud Connector : TCP - CGP - ICA

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, le service Citrix Virtual Apps and Desktops authentifie les informations d'identification avec Active Directory à l'aide du canal Cloud Connector.
4. Citrix Workspace affiche les ressources énumérées de Citrix Virtual Apps and Desktops Service.
5. Sélectionnez des ressources dans Citrix Workspace. Le service Citrix Virtual Apps and Desktops 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 supposée être 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 le service Citrix Virtual Apps and Desktops via Cloud Connector.
13. Le service Citrix Virtual Apps and Desktops envoie des stratégies de session au VDA via Cloud Connector. Ces stratégies sont appliquées.

Transport adaptatif

November 5, 2021

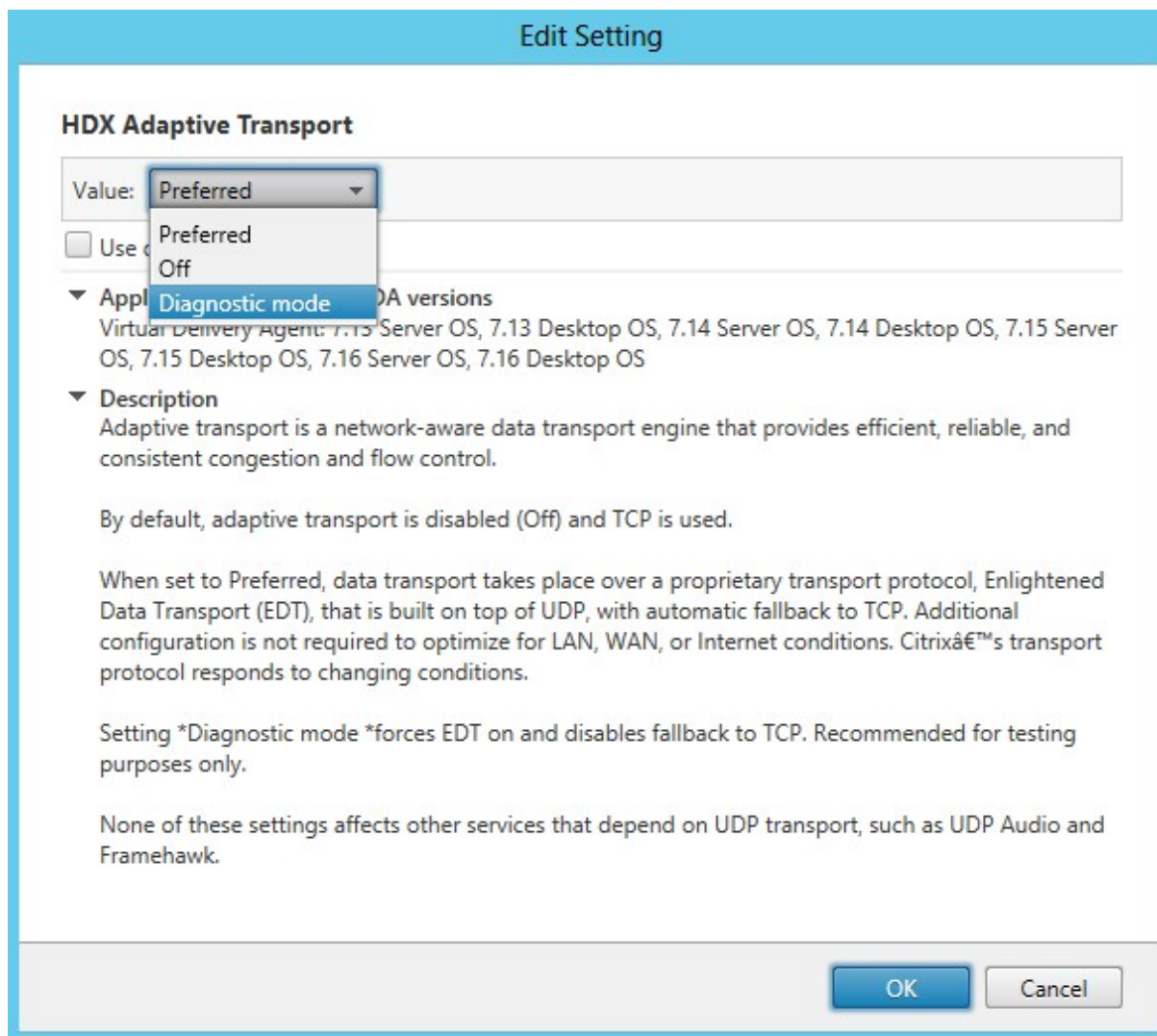
Le transport adaptatif est un mécanisme de transport de données pour Citrix Virtual Apps and Desktops. Plus rapide et plus évolutif, il améliore l'interactivité avec les applications et il est plus adapté aux connexions WAN et Internet longue distance difficiles. Pour plus d'informations sur le transport adaptatif, consultez la section [Transport adaptatif](#).

Activer le transport adaptatif

Dans Citrix Studio, vérifiez que la stratégie **HDX Adaptive Transport** est définie sur le mode **Préféré** ou **Diagnostic**. Le paramètre **Préféré** est sélectionné par défaut.

- **Préféré** : le transport adaptatif via EDT (Enlightened Data Transport) est utilisé autant que possible, avec retour vers TCP.

- **Mode Diagnostic** : EDT est activé de force et le retour vers TCP est désactivé.



Désactiver le transport adaptatif

Pour désactiver le transport adaptatif, définissez la stratégie **HDX Adaptive Transport** sur **Off** dans Citrix Studio.

Vérifier si le transport adaptatif est activé

Exécutez la commande suivante pour vérifier si les écouteurs UDP sont en cours d'exécution.

```
1 netstat -an | grep "1494|2598"
```

Dans des circonstances normales, la sortie est similaire à ce qui suit.

1	udp	0	0 0.0.0.0:2598	0.0.0.0:*
2				
3	udp	0	0 :::1494	:::*

Découverte MTU EDT

EDT détermine automatiquement l'unité de transmission maximale (MTU) lors de l'établissement d'une session. Cela empêche la fragmentation des paquets EDT, qui pourrait entraîner une dégradation des performances ou l'échec de l'établissement d'une session.

Configuration minimale requise :

- Linux VDA 2012
- Application Citrix Workspace 1911 pour Windows
- Citrix ADC :
 - 13.0.52.24
 - 12.1.56.22
- La fiabilité de session doit être activée

Si vous utilisez des versions des plates-formes de client qui ne prennent pas en charge cette fonctionnalité, consultez l'article du Centre de connaissances [CTX231821](#) pour plus de détails sur la configuration d'un MTU EDT personnalisé adapté à votre environnement.

Avertissement :

la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Activer ou désactiver la découverte MTU EDT sur le VDA

La découverte MTU EDT est désactivée par défaut.

- Pour activer la découverte MTU EDT, définissez la clé de registre [MtuDiscovery](#) à l'aide de la commande suivante, redémarrez le VDA et attendez que le VDA s'enregistre :

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\icawd"-t "REG_DWORD"-v "MtuDiscovery"-d "0x00000001"--force
```

- Pour désactiver la découverte MTU EDT, supprimez la valeur de registre `MtuDiscovery`.

Ce paramètre s'applique à l'échelle de la machine et affecte toutes les sessions se connectant à partir d'un client pris en charge.

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.

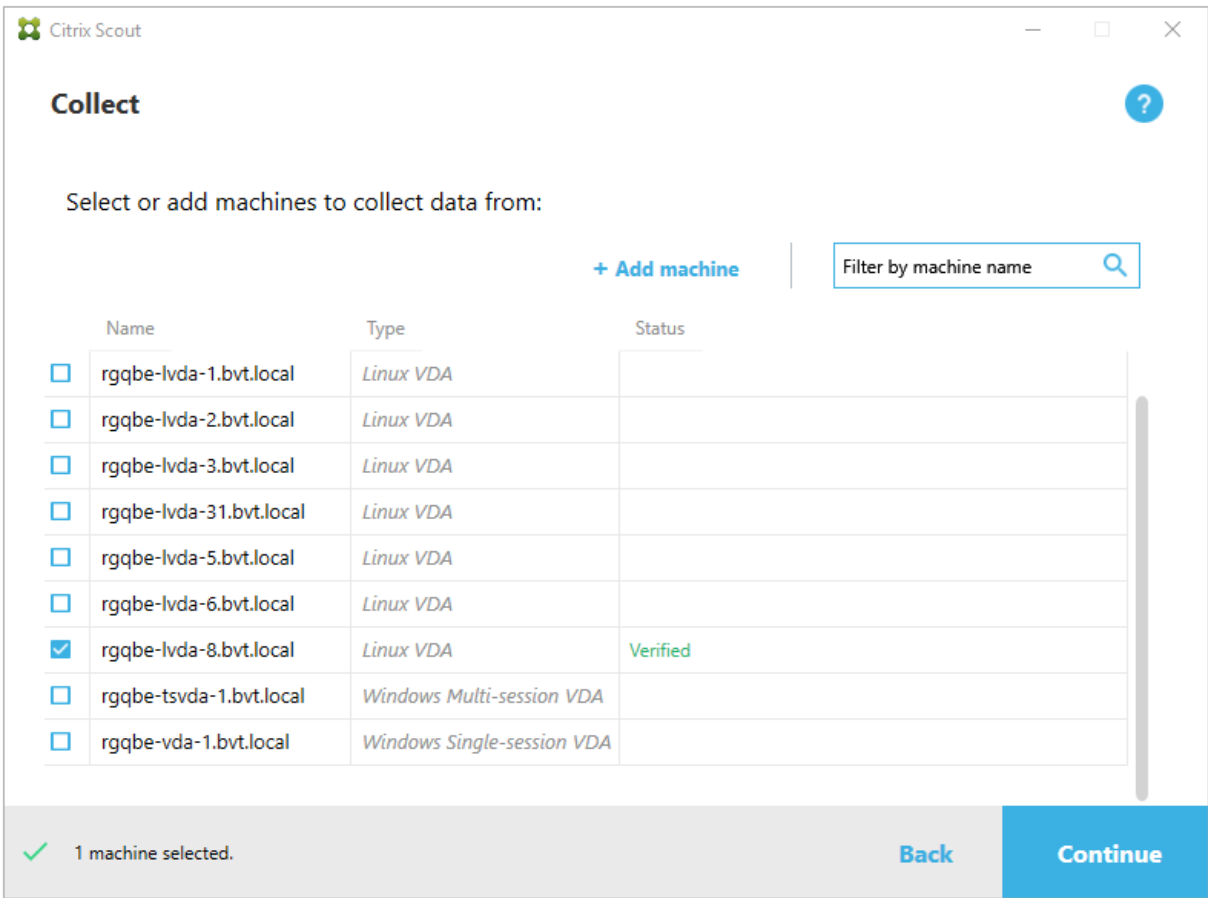
IMPORTANT :

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.

Intégrer avec Citrix Telemetry Service

November 5, 2021

Avec Citrix Telemetry Service (ctxtelemetry) intégré au logiciel VDA Linux, vous pouvez exécuter Citrix Scout, qui utilise ensuite le script `/opt/Citrix/vda/bin/xdlcollect.sh`, pour collecter des journaux sur le VDA Linux.



Remarque :

après la mise à niveau à partir de Linux VDA 1912 et versions antérieures, vous devez réexécuter `/opt/Citrix/VDA/sbin/ctxsetup.sh` pour configurer les variables du service de télémétrie Citrix (ctx-telemetry). Pour de plus amples informations sur les variables, consultez la section [Easy Install](#).

Activer et désactiver le service de télémétrie Citrix

- Pour activer le service, exécutez la commande **sudo systemctl enable ctxtelemetry.socket**.
- Pour désactiver le service, exécutez **sudo systemctl disable ctxtelemetry.socket**.

Ports

Le service de télémétrie Citrix (ctxtelemetry), par défaut, utilise le port TCP/IP 7503 pour écouter Citrix Scout. Il utilise le port TCP/IP 7502 sur le Delivery Controller pour communiquer avec Citrix Scout.

Vous pouvez utiliser les ports par défaut ou modifier les ports via les variables suivantes lorsque vous installez le VDA Linux.

- **CTX_XDL_TELEMETRY_SOCKET_PORT** : port socket permettant d'écouter Citrix Scout. Le port par défaut est 7503.
- **CTX_XDL_TELEMETRY_PORT** : port de communication avec Citrix Scout. Le port par défaut est 7502.

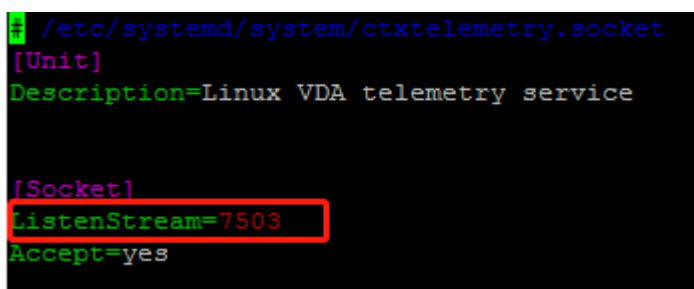
Pour modifier les ports après avoir installé votre VDA, procédez comme suit :

1. Pour modifier un port de communication avec Scout, exécutez la commande suivante.

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\VirtualDesktopAgent" -v "TelemetryServicePort" -d <port number> -t REG_DWORD
```

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
```



```
/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 une distribution Ubuntu, par exemple, exécutez la commande **sudo ufw allow 7503** pour activer le port 7503.

Mode débogage

Si le service de télémétrie Citrix ne fonctionne pas comme prévu, vous pouvez activer le mode de débogage pour en déterminer les causes.

1. Pour activer le mode de débogage, exécutez la commande suivante pour ouvrir le fichier `ctxtelemetry`, puis modifiez la valeur `DebugMode` sur 1.

```
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 0.0.0.0:53:53          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 0.0.0.0:631            0.0.0.0:*               LISTEN      25158/cupsd
tcp        0      0 0.0.0.0:5432           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.

Traçage activé

November 5, 2021

Vue d'ensemble

La collecte de journaux et la reproduction des problèmes ralentissent les diagnostics et dégradent l'expérience utilisateur. La fonction de traçage facilite ces efforts. Par défaut, le traçage est activé pour le Linux VDA.

Configuration

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.

démon `ctxlogd`

Tous les autres services qui font l'objet d'un suivi dépendent du démon `ctxlogd`. Vous pouvez arrêter le démon `ctxlogd` si vous ne souhaitez pas que le Linux VDA fasse l'objet d'un suivi.

Utilitaire `setlog`

La fonctionnalité de traçage est configurée à l'aide de l'utilitaire `setlog`, qui se trouve sous `/opt/Citrix/VDA/bin/`. Seul l'utilisateur racine est autorisé à l'exécuter. Vous pouvez utiliser l'interface utilisateur ou exécuter des commandes pour afficher et modifier les configurations. Pour obtenir de l'aide sur l'utilitaire `setlog`, exécutez la commande suivante :

```
1 setlog help
```

Valeurs Par défaut, **Log Output Path** est défini sur **/var/log/xdl/hdx.log**, **Max Log Size** est défini sur 200 Mo, et vous pouvez enregistrer jusqu'à deux anciens fichiers journaux sous **Log Output Path**.

Afficher les valeurs `setlog` actuelles :

```
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
```

Afficher ou définir une valeur `setlog` unique :

```
1 setlog value <name> [<value>]
```

Par exemple :

```
1 setlog value log_size 100
```

Niveaux Par défaut, le niveau de journalisation est défini sur **Warnings**.

Afficher les niveaux de journalisation définis pour différents composants :

```
1 setlog levels
```

Vous pouvez définir tous les niveaux de journalisation (y compris Disable, Inherited, Verbose, Information, Warnings, Errors et Fatal Errors) à l'aide de la commande suivante :

```
1 setlog level <class> [<level>]
```

La variable **<class>** spécifie un composant de l'agent Linux VDA. Pour couvrir tous les composants, définissez-la sur tous :

```
1 setlog level all error
2
3 Setting log class ALL to ERROR.
```

Indicateurs Par défaut, les indicateurs sont définis comme suit :

```
1 setlog flags
2
3 DATE = true
4
5 TIME = true
6
7 NAME = true
8
```

```
9  PID = true
10
11  TID = false
12
13  SID = true
14
15  UID = false
16
17  GID = false
18
19  CLASS = false
20
21  LEVEL = false
22
23  FUNC = true
24
25  FILE = false
```

Afficher les indicateurs actuels :

```
1  setlog flags
```

Afficher ou définir un indicateur de journalisation unique :

```
1  setlog flag <flag> [<state>]
```

Restaurer paramètres par défaut Rétablir les paramètres par défaut de tous les niveaux, de tous les indicateurs 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.

Résolution des problèmes

Le démon `ctxlogd` échoue et vous ne pouvez pas redémarrer le service `ctxlogd` lorsque le fichier `/var/xdl.ctxlog` est manquant (s'il a été supprimé accidentellement par exemple).

`/var/log/messages` :

```
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 racine pour créer le fichier `/var/xdm/ctxlog`. Redémarrez le service `ctxlogd` dont dépendent d'autres services.

Observer des sessions

November 5, 2021

La fonctionnalité d'observation de session 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 et est prise en charge uniquement avec RHEL 7.x et Ubuntu 16.04.

Remarque :

Pour utiliser la fonctionnalité d'observation de session, la version de Citrix Director doit être 7.16 ou ultérieure.

Installation et configuration

Dépendances

Deux nouvelles dépendances, `python-websocketify` et `x11vnc`, sont nécessaires pour l'observation de session. Les dépendances `python-websocketify` et `x11vnc` sont automatiquement installées lorsque vous installez le Linux VDA sur Ubuntu 16.04. Sur RHEL 7.x, vous devez installer manuellement `python-websocketify` et `x11vnc` après avoir installé le Linux VDA.

Exécutez la commande suivante sur RHEL 7.x pour installer `python-websocketify` et `x11vnc` (`x11vnc` version 0.9.13 ou ultérieure).

```
1 sudo yum install -y python-websocketify x11vnc
```

Pour résoudre `python-websocketify` et `x11vnc`, activez les référentiels suivants sur RHEL 7.x :

- Packages supplémentaires pour Enterprise Linux (EPEL)

Le référentiel EPEL est requis pour `python-websocketify` et `x11vnc`. Pour activer le référentiel EPEL, exécutez la commande suivante :

```
1 sudo yum install https://dl.fedoraproject.org/pub/epel/epel-
   release-latest-$(rpm -E '%{
2   rhel }
3   ').noarch.rpm
```

• RPM facultatifs

Exécutez l’une des commandes suivantes pour activer le référentiel de RPM facultatifs pour l’installation de certains packages de dépendances de `x11vnc` :

Pour un poste de travail :

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

Pour un serveur :

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

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 l’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://` est déterminé par le 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. Pour des raisons pratiques, vous pouvez utiliser un certificat générique pour la totalité du domaine. Dans ce cas, vous devez connaître au moins le nom de domaine.

Outre l'installation d'un certificat de serveur sur chaque serveur, vous devez installer un certificat racine de la même autorité de certification (CA) sur chaque client Citrix Director qui communique avec le serveur Linux VDA. Les autorités de certification émettant des certificats de serveur émettent aussi les certificats racines. Vous pouvez installer les certificats de serveurs et racines à partir d'une autorité de certification (CA) intégrés à votre système d'exploitation, d'une CA d'entreprise (soit une CA à laquelle votre organisation vous donne accès) ou d'une CA non intégrée à 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 serveur Linux VDA ou, au moins, les caractères générique + domaine corrects. Par exemple, `vda1.basedomain.com` ou `*.basedomain.com`.
- Les algorithmes de hachage, y compris SHA1 et MD5, sont trop faibles pour les signatures dans les certificats numériques pour certains navigateurs. SHA-256 est donc spécifié comme standard minimum.

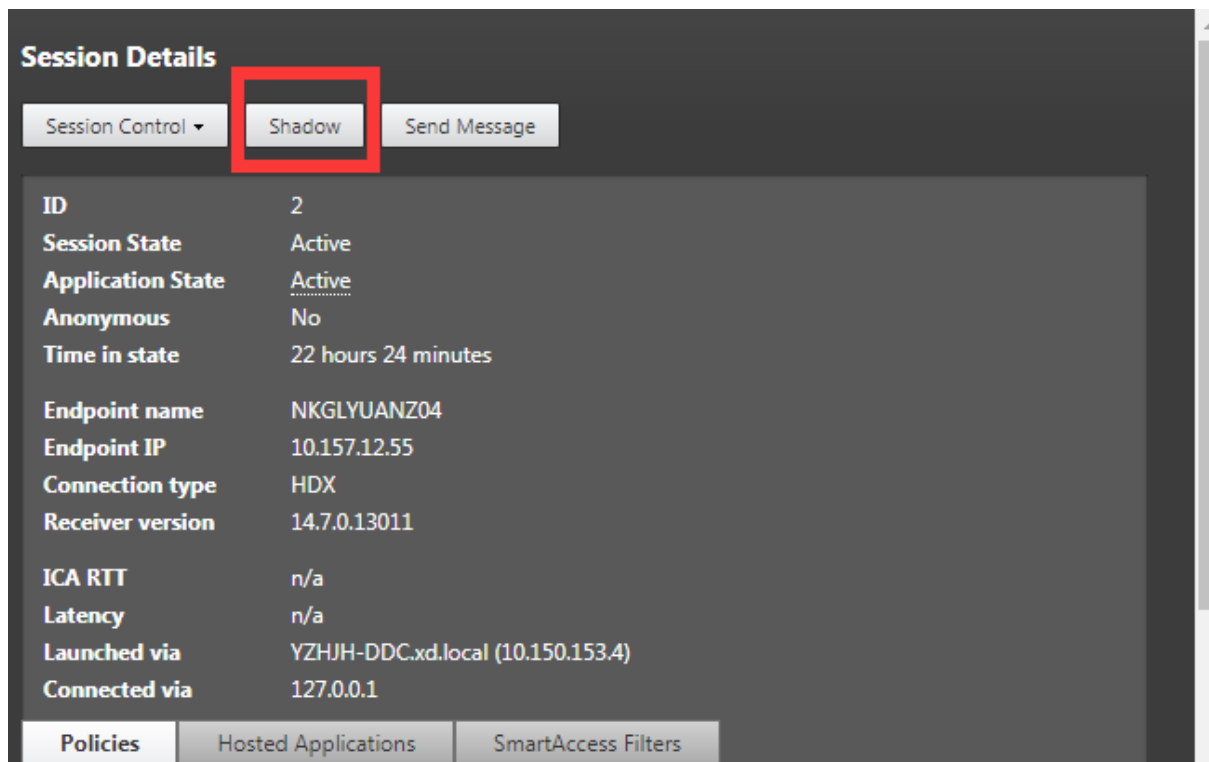
Installer un certificat racine sur chaque client Citrix Director L'observation de session utilise le même magasin de certificats qu'IIS (reposant sur le registre). Par conséquent, vous pouvez installer

les certificats à l'aide d'IIS ou du composant logiciel enfichable MMC (Microsoft Management Console). Après avoir reçu un certificat d'une autorité de certification, vous pouvez redémarrer l'assistant Certificat de serveur Web d'IIS. L'assistant installe alors le certificat. Vous pouvez également afficher et importer des certificats sur l'ordinateur en utilisant la console MMC et ajouter le certificat en tant que composant logiciel enfichable autonome. Internet Explorer et Google Chrome importent les certificats installés sur votre système d'exploitation par défaut. Pour Mozilla Firefox, vous devez importer vos certificats SSL racine dans l'onglet **Autorités** du gestionnaire de certificats.

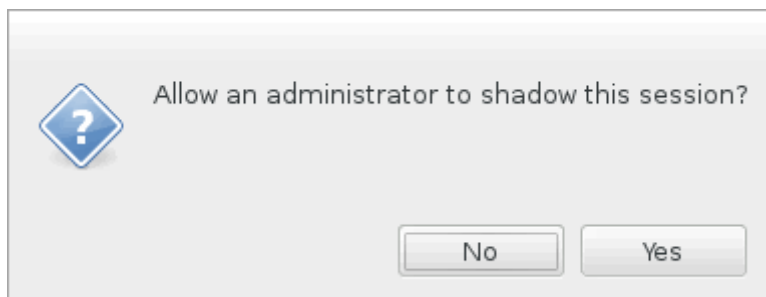
Installer un certificat de serveur et sa clé sur chaque serveur Linux VDA Appelez les certificats de serveur « shadowingcert.* » et le fichier de clé « shadowingkey.* » (* peut indiquer le format, par exemple, shadowingcert.csr et shadowingkey.key). Placez les certificats de serveur et les fichiers de clés sous le chemin d'accès **/etc/xdl/shadowingssl** et protégez-les correctement avec des autorisations restreintes. Si le nom ou le chemin est incorrect, le Linux VDA est incapable de trouver un certificat ou un fichier de clé spécifique et, par conséquent, cela entraîne une défaillance de la connexion avec Citrix Director.

Utilisation

Dans Citrix Director, recherchez la session cible et cliquez sur **Observer** dans la vue **Détails de la session** pour envoyer une demande d'observation à l'agent Linux VDA.



Une fois que la connexion s’initialise, une confirmation s’affiche sur le client de session ICA (pas le client Citrix Director) pour demander l’autorisation d’observer la session.



Si l'utilisateur clique sur **Oui**, une fenêtre s’affiche du côté Citrix Director, indiquant que la session ICA est en cours d’observation.

Pour de plus amples informations sur l'utilisation, veuillez consulter la [documentation de Citrix Director](#).

Limitations

- L’observation de session est conçue pour une utilisation dans un intranet uniquement. Elle ne fonctionne pas pour les réseaux externes même en se connectant via Citrix Gateway. Citrix décline toute responsabilité en ce qui concerne l’observation de session de Linux VDA dans un réseau externe.
- Lorsque l’observation de session est activée, un administrateur de domaine peut uniquement afficher les sessions ICA, et n’a pas l’autorisation d’écrire dessus ou de le contrôler.
- Une fois qu’un administrateur a cliqué sur **Observer** depuis Citrix Director, une confirmation s’affiche pour demander l’autorisation à l’utilisateur d’observer la session. Une session peut être observée uniquement lorsque l’utilisateur de la session en donne l’autorisation.
- La confirmation mentionnée précédemment a un délai d’expiration, qui est de 20 secondes. Une demande d’observation échoue lorsque ce délai est écoulé.
- Une session ICA peut être observée par un seul administrateur dans une seule fenêtre Citrix Director. Si une session ICA a été observée par l’administrateur A et pendant ce temps, l’administrateur B envoie une demande d’observation, 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. Il en est de même si une autre demande d’observation pour la même session ICA est envoyée par le même administrateur.
- 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.

Résolution des problèmes

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 au nom de domaine complet du Linux 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 `service ctxvda restart` pour redémarrer le service `ctxvda`.

En cas d'erreur lors de l'établissement de la connexion, procédez comme suit :

1. Recherchez toute limitation de pare-feu qui empêche l'observation de session d'ouvrir le port.
2. Vérifiez que les certificats et les fichiers de clés sont correctement nommés et placés sous le bon chemin pour un scénario SSL.
3. Vérifiez qu'il reste suffisamment de ports entre 6001 et 6099 pour les nouvelles demandes d'observation.

Redirection du contenu du navigateur

February 3, 2022

Vue d'ensemble

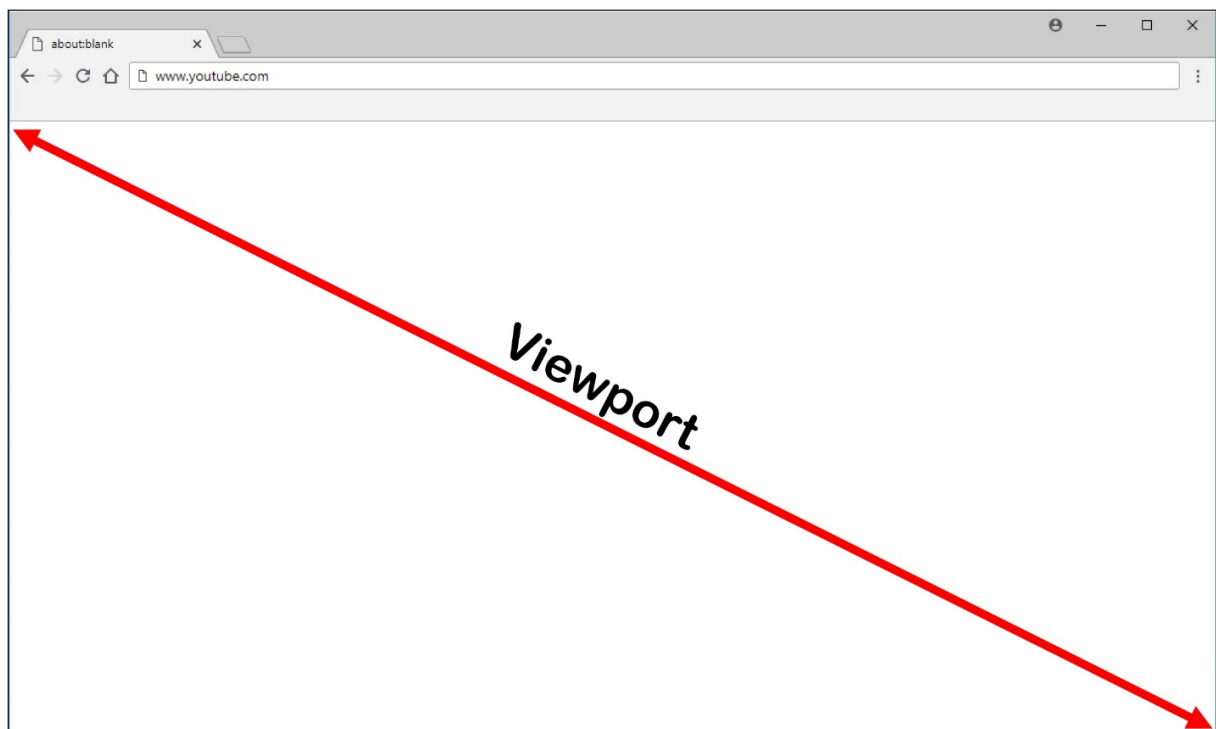
Le VDA Linux prend en charge la redirection du contenu du navigateur dans Google Chrome. La redirection du contenu du navigateur permet d'afficher les pages Web dans la liste verte du côté client. Cette fonctionnalité utilise l'application Citrix Workspace pour instancier un moteur de rendu correspondant côté client, qui récupère le contenu HTTP et HTTPS de l'URL.

Remarque :

vous pouvez spécifier les pages Web qui sont redirigées sur le client à l'aide d'une liste verte. Inversement, vous pouvez spécifier les pages Web qui ne sont pas redirigées sur le côté client à l'aide d'une liste rouge.

Ce moteur d'affichage Web en superposition est exécuté sur le client plutôt que sur le VDA et utilise l'UC, le GPU, la RAM et le réseau du client.

Seule la fenêtre d'affichage du navigateur est redirigée. La fenêtre d'affichage est la zone rectangulaire de votre navigateur dans laquelle le contenu s'affiche. La fenêtre d'affichage n'inclut pas d'éléments tels que la barre d'adresse, la barre de favoris et la barre d'état. Ces éléments sont toujours en cours d'exécution dans le navigateur du VDA.



Configuration système requise

Client Windows :

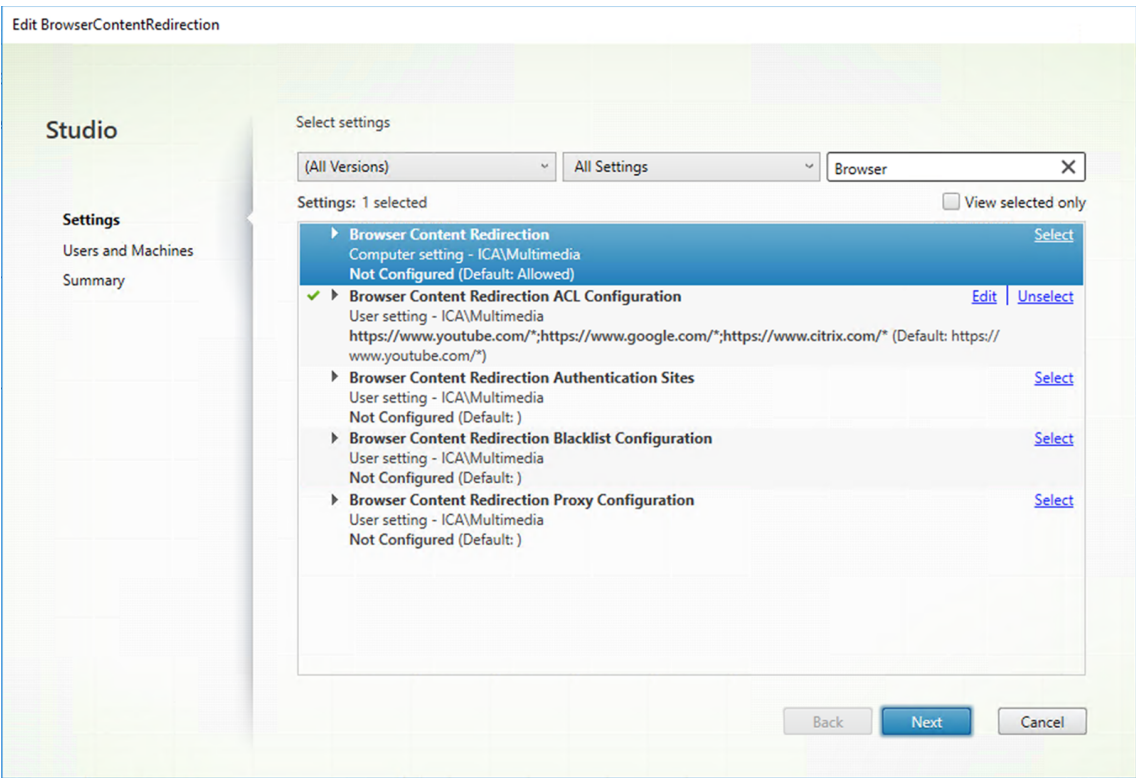
- Application Citrix Workspace 1809 pour Windows ou version ultérieure

Linux VDA :

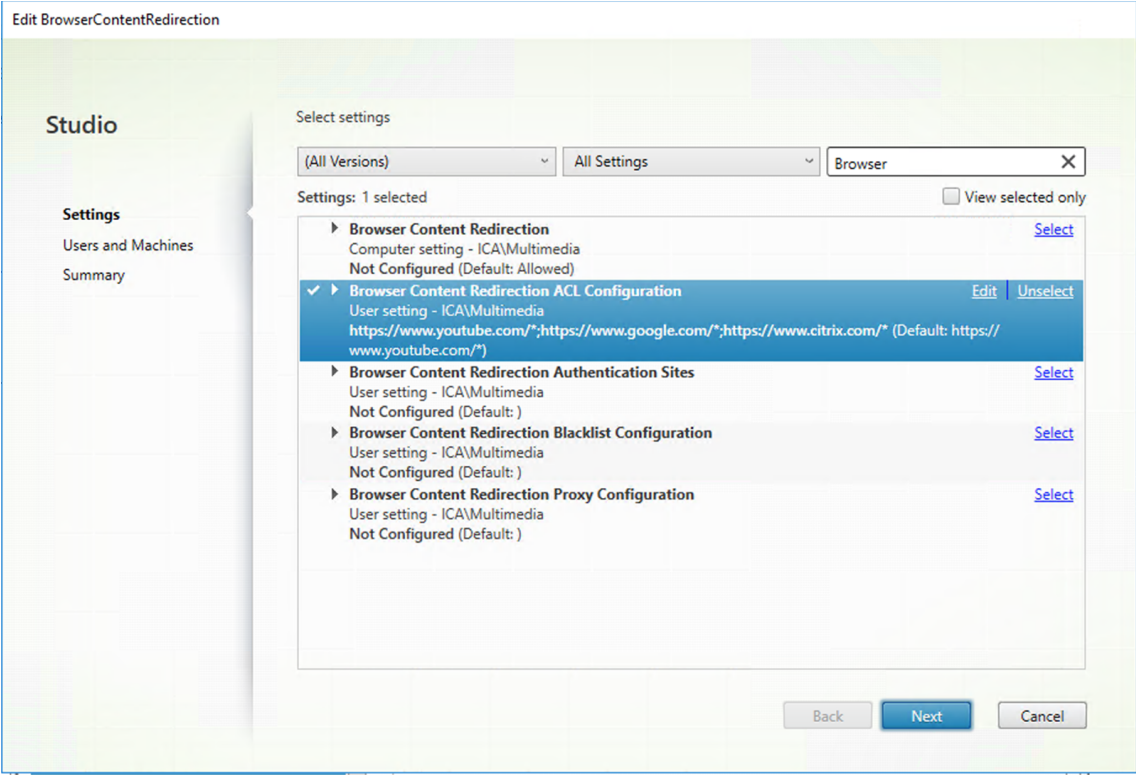
- Système d'exploitation VDA : Ubuntu 16.04, Ubuntu 18.04, RHEL 7.8, RHEL 8.2, RHEL 8.1, SLES 12.5
- Navigateur sur le VDA : Google Chrome v66 ou version ultérieure avec l'extension de redirection de contenu du navigateur Citrix ajoutée

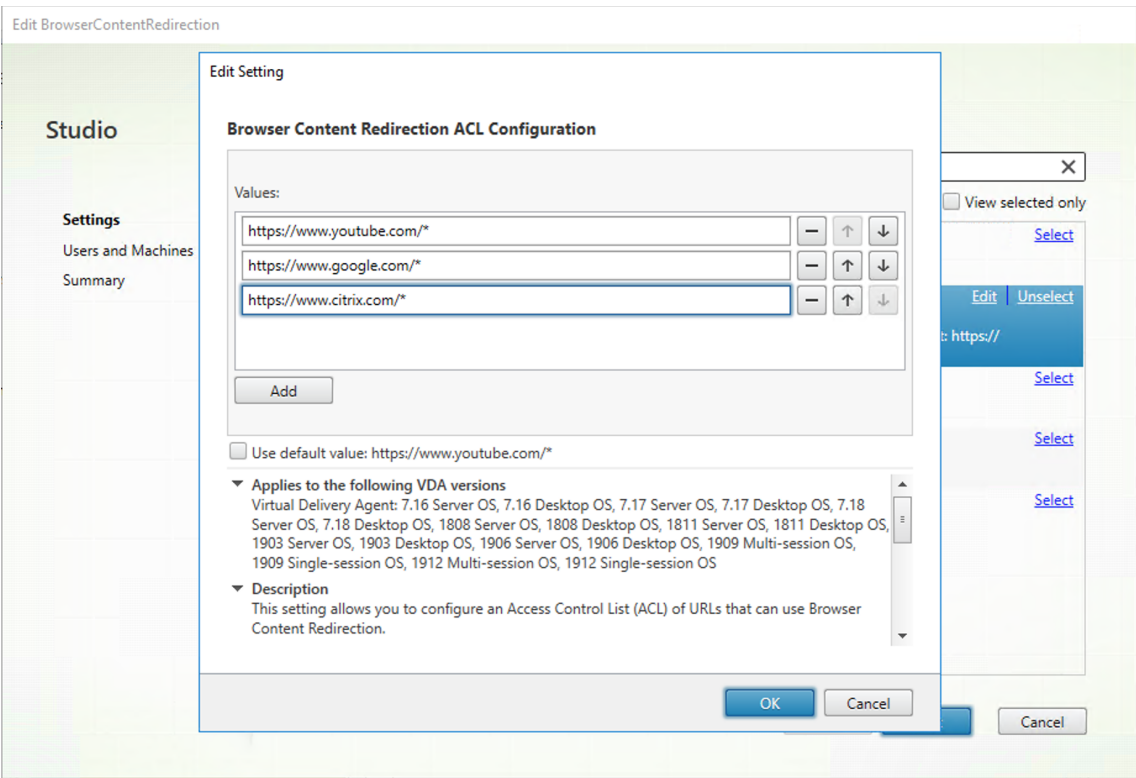
Configurer la redirection du contenu du navigateur

1. Dans Citrix Studio, configurez une stratégie qui spécifie une liste verte d'URL pouvant utiliser la redirection du contenu du navigateur et une liste rouge d'URL non autorisées à utiliser la redirection du contenu du navigateur. La redirection du contenu du navigateur est définie sur **Autorisé** par défaut.

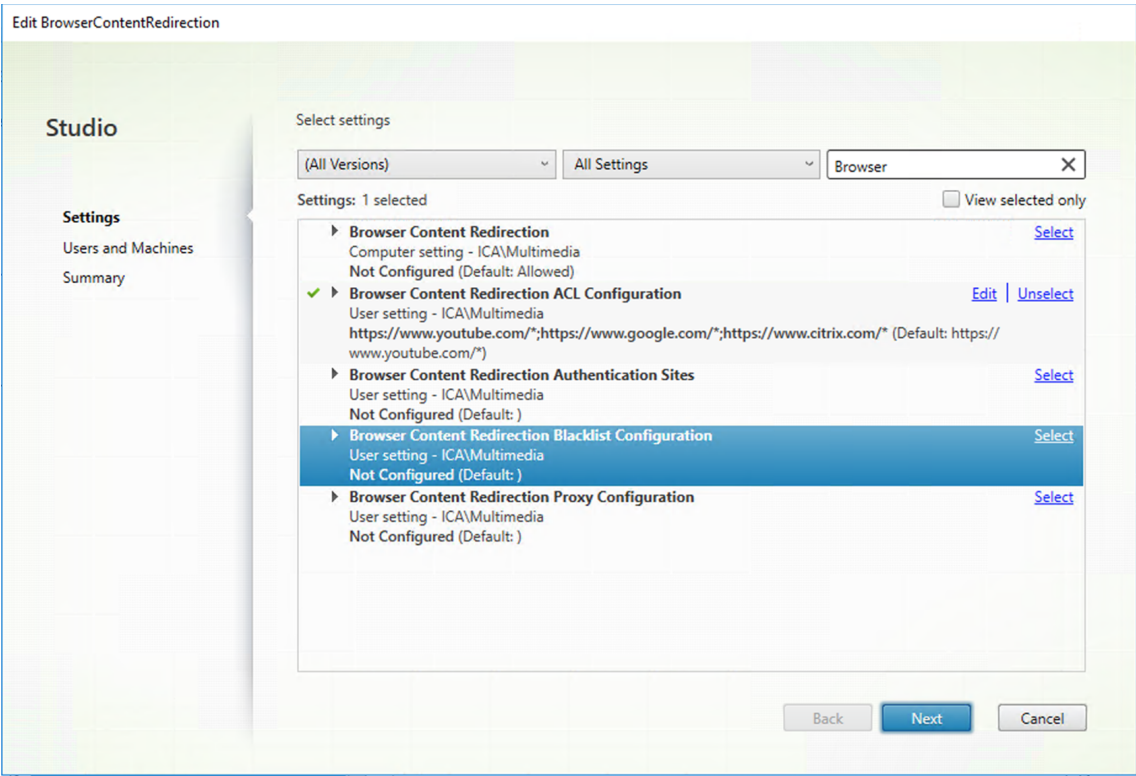


Le paramètre **Configuration de l'ACL de redirection du contenu de navigateur** spécifie une liste verte d'URL pouvant utiliser la redirection du contenu du navigateur.





Le paramètre **Configuration d'une liste noire de redirection du contenu de navigateur** spécifie une liste rouge d'URL qui ne peuvent pas utiliser la redirection du contenu du navigateur.



Remarque:

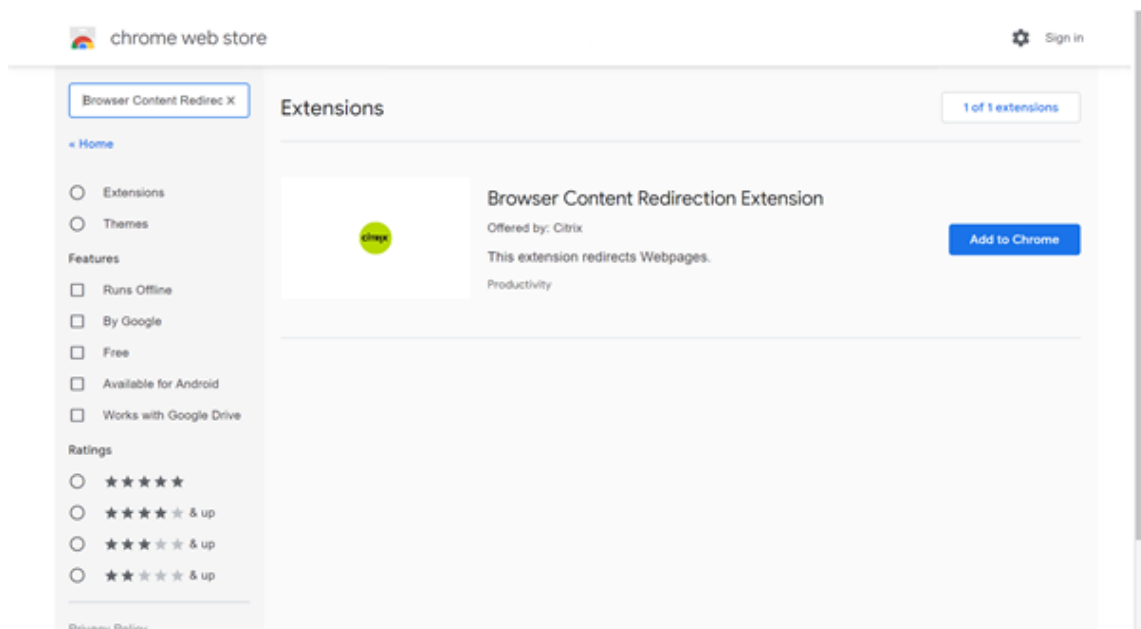
le Linux VDA ne prend actuellement pas en charge le paramètre **Configuration du proxy de redirection du contenu de navigateur**.

2. Pour que le navigateur du VDA détecte si une URL (à laquelle vous souhaitez accéder) correspond à une liste verte ou à une liste rouge, ajoutez l'extension de redirection de contenu du navigateur Citrix à partir du Chrome Web Store. Cliquez sur **Ajouter à Chrome** sur le VDA.

Important :

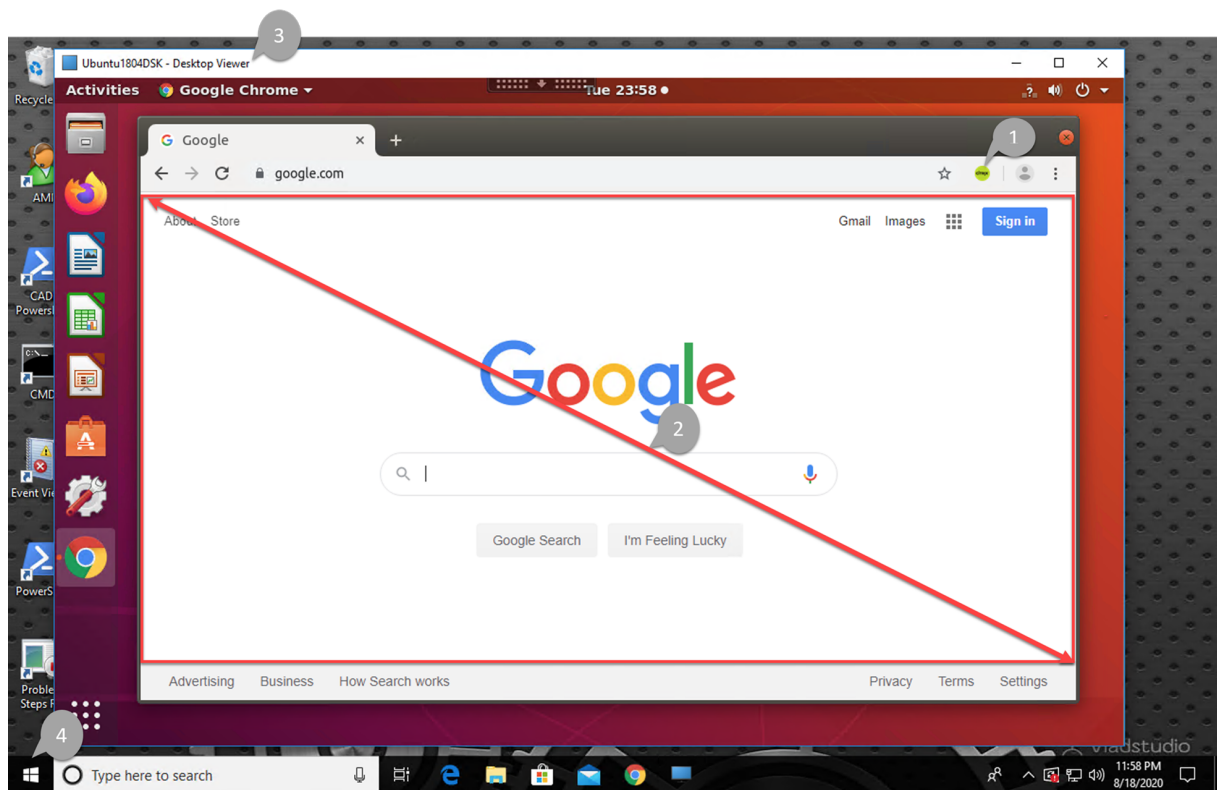
l'extension n'est pas requise sur le client. Ajoutez-la uniquement sur le VDA.

Les extensions Chrome sont installées utilisateur par utilisateur. La mise à jour d'une image principale pour ajouter ou supprimer une extension n'est pas requise.



Si une correspondance avec une URL est trouvée dans une liste verte (par exemple, <https://www.mycompany.com/>) mais pas dans une liste rouge, un canal virtuel (CTXCSB) indique à l'application Citrix Workspace qu'une redirection est requise et relaie l'URL. L'application Citrix Workspace instancie alors un moteur de rendu local et affiche le site Web.

L'application Citrix Workspace reproduit ensuite de manière transparente le site Web dans la zone de contenu du navigateur de bureau virtuel.



1. Icône de l'extension de redirection de contenu du navigateur Citrix

La couleur de l'icône d'extension indique l'état de l'extension Chrome. Couleurs des différents états :

- Vert : active et connectée
- Gris : inactive sur l'onglet actuel
- Rouge : interrompue/ne fonctionne pas

2. Affichage sur le client ou reproduit sur le bureau virtuel

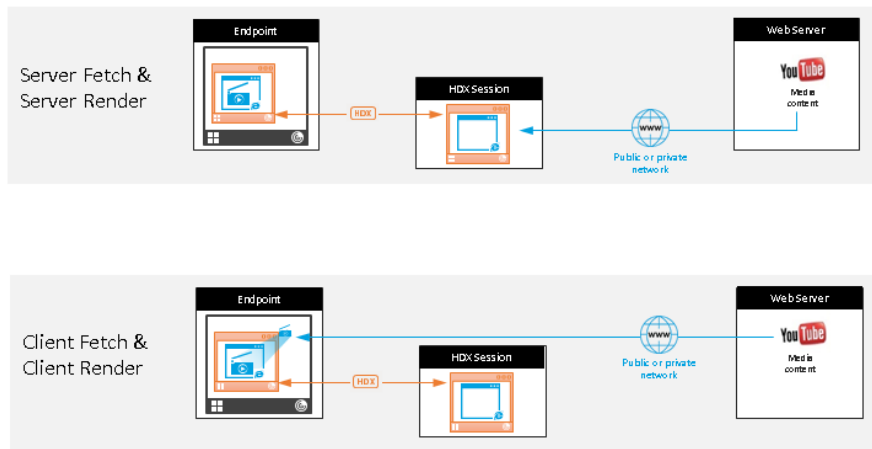
3. Linux VDA

4. Client Windows

Scénarios de redirection

L'application Citrix Workspace peut récupérer le contenu de trois façons :

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 d'autorisation ou la redirection a échoué. Nous revenons au rendu de page Web sur le VDA et utilisons Thinwire pour utiliser à distance les graphiques. Utiliser les stratégies pour contrôler le comportement de secours. Ce scénario provoque une consommation élevée de CPU, de RAM et de bande passante sur le VDA.
- **Récupération client et rendu client** : l'application Citrix Workspace contacte directement le serveur Web, ce qui nécessite un accès Internet. Ce scénario décharge toute l'utilisation du réseau, du processeur et de la RAM de votre site Citrix Virtual Apps and Desktops.

Mécanisme de secours

Il peut arriver que la redirection du client échoue. Par exemple, si la machine client n'a pas d'accès direct à Internet, une réponse d'erreur peut revenir au VDA. Dans ce cas, le navigateur du VDA peut recharger et afficher la page sur le serveur.

Prise en charge de l'application Citrix Workspace pour HTML5

November 5, 2021

À partir de cette version, 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](#).

Surveiller les sessions Linux et les VM Linux dans Citrix Director

June 16, 2023

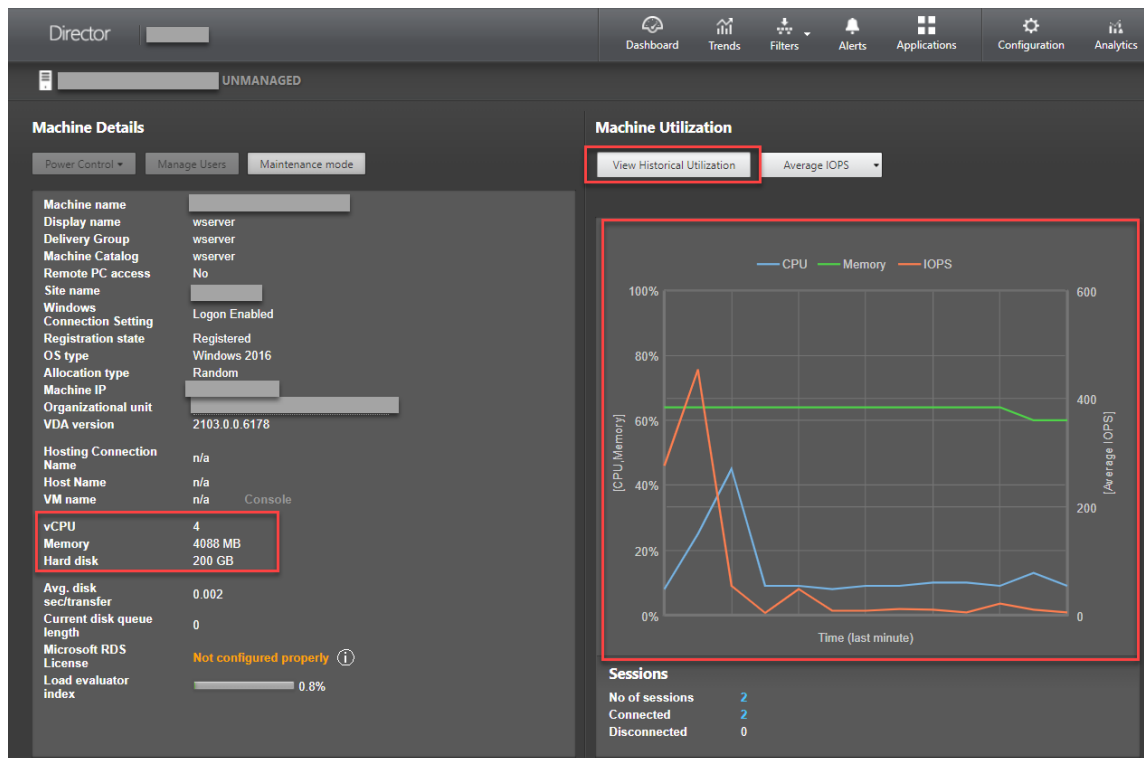
Cet article répertorie certaines des mesures disponibles pour les machines virtuelles Linux et les sessions Linux dans Citrix Director.

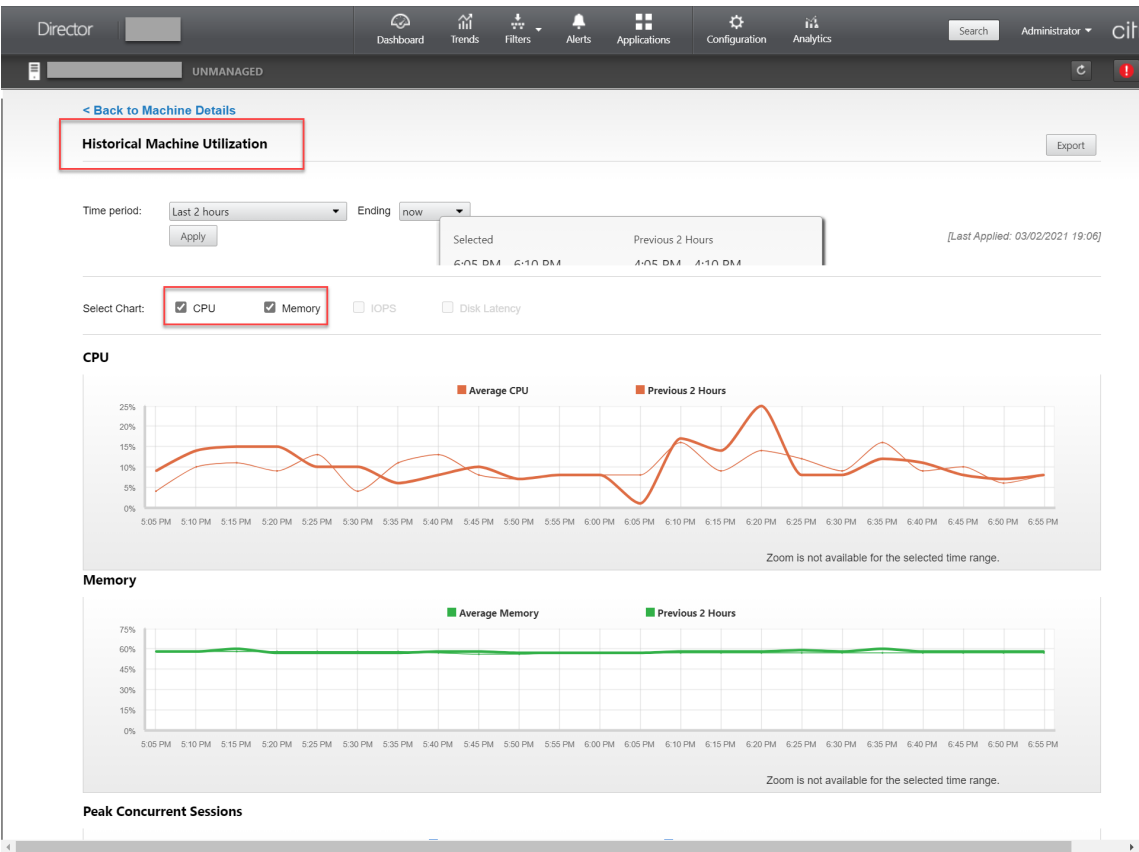
Mesures pour les machines virtuelles Linux

Pour accéder aux mesures d'une machine virtuelle Linux, recherchez la VM dans Citrix Director et vérifiez le panneau **Détails de la machine**.

À partir de la version 2103 du Linux VDA, les mesures suivantes pour les machines virtuelles Linux sont disponibles dans Citrix Director.

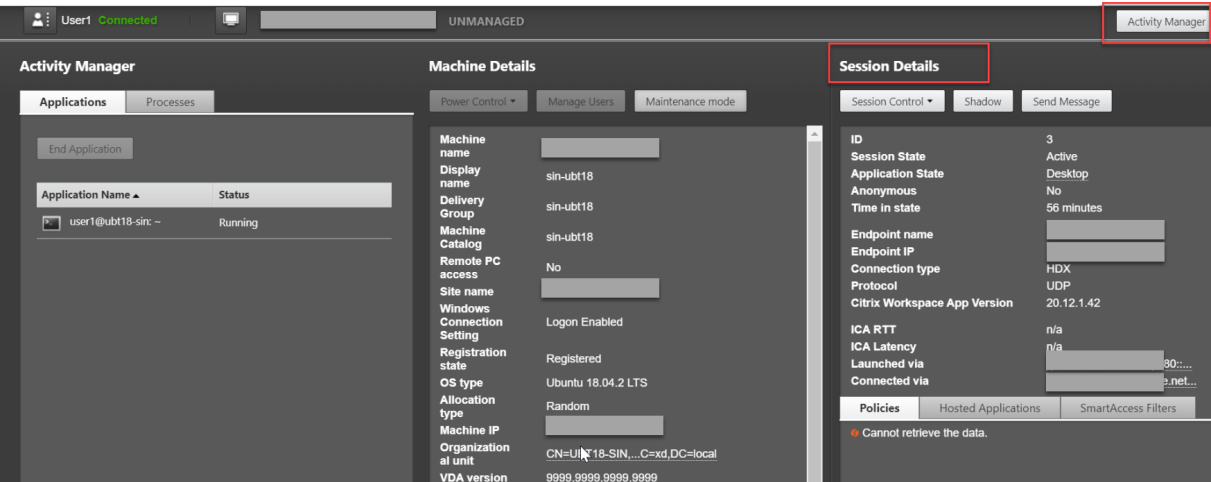
- Nombre de cœurs de processeur
- Taille de la mémoire
- Capacité du disque dur
- Utilisation actuelle et historique du processeur et de la mémoire





Mesures pour les sessions Linux

Pour afficher les mesures d'une session Linux, ouvrez la page **Toutes les sessions** en sélectionnant **Filtres > Sessions > Toutes les sessions** ou accédez au panneau **Détails de la session**. Pour accéder au panneau **Détails de la session**, ouvrez la page **Toutes les sessions** et cliquez sur une session cible pour accéder à la vue **Gestionnaire d'activités**. Par exemple :



- RTT ICA

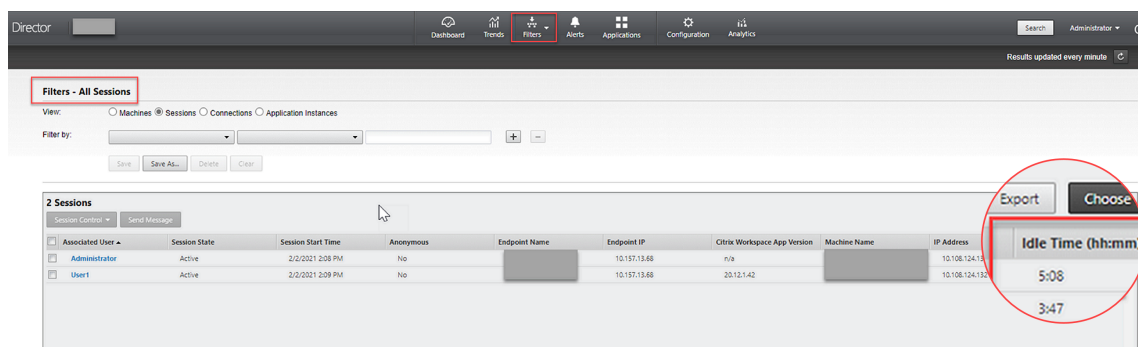
Les mesures RTT ICA sont disponibles à partir de la version 1903 de Linux VDA. Pour afficher les mesures RTT ICA, utilisez Citrix Director 1903 ou version ultérieure et créez les stratégies **Calcul des boucles ICA** et **Intervalle de calcul des boucles ICA** dans Citrix Studio. Pour de plus amples informations sur la création de stratégies, consultez la section [Créer une stratégie à l'aide de Studio](#).

- Protocole

Des informations sur le protocole sont disponibles à partir de la version 1909 de Linux VDA. Le protocole de transport d'une session Linux apparaît comme **UDP** ou **TCP** dans le panneau **Détails de la session**.

- Délai d'inactivité

À partir de la version 2103 du Linux VDA, la mesure du délai d'inactivité est disponible pour les sessions Linux. Pour accéder à cette mesure, ouvrez la boîte de dialogue **Toutes les sessions** en sélectionnant **Filtres > Sessions > Toutes les sessions**.



Démon du service de surveillance

March 3, 2022

Le démon du service de surveillance surveille les services clés en effectuant des analyses périodiques. Lors de la détection des exceptions, le démon redémarre ou arrête les processus de service et nettoie les données résiduelles du processus pour libérer les ressources. Les exceptions détectées sont enregistrées dans le fichier **/var/log/xdl/ms.log**.

Configuration

Le démon du service de surveillance démarre automatiquement lorsque vous démarrez le VDA.

Vous pouvez configurer la fonctionnalité via les fichiers **scanningpolicy.conf**, **rulesets.conf** et **whitelist.conf** dotés des privilèges d'administrateur. Les fichiers de configuration se trouvent dans **/opt/Citrix/VDA/sbin**.

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 service ctxmonitorservice restart
```

- **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
```

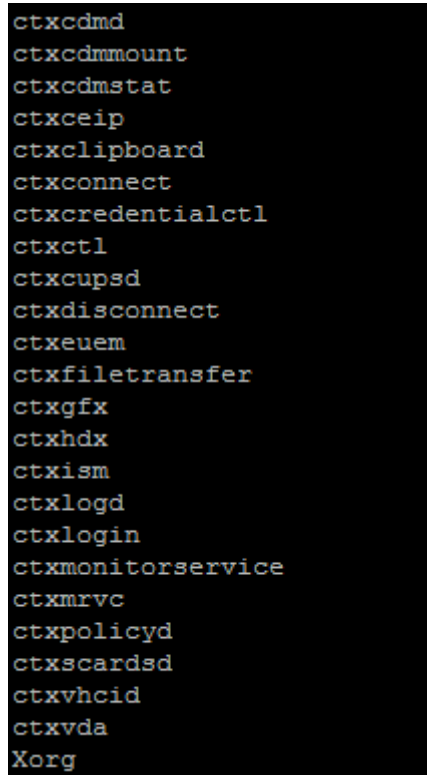
Pour configurer chaque service à surveiller, définissez les champs suivants.

- 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 = nettoyer 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.



```
ctxcdmnd
ctxcdmmount
ctxcdmstat
ctxceip
ctxclipboard
ctxconnect
ctxcredentialctl
ctxctl
ctxcupsd
ctxdisconnect
ctxeuem
ctxfiletransfer
ctxgfx
ctxhdx
ctxism
ctxlogd
ctxlogin
ctxmonitorservice
ctxmrvc
ctxpolicyd
ctxscardsd
ctxvhcid
ctxvda
Xorg
```

Remarque :

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

Sécuriser les sessions utilisateur en utilisant TLS

March 3, 2022

À compter de la version 7.16, l'agent Linux VDA prend en charge le chiffrement TLS pour des sessions utilisateur sécurisées. Le chiffrement TLS est désactivé par défaut.

Activer le chiffrement TLS

Pour activer le chiffrement TLS pour des sessions utilisateur sécurisées, obtenez des certificats et activez le chiffrement TLS sur le Linux VDA et le Delivery Controller (le Controller).

Obtenir des certificats

Procurez-vous des certificats de serveur au format PEM et des certificats racine au format CRT auprès d'une autorité de certification (CA) de confiance. Un certificat de serveur contient les sections suivantes :

- Certificat
- Clé privée non chiffrée
- Certificats intermédiaires (facultatif)

Exemple de certificat de serveur

```
-----BEGIN CERTIFICATE-----

MIIDTCCArAgAwIBAgIJALtuncp1qGXCMAGCSqGSIb3DQEBBQUAMGcxCA3BgNV
BAYTA1VLMRkwEAYDVQIEwTDYwL1cm1kZ2UxEjAQBgNVBACTUNhbwJvdXJzUTEU
MBIGA1UECHMLQ210cm14IFRlc3QxGjAYBgNVBAMTEWnhMDAxLmNpdHJpdGUubmV0
MB4XDTA4MDkzMDEwNTk1M1oXDTI4MDkyNTEwNTk1M1owgYoxCA3BgNVBAYTA1VL
MRkwEAYDVQIEwTDYwL1cm1kZ2UxEjAQBgNVBACTUNhbwJvdXJzUTEUMBIGA1UE
CHMLQ210cm14IFRlc3QxGzA2BgNVBAStE1N1cnZ1c18DZXJ0aWZpY2FOZTEgMB4G
A1UEAXMYZ2EwMDEtc2MwMDEuY210cm10ZS5uZXQwZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALCTT0dxc1vbIOL0F66xg05gkNeIGKVP+37p5KV8B661wCVzr6p9
t72Fa+9oCcF2x/ue274NXFcG4fqGRDsrEwL3yxM6CoYBf7L6psrSCDNnBP1q8TJH
4xoPIXUeaw4MvK/3PvyfHhks4fz8yy1I4vDnXVhwi+OfQ2Bq3NhwsRhnAgMBAAGj
gdwgdKwCQYDVROTBAlwADADBGNVHQ4fGgQURLiDzYot+CUXSh9xHfp1M+/O8yOw
gZkGAlUdIwSBkTCBjOAU85kN1EP30cVhcoss1s1seDQwGSKha6RpMGcxCzA3BgNV
BAYTA1VLMRkwEAYDVQIEwTDYwL1cm1kZ2UxEjAQBgNVBACTUNhbwJvdXJzUTEU
MBIGA1UECHMLQ210cm14IFRlc3QxGjAYBgNVBAMTEWnhMDAxLmNpdHJpdGUubmV0
ggkAy8nC8dc32EwEQYJYIZIAWb4QgEBBAQDAgVgMAOGCSqGSIb3DQEBBQUAA4GB
AD5ax8YHwIxJC3Znt2zdXnbp200yUTowE1Bwqe/9cGaP6CpjoXJ7F3a2/8IpaT68
Ve1Bu1SEY1GKGCcn93pc7SPKqb8pGBRIS/dygb+geFkiQ7Kyvbu0Ijotr3pkx4e
b6CF3tNLudHUwF610rB72zbyz3PiIx+HEnt1j0j8z4K

-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----

MIICXgIBAAKBgqCnk0ncXIr2yNc98eusyYUjDXi811T/t+6U11fAeupvg1c6+q
fBe9HwvvaAnH9s7ntu+DVXXIOH6hkQ7KxMNd2MTGjsgX+y+qbK7AgzWt9avEy
R+MaDyF1Hm1uDFZP9Z1cn4RyrOH8/MstSOFO511R4cPtBUNgatZyCLY2nIDAQAB
AoGBAKwBgZu/bk18edgB8YPYU7d1i8X89I0s4b/apJM+3dmjxb8N96RsPQ24p9Ea
FTUC9+1L8mEroLubSicCXjsjFc+cxg9VvaNa6EEkkBj75oCUERqSx0yb/1Adck/
FXzu0tqtUe/KHgcSgjtjrSeqlJqMm+yxzBAaTVRTTzGdwAhAKEA311KRZjINSuz
Enmi2RTI3ngBhEP/S3GEbvjFksD5n2R190+ooEPxc1vvp5ne8Q0zupshbjFEpbOC
ykZ6UassFw3BAMTI5yPnV9ewPzJoanJZiZCMNXDch51xx1jiyzv+Qmr8RuQz9Pv
fIenmTrfZ+wo4DaKg+8ar20vOnKF0HFAMDECOQDEwR1H6cE3wyCfNu942M9Xkhr
GvSpr7+b///vL6Nwv3CwPV9n8DTPL+wuDKJ29nCVRte1T9M1aMTYjs3a1NvAKEA
qy5JzZcBnryZMbV032jju7ZPISnhTG01xdjzMSLLPtGpNLN34b0k3sTc1r8L42E
uQjTtQrm+wdsrVF31FazkQJANudmsUVv3gZkhWGaV2hzIdXIfhYOIVv+31eZhQY6
h5EmxSZS50TvynGt2e6m2ZgaZmjTagH59TCBHV85nof2g==

-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----

MIIDGTCCAokAgAwIBAgIJAMVjwvHXAd9HMAOGCSqGSIb3DQEBBQUAMGcxCA3BgNV
BAYTA1VLMRkwEAYDVQIEwTDYwL1cm1kZ2UxEjAQBgNVBACTUNhbwJvdXJzUTEU
MBIGA1UECHMLQ210cm14IFRlc3QxGjAYBgNVBAMTEWnhMDAxLmNpdHJpdGUubmV0
MB4XDTA4MDkzMDEwNTk1M1oXDTI4MDkyNTEwNTk1M1owgYoxCA3BgNVBAYTA1VL
EjAQBgNVBAgTCUNhbwJyaWRnZTESMBAGA1UEBxMjQ2Ftcm91cm51MRQwEgYDVQQK
EwtdaXRxYXkgVGZvdDEaMBGA1UEAxMRyY2EwMDEuY210cm10ZS5uZXQwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKVzmF7Uj7u0nvo3Qwdf1Onr3qkNH2DxpwrZ
Zh8cI9Vv+UFRU1C6o87izLtbMFn3FOUP712cfkHN3ZG17pB8pdyjket1Ms1VeJw
acoqrYvD+fNNSvjJuntBaCywvtaLjmfSfHHeZJXV5ckrpEhkn0nkMS16tcrya/K/
oss1Zv3AgMBAAGjgcwgcKwDAYDVROTBAlwAwEB/zAdBgNVHQ4EFgQU85kN1EP3
0cVhcoss1s1seDQwGSIwqZkGAlUdIwSBkTCBjOAU85kN1EP30cVhcoss1s1seDQw
GSKha6RpMGcxCzA3BgNVBAYTA1VLMRkwEAYDVQIEwTDYwL1cm1kZ2UxEjAQBgNV
BACTUNhbwJvdXJzUTEUMBIGA1UECHMLQ210cm14IFRlc3QxGjAYBgNVBAMTEWnh
MDAxLmNpdHJpdGUubmV0ggkAy8nC8dc32EwDQYJKoZIhvcNAQEFBQADgYEAI24Z
gXLXf12RNqh/awtsb44Ug8BZKasg5zhNa1TiXbzz8C13ec53Fb6nigMwc5T1i
UNCLXmXRU1D400tESLX9ACUNH3194yxOgujKS0S8ni21jj2TVfB832Rmr5DBY3g
UmKORn/hdqM1cope5wO6as6+HN4wU0i+hETUMME=

-----END CERTIFICATE-----
```


Activer le chiffrement TLS

Activer le chiffrement TLS sur le Linux VDA Sur Linux VDA, utilisez l'outil `enable_vdassl.sh` pour activer (ou désactiver) le chiffrement TLS. L'outil est situé dans le répertoire `/opt/Citrix/VDA/sbin`. Pour plus d'informations sur les options disponibles dans l'outil, exécutez la commande `/opt/Citrix/VDA/sbin/enable_vdassl.sh -help`.

Conseil : un certificat de serveur doit être installé sur chaque serveur Linux VDA et des certificats racine doivent être installés sur chaque serveur et client Linux VDA.

Activer le chiffrement TLS sur le Controller

Remarque :

Vous pouvez activer le chiffrement TLS uniquement pour les groupes de mise à disposition entiers. Vous ne pouvez pas activer le chiffrement TLS pour des applications spécifiques.

Dans une fenêtre PowerShell sur le Controller, exécutez les commandes suivantes dans l'ordre pour activer le chiffrement TLS pour le groupe de mise à disposition cible.

1. `Add-PSSnapin citrix.*`
2. `Get-BrokerAccessPolicyRule -DesktopGroupName 'GROUPNAME' | Set-BrokerAccessPolicyRule -HdxSslEnabled $true`

Remarque :

Pour vous assurer que seuls les noms de domaine complets VDA sont contenus dans un fichier de session ICA, vous pouvez également exécuter la commande `Set-BrokerSite -DnsResolutionEnabled $true`. La commande active la résolution DNS. Si vous désactivez la résolution DNS, un fichier de session ICA divulgue les adresses IP du VDA et fournit des noms de domaine complets uniquement pour les éléments liés à TLS tels que `SSLProxyHost` et `UDPDTLSPort`.

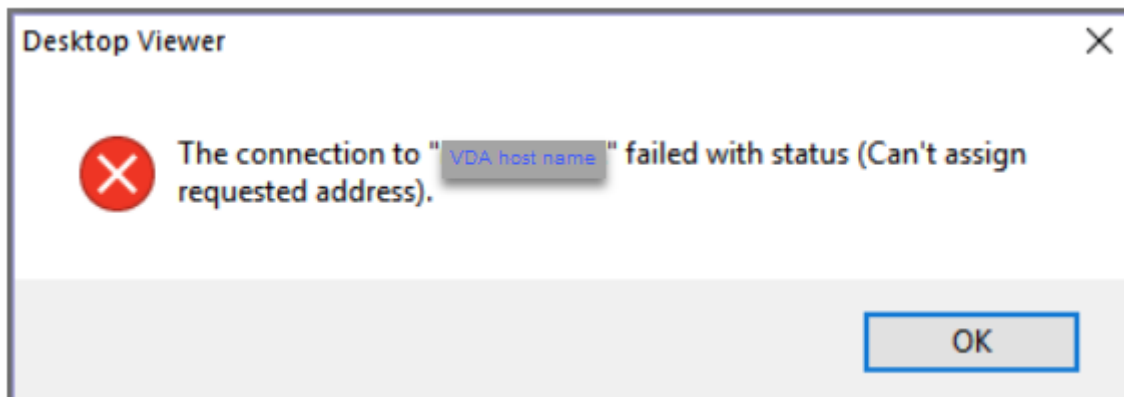
Pour désactiver le chiffrement TLS sur le Controller, exécutez les commandes suivantes dans l'ordre :

1. `Add-PSSnapin citrix.*`
2. `Get-BrokerAccessPolicyRule -DesktopGroupName 'GROUPNAME' | Set-BrokerAccessPolicyRule -HdxSslEnabled $false`
3. `Set-BrokerSite -DnsResolutionEnabled $false`

Résolution des problèmes

Le message d'erreur « Can't assign requested address » (Impossible d'attribuer l'adresse demandée) peut s'afficher dans l'application Citrix Workspace pour Windows lorsque vous tentez d'accéder à une

session de bureau publié :



Pour résoudre ce problème, ajoutez une entrée au fichier **hosts**, comme :

<IP address of the Linux VDA> <FQDN of the Linux VDA>

Sur les machines Windows, le fichier **hosts** est généralement situé dans `C:\Windows\System32\drivers\etc\hosts`.

Sécuriser les sessions utilisateur en utilisant DTLS

November 5, 2021

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` pour activer (ou désactiver) le chiffrement SSL. L'outil se trouve dans `/opt/Citrix/VDA/sbin`. Pour plus d'informations sur les options disponibles dans l'outil, exécutez la commande `/opt/Citrix/VDA/sbin/enable_vdassl.sh -h`.

Remarque :

Le Linux VDA prend actuellement en charge DTLS 1.0 et DTLS 1.2. DTLS 1.2 nécessite Citrix Receiver pour Windows 4.12 ou l'application Citrix Workspace 1808 pour Windows ou version ultérieure. Si votre client prend en charge uniquement DTLS 1.0 (par exemple, Citrix Receiver pour Windows 4.11), définissez `SSLMinVersion` sur `TLS_1.0` et `SSLCipherSuite` sur `COM` ou `ALL` à l'aide de l'outil `enable_vdassl.sh`.

Filigrane de session textuel

November 5, 2021

Filigranes de session textuels pour dissuader et suivre le vol de données. Ces informations traçables apparaissent sur le bureau de la session comme un moyen de dissuasion pour ceux qui utilisent des photographies et des captures d'écran pour voler des données. Vous pouvez spécifier un filigrane ou une couche de texte qui s'affiche sur l'intégralité de l'écran de session sans modifier le contenu du document d'origine.

Important :

Le filigrane de session textuel n'est pas un élément de sécurité. Cette solution n'empêche pas complètement le vol de données, mais elle offre un certain niveau de dissuasion et de traçabilité. Nous ne garantissons pas la traçabilité complète des informations lors de l'utilisation de cette fonctionnalité. Toutefois, nous vous recommandons de combiner cette fonctionnalité avec d'autres solutions de sécurité, le cas échéant.

Le filigrane de session est du texte appliqué à la session délivrée à l'utilisateur. Le filigrane de session contient des informations utilisées pour le suivi du vol de données. La donnée la plus importante est l'identité de l'utilisateur de connexion de la session en cours dans laquelle l'image d'écran a été prise. Pour suivre plus efficacement les fuites de données, incluez d'autres informations telles que l'adresse du protocole Internet du serveur ou du client et une heure de connexion.

Pour ajuster l'expérience utilisateur, utilisez les paramètres de stratégie [Filigrane de session](#) pour configurer l'emplacement et l'apparence du filigrane sur l'écran.

Limitations

- Les filigranes de session ne sont 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).
- Les filigranes ne sont pas visibles 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 les filigranes. Nous vous recommandons de prendre des mesures pour éviter que les captures d'écran ne soient copiées.

Authentification unique avec des cartes à puce

November 15, 2021

Les utilisateurs peuvent utiliser une carte à puce connectée à la machine cliente pour s'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. Les utilisateurs peuvent également utiliser la carte à puce dans la session. Les cas d'utilisation incluent l'ajout d'une signature numérique à un document, le cryptage ou le décryptage d'un e-mail et l'authentification sur un site Web nécessitant l'authentification par carte à puce.

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](#).

La disponibilité de l'authentification pass-through avec des cartes à puce dépend des conditions suivantes :

- Le VDA Linux est installé sur RHEL 7 ou RHEL 8.
- Des cartes à puce prises en charge par OpenSC sont utilisées.
- L'application Citrix Workspace pour Windows est utilisée.

Remarque :

L'utilisation d'une carte à puce mappée dans une session Linux VDA pour se connecter à Citrix Gateway n'est pas officiellement prise en charge.

Prise en charge des cartes à puce sur RHEL 8

L'authentification par carte à puce dépend du module `pam_krb5`, qui est obsolète sur RHEL 8. Pour utiliser l'authentification par carte à puce sur RHEL 8, créez le module `pam_krb5` comme suit :

1. Téléchargez le code source `pam_krb5-2.4.8-6` à partir de https://centos.pkgs.org/7/centos-x86_64/pam_krb5-2.4.8-6.el7.x86_64.rpm.html.

2. Créez et installez le module pam_krb5 sur RHEL 8.

```
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
```

Installer le logiciel Linux VDA sur RHEL 7 et RHEL 8

Installez le logiciel Linux VDA à l'aide du gestionnaire de packages RPM ou de l'installation [easy install](#). Consultez la section [Présentation de l'installation](#).

Une fois l'installation du VDA terminée, vérifiez que le VDA peut s'enregistrer auprès du Delivery Controller et que les sessions de bureau Linux publiées peuvent être lancées avec succès à l'aide de l'authentification par mot de passe.

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 4 est utilisée comme exemple pour illustrer la configuration. YubiKey 4 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 4.



Si votre organisation a besoin d'une autre carte à puce plus avancée, préparez une machine physique avec les packages RHEL 7 ou RHEL 8 et OpenSC installés. 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. Procédez comme suit pour télécharger et installer un certificat racine.

1. Procurez-vous 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>`.

Configurer l'environnement de la carte à puce

Vous pouvez utiliser le script `ctxsmartlogon.sh` pour configurer l'environnement de carte à puce ou effectuer la configuration manuellement.

- Utiliser le script `ctxsmartlogon.sh` pour configurer l'environnement de carte à puce

Remarque :

Le script `ctxsmartlogon.sh` ajoute des informations PKINIT au domaine par défaut. Vous pouvez modifier ce paramètre via le fichier de configuration **/etc/krb5.conf**.

Avant d'utiliser les cartes à puce pour la première fois, exécutez le script `ctxsmartlogon.sh` pour configurer l'environnement de la carte à puce.

```
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.
```

Pour désactiver les cartes à puce :

```
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.
```

- 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 4, consultez l'article [CTX206156](#) du Centre de connaissances.

Avant de passer à l'étape suivante, vérifiez que tous les composants sont correctement configurés, que la clé privée et le certificat utilisateur sont téléchargés sur la carte à puce et que vous pouvez ouvrir une session sur le VDA Windows 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.

```
1 yum install pcsc-lite pcsc-lite-ccid pcsc-lite-libs
```

Installer le pilote de la carte à puce

OpenSC est un pilote de carte à puce largement utilisé sur RHEL. Si OpenSC n'est pas installé, exécutez la commande suivante pour l'installer.

```
1 yum install 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 :

```
1 yum install pam_krb5 krb5-pkinit
```

RHEL 8 :

```
1 yum install krb5-pkinit
```

Le module `pam_krb5` est un module d'authentification enfichable que les applications prenant en charge PAM peuvent utiliser pour vérifier les mots de passe et obtenir des tickets d'octroi de tickets depuis le 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     kdc = KDC.EXAMPLE.COM
4
5     auth_to_local = RULE:[1:$1@$0]
6
7     pkinit_anchors = FILE:<path where you install the root certificate
8                     >/certnew.pem
9
```

```

10     pkinit_kdc_hostname = KDC.EXAMPLE.COM
11
12     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:/usr/lib64/pkcs11/opensc-pkcs11.so
```

Le fichier de configuration ressemble à ce qui suit après les modifications si Winbind 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_options=X509_user_identity=PKCS11:/usr/lib64/pkcs11/libcoolkeypk11.so
auth      sufficient    pam_permit.so
auth      required      pam_deny.so

account    required      pam_unix.so broken_shadow
account    sufficient    pam_localuser.so
account    sufficient    pam_succeed_if.so uid < 1000 quiet
account    [default=bad success=ok user_unknown=ignore] pam_winbind.so
account    [default=bad success=ok auth_err=ignore user_unknown=ignore ignore=ignore] pam_krb5.so
account    required      pam_permit.so

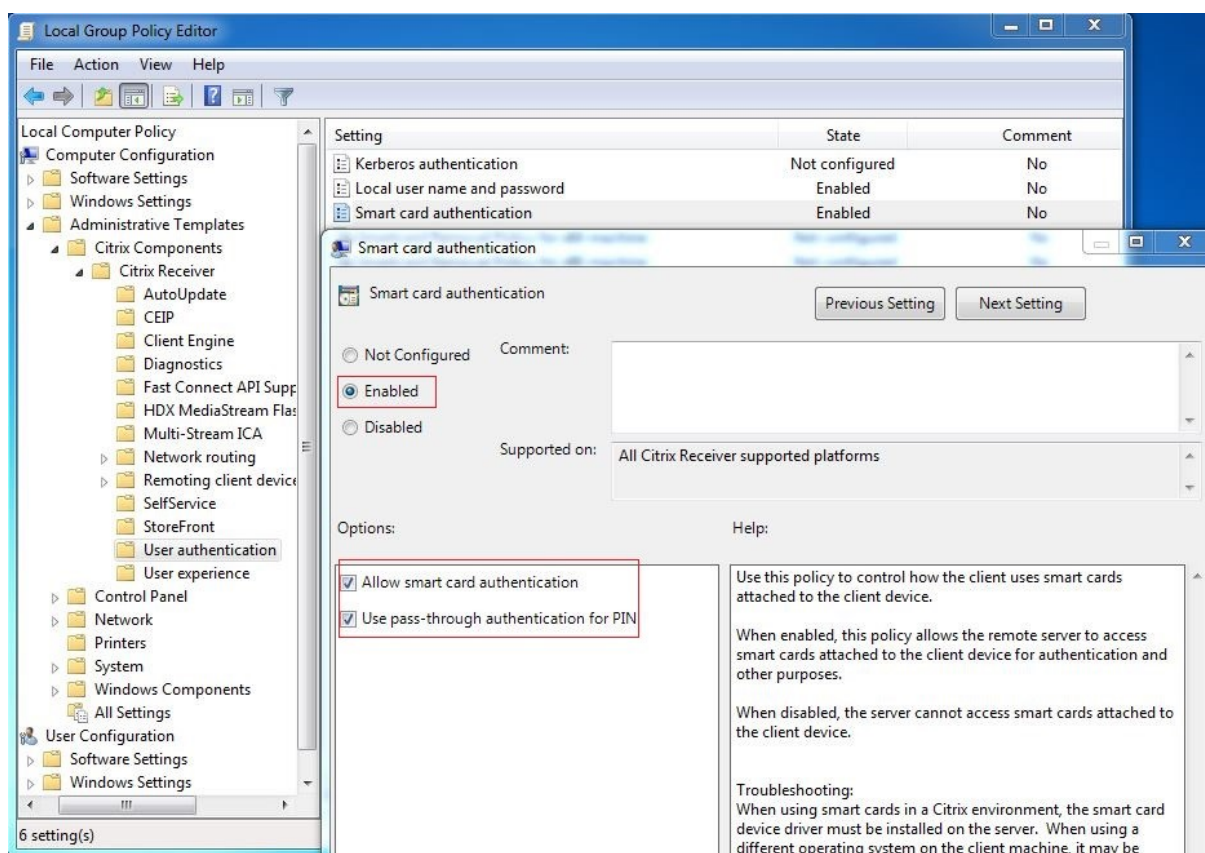
password   required      pam_pkcs11.so

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_winbind.so
session    optional      pam_krb5.so
```

(Facultatif) Single Sign-On avec cartes à puce

Citrix Single Sign-On (SSO) est une fonctionnalité qui implémente l'authentification unique lors du lancement de bureaux virtuels et d'applications. Cette fonctionnalité réduit le nombre de fois que les utilisateurs entrent leur code PIN. Pour utiliser l'authentification SSO avec le Linux VDA, configurez l'application Citrix Workspace. La configuration est la même avec le VDA Windows. Pour plus d'informations, consultez l'article [CTX133982](#) du centre de connaissances.

Activez l'authentification par carte à puce comme suit lors de la configuration de la stratégie de groupe dans l'application Citrix Workspace.



Connexion par carte à puce rapide

La carte à puce rapide constitue une amélioration par rapport à la redirection de carte à puce PC/SC HDX existante. Elle améliore les performances lorsque les cartes à puce sont utilisées dans des environnements WAN à latence élevée. Pour plus d'informations, veuillez consulter la section [Cartes à puce](#).

Le Linux VDA prend en charge les cartes à puce rapides sur les versions suivantes de l'application Citrix Workspace :

- Citrix Receiver pour Windows 4.12
- Application Citrix Workspace 1808 pour Windows et versions ultérieures

Activer une connexion par carte à puce rapide sur le client La connexion par carte à puce rapide est activée par défaut sur le VDA et désactivée par défaut sur le client. Sur le client, pour activer la connexion par carte à puce rapide, incluez le paramètre suivant dans le fichier default.ica du site StoreFront associé :

```
1 [WFClient]
2 SmartCardCryptographicRedirection=On
```

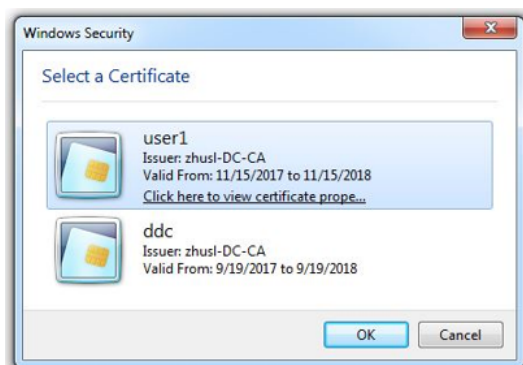
Désactiver une connexion par carte à puce rapide sur le client Pour désactiver la connexion par carte à puce rapide sur le client, supprimez le paramètre **SmartCardCryptographicRedirection** dans le fichier default.ica du site StoreFront associé.

Utilisation

Se connecter au Linux VDA en utilisant une carte à puce

Les utilisateurs peuvent utiliser une carte à puce pour se connecter au Linux VDA dans les scénarios SSO et non SSO.

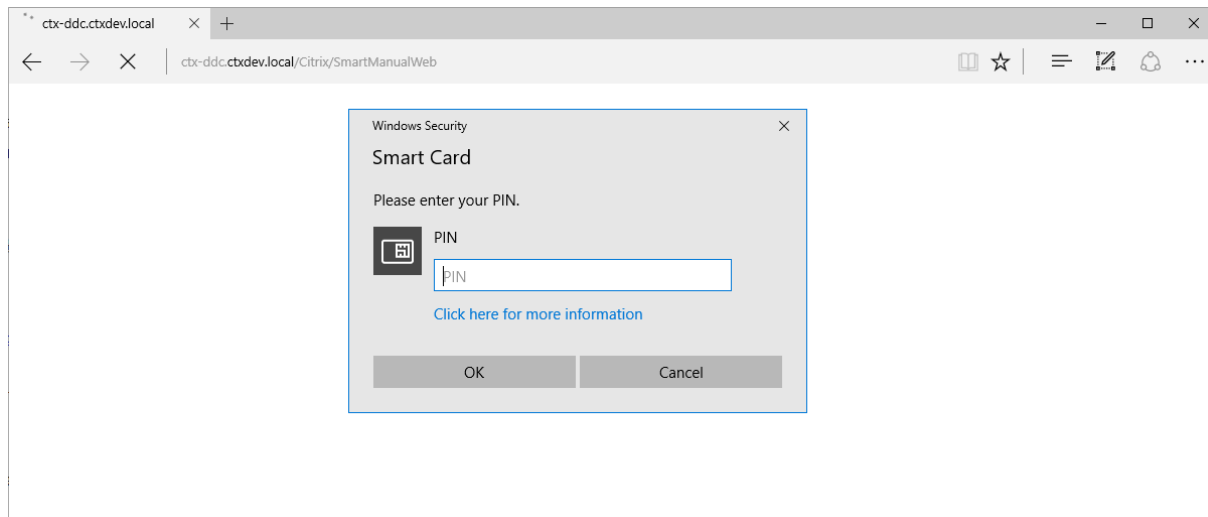
- Dans le scénario SSO, les utilisateurs sont automatiquement connectés à StoreFront avec le certificat et le code PIN de la carte à puce mis en cache. Lorsque les utilisateurs lancent une session de bureau virtuel Linux dans StoreFront, le code PIN est transmis au Linux VDA pour l'authentification par carte à puce.
- Dans le scénario non SSO, les utilisateurs sont invités à sélectionner un certificat et à entrer un code PIN pour se connecter à StoreFront.



Lorsque les utilisateurs lancent 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 les utilisateurs doivent le saisir de nouveau pour l'authentification de connexion.

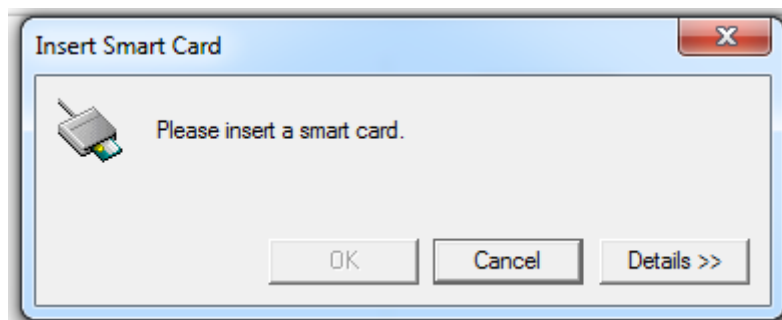
Le comportement est le même avec le VDA Windows.



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 essayez de vous reconnecter à une session, le site Web StoreFront peut afficher une alerte comme suit.



Limitation

Stratégie de retrait de carte à puce

Actuellement, le Linux VDA utilise uniquement le comportement par défaut pour le retrait de la carte à puce. Lorsque vous retirez la carte à puce après vous être connecté au Linux VDA, la session reste

connectée et l'écran de session n'est pas verrouillé.

Prise en charge des autres cartes à puce et de la bibliothèque PKCS#11

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 car Citrix fournit une solution générique de redirection de carte à puce. 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.

Authentification Single Sign-On double-hop

November 5, 2021

La fonctionnalité injecte les informations d'identification utilisateur 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.

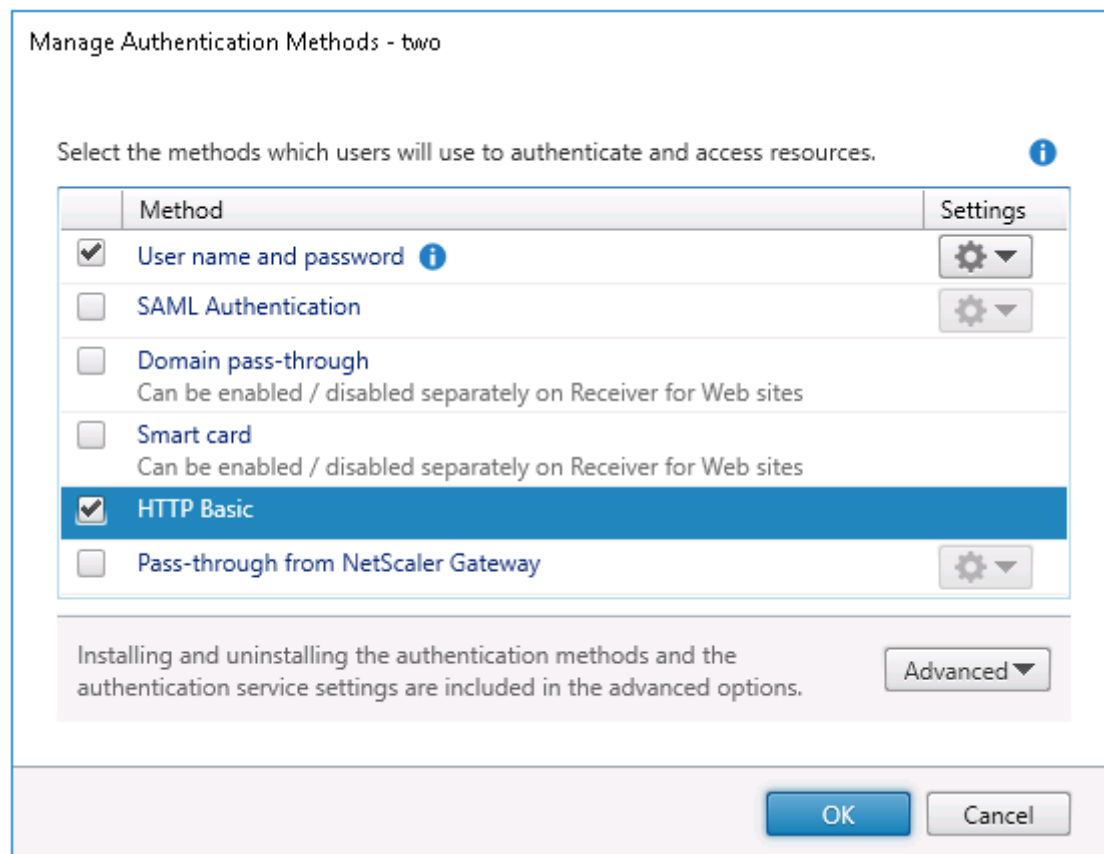
Pour activer la fonctionnalité :

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 :

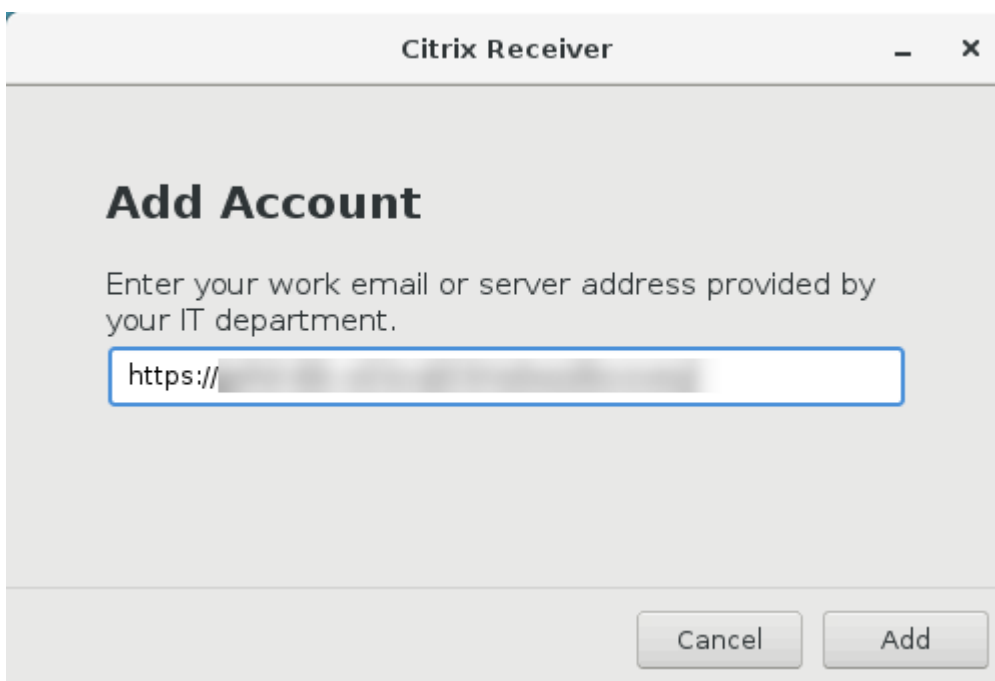
```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
  CurrentControlSet\Control\Citrix" -v "LurSsonEnabled" -d "0
  x00000001"
```

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 entrer un compte de magasin la première fois que vous démarrez l'application Citrix Workspace pour Linux ou Citrix Receiver pour Linux 13.10 dans une session de bureau virtuel Linux. Ensuite, vous serez automatiquement connecté au magasin que vous avez spécifié précédemment.

Remarque :

entrez une URL HTTPS comme compte de magasin.



Configurer des sessions non authentifiées

April 18, 2024

Utilisez les informations de cet article pour configurer des sessions non authentifiées. Aucun paramètre spécial n'est requis lors de l'installation de Linux VDA pour utiliser cette fonctionnalité.

Remarque :

Lorsque vous configurez des sessions non authentifiées, n'oubliez pas que le pré-lancement de session n'est pas pris en charge. Le pré-lancement de session n'est pas non plus pris en charge sur l'application Citrix Workspace pour Android.

Créer un magasin non authentifié

Vous devez [créer un magasin non authentifié](#) à l'aide de StoreFront pour prendre en charge une session non authentifiée sur l'agent Linux VDA.

Autoriser les utilisateurs non authentifiés dans un groupe de mise à disposition

Après la création d'un magasin non authentifié, activez les utilisateurs non authentifiés dans un groupe de mise à disposition pour prendre en charge une session non authentifiée. Pour activer les utilisateurs non authentifiés dans un groupe de mise à disposition, suivez les instructions de la [documentation Citrix Virtual Apps and Desktops](#).

Définir le délai d'inactivité de sessions non authentifiées

Une session non authentifiée a un délai d'inactivité par défaut de 10 minutes. Cette valeur est configurée avec le paramètre de registre **AnonymousUserIdleTime**. Utilisez l'outil **ctxreg** pour modifier cette valeur. Par exemple, pour définir ce paramètre de registre sur cinq minutes, procédez comme suit :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
  CurrentControlSet\Control\Citrix" -v AnonymousUserIdleTime -d 0
  x00000005
```

Définir le nombre maximal d'utilisateurs non authentifiés

Pour définir le nombre maximal d'utilisateurs non authentifiés, utilisez la clé de registre **MaxAnonymousUserNumber**. Ce paramètre limite le nombre de sessions non authentifiées s'exécutant simultanément sur un seul agent Linux VDA. Utilisez l'outil **ctxreg** pour configurer ce paramètre de registre. Par exemple, pour définir la valeur sur 32 bits :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
  CurrentControlSet\Control\Citrix" -v MaxAnonymousUserNumber -d 0
  x00000020
```

Important :

Limitez le nombre de sessions non authentifiées. Le lancement d'un trop grand nombre de sessions simultanées peut entraîner des problèmes sur le VDA, y compris la saturation de la mémoire.

Résolution des problèmes

Tenez compte des éléments suivants lors de la configuration de sessions non authentifiées :

- **Impossible de se connecter à une session non authentifiée.**

Vérifiez que le registre a été mis à jour comme suit (défini sur 0):

```
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/ncsd.conf | grep 'passwd' | grep 'enable-cache'
```

Définissez la variable du cache **passwd** sur **no** s'il est activé, puis redémarrez le service **ncsd**. Vous devrez peut-être réinstaller le Linux VDA après la modification de cette configuration.

- **Le bouton de l'écran de verrouillage est affiché dans une session non authentifiée avec KDE.**

Le bouton et le menu de l'écran de verrouillage sont désactivés par défaut dans une session non authentifiée. Toutefois, ils peuvent toujours être visibles dans KDE. Dans KDE, pour désactiver le bouton et le menu de l'écran de verrouillage pour un utilisateur spécifique, ajoutez les lignes suivantes au fichier de configuration **\$Home/.kde/share/config/kdeglobals**. Par exemple :

```
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](#).

Configurer LDAPS

November 5, 2021

Le protocole LDAPS (LDAP sécurisé) vous permet d'activer le protocole LDAPS (Secure Lightweight Directory Access Protocol) pour vos domaines gérés Active Directory afin de pouvoir utiliser SSL (Secure Socket Layer) ou TLS (Transport Layer Security) pour les communications.

Par défaut, les communications LDAP entre les applications du client et du serveur ne sont pas cryptées. L'utilisation de LDAP en conjonction avec SSL/TLS (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

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 :

LDAP sur SSL/TLS (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](#) sur le site de support de Microsoft.

Lorsque vous disposez d'une hiérarchie d'autorité de certification à plusieurs niveaux (à deux ou trois niveaux par exemple), 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](#) sur le site Microsoft TechNet.

Activer l'autorité de certification racine pour le client

Le client doit utiliser un certificat provenant d'une autorité de certification approuvée par le serveur LDAP. Pour activer l'authentification LDAPS pour le client, importez le certificat d'autorité de certification racine sur le keystore approuvé.

Pour de plus amples informations sur la manière d'exporter l'autorité de certification racine, consultez l'article [Comment faire pour exporter le certificat d'autorité de Certification racine](#) sur le site Web de support de Microsoft.

Activer ou désactiver LDAPS sur le Linux VDA

Pour activer ou désactiver LDAPS sur le Linux VDA, exécutez le script suivant (vous devez être connecté en tant qu'administrateur) :

La syntaxe de cette commande comprend les éléments suivants :

- Activer LDAP sur SSL/TLS avec le certificat d'autorité de certification racine fourni :

```
1 /opt/Citrix/VDA/sbin/enable_ldaps.sh -Enable pathToRootCA
```

- 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. Avant d'activer la liaison de canal, assurez-vous de créer un environnement virtuel Python3. Pour plus d'informations, consultez la section [Créer un environnement virtuel Python3](#).

- Retour à LDAP sans SSL/TLS

```
1 /opt/Citrix/VDA/sbin/enable_ldaps.sh -Disable
```

Le keystore Java dédié à LDAPS se trouve dans **/etc/xdl/.keystore**. Clés de registre affectées :

```
1 HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServers
2
3 HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServersForPolicy
4
5 HKLM\Software\Citrix\VirtualDesktopAgent\UseLDAPS
6
7 HKLM\Software\Policies\Citrix\VirtualDesktopAgent\Keystore
8
9 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 **ldap.conf** dans **/etc/openldap/ldap.conf** et **smb.conf** dans **/etc/samba/smb.conf**. Modifiez les fichiers comme suit :

```
1 ldap.conf:
2
3 TLS_REQCERT never
4
5 smb.conf:
6
7 ldap ssl = start tls
8 ldap ssl ads = yes
9 client ldap sasl wrapping = plain
```

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** :

```
1 smb.conf:
2
3 ldap ssl = off
4 ldap ssl ads = no
5 client ldap sasl wrapping = seal
```

Centrify

Centrify ne prend pas en charge LDAPS sur le port 636. Toutefois, il fournit un cryptage sécurisé sur le port 389. Pour de plus amples informations, consultez le [site Centrify](#).

Quest

Quest Authentication Service ne prend pas en charge LDAPS sur le port 636, mais il offre un cryptage sécurisé sur le port 389 à l'aide d'une autre méthode.

Résolution des problèmes

Les problèmes suivants peuvent se produire lors de l'utilisation de cette fonctionnalité :

- **Disponibilité du service LDAPS**

Vérifiez que la connexion LDAPS est disponible sur le serveur AD/LDAP. Le port par défaut est 636.

- **Échec de l'enregistrement du Linux VDA lorsque LDAPS est activé**

Vérifiez que le serveur LDAP et les ports sont configurés correctement. Vérifiez le certificat d'autorité de certification racine et assurez-vous qu'il correspond au serveur AD/LDAP.

- **Modification incorrecte du registre effectuée accidentellement**

Si les clés liées à LDAPS ont été mises à jour 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.

Créer un environnement virtuel Python3

May 30, 2022

Cet article détaille les conditions préalables et les étapes à suivre pour créer un environnement virtuel Python3 sans connexion réseau. Si vous vous connectez au réseau, vous pouvez également exécuter `ctxsetup.sh` pour créer un environnement virtuel Python3.

Conditions préalables

- Vous devez disposer de privilèges d'administrateur pour accéder au répertoire `/opt/Citrix/VDA/sbin/ctxpython3`.
- Les fichiers wheel des packages Python3 sont installés. Vous pouvez télécharger les fichiers wheel à partir de <https://pypi.org/>.

Créer un environnement virtuel Python3

Procédez comme suit pour créer un environnement virtuel Python3 :

1. Installez les dépendances Python3.

Pour RHEL :

```
1 yum -y install python36-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 Ubuntu, Debian :

```
1 apt-get -y install python3-dev python3-pip python3-venv libkrb5-dev
```

Pour SUSE :

```
1 zypper -i -n install python3-devel python3-setuptools krb5-devel gcc libffi48-devel
```

Remarque :

Vous devrez peut-être activer le référentiel `SUSE_Linux_Enterprise_Software_Development` pour installer certaines dépendances.

2. Créez un environnement virtuel Python3.

Pour RHEL, Ubuntu, Debian :

```
1 sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
```

Pour SUSE :

```
1 sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
2
3 sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
   setuptools==40.6.2
```

3. Installez les dépendances LDAPS.

Pour RHEL, Ubuntu, Debian :


```
1 sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
  cffi == 1.14.2 cryptography == 3.1 decorator == 4.4.2 gssapi
  ==1.6.2 ldap3==2.8.1 netifaces == 0.10.9 pg8000 == 1.17.0
  psutil == 5.8.0 pyasn1 == 0.4.8 pycparser == 2.20 scramp ==
  1.2.0 six == 1.15.0 termcolor == 1.1.0
```

Pour SUSE :

```
1 sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m easy_install
  cffi == 1.14.2 cryptography == 3.1 decorator == 4.4.2 gssapi
  ==1.6.2 ldap3==2.8.1 netifaces == 0.10.9 pg8000 == 1.17.0
  psutil == 5.8.0 pyasn1 == 0.4.8 pycparser == 2.20 scramp ==
  1.2.0 six == 1.15.0 termcolor == 1.1.0
```

4. Installez les dépendances [XDPing](#).

Pour RHEL, Ubuntu, Debian :

```
1 sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
  cffi == 1.14.2 cryptography == 3.1 decorator == 4.4.2 gssapi
  ==1.6.2 ldap3==2.8.1 netifaces == 0.10.9 pg8000 == 1.17.0
  psutil == 5.8.0 pyasn1 == 0.4.8 pycparser == 2.20 scramp ==
  1.2.0 six == 1.15.0 termcolor == 1.1.0
2
3 sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install /
  opt/Citrix/VDA/sbin/ctxpython3/packages/xdping-*.whl
```

Pour SUSE :

```
1 sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m easy_install
  cffi == 1.14.2 cryptography == 3.1 decorator == 4.4.2 gssapi
  ==1.6.2 ldap3==2.8.1 netifaces == 0.10.9 pg8000 == 1.17.0
  psutil == 5.8.0 pyasn1 == 0.4.8 pycparser == 2.20 scramp ==
  1.2.0 six == 1.15.0 termcolor == 1.1.0
2
3 sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m easy_install /
  opt/Citrix/VDA/sbin/ctxpython3/packages/xdping-*.whl
```

XDPing

November 5, 2021

Description

L'outil XDPing Linux est une application basée sur la ligne de commande qui automatise le processus de vérification des problèmes de configuration courants avec un environnement VDA Linux.

L'outil XDPing Linux effectue plus de 150 tests individuels sur le système, qui sont généralement classés comme suit :

- Vérifier si la configuration système du VDA Linux est respectée
- Identifier et afficher les informations de la machine, y compris les distributions Linux
- Vérifier la compatibilité du noyau Linux
- Vérifier les problèmes de distribution Linux connus qui peuvent avoir un impact sur le fonctionnement du VDA Linux
- Vérifier le mode de sécurité Security-Enhanced Linux (SELinux) et sa compatibilité
- Identifier les interfaces réseau et vérifier les paramètres réseau
- Vérifier le partitionnement du stockage et l'espace disque disponible
- Vérifier la configuration du nom d'hôte et du nom de domaine de la machine
- Vérifier la configuration DNS et effectuer des tests de recherche
- Identifier les hyperviseurs sous-jacents et vérifier la configuration de la machine virtuelle. Prise en charge de :
 - Citrix Hypervisor
 - Microsoft HyperV
 - VMware vSphere
- Vérifier les paramètres d'heure et vérifier si la synchronisation de l'heure réseau est opérationnelle
- Vérifier si le service PostgreSQL est correctement configuré et opérationnel
- Vérifier si le pare-feu est activé et si les ports requis sont ouverts
- Vérifier la configuration de Kerberos et effectuer des tests d'authentification
- Vérifier l'environnement de recherche LDAP pour Group Policy Engine Service
- Vérifier si l'intégration Active Directory est correctement configurée et que la machine actuelle est jointe au domaine. Prise en charge de :
 - Samba Winbind
 - Dell Quest Authentication Services
 - Centrify DirectControl
 - SSSD
- Vérifier l'intégrité de l'objet ordinateur Linux dans Active Directory
- Vérifier la configuration du module d'authentification enfichable (PAM)
- Vérifier le modèle de l'image mémoire
- Vérifier si les packages requis par le VDA Linux sont installés
- Identifier le package du VDA Linux et vérifier l'intégrité de l'installation
- Vérifier l'intégrité de la base de données de registre PostgreSQL
- Vérifier si les services du VDA Linux sont correctement configurés et opérationnels
- Vérifier l'intégrité de la configuration VDA et HDX

- Analyser la configuration de chaque Delivery Controller pour vérifier que le Broker Service est accessible, opérationnel et réactif
- Vérifier si la machine est enregistrée auprès de la batterie du Delivery Controller
- Vérifier l'état de chaque session HDX active ou déconnectée
- Analyser les fichiers journaux pour les erreurs et avertissements liés au VDA Linux
- Vérifier si la version de Xorg est adaptée

Utiliser l'outil XDPing Linux

Remarque :

Avant d'utiliser XDPing, assurez-vous de [créer un environnement virtuel Python3](#).

L'outil XDPing est fourni avec l'exécutable unique nommé `xdping` qui est exécuté à partir de l'interface de commande.

Pour afficher les options de ligne de commande, utilisez l'option `--help` :

```
1 sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m xdping --help
```

Pour exécuter la suite complète de tests, exécutez `xdping` sans aucune option de ligne de commande :

```
1 sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m xdping
```

Pour vérifier l'environnement avant d'installer le package du VDA Linux, exécutez les tests `pre-flight` :

```
1 sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m xdping --preflight
```

Pour exécuter uniquement des catégories de test spécifiques, par exemple les tests liés à l'heure et à Kerberos, utilisez l'option `-T` :

```
1 sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m xdping -T time,
  kerberos
```

Pour analyser un contrôleur XenDesktop spécifique :

```
1 sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m xdping -d myddc.
  domain.net
```

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]
```

Configurer Xauthority

November 5, 2021

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 personnel 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.

Résolution des problèmes

Si Xauthority ne fonctionne pas, suivez la procédure de dépannage ci-dessous :

1. En tant qu'administrateur avec privilège root, récupérez tous les cookies Xorg :

```
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 (par exemple, 10.158.11.11) et le numéro d'affichage du bureau publié (par exemple, 160).

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.

Configurer le service d'authentification fédérée

May 3, 2023

Le Linux VDA prend en charge l'utilisation de FAS pour vous connecter à votre environnement Citrix Virtual Apps and Desktops. Il 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.

Configurer FAS sur le Linux VDA

Prise en charge FAS sur RHEL 8/CentOS 8

FAS dépend du module pam_krb5, qui est obsolète sur RHEL 8/CentOS 8. Pour utiliser FAS sur RHEL 8/CentOS 8, créez le module pam_krb5 comme suit :

1. Téléchargez le code source pam_krb5-2.4.8-6 à partir du site Web suivant :

https://centos.pkgs.org/7/centos-x86_64/pam_krb5-2.4.8-6.el7.x86_64.rpm.html.

2. Créez et installez le module pam_krb5 sur RHEL 8/CentOS 8.

```
1 yum install make gcc krb5-devel pam-devel autoconf libtool
2 rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio -div
3 tar xvfz pam_krb5-2.4.8.tar.gz
4 cd pam_krb5-2.4.8
5 ./configure --prefix=/usr
6 make
7 make install
```

3. Vérifiez que pam_krb5.so existe sous /usr/lib64/security/.

```
1 ls -l /usr/lib64/security | grep pam_krb5
```

Définir les serveurs FAS

Dans le cadre d'une nouvelle installation Linux VDA, pour utiliser FAS, tapez le nom de domaine complet de chaque serveur FAS lorsque CTX_XDL_FAS_LIST vous est demandé lors de l'exécution de ctxin-

stall.sh ou de ctxsetup.sh. Comme le Linux VDA ne prend pas en charge la stratégie de groupe AD, vous pouvez fournir une liste de serveurs FAS séparés par des points-virgules. Si une adresse de serveur est supprimée, remplissez son espace vide avec la chaîne de texte **<none>** et ne modifiez pas l'ordre des adresses de serveur.

Pour mettre à niveau une installation Linux VDA existante, vous pouvez réexécuter `ctxsetup.sh` pour définir les serveurs FAS. Vous pouvez également exécuter les commandes suivantes pour définir les serveurs FAS et redémarrer le service `ctxvda` pour que vos paramètres prennent effet.

```
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 service ctxjproxy restart  
4  
5 service ctxvda restart
```

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 service ctxjproxy restart  
4  
5 service ctxvda restart
```

Installation des certificats

Pour la vérification des certificats des utilisateurs, installez le certificat d'autorité de certification racine et tous les certificats intermédiaires sur le VDA. Par exemple, pour installer le certificat d'autorité de certification racine, vous pouvez obtenir le certificat racine AD depuis l'étape précédente **Récupérer le certificat CA à partir de l'autorité de certification Microsoft (sur AD)** ou télécharger son format DER à partir du serveur de l'autorité de certification racine <http://CA-SERVER/certsrv>.

Remarque :

Les commandes suivantes s'appliquent également à la configuration d'un certificat intermédiaire.

Vous pouvez exécuter une commande similaire à la suivante pour convertir un fichier DER (.crt, .cer, .der) en PEM.

```
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, FAS n'a pas l'autorisation de lecture sur le certificat d'autorité de certification racine.

Exécuter ctxfascfg.sh

Exécutez le script ctxfascfg.sh pour configurer les paramètres du service FAS :

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

Deux variables d'environnement sont ajoutées pour pouvoir exécuter **ctxfascfg.sh** en mode silencieux :

- **CTX_FAS_ADINTEGRATIONWAY=winbind | sssd | centrify** : 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.

Choisissez la méthode d'intégration Active Directory correcte, puis tapez le chemin correct des certificats (par exemple, [/etc/pki/CA/certs/](#)).

Le script installe ensuite les packages krb5-pkinit et pam_krb5 et définit les fichiers de configuration pertinents.

Limitation

- FAS prend en charge des plateformes Linux et des méthodes d'intégration AD limitées. Reportez-vous à la matrice suivante :

	Winbind	SSSD	Centrify
RHEL 8.3	Oui	Oui	Oui
RHEL 8.2	Oui	Oui	Oui
RHEL 8.1	Oui	Oui	Oui

	Winbind	SSSD	Centrify
RHEL 7.9	Oui	Oui	Oui
RHEL 7.8	Oui	Oui	Oui
Ubuntu 20.04	Oui	Non	Oui
Ubuntu 18.04	Oui	Non	Oui
Ubuntu 16.04	Oui	Non	Oui
SLES 12.5	Oui	Non	Oui

- FAS ne prend pas encore en charge l'écran de verrouillage. Si vous cliquez sur le bouton de verrouillage dans une session, vous ne pouvez plus vous reconnecter à la session en utilisant FAS.
- Cette version ne prend en charge que les déploiements FAS courants décrits dans l'article [Vue d'ensemble de l'architecture du Service d'authentification fédérée](#), dont **Windows 10 Azure AD Join** est exclu.

Dépannage

Avant de résoudre les problèmes dans FAS, assurez-vous que le Linux VDA est installé et configuré correctement afin qu'une session non FAS puisse être lancée dans le magasin commun en utilisant l'authentification par mot de passe.

Si les sessions non FAS fonctionnent correctement, définissez le niveau de journalisation HDX de la classe **Login** sur VERBOSE et le niveau de journalisation VDA sur TRACE. Pour plus d'informations sur l'activation de la consignation de trace pour Linux VDA, consultez l'article du centre de connaissances [CTX220130](#).

Erreur de configuration du serveur FAS

Le lancement d'une session à partir du magasin FAS échoue.

Vérifiez **/var/log/xdl/hdx.log** et recherchez le journal des erreurs semblable au suivant :

```
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

```

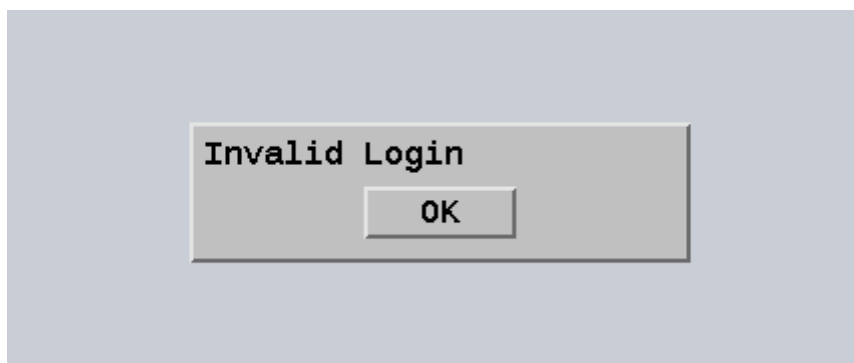
Solution Exécutez la commande suivante pour vérifier que la valeur de Registre Citrix « HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent\Authentication\UserCredentialService » est définie sur <Your-FAS-Server-List>.

```
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 le chemin complet qui stocke le certificat d'autorité de certification racine et tous les certificats intermédiaires est correctement défini dans `/etc/krb5.conf`. Le chemin d'accès complet est similaire au suivant :

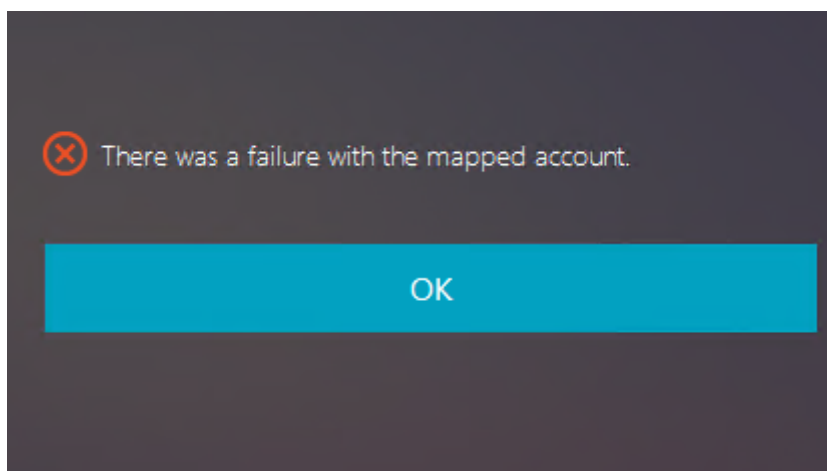
```
1  [realms]
2
3  EXAMPLE.COM = {
4
5
6      .....
7
8      pkinit_anchors = DIR:/etc/pki/CA/certs/
9
10     .....
11
12 }
```

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.

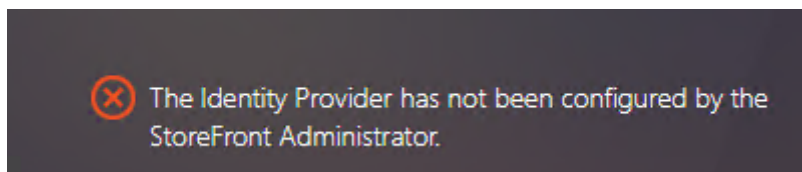


Cette erreur indique que l'utilisateur ADFS a été vérifié, mais qu'aucun utilisateur fictif n'est configuré sur AD.

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 le magasin FAS est configuré pour utiliser l'authentification SAML mais que le déploiement ADFS est manquant.

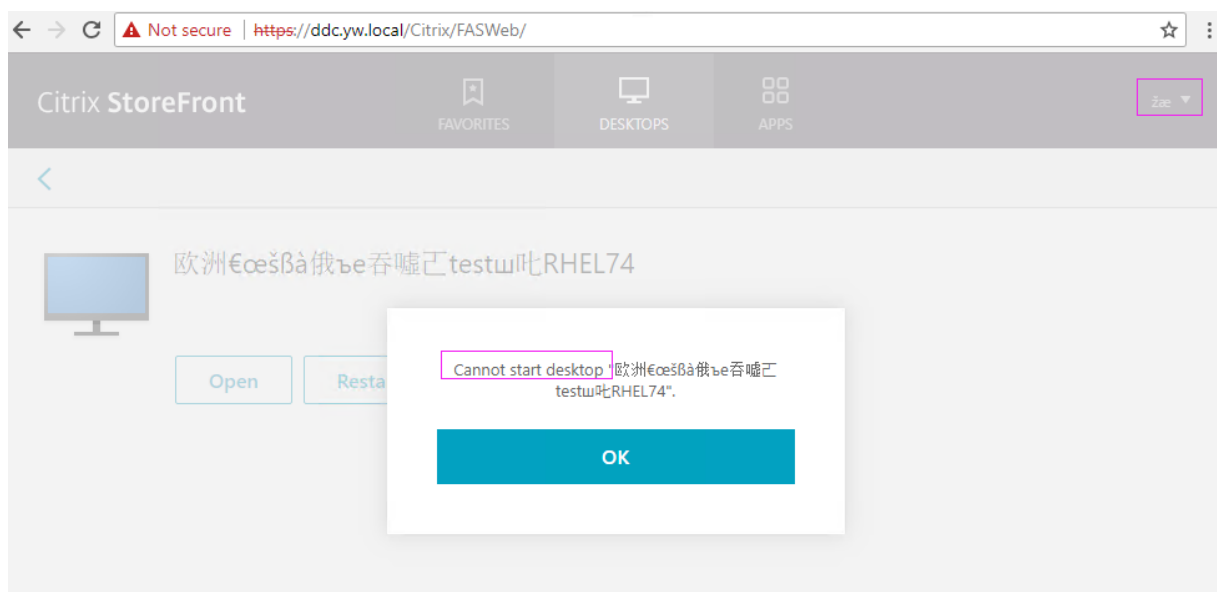
Solution Déployez le fournisseur d'identité ADFS du Service d'authentification fédérée. Pour plus d'informations, consultez la section [Déploiement ADFS du Service d'authentification fédérée](#).

Informations connexes

- Les déploiements FAS courants sont décrits dans l'article [Vue d'ensemble de l'architecture du Service d'authentification fédérée](#).
- Des informations pratiques sont disponibles dans le chapitre [Configuration avancée du Service d'authentification fédérée](#).

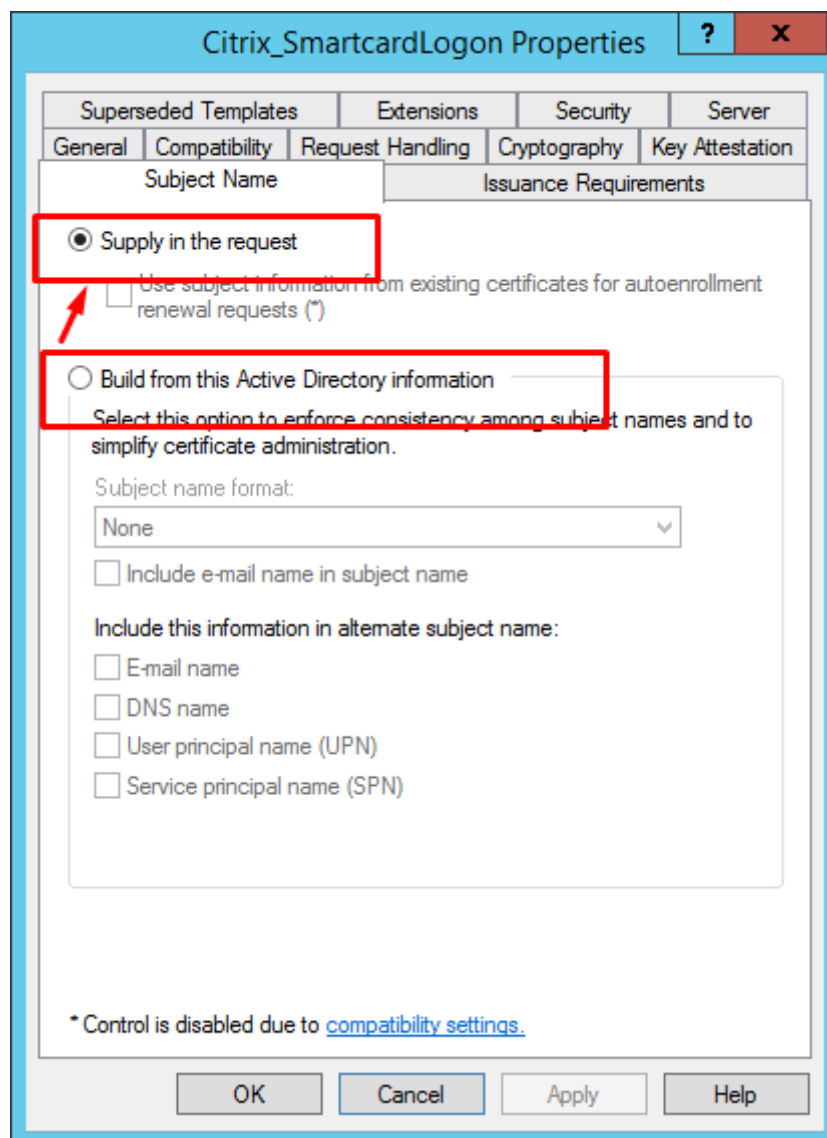
Problème connu

Lorsque FAS est utilisé, la tentative de lancement d'une session de bureau ou d'application publiée avec des caractères non anglais peut 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** :





© 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).