Linux Virtual Delivery Agent 7.15

Contents

Nouveautés

October 6, 2022

Date de publication : 7 juillet 2022

Nouveautés dans 7.15

La mise à jour cumulative 9 (CU9) est la dernière version de Linux VDA 7.15 LTSR. La mise à jour cumulative CU9 ajoute un correctif par rapport au Linux VDA 7.15 CU8.

Impression PDF

Préalablement disponible en tant que fonctionnalité expérimentale, l'impression PDF est une fonctionnalité entièrement prise en charge dans cette version. Elle permet aux utilisateurs de Citrix Receiver pour Chrome et HTML5 d'imprimer des PDF convertis depuis leurs sessions VDA Linux.

Changement du comportement du système

À partir de cette version, vous n'avez pas besoin d'exécuter le script ctxsetup.sh après la mise à niveau de votre VDA Linux.

Problèmes résolus

August 8, 2022

Problèmes résolus dans CU9

- La désinstallation des VDA Linux sur SUSE ou RHEL peut ne pas supprimer les dossiers vides de l'emplacement /opt/Citrix/. [CVADHELP-18241]

Problèmes résolus dans CU8

- Lorsque la liaison de canal est activée, les tentatives d'enregistrement d'un Linux VDA auprès du Delivery Controller peuvent échouer. [CVADHELP-14481]

Problèmes résolus dans CU6

- Une session sur une machine Linux risque de ne plus répondre si la souris et le clavier ne sont pas focalisés sur la même fenêtre ou si la souris ne parvient pas à changer de focus. [CVADHELP-12768]
- Les tentatives de redirection générique d'un lecteur USB amovible vers un VDA Linux peuvent échouer. Le problème se produit lorsque le lecteur USB est formaté NTFS (New Technology File System). [CVADHELP-13675]
- Les VDA Linux peuvent ne pas atteindre les débits d'images par seconde comme spécifié dans le paramètre **Taux de trames cible** (FramesPerSecond). Le problème se produit lorsqu'un GPU est installé sur un VDA Linux. [CVADHELP-14267]

Problèmes résolus dans CU5

- Les tentatives de copier-coller du contenu entre un client et une session à l'aide de la fonctionnalité Presse-papiers peuvent échouer. [LD2047]
- Lorsque vous lancez une session sur un VDA Linux et effectuez une action, la session peut se déconnecter. [LD2257]

Problèmes résolus dans CU4

- Lorsque vous tentez de copier du contenu à partir d'un point de terminaison et de le coller dans une application qui s'exécute sur un VDA Linux, le contenu peut ne pas être copié. [LC8760]
- Le clavier peut ne pas fonctionner sur SUSE Linux Enterprise Server 11 Service Pack 4. Par conséquent, les frappes ne sont pas affichées à l'écran et la disposition du clavier n'est pas définie correctement. [LC9906]
- Le processus **ctxctl** peut échouer dans une session utilisateur sur un VDA Linux. [LD0353]

Problèmes résolus dans CU3

- Le VDA Linux peut ne pas appliquer les stratégies Citrix. Le problème se produit lorsque vous configurez une stratégie pour utiliser le type de connexion d'élément Access Control avec NetScaler Gateway. [LC9842]

Problèmes résolus dans CU2

- L'enregistrement d'un VDA Linux à l'aide du Delivery Controller peut échouer par intermittence. [LC7982]

- Citrix Director 7.13 qui s'exécute sur un serveur Red Hat Enterprise Linux 7.3 peut ne pas afficher les détails de la session de la machine. Le message d'erreur suivant s'affiche :

  Impossible de récupérer les données. [LC8204]

- Un VDA Linux peut s'enregistrer auprès du Delivery Controller et annuler l'enregistrement après un certain temps. [LC8205]
- Certaines applications tierces utilisées pour vérifier l'affichage de la session d'un VDA Linux peuvent ne pas afficher tous les pixels. [LC8419]
- Lorsqu'il existe plusieurs serveurs LDAP, les tentatives de lancement d'une application sur un VDA Linux peuvent échouer après la mise à jour des stratégies et l'expiration d'une session. [LC8444]
- Le processus ctxhdx peut se fermer de manière inattendue avec une erreur **segfault** lorsque la session est connectée à un VDA Linux. [LC8611]
- Lorsque vous utilisez la version Linux VDA 7.16 Early Access, l'agent Broker peut ne pas obtenir le nom de l'application. Cet échec oblige Director à afficher l'erreur **Agent requis**, après quoi le réenregistrement commence. [LC9243]

Problèmes résolus dans CU1

- Un VDA Linux peut s'enregistrer auprès du Delivery Controller et annuler l'enregistrement après un certain temps. [LC8205]
- Certaines applications tierces utilisées pour vérifier l'affichage de la session d'un VDA Linux peuvent ne pas afficher tous les pixels. [LC8419]
- Lorsqu'il existe plusieurs serveurs LDAP, les tentatives de lancement d'une application sur un VDA Linux peuvent échouer après la mise à jour des stratégies et l'expiration d'une session. [LC8444]

Problèmes résolus dans 7.15 LTSR

Les problèmes suivants ont été résolus dans cette version du VDA Linux :

- Easy Install peut entraîner la déconnexion du réseau du VDA Linux lorsque vous entrez l'adresse IP DNS. [LNXVDA-2152]
- Lors de la lecture d'une vidéo, l'itinérance de session de Citrix Receiver pour Windows vers Citrix Receiver pour Android échoue. [LNXVDA-2164]

Problèmes connus

August 8, 2022

Les problèmes suivants ont été identifiés dans cette version :

- Citrix Scout intégré à XenApp et XenDesktop 7.15 LTSR CU6 ne peut pas collecter les journaux du VDA Linux 7.15. Le VDA Linux 7.15 ne prend pas en charge Citrix Telemetry Service que Citrix Scout utilise pour collecter les journaux.
- 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 Citrix Receiver 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 Citrix Receiver 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 VDA Linux à l'aide de Citrix Receiver pour Mac. Citrix Receiver pour Mac envoie AltGr pour les touches Options/Alt droite et gauche par défaut. Vous pouvez modifier ce comportement dans les paramètres de Citrix Receiver, mais les résultats varient selon les applications .
- L'enregistrement échoue lorsque le Linux VDA est à nouveau associé au domaine. Cette nouvelle association génère un nouvel ensemble de clés Kerberos. Le broker peut utiliser un ticket de service VDA mis en cache obsolète basé sur le jeu de clés Kerberos précédent. Lorsque le VDA tente de se connecter au broker, le broker peut ne pas être en mesure d'établir un contexte de sécurité pour le VDA. Le symptôme courant est l'échec de l'enregistrement du VDA.

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

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

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

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.
- Citrix Receiver pour Windows peut rencontrer une distorsion audio lors de l'enregistrement audio.

Avis de tiers

December 9, 2022

Linux Virtual Desktop version 7.15 (PDF)

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

Configuration système requise

November 5, 2021

Distributions Linux

Linux VDA prend en charge les distributions Linux suivantes :

- SUSE Linux Enterprise :
  - Desktop 12 Service Pack 2

  - Server 12 Service Pack 2
  - Server 11 Service Pack 4

- Red Hat Enterprise Linux
  - Workstation 7.3
  - Workstation 6.9
  - Workstation 6.6
  - Server 7.3
  - Server 6.9
  - Server 6.6

- CentOS Linux
  - CentOS 7.3
  - CentOS 6.6

- Ubuntu Linux
  - Ubuntu Desktop 16.04 (avec le noyau 4.4.x)
  - Ubuntu Server 16.04 (avec le noyau 4.4.x)

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 7.3, CentOS 7.3	1.17
RHEL 6.9	1.17
RHEL 6.6, CentOS 6.6	1.15
Ubuntu 16.04	1.18
SUSE 12.2	1.18
SUSE 11.4	1.6.5

N'utilisez pas le serveur HWE Xorg 1.19 sur Ubuntu 16.04.

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, RHEL et CentOS. Le bureau Unity est uniquement pris en charge sur Ubuntu. Au moins un bureau doit être installé.

XenDesktop

Linux VDA est compatible avec toutes les versions de XenDesktop actuellement prises en charge. Pour de plus amples informations sur le cycle de vie de XenDesktop 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.

> **Remarque :**
>
> le VDA Linux n'est pas compatible avec la version XenDesktop 7.0 ou une version antérieure.

Citrix Receiver

Les versions suivantes de Citrix Receiver sont prises en charge :

- Citrix Receiver pour la plateforme Windows universelle (UWP) version 1.0
- Citrix Receiver pour Windows version 4.8 ou ultérieure
- Citrix Receiver pour Linux version 13.5
- Citrix Receiver pour Mac OSX version 12.6
- Citrix Receiver pour Android version 3.11
- Citrix Receiver pour iOS version 7.2
- Citrix Receiver pour Chrome version 2.5
- Citrix Receiver pour HTML5 version 2.5 (uniquement via Access Gateway)

Hyperviseurs

Les hyperviseurs suivants sont pris en charge pour l'hébergement des VM invité de VDA Linux :

- XenServer
- VMware ESX et ESXi
- Microsoft Hyper-V
- Nutanix AHV

L'hébergement de bare metal est également pris en charge.

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

Packages d'intégration d'Active Directory

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

- Samba Winbind
- Quest Authentication Services v4.1 ou version ultérieure
- Centrify DirectControl
- SSSD

> **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, distributions Linux et processeurs graphiques NVIDIA GRID™ suivants sont requis pour la prise en charge de HDX 3D Pro.

Hyperviseurs

Les hyperviseurs suivants sont pris en charge :

- XenServer
- VMware ESX et ESXi
- Nutanix AHV

Distributions Linux

Les distributions Linux suivantes prennent en charge HDX 3D Pro :

- Red Hat Enterprise Linux - Workstation 7.3
- Red Hat Enterprise Linux - Server 7.3
- Red Hat Enterprise Linux - Workstation 6.9
- Red Hat Enterprise Linux - Server 6.9
- Red Hat Enterprise Linux - Workstation 6.6

- Red Hat Enterprise Linux - Server 6.6
- SUSE Linux Enterprise Desktop 12 Service Pack 2
- SUSE Linux Enterprise Server 12 Service Pack 2
- Ubuntu Linux Desktop 16.04
- Ubuntu Linux Server 16.04

Processeur graphique

Les processeurs graphiques (GPU) suivants sont pris en charge pour la fonctionnalité GPU pass-through :

- NVIDI GTX750Ti
- NVIDIA GRID - Tesla M60
- NVIDIA GRID - K2

Les processeurs graphiques suivants sont pris en charge pour la fonctionnalité vGPU :

- NVIDIA GRID - Tesla M60
- NVIDIA GRID - Tesla M10

Présentation de l'installation

August 10, 2021

L'installation du Virtual Delivery Agent (VDA) Linux suit les mêmes étapes que pour toutes les distributions Linux prises en charge.

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 XenApp ou XenDesktop.
7. Créez le groupe de mise à disposition dans XenApp ou XenDesktop.

Les variantes et commandes spécifiques sont documentées par la distribution.

Configurer Delivery Controller

May 11, 2020

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 : Hotfix Update 2 - pour Delivery Controller 7.6 (32 bits) –Anglais
- CTX142439 : Hotfix Update 2 - pour Delivery Controller 7.6 (64 bits) –Anglais

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

- citrix-linuxvda-scripts.zip

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

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

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

> **Conseil :**
>
> par défaut, PowerShell est configuré pour empêcher l'exécution des scripts PowerShell. Si le script ne réussit pas à s'exécuter, modifiez la stratégie d'exécution PowerShell avant d'essayer à nouveau :
>
> ```
> Set-ExecutionPolicy Unrestricted
> ```

Le script **Update-BrokerServiceConfig.ps1** met à jour le fichier de configuration du Broker Service en utilisant de nouveaux points de terminaison WCF requis par le Linux VDA et redémarre le Broker Service. Le script détermine automatiquement l'emplacement du fichier de configuration du Broker

Service. Une copie de sauvegarde du fichier de configuration d'origine est créée dans le même répertoire avec l'extension **.prelinux** ajoutée au nom du fichier.

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

Vérifier la configuration d'un Delivery Controller

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

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

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

Easy Install

June 17, 2022

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

Distributions prises en charge

	Winbind	SSSD	Centrify
RHEL 7.3	Oui	Oui	Oui
RHEL 6.9	Oui	Oui	Oui
RHEL 6.6	Oui	Oui	Oui
CentOS 7.3	Oui	Oui	Oui
Ubuntu 16.04	Oui	Oui	Oui
SUSE 12.2	Oui	Non	Oui

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 au site Web Citrix et téléchargez le package Linux VDA en fonction de la distribution Linux appropriée.
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.

Étape 2 : installer le package Linux VDA

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

Pour les distributions RHEL et CentOS :

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

Pour les distributions Ubuntu :

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

Pour les distributions SUSE :

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


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

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

Mode interactif :

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

```
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-ntps : adresse IP ou nom de chaîne du serveur NTP.
- **CTX_EASYINSTALL_DOMAIN**=domain-name : nom NetBIOS du domaine.
- **CTX_EASYINSTALL_REALM**=realm-name : nom de la zone Kerberos.
- **CTX_EASYINSTALL_FQDN**=ad-fqdn-name
- **CTX_EASYINSTALL_ADINTEGRATIONWAY**=winbind | sssd | centrify : 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.

Les variables suivantes sont utilisées par ctxsetup.sh :

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N** : le Linux VDA prend en charge la spécification d'un nom de Delivery Controller à l'aide d'un enregistrement DNS CNAME.
- **CTX_XDL_DDC_LIST**=list-ddc-fqdns : le Linux VDA requiert une liste séparée par des espaces de noms de domaines complets de Delivery Controller. Cette dernière sera utilisée pour l'enregistrement auprès d'un Delivery Controller. Au moins un nom de domaine complet (FQDN) ou CNAME doit être spécifié.
- **CTX_XDL_VDA_PORT**=port-number : le Linux VDA communique avec les Delivery Controller via un port TCP/IP.
- **CTX_XDL_REGISTER_SERVICE=Y | N** : les services Linux Virtual Desktop sont lancés après le démarrage de la machine.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** : les services Linux 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.

- **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 port 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_START_SERVICE=Y | N** : indique si les services Linux VDA sont démarrés lorsque la configuration est terminée.

Si aucun paramètre n'est défini, l'installation retourne en mode interactif et l'utilisateur est invité à intervenir. Le script ctxinstall.sh ne demande aucune réponse à condition que tous les paramètres soient déjà fournis par des variables d'environnement.

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

```
export CTX_EASYINSTALL_HOSTNAME=host-name

export CTX_EASYINSTALL_DNS=ip-address-of-dns

export CTX_EASYINSTALL_NTPS=address-of-ntps

export CTX_EASYINSTALL_DOMAIN=domain-name

export CTX_EASYINSTALL_REALM=realm-name

export CTX_EASYINSTALL_FQDN=ad-fqdn-name

```



```
export CTX_EASYINSTALL_ADINTEGRATIONWAY=winbind | sssd | centrify

export CTX_EASYINSTALL_USERNAME=domain-user-name

export CTX_EASYINSTALL_PASSWORD=password

export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N

export CTX_XDL_DDC_LIST=list-ddc-fqdns

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y | N

export CTX_XDL_ADD_FIREWALL_RULES=Y | N

export CTX_XDL_HDX_3D_PRO=Y | N

export CTX_XDL_VDI_MODE=Y | N

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

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

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

export CTX_XDL_START_SERVICE=Y | N

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. Citrix vous recommande de créer un fichier de script shell à partir des commandes précédentes avec **#!/bin/bash** en tant que première ligne.

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

```
sudo CTX_EASYINSTALL_HOSTNAME=host-name \

CTX_EASYINSTALL_DNS=ip-address-of-dns \

CTX_EASYINSTALL_NTPS=address-of-ntps \

CTX_EASYINSTALL_DOMAIN=domain-name \

CTX_EASYINSTALL_REALM=realm-name \

......

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_START_SERVICE=Y \

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


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.

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

- Pour Centrify sur CentOS, Easy Install peut échouer au niveau de `adcheck`, l'outil de vérification de l'environnement Centrify, et signale l'erreur suivante :

  Journal :

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

  Ce problème est dû à la configuration spéciale de Centrify. Procédez comme suit pour résoudre ce problème :

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

- Si vous choisissez Centrify comme méthode pour rejoindre un domaine, le script ctxinstall.sh a besoin du package Centrify. Il existe deux façons pour ctxinstall.sh d'obtenir le package Centrify :

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

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

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

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

    Ubuntu : wget http://edge.centrify.com/products/centrify-suite/2016-update-1/installers/centrify-suite-2016.1-deb7-x86_64.tgz?_ga=1.178323680.558673738.1478847956

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

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

  Par exemple :

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

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 :

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

/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 avec OS de serveur 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 du répertoire de base manquant

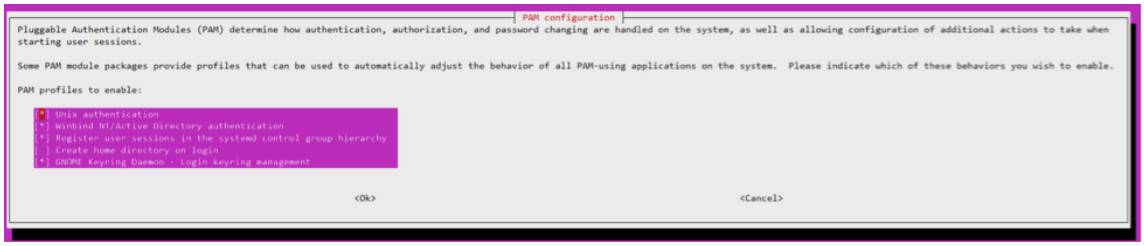
/var/log/xdl/hdx.log:

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

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

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

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

> **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 fenêtre contextuelle qui s'affiche, vérifiez que **Create home directory login** est sélectionné.



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

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

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

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

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

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

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

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

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

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

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

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

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

Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: [pulseaudio] core-
```



```
    util.c: Failed to connect to system bus: Did not receive a reply.
    Possible causes include: the remote application did not send a reply
    , the message bus security policy blocked the reply, the reply
    timeout expired, or the network connection was broken.

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

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

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

SELinux empêche SSHD d'accéder au répertoire de base

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

/var/log/ctxinstall.log :

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

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

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

If you want to allow polyinstantiation to enabled

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

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

    Do

       setsebool -P polyinstantiation_enabled 1

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

```



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

Then you should report this as a bug.

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

      Do

       allow this access for now by executing:

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

# semodule -i mypol.pp
```

Pour résoudre ce problème :

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

   SELINUX=disabled

2. Redémarrez le VDA.

Installer Linux Virtual Delivery Agent pour RHEL/CentOS

August 20, 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 7/CentOS 7, RHEL 6/CentOS 6 pour l'installation sur un VDA

Étape 1a : vérifier la configuration réseau

Citrix recommande que le réseau soit connecté et correctement configuré avant de continuer.

Étape 1b : définir le nom d'hôte

> **Remarque :**
>
> le VDA Linux 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.

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=`**hostname**

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

> **Remarque :**
>
> le VDA Linux 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.

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.

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

Étape 1d : vérifier le nom d'hôte

Vérifiez que le nom d'hôte est correctement configuré :

```
hostname
```

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

Vérifiez que le nom de domaine complet est correctement configuré :

```
hostname -f
```

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

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

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

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

ping delivery-controller-fqdn
```

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.

RHEL 6.x et versions antérieures utilisent le démon NTP (`ntpd`) pour la synchronisation d'horloge, tandis qu'un environnement RHEL 7.x par défaut utilise le démon Chrony le plus récent (`chronyd`). Le processus de configuration et de fonctionnement entre les deux services est similaire.

Configurer le service NTP (RHEL 6/CentOS 6 uniquement) En tant qu'utilisateur racine, modifiez **/etc/ntp.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 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 NTP :

```
sudo /sbin/service ntpd restart
```


Configurer le service NTP (RHEL 7/CentOS 7 uniquement) En tant qu'utilisateur racine, modifiez **/etc/chrony.conf** et ajoutez une entrée de serveur pour chaque serveur de temps distant :

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

server peer2-fqdn-or-ip-address iburst
```

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

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

Enregistrez les modifications et redémarrez le démon Chrony :

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

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 :

- RHEL 7/CentOS 7 :

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

- RHEL 6/CentOS 6 :

```
sudo yum info java-1.7.0-openjdk
```

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

- RHEL 7/CentOS 7 :

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

- RHEL 6/CentOS 6 :

```
sudo yum -y update java-1.7.0-openjdk
```

Définissez la variable d'environnement **JAVA_HOME** en ajoutant la ligne suivante au fichier **~/.bashrc** :

```
export JAVA\\_HOME=/usr/lib/jvm/java
```


Ouvrez un nouveau shell et vérifiez la version de Java :

```
1 java -version
```

> **Conseils :**
>
> pour éviter les problèmes, assurez-vous que vous avez installé uniquement OpenJDK version 1.7.0 ou 1.8.0 pour RHEL 6/CentOS 6 ou uniquement OpenJDK version 1.8.0 pour RHEL 7/CentOS 7. Supprimez toutes les autres versions de Java de votre système.

Étape 1h : installer PostgreSQL

Linux VDA requiert PostgreSQL 8.4 ou version ultérieure sur RHEL 6 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 8 et PostgreSQL 9 :

- RHEL 7 uniquement : PostgreSQL 9

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

- RHEL 6 uniquement : PostgreSQL 8

```
1 sudo /sbin/service postgresql initdb
```

Étape 1i : démarrer PostgreSQL

Une fois la machine démarrée, démarrez le service immédiatement :

- RHEL 7 uniquement : PostgreSQL 9

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

- RHEL 6 uniquement : PostgreSQL 8


```
sudo /sbin/chkconfig postgresql on

sudo /sbin/service postgresql start
```

Vérifiez la version de PostgreSQL avec :

```
psql --version
```

Vérifiez que le répertoire de données est défini à l'aide de l'utilitaire de ligne de commande **psql** :

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

> **Important :**
>
> dans cette version, une nouvelle dépendance pour gperftools-libs a été ajoutée, mais elle n'existe pas dans le référentiel d'origine. Ajoutez un nouveau référentiel à l'aide de la commande `sudo rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-6.noarch.rpm`.
> Seul RHEL 6/CentOS 6 est affecté. Exécutez la commande suivante avant l'installation du package Linux VDA.

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 XenServer

Si la fonctionnalité de synchronisation de l'heure de XenServer est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée car XenServer et NTP 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 XenServer Tools installé, vous pouvez vérifier si la fonctionnalité de synchronisation de l'heure de XenServer est présente et activée à partir de la VM Linux :

```
su -
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/indepent_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 :

```
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 :

```
su -

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 XenServer et VMware, pour lesquels la synchronisation de l'heure est désactivée afin d'éviter tout conflit avec NTP. La synchronisation de l'heure Hyper-V peut coexister 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 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 VDA Linux et le compte dans AD.

Samba Winbind

Installez ou mettez à jour les packages requis :

```
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 :

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


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

```
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.

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
```

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 :

```
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 l'agent Linux VDA, vérifiez que le fichier keytab système a été créé et contient des clés valides :

```
1 sudo klist -ke
```

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

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

Les noms de machine et de domaine doivent être spécifiés en majuscules. Le signe dollar ($) doit être placé dans une séquence d'échappement avec une barre oblique inversée (\) pour empêcher le remplacement shell. Dans certains environnements, le nom de domaine DNS est différent du nom

de domaine Kerberos. Assurez-vous que le nom de domaine est utilisé. Si cette commande réussit, aucun résultat n'est affiché.

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

```
sudo klist
```

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

```
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 :

```
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 à l'aide d'un compte d'utilisateur de domaine sur le VDA Linux. Le compte d'utilisateur de domaine n'a pas été utilisé auparavant.

```
ssh localhost -l domain\username

id -u
```

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

```
klist
```

Quittez la session :

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

Configurer Quest sur un Linux VDA

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

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

```
SELINUX=permissive
```

Cette modification nécessite le redémarrage de la machine :

```
reboot
```

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

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

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

sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-auth false
```


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

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

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

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

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

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

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 :

```
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, utilisez un compte d'utilisateur de domaine pour vous connecter au VDA Linux. Le compte d'utilisateur de domaine n'a pas été utilisé auparavant.

```
ssh localhost -l domain\username

id -u
```


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

```
ls /tmp/krb5cc_uid
```

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

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

Quittez la session :

```
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` :

```
su -
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 :

```
su -

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 :

```
adinfo --sysinfo all

adinfo -diag
```


Testez la connectivité avec les différents services Active Directory et Kerberos. Passez à l'étape 4 : installer le Linux VDA après vérification de la jonction du domaine.

```
adinfo --test
```

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 avec Samba
2. Configurer SSSD
3. Configurer NSS/PAM
4. Vérifier la configuration de Kerberos
5. Vérifier l'authentification utilisateur

Logiciel requis Le fournisseur Active Directory a été introduit avec SSSD version 1.9.0. Si vous utilisez une version antérieure, suivez les instructions fournies dans la section Configuration du fournisseur LDAP avec Active Directory.

Les environnements suivants ont été testés et vérifiés lors de l'utilisation des instructions figurant dans cet article :

- RHEL 7.3 ou version ultérieure/CentOS 7.3 ou version ultérieure
- Version 1.3 ou ultérieure du VDA Linux

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. Vous pouvez utiliser `adcli`, `realmd`, `Winbind` ou `Samba` à la place.

Les informations contenues dans cette section décrivent l'approche `Samba` uniquement. Pour `realmd`, reportez-vous à la documentation de RHEL ou CentOS. Ces étapes doivent être suivies avant la configuration de SSSD.

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 :


```
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.

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
```

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

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

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 Linux VDA.
- Apportez des modifications de configuration à plusieurs fichiers (par exemple, sssd.conf).
- Démarrez le service **sssd**.

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

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

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

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

```



```
16 # Should be specified as the lower-case version of the long version of
      the Active Directory domain.
17 ad_domain = ad.example.com
18
19 # Kerberos settings
20 krb5_ccachedir = /tmp
21 krb5_ccname_template = FILE:%d/krb5cc_%U
22
23 # Uncomment if service discovery is not working
24 # ad_server = server.ad.example.com
25
26 # Comment out if the users have the shell and home dir set on the AD
      side
27 default_shell = /bin/bash
28 fallback_homedir = /home/%d/%u
29
30 # Uncomment and adjust if the default principal SHORTNAME$@REALM is not
       available
31 # ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
```

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

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

```
chown root:root /etc/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 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 :


```
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 :

```
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 :

```
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.

```
sudo ssh localhost -l DOMAIN\username

id -u
```

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

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

Vérifiez que les tickets dans le cache d'identification de Kerberos de l'utilisateur sont valides et n'ont pas expiré. Passez à l'étape 4 : installer le Linux VDA après vérification de la jonction du domaine.

```
klist
```


Étape 4 : installer le Linux VDA

Étape 4a : désinstaller l'ancienne version

Si vous avez déjà installé une version antérieure de VDA Linux, désinstallez-la avant d'installer la nouvelle version.

1. Arrêtez les services Linux VDA :

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
```

2. Désinstallez le package :

```
sudo rpm -e XenDesktopVDA
```

> **Remarque :**
>
> La mise à niveau à partir des deux versions précédentes est prise en charge.
>
> **Remarque :**
>
> À compter de la version 1.3, le chemin d'installation est différent. Dans les versions précédentes, les composants d'installation se trouvaient dans **/usr/local/**. Le nouvel emplacement est **/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 au site Web Citrix et téléchargez le package Linux VDA en fonction de la distribution Linux appropriée.

Étape 4c : installer le Linux VDA

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

Pour RHEL 7/CentOS 7 :

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el7_3.x86_64.rpm
```

Pour RHEL 6.9 :

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
```


For RHEL 6.6/CentOS 6.6 :

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_6.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 7/CentOS 7 :

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.el7_3.x86_64.rpm
```

Pour RHEL 6.9 :

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
```

For RHEL 6.6/CentOS 6.6 :

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
```

Liste des dépendances RPM pour RHEL 7 :

```
postgresql-server >= 9.2

postgresql-jdbc >= 9.2

java-1.8.0-openjdk >= 1.8.0

ImageMagick >= 6.7.8.9

firewalld >= 0.3.9

policycoreutils-python >= 2.0.83

dbus >= 1.6.12

dbus-x11 >= 1.6.12

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.2

libXpm >= 3.5.10

libXrandr >= 1.4.1

libXtst >= 1.2.2

motif >= 2.3.4

pam >= 1.1.8

util-linux >= 2.23.2

```



```
bash >= 4.2

findutils >= 4.5

gawk >= 4.0

sed >= 4.2

cups >= 1.6.0

foomatic-filters >= 4.0.9

openldap >= 2.4

cyrus-sasl >= 2.1

cyrus-sasl-gssapi >= 2.1

libxml2 >= 2.9

python-requests >= 2.6.0

gperftools-libs >= 2.4

xorg-x11-server-Xorg >= 1.17

xorg-x11-server-Xorg < 1.18

rpmlib(FileDigests) <= 4.6.0-1

rpmlib(PayloadFilesHavePrefix) <= 4.0-1

rpmlib(CompressedFileNames) <= 3.0.4-1

rpmlib(PayloadIsXz) <= 5.2-1
```

Liste des dépendances RPM pour RHEL 6.9 :

```
postgresql-jdbc >= 8.4

postgresql-server >= 8.4

java-1.7.0-openjdk >= 1.7.0

ImageMagick >= 6.5.4.7

GConf2 >= 2.28.0

system-config-firewall-base >= 1.2.27

policycoreutils-python >= 2.0.83

xorg-x11-server-utils >= 7.7
```



```
xorg-x11-xinit >= 1.0.9

ConsoleKit >= 0.4.1

dbus >= 1.2.24

dbus-x11 >= 1.2.24

libXpm >= 3.5.10

libXrandr >= 1.4.1

libXtst >= 1.2.2

openmotif >= 2.3.3

pam >= 1.1.1

util-linux-ng >= 2.17.2

bash >= 4.1

findutils >= 4.4

gawk >= 3.1

sed >= 4.2

cups >= 1.4.0

foomatic >= 4.0.0

openldap >= 2.4

cyrus-sasl >= 2.1

cyrus-sasl-gssapi >= 2.1

libxml2 >= 2.7

python-requests >= 2.6.0

gperftools-libs >= 2.0

xorg-x11-server-Xorg >= 1.17

xorg-x11-server-Xorg < 1.18

rpmlib(FileDigests) <= 4.6.0-1

rpmlib(PayloadFilesHavePrefix) <= 4.0-1

```



```
rpmlib(CompressedFileNames) <= 3.0.4-1

rpmlib(PayloadIsXz) <= 5.2-1
```

Liste des dépendances RPM pour RHEL 6.6/CentOS 6.6 :

```
postgresql-jdbc >= 8.4

postgresql-server >= 8.4

java-1.7.0-openjdk >= 1.7.0

ImageMagick >= 6.5.4.7

GConf2 >= 2.28.0

system-config-firewall-base >= 1.2.27

policycoreutils-python >= 2.0.83

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.0.9

ConsoleKit >= 0.4.1

dbus >= 1.2.24

dbus-x11 >= 1.2.24

libXpm >= 3.5.10

libXrandr >= 1.4.1

libXtst >= 1.2.2

openmotif >= 2.3.3

pam >= 1.1.1

util-linux-ng >= 2.17.2

bash >= 4.1

findutils >= 4.4

gawk >= 3.1

sed >= 4.2

cups >= 1.4.0

foomatic >= 4.0.0
```



```
48
49 openldap >= 2.4
50
51 cyrus-sasl >= 2.1
52
53 cyrus-sasl-gssapi >= 2.1
54
55 libxml2 >= 2.7
56
57 python-requests >= 2.6.0
58
59 gperftools-libs >= 2.0
60
61 xorg-x11-server-Xorg >= 1.15
62
63 xorg-x11-server-Xorg < 1.16
64
65 rpmlib(FileDigests) <= 4.6.0-1
66
67 rpmlib(PayloadFilesHavePrefix) <= 4.0-1
68
69 rpmlib(CompressedFileNames) <= 3.0.4-1
70
71 rpmlib(PayloadIsXz) <= 5.2-1
```

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

Vous pouvez mettre à niveau le logiciel VDA Linux à partir des versions 7.14 et 7.13 à l'aide de Yum :

Pour RHEL 7/CentOS 7 :

```
1 sudo yum install -y XenDesktopVDA-7.15.0.404-1.el7_3.x86_64.rpm
```

Pour RHEL 6.9 :

```
1 sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
```

For RHEL 6.6/CentOS 6.6 :

```
1 sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
```

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

Pour RHEL 7/CentOS 7 :

```
1 sudo rpm -U XenDesktopVDA-7.15.0.404-1.el7_3.x86_64.rpm
```

Pour RHEL 6.9 :

```
1 sudo rpm -U XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
```


For RHEL 6.6/CentOS 6.6 :

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
```

> **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 XenServer
2. VMware ESX

Suivez les instructions pour l'hyperviseur choisi.

Citrix XenServer :

Cette section détaillée décrit l'installation et la configuration des pilotes NVIDIA GRID sur Citrix XenServer.

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 :

```
yum install gcc

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

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.

```
nvidia-smi

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

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

Définissez la configuration correcte pour la carte :

```
etc/X11/ctx-nvidia.sh
```

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

Étape 6 : configurer le Linux VDA

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

Vous pouvez exécuter le script manuellement avec invite, ou automatiquement avec réponses préconfigurées. 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 :

```
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 composant 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** : 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 –Quest Authentication Service
  - 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 est 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 port 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_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.

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

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST=list-ddc-fqdns

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3|4

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base-set

export CTX_XDL_START_SERVICE=Y|N

```



```
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. Citrix vous recommande de créer un fichier de script shell à partir des commandes précédentes avec **#!/bin/bash** en tant que première ligne.

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

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST=list-ddc-fqdns \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST=list-ldap-servers \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_START_SERVICE=Y|N \

/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 :

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
```

Pour supprimer les modifications de configuration :

```
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 :

```
sudo /sbin/service ctxhdx start

sudo /sbin/service ctxvda start
```

Arrêter Linux VDA :

Pour arrêter les services Linux VDA :

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
```

Redémarrer Linux VDA :

Pour redémarrer les services Linux VDA :

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx restart

sudo /sbin/service ctxvda start
```

Vérifier l'état de Linux VDA :

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

```
sudo /sbin/service ctxvda status

sudo /sbin/service ctxhdx status
```


Étape 8 : créer le catalogue de machines dans XenApp ou XenDesktop

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'OS de serveur pour un modèle de mise à disposition de bureaux partagés hébergés
  - L'OS de bureau pour un modèle de mise à disposition de bureaux dédiés VDI
- Assurez-vous que les machines sont définies avec une alimentation non gérée.
- MCS n'étant pas pris en charge pour les VDA Linux, choisissez la méthode de déploiement PVS ou **Autre service ou technologie** (images existantes).
- 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 XenApp ou XenDesktop

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 :

- Pour le type de mise à disposition, sélectionnez Bureaux ou Applications.

- 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.

Installer Linux Virtual Delivery Agent pour SUSE

February 9, 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 l'installation

Étape 1 a : démarrer l'outil YaST

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

Pour démarrer l'outil YaST basé sur texte :

```
su -

yast
```

Vous pouvez également démarrer l'outil YaST basé sur interface utilisateur :

```
su -

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 :

```
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 :

```
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 :

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

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 :

- PostgreSQL
  - SLED/SLES 11 : version 9.1 ou ultérieure
  - SLED/SLES 12 : version 9.3 ou ultérieure
- OpenJDK 1.7.0
- OpenMotif Runtime Environment 2.3.1 ou version ultérieure
- Cups
  - SLED/SLES 11 : version 1.3.7 ou ultérieure
  - SLED/SLES 12 : version 1.6.0 ou ultérieure
- Filtres Foomatic
  - SLED/SLES 11 : version 3.0.0 ou ultérieure
  - SLED/SLES 12 : version 1.0.0 ou ultérieure
- ImageMagick
  - SLED/SLES 11 : version 6.4.3.6 ou ultérieure
  - SLED/SLES 12 : version 6.8 ou ultérieure

Ajouter des référentiels Certains packages requis ne sont pas disponibles dans tous les référentiels SUSE Linux Enterprise :

- SLED 11 : PostgreSQL est disponible pour SLES 11 mais pas SLED 11.
- SLES 11 : OpenJDK et OpenMotif sont disponibles pour SLED 11 mais pas SLES 11.

- SLED 12 : PostgreSQL est disponible pour SLES 12 mais pas SLED 12. ImageMagick est disponible via le fichier ISO SDK SLE 12 ou le référentiel en ligne.
- SLES 12: il n'existe aucun problème. Tous les packages sont disponibles. ImageMagick est disponible via le fichier ISO SDK SLE 12 ou le référentiel en ligne.

Pour résoudre ce problème, obtenez les packages manquants depuis le support de l'autre édition de SLE que vous installez. Autrement dit, sur SLED, installez les packages manquants depuis le support SLES et sur SLES, installez les packages manquants depuis le support SLED. L'approche suivante monte les fichiers de support ISO SLED et SLES et ajoute les référentiels.

- Sur SLED 11, exécutez les commandes :

```
sudo mkdir -p /mnt/sles

sudo mount -t iso9660 path-to-iso/SLES-11-SP4-DVD-x86_64-GM-DVD1.iso /
    mnt/sles

sudo zypper ar -f /mnt/sles sles
```

- Sur SLES 11, exécutez les commandes :

```
sudo mkdir -p /mnt/sled

sudo mount -t iso9660 path-to-iso/SLED-11-SP4-DVD-x86_64-GM-DVD1.iso /
    mnt/sled

sudo zypper ar -f /mnt/sled sled
```

- Sur SLED 12, exécutez les commandes :

```
sudo mkdir -p /mnt/sles

sudo mount -t iso9660 path-to-iso/SLES-12-SP2-DVD-x86_64-GM-DVD1.iso /
    mnt/sles

sudo zypper ar -f /mnt/sles sles
```

- Sur SLED/SLES 12, exécutez les commandes :

```
sudo mkdir -p /mnt/sdk

sudo mount -t iso9660 path-to-iso/SLE-12-SP3-SDK-DVD-x86_64-GM-DVD1.iso
     /mnt/sdk

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 :


```
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 1.7.0.

> **Conseil :**
>
> Pour éviter les problèmes, assurez-vous que vous avez uniquement installé OpenJDK version 1.7.0. 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 :

```
sudo zypper info java-1_7_0-openjdk
```

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

```
sudo zypper update java-1_7_0-openjdk
```

3. Vérifiez la version Java :

```
java -version
```

- **SLES :**

1. Sur SLES, installez Java Runtime Environment :

```
sudo zypper install java-1_7_0-openjdk
```

2. Vérifiez la version Java :

```
java -version
```

Installer PostgreSQL

- Sur SLED/SLES 11, installez les packages :

```
sudo zypper install libecpg6

sudo zypper install postgresql-init

sudo zypper install postgresql

sudo zypper install postgresql-server
```



```

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.

```
sudo /sbin/insserv postgresql

sudo /etc/init.d/postgresql restart
```

- Sur SLED/SLES 12, installez les packages :

```
sudo zypper install postgresql-init

sudo zypper install postgresql-server

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.

```
sudo systemctl enable postgresql

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, les référentiels de l'autre édition configurés auparavant peuvent être supprimés et le support démonté :

- Sur SLED 11, exécutez les commandes pour supprimer les packages :

```
sudo zypper rr sles

sudo umount /mnt/sles

sudo rmdir /mnt/sles
```

- Sur SLES 11, exécutez les commandes pour supprimer les packages :

```
sudo zypper rr sled

sudo umount /mnt/sled

sudo rmdir /mnt/sled
```

- sur SLED 12, exécutez les commandes pour supprimer les packages :

```
sudo zypper rr sles

```



```
sudo umount /mnt/sles

sudo rmdir /mnt/sles
```

- Sur SLED/SLES 12, exécutez les commandes pour supprimer les packages :

```
sudo zypper rr sdk

sudo umount /mnt/sdk

sudo rmdir /mnt/sd
```

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 XenServer

Si la fonctionnalité de synchronisation de l'heure de XenServer est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée car XenServer et NTP 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 XenServer Tools installé, vous pouvez vérifier si la fonctionnalité de synchronisation de l'heure de XenServer est présente et activée à partir de la VM Linux :

```
su -



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/indepent_wallclock** n'existe pas, les étapes suivantes ne sont pas nécessaires.

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

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

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

```
xen.independent_wallclock = 1
```

Pour vérifier ces modifications, redémarrez le système :

```
reboot
```

Après le redémarrage, vérifiez que le paramètre est correct :

```
su -
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 XenServer et VMware, pour lesquels la synchronisation de l'heure est désactivée pour éviter tout conflit avec NTP. La synchronisation de l'heure Hyper-V peut coexister 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, 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.

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

Suivez les instructions en fonction de la méthode choisie.

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 Authentification** (Authentification en mode déconnecté) n'est pas sélectionné. Cette option n'est pas compatible avec le Linux VDA.
3. Cliquez sur **OK**. Si vous êtes invité(e) à installer des packages, cliquez sur **Install**.

4. Si un contrôleur de domaine est trouvé, vous êtes invité à joindre le domaine. Cliquez sur **Oui**.
5. Lorsque vous y êtes invité(e), saisissez les informations d'identification d'un utilisateur de domaine avec les autorisations nécessaires pour ajouter des 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 :

```
su -

reboot
```

SLED/SLES 12 uniquement : correctif du nom du fichier cache d'identification Kerberos SLED/SLES 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 :

```
sudo net ads testjoin
```

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

```
sudo net ads info
```

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

```
sudo klist -ke
```


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

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

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

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

```
sudo klist
```

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

```
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 :

```
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 à l'aide d'un compte d'utilisateur de domaine sur le VDA Linux. Le compte d'utilisateur de domaine n'a pas été utilisé auparavant.

```
ssh localhost -l domain\username

id -u
```

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

```
ls /tmp/krb5cc_uid
```

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

```
klist
```


Quitter la session

```
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 :

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

sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-
    auth false
```

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

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

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

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

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

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

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

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

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

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, utilisez un compte d'utilisateur de domaine pour vous connecter au VDA Linux. Le compte d'utilisateur de domaine n'a pas été utilisé auparavant.

```
ssh localhost -l domain\username

id -u
```

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

```
ls /tmp/krb5cc_uid
```


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

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

Quittez la session.

```
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** :

```
su -

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 :

```
su -

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 :

```
adinfo --sysinfo all

adinfo -diag
```

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

```
adinfo --test
```

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 :

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
```

2. Désinstallez le package :

```
sudo rpm -e XenDesktopVDA
```

> **Important :**
>
> La mise à niveau à partir des deux versions précédentes 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 au site Web Citrix et téléchargez le package Linux VDA en fonction de la distribution Linux appropriée.

Étape 4c : installer le Linux VDA

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

Pour SUSE 12 :

```
sudo zypper install XenDesktopVDA-7.15.0.404-1.sle12_2.x86_64.rpm
```

Pour SUSE 11 :

```
sudo zypper install XenDesktopVDA-7.15.0.404-1.sle11_4.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 :

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.sle12_2.x86_64.rpm
```

Pour SUSE 11 :

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.sle11_4.x86_64.rpm
```

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

Vous pouvez mettre à niveau le logiciel VDA Linux à partir des versions 7.14 et 7.13 à l'aide du gestionnaire de package RPM :

Pour SUSE 12 :

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.sle12_2.x86_64.rpm
```

Pour SUSE 11 :

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.sle11_4.x86_64.rpm
```

Liste des dépendances RPM pour SUSE 12 :

```
postgresql-server >= 9.3

postgresql-jdbc >= 9.2

java-1.7.0-openjdk >= 1.7.0

ImageMagick >= 6.8

dbus-1 >= 1.8.8

dbus-1-x11 >= 1.8.8

libXpm4 >= 3.5.11

libXrandr2 >= 1.4.2

libXtst6 >= 1.2.2

motif >= 2.3

pam >= 1.1.8

bash >= 4.2

findutils >= 4.5

gawk >= 4.1

```



```
sed >= 4.2

cups >= 1.6.0

cups-filters-foomatic-rip >= 1.0.0

openldap2 >= 2.4

cyrus-sasl >= 2.1

cyrus-sasl-gssapi >= 2.1

libxml2 >= 2.9

python-requests >= 2.8.1

rpmlib(PayloadFilesHavePrefix) <= 4.0-1

rpmlib(CompressedFileNames) <= 3.0.4-1

rpmlib(PayloadIsLzma) <= 4.4.6-1
```

Liste des dépendances RPM pour SUSE 11 :

```
postgresql-server >= 9.1.

postgresql-jdbc >= 9.1

java-1_7_0-openjdk >= 1.7.0.6

ImageMagick >= 6.4.3.6

ConsoleKit >= 0.2.10

dbus-1 >= 1.2.10

dbus-1-x11 >= 1.2.10

xorg-x11-libXpm >= 7.4

xorg-x11-libs >= 7.4

openmotif-libs >= 2.3.1

pam >= 1.1.5

libdrm >= 2.4.41

libpixman-1-0 >= 0.24.4

Mesa >= 9.0

openssl >= 0.9.8j
```



```
30
31 xorg-x11 >= 7.4
32
33 xorg-x11-fonts-core >= 7.4
34
35 xorg-x11-libXau >= 7.4
36
37 xorg-x11-libXdmcp >= 7.4
38
39 bash >= 3.2
40
41 findutils >= 4.4
42
43 gawk >= 3.1
44
45 sed >= 4.1
46
47 cups >= 1.3.7
48
49 foomatic-filters >= 3.0.0
50
51 openldap2 >= 2.4
52
53 cyrus-sasl >= 2.1
54
55 cyrus-sasl-gssapi >= 2.1
56
57 libxml2 >= 2.7
58
59 python-requests >= 2.0.1
60
61 rpmlib(PayloadFilesHavePrefix) <= 4.0-1
62
63 rpmlib(CompressedFileNames) <= 3.0.4-1
64
65 rpmlib(PayloadIsLzma) <= 4.4.6-1
```

> **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 préconfigurées. Consultez l'aide sur le script avant de continuer :


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

Configuration avec invites

Exécutez une configuration manuelle avec questions :

```
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 est 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 port 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, 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_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.

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

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST=list-ddc-fqdns

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3|4

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base-set
```



```

export CTX_XDL_START_SERVICE=Y|N

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. Citrix vous recommande de créer un fichier de script shell à partir des commandes précédentes avec **#!/bin/bash** en tant que première ligne.

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

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST=list-ddc-fqdns \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST=list-ldap-servers \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_START_SERVICE=Y|N \

/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 :

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

Pour supprimer les modifications de configuration :

```
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 :

```
sudo /sbin/service ctxhdx start

sudo /sbin/service ctxvda start
```

Arrêter Linux VDA :

Pour arrêter les services Linux VDA :

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
```

Redémarrer Linux VDA :

Pour redémarrer les services Linux VDA :

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx restart

sudo /sbin/service ctxvda start
```

Vérifier l'état de Linux VDA :

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


```
sudo /sbin/service ctxvda status

sudo /sbin/service ctxhdx status
```

Étape 7 : créer le catalogue de machines dans XenApp ou XenDesktop

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'OS de serveur pour un modèle de mise à disposition de bureaux partagés hébergés
  - L'OS de bureau pour un modèle de mise à disposition de bureaux dédiés VDI
- Assurez-vous que les machines sont définies avec une alimentation non gérée.
- MCS n'étant pas pris en charge pour les VDA Linux, choisissez la méthode de déploiement PVS ou **Autre service ou technologie** (images existantes).
- 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 8 : créer le groupe de mise à disposition dans XenApp ou XenDesktop

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 :

- Pour le type de mise à disposition, sélectionnez Bureaux ou Applications.
- 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.

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

Assurez-vous que vous disposez 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
```

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 :

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

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 :

```
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 :

```
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. Vérifiez qu'il a été installé avec :

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

Étape 1i : installer PostgreSQL

Le VDA Linux requiert PostgreSQL version 9.x sur Ubuntu 16.04 :

```
sudo apt-get install -y postgresql

sudo apt-get install -y libpostgresql-jdbc-java
```

Étape 1j : installer Motif

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

Étape 1k : installer les autres packages

```
sudo apt-get install -y libsasl2-2

sudo apt-get install -y libsasl2-modules-gssapi-mit

sudo apt-get install -y libldap-2.4-2

sudo apt-get install -y krb5-user

sudo apt-get install -y cups
```


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 XenServer

Si la fonctionnalité de synchronisation de l'heure de XenServer est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée car XenServer et NTP 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 XenServer Tools installé, vous pouvez vérifier si la fonctionnalité de synchronisation de l'heure de XenServer est présente et activée à partir de la VM Linux :

```
su -

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/indepent_wallclock n'existe pas, les étapes suivantes ne sont pas nécessaires.

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

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

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

```
xen.independent_wallclock = 1
```

Pour vérifier ces modifications, redémarrez le système :

```
su -

cat /proc/sys/xen/independent_wallclock
```

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, 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 XenServer et VMware, pour lesquels la synchronisation de l'heure est désactivée afin d'éviter tout conflit avec NTP. La synchronisation de l'heure Hyper-V peut coexister 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

Suivez les instructions en fonction de la méthode choisie.

Samba Winbind

Installer ou mettre à jour les packages requis

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

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

```
sudo systemctl enable winbind
```

Configurer Kerberos Ouvrez `/etc/krb5.conf` en tant qu'utilisateur racine et configurez les paramètres suivants :

```
[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**.

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 effectuez 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 :

```
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

```
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 :

```
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 :

```
sudo net ads testjoin
```

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

```
sudo net ads info
```

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

```
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 :

```
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 :


```
sudo klist
```

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

```
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 :

```
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 à l'aide d'un compte d'utilisateur de domaine sur le VDA Linux. Le compte d'utilisateur de domaine n'a pas été utilisé auparavant.

```
ssh localhost -l domain\username

id -u
```

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

```
ls /tmp/krb5cc_uid
```

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

```
klist
```

Quittez la session.

```
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 :

```
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 :

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

sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-auth false
```

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

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

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

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

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

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

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

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

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

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, utilisez un compte d'utilisateur de domaine pour vous connecter au VDA Linux. Le compte d'utilisateur de domaine n'a pas été utilisé auparavant.

```
ssh localhost -l domain\username

id -u
```

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

```
ls /tmp/krb5cc_uid
```

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

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

Quittez la session.

```
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` :

```
su -

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 :

```
su -

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 :

```
adinfo --sysinfo all

adinfo --diag
```

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

```
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 :

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

Pour configurer Kerberos, ouvrez `/etc/krb5.conf` en tant qu'utilisateur racine et configurez les paramètres suivants :

```
[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`. Le `REALM` est le nom du domaine Kerberos en majuscules, tel que `EXAMPLE.COM`.

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

> **Remarque :**
>
> Cette section fournit uniquement des informations pour `adcli` et `Samba`.

Utilisez adcli pour rejoindre le domaine :

Installer adcli :

Installez les packages requis :

```
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 :

```
su -

rm -rf /etc/krb5.keytab

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 :

Les fonctionnalités de l'outil **adcli** sont limitées et ne permettent pas de tester si une machine est jointe au domaine. Le meilleur moyen consiste à vérifier que le fichier keytab système a été créé :

```
sudo klist -ket
```

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 :

```
sudo apt-get install samba
```

Configurer samba :

Ouvrez `/etc/samba/smb.conf` et effectuez 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.

```
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 :

```
sudo apt-get install sssd
```

Si les packages sont déjà installés, une mise à jour est recommandée :

```
sudo apt-get update 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/sssd/sssd.conf** n'est pas installé par défaut et doit être créé manuellement. En tant qu'utilisateur racine, créez ou ouvrez **/etc/sssd/sssd.conf** et configurez les paramètres suivants :

```
[sssd]
```



```
2
3  services = nss, pam
4
5  config_file_version = 2
6
7  domains = domain-dns-name
8
9  [domain/domain-dns-name]
10
11 id_provider = ad
12
13 access_provider = ad
14
15 auth_provider = krb5
16
17 krb5_realm = REALM
18
19 # Set krb5_renewable_lifetime higher if TGT renew lifetime is longer
      than 14 days
20
21 krb5_renewable_lifetime = 14d
22
23 # Set krb5_renew_interval to lower value if TGT ticket lifetime is
      shorter than 2 hours
24
25 krb5_renew_interval = 1h
26
27 krb5_ccachedir = /tmp
28
29 krb5_ccname_template = FILE:%d/krb5cc_%U
30
31 # This ldap_id_mapping setting is also the default value
32
33 ldap_id_mapping = true
34
35 override_homedir = /home/%d/%u
36
37 default_shell = /bin/bash
38
39 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.

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. Il n'est pas nécessaire de configurer le nom de domaine NetBIOS.

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

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

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

Démarrer le démon SSSD Exécutez les commandes suivantes pour démarrer le démon SSSD maintenant et pour permettre le lancement du démon au démarrage de la machine :

```
sudo systemctl start sssd

sudo systemctl enable sssd
```

Configuration de PAM Exécutez la commande suivante et assurez-vous que les options **SSS authentication** et **Create home directory on login** sont sélectionnées :

```
sudo pam-auth-update
```

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 :

```
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 :

```
sudo net ads testjoin
```

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

```
sudo net ads info
```


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

```
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 :

```
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 :

```
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 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.

```
ssh localhost -l domain\username

id -u

klist

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 :

```
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.

Étape 4 : installer le Linux VDA

Étape 4a : télécharger le package Linux VDA

Accédez au site Web Citrix et téléchargez le package Linux VDA en fonction de la distribution Linux appropriée.

Étape 4b : installer le Linux VDA

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

```
sudo dpkg -i xendesktopvda_7.15.0.404-1.ubuntu16.04_amd64.deb
```

Liste des dépendances Debian pour Ubuntu :

```
postgresql >= 9.5

libpostgresql-jdbc-java >= 9.2

default-jdk >= 2:1.8

imagemagick >= 8:6.8.9.9

ufw >= 0.35

ubuntu-desktop >= 1.361

libxrandr2 >= 2:1.5.0

libxtst6 >= 2:1.2.2

libxm4 >= 2.3.4

util-linux >= 2.27.1

bash >= 4.3

findutils >= 4.6.0

sed >= 4.2.2

cups >= 2.1

libldap-2.4-2 >= 2.4.42

libsasl2-modules-gssapi-mit >= 2.1.~

python-requests >= 2.9.1

libgoogle-perftools4 >= 2.4~
```


Étape 4c : configurer le Linux VDA

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

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

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

Configuration avec invites Exécutez une configuration manuelle avec questions :

```
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** : le VDA Linux 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 est 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 port 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, 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_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.

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

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST=list-ddc-fqdns

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3|4

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N
```



```

export CTX_XDL_SITE_NAME=dns-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base-set

export CTX_XDL_START_SERVICE=Y|N

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. Citrix vous recommande de créer un fichier de script shell à partir des commandes précédentes avec **#!/bin/bash** en tant que première ligne.

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

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST=list-ddc-fqdns \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST=list-ldap-servers \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_START_SERVICE=Y|N \

/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 :

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
```


Pour supprimer les modifications de configuration :

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

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

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

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

Désinstaller le logiciel Linux VDA Pour vérifier que le Linux VDA est installé et pour afficher la version du package installé :

```
dpkg -l xendesktopvda
```

Pour afficher des informations plus détaillées :

```
apt-cache show xendesktopvda
```

Pour désinstaller le logiciel Linux VDA :

```
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 :


```
sudo systemctl start ctxhdx

sudo systemctl start ctxvda
```

Arrêter Linux VDA :

Pour arrêter les services Linux VDA :

```
sudo systemctl stop ctxvda

sudo systemctl stop ctxhdx
```

Redémarrer Linux VDA :

Pour redémarrer les services Linux VDA :

```
sudo systemctl stop ctxvda

sudo systemctl restart ctxhdx

sudo systemctl restart ctxvda
```

Vérifier l'état de Linux VDA :

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

```
sudo systemctl status ctxvda

sudo systemctl status ctxhdx
```

Étape 6 : créer le catalogue de machines dans XenApp ou XenDesktop

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'OS de serveur pour un modèle de mise à disposition de bureaux partagés hébergés
  - L'OS de bureau pour un modèle de mise à disposition de bureaux dédiés VDI
- Assurez-vous que les machines sont définies avec une alimentation non gérée.
- MCS n'étant pas pris en charge pour les VDA Linux, choisissez la méthode de déploiement PVS ou **Autre service ou technologie** (images existantes).

- 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 7 : créer le groupe de mise à disposition dans XenApp ou XenDesktop

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 :

- Pour le type de mise à disposition, sélectionnez **Bureaux**. Les VDA Linux pour Ubuntu ne prennent pas en charge la mise à disposition d'applications.
- 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.

Configurer le Linux VDA

December 15, 2020

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

Intégrer NIS avec Active Directory

November 15, 2021

Cet article décrit comment intégrer NIS avec Windows Active Directory (AD) sur le Linux VDA à l'aide de SSSD. Le VDA Linux est considéré comme un composant de Citrix XenApp et XenDesktop. 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.

Logiciel requis

Le fournisseur Active Directory a été introduit avec la version 1.9.0 de SSSD.

Les environnements suivants ont été testés et vérifiés lors de l'utilisation des instructions figurant dans cet article :

- RHEL 7.3 ou version ultérieure/CentOS 7.3 ou version ultérieure
- Version 1.3 ou ultérieure du VDA Linux

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 :

```
yum – y install ypbind rpcbind oddjob-mkhomedir
```

Définissez le domaine NIS :

```
ypdomainname nis.domain
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 :

```
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 :

```
sudo systemctl start rpcbind ypbind

sudo systemctl enable rpcbind ypbind
```

Assurez-vous que la configuration NIS est correcte :

```
ypwhich
```

Vérifiez que les informations de compte sont disponibles à partir du serveur NIS :

```
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 :

```
--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
```

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.


```
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/sssd/sssd.conf Exemple de configuration **sssd.conf** (des options supplémentaires peuvent être ajoutées si nécessaire) :

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

[domain/example]
# Uncomment if you need offline logins
# cache_credentials = true
re_expression = (((?P<domain>[^\\]+)\\(?P<name>.+$))|((?P<name>[^@]+)@(?P<domain>.+$))|(^(?P<name>[^@\\]+)$))
id_provider = proxy
proxy_lib_name = nis
auth_provider = ad
access_provider = ad

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

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

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

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

```



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

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

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 :

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

sudo systemctl start sssd

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 :

```
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 :

```
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 :

```
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 :

```
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.

```
sudo localhost  – l DOMAIN\username

id -u
```

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

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

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

```
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, Citrix recommande 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 StoreFront. Le mode transparent est activé par défaut. Si vous l'avez déjà désactivé en définissant « TWIMode=Off », supprimez ce paramètre au lieu de le modifier sur « TWIMode=On ». Sinon, il est possible que vous ne puissiez pas lancer de bureau publié.

Résolution des problèmes

Il est possible que le lancement d'une application publiée prenne plus de deux minutes et que cette dernière n'affiche pas les fenêtres en mode transparent. Si le problème se produit, vérifiez que le

mode transparent a été activé sur le Linux VDA et StoreFront.

La commande permettant de vérifier si le mode transparent est activé sur le Linux VDA :

```
sudo /opt/Citrix/VDA/bin/ctxreg list -k "HKEY_LOCAL_MACHINE\System\
    CurrentControlSet\Control\Citrix"  |  grep "SeamlessEnabled"
```

Si elle affiche « SeamlessEnabled = 0x00000000 », le mode transparent est désactivé. Pour l'activer, exécutez la commande suivante :

```
sudo /opt/Citrix/VDA/bin/ctxreg update  -k "HKEY_LOCAL_MACHINE\System\
    CurrentControlSet\Control\Citrix"  -v "SeamlessEnabled" -d "0
    x00000001"
```

Problèmes connus

Les problèmes connus suivants sont identifiés lors de la publication d'applications :

- Les applications publiées non transparentes ne se lancent pas lorsque le mode transparent est désactivé sur StoreFront, et qu'il est toujours activé sur le Linux VDA. Activez ou désactivez le mode transparent sur le Linux VDA et StoreFront en même temps.
- 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 : (CentOS7.3\RHEL7.3\SUSE12.2), Metacity (CentOS6.6\RHEL6.6\SUSE 11.4) 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/index.php/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.

Imprimer

November 5, 2021

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

Installation

Linux VDA requiert les filtres **cups** et **foomatic**. Exécutez les commandes suivantes en fonction de votre distribution Linux :

Prise en charge des impressions RHEL 7 :

```
sudo yum -y install cups

sudo yum -y install foomatic-filters
```

Prise en charge des impressions RHEL 6 :

```
sudo yum -y install cups

sudo yum -y install foomatic
```

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. Le nom de l'imprimante doit être différent pour les bureaux et les applications. Tenez compte des considérations suivantes :

- 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

Il existe différents éléments à vérifier si l'impression ne fonctionne pas correctement. Le démon d'impression est un processus par session et doit être en cours d'exécution pour la durée de la session. Vérifiez que le démon d'impression est en cours d'exécution.

```
ps -ef | grep ctxlpmngt
```


Si le processus **ctxlpmngt** n'est pas exécuté, démarrez manuellement **ctxlpmngt** à partir d'une ligne de commande. 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 par :

```
service ctxcups status
```

Journal supplémentaire lors de l'impression avec CUPS

En tant que composant du VDA Linux, la méthode permettant d'obtenir le journal d'un composant d'impression est similaire à d'autres composants.

Pour RHEL, certaines étapes supplémentaires sont nécessaires pour configurer le fichier du service CUPS. Sinon, certains journaux ne peuvent pas être consignés dans **hdx.lo** :

```
sudo service cups stop

sudo vi /etc/systemd/system/printer.target.wants/cups.service

PrivateTmp=false

sudo service cups start

sudo systemctl daemon-reload
```

> **Remarque :**
>
> Cette configuration sert uniquement à collecter le journal d'impression complet lorsqu'un problème survient. En général, cette configuration n'est pas recommandée car cette opération enfreint la sécurité CUPS.

L'impression est illisible

Un pilote d'imprimante incompatible peut causer une impression illisible. Une configuration pilote par utilisateur est disponible et peut être configurée en modifiant le fichier de configuration **~/.CtxlpProfile$CLIENT_NAME** :

```
[DEFAULT_PRINTER]

printername=

model=

ppdpath=

drivertype=
```


> **Important :**
>
> le champ **printername** contient le nom de l'imprimante par défaut actuelle côté client. Il s'agit d'une valeur en lecture seule. Ne la modifiez pas.
>
> Les champs **ppdpath**, **model** et **drivertype** ne peuvent pas être définis en même temps car un seul est appliqué pour l'imprimante mappée.

Si le pilote d'imprimante universel n'est pas compatible avec l'imprimante cliente, configurez le modèle du pilote d'imprimante natif avec l'option **model**=. Vous pouvez trouver le nom du modèle actuel de l'imprimante avec la commande **lpinfo** :

```
lpinfo -m

...

xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
```

Vous pouvez ensuite définir le modèle pour qu'il corresponde à l'imprimante :

```
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 :

```
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 si aucun pilote d'imprimante natif n'est disponible.

Par exemple, si le pilote d'imprimante par défaut est de type PCL5 :

```
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 :

Pour identifier ce problème :

1. Ouvrez une session sur le bureau de session ICA.
2. vi ~/.CtxlProfile$CLIENT_NAME
3. Ajoutez le champ suivant au fichier de spouleur sur le VDA Linux :

   ```
   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 que 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. Une fois cette étape effectuée, testez-le en utilisant l'autre pilote d'imprimante.
8. Pour associer l'imprimante mappée à un autre pilote d'imprimante tiers, utilisez par exemple l'imprimante cliente postscript :

   a) Connectez-vous à une session active et ouvrez un navigateur sur le bureau client.

   b) Ouvrez le portail de gestion de l'impression :

      ```
      localhost:631
      ```

   c) Sélectionnez l'imprimante mappée **CitrixUniversalPrinter:$ClientName:app/dek$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 la page Make and Model, choisissez un pilote postcript au lieu du pilote Citrix UPD (par exemple, Citrix Universal Driver Postscript). Par exemple, si l'imprimante virtuelle

CUPS-PDF est installée, sélectionnez Generic CUPS-PDF Printer. Enregistrez les modifications.

f) Si ce processus réussit, configurez le chemin d'accès au fichier PPD du pilote dans **.CtxlpProfile$CLIENT_NAME** pour autoriser l'imprimante mappée à utiliser ce pilote tiers.

Problèmes connus

Les problèmes suivants ont été identifiés lors de l'impression sur le Linux VDA :

Le pilote CTXPS n'est pas compatible avec certaines imprimantes PLC

Si l'impression présente des anomalies, définissez le pilote d'imprimante sur le pilote d'imprimante natif fourni par le fabricant.

Impression lente avec les documents volumineux

Lorsque vous imprimez un document volumineux sur une imprimante cliente locale, le document est transféré sur une connexion serveur. Si la connexion est lente, le transfert risque de durer longtemps.

Notifications d'imprimante et de travaux d'impression d'autres sessions

Le concept de session de Linux n'est pas le même que celui du système d'exploitation Windows. Par conséquent, tous les utilisateurs reçoivent les notifications de l'ensemble du système. Vous pouvez désactiver ces notifications en modifiant le fichier de configuration CUPS : **/etc/cups/cupsd.conf**.

Recherchez le nom de stratégie configuré dans le fichier.

```
DefaultPolicy default
```

Si le nom de la stratégie est *default*, ajoutez les lignes suivantes dans le bloc XML de la stratégie par défaut :

```
<Policy default>

     # Job/subscription privacy...

     JobPrivateAccess default

     JobPrivateValues default

     SubscriptionPrivateAccess default

```



```
11      SubscriptionPrivateValues default
12
13      … …
14
15      <Limit Create-Printer-Subscription>
16
17           Require user @OWNER
18
19           Order deny,allow
20
21      </Limit>
22
23      <Limit All>
24
25           Order deny,allow
26
27      </Limit>
28
29 </Policy>
```

Impression PDF

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

November 30, 2022

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.

Paramètres de configuration

Il existe plusieurs paramètres de configuration liés aux graphiques dans **HKEY_LOCAL_MACHINE\System\Current** que vous pouvez régler avec l'outil **ctxreg**.

Comment activer Thinwire Plus

Thinwire Plus est activé par défaut pour les VDA standard et 3D Pro.

Comment activer H.264

Outre la configuration requise pour le système d'exploitation, H.264 requiert une version minimale de l'application Citrix Workspace (anciennement Citrix Receiver). Si le client ne répond pas aux exigences, il utilise Thinwire Plus.

Système d'exploitation	Version minimale requise pour H.264
Windows	3.4 ou version ultérieure
Mac OS X	11.8 ou version ultérieure
Linux	13.0 ou version ultérieure
Android	3.5

Système d'exploitation	Version minimale requise pour H.264
iOS	5.9
Chrome OS	1.4

Le dernier tableau des fonctionnalités de l'application Citrix Workspace est disponible sur https://docs.citrix.com/fr-fr/citrix-workspace-app/citrix-workspace-app-feature-matrix.html.

Exécutez la commande suivante pour publier l'encodage H.264 sur le VDA :

```
sudo ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\
    Thinwire" -t "REG_DWORD" -v "AdvertiseH264" -d "0x00000001" --force
```

Comment activer l'encodage matériel dans HDX 3D Pro

Pour HDX 3D Pro, le paramètre **AdvertiseH264** active uniquement permet l'encodage H.264 logiciel. Exécutez la commande pour activer l'encodage matériel :

```
sudo ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\
    Thinwire" -t "REG_DWORD" -v "HardwareEncoding" -d "0x00000001" --
    force
```

> **Remarque :**
>
> Si vous recevez le message d'erreur `ctxreg command can't be found`, utilisez la commande `ctxreg` avec un chemin d'accès complet. Par exemple, utilisez `sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire"-t "REG_DWORD"-v "AdvertiseH264"-d "0x00000001"–force` au lieu de `sudo ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire"-t "REG_DWORD"-v "AdvertiseH264"-d "0x00000001"–force`.

Comment régler Thinwire Plus pour une bande passante plus faible

- MaxColorDepth

  ```
  Default 0x20, type DWORD
  ```

  Cette option spécifie le nombre de couleurs des graphiques transférés via le protocole Thinwire vers le client.

Pour économiser la bande passante, définissez-la sur 0x10 (qui représente le nombre de couleurs préféré pour les graphiques simples) ou 0x8 (mode faible bande passante expérimental).

- Qualité

  Qualité visuelle

  ```
  Default: 0x1(medium), type: DWORD, valid values: 0x0(low), 0x1(medium), 0x2(high), 0x3(build to lossless), 0x4 always lossless.
  ```

  Pour économiser la bande passante, définissez la qualité sur 0x0 (faible).

- Paramètres supplémentaires

  - TargetFPS

    Taux de trames cible

    ```
    Default: 0x1e (30), Type: DWORD
    ```

  - MinFPS

    Taux de trame minimum cible

    ```
    Default: 0xa (10), Type: DWORD
    ```

  - MaxScreenNum

    Nombre maximal de moniteurs dont le client peut disposer

    ```
    Default: 0x2, Type: DWORD
    ```

    Pour un VDA standard, vous pouvez définir une valeur maximale de 10. Pour 3D Pro, la valeur maximale autorisée est de 4.

Résolution des problèmes

Vérifier que l'encodage est utilisé

Exécutez la commande suivante pour vérifier si l'encodage H.264 est utilisé (**1** représente H.264 et **0** représente TW+) :

```
sudo ctxreg dump | grep H264
```

Le résultat se présente comme suit :

```
create -k "HKLM\Software\Citrix\Ica\Session\1\Graphics"-t "REG_DWORD" -v "H264"-d "0x00000001"--force
```



```
create -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire"-t "
REG_DWORD"-v "AdvertiseH264"-d "0x00000001"--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
     Uncorr. ECC |
6  | Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
     Compute M. |
7  |===============================+======================+======================|

8  |   0  GRID K1             Off  | 0000:00:05.0     Off |
                       N/A |
9  | N/A   42C    P0    14W /  31W |    207MiB /  4095MiB |      8%
     Default |
10 +-------------------------------+----------------------+----------------------+

11
12 +-----------------------------------------------------------------------------+

13 | Processes:                                                       GPU
     Memory |
14 |  GPU       PID  Type  Process name
     Usage      |
15 |=============================================================================|

16 |    0      2164  C+G   /usr/local/bin/ctxgfx
     106MiB |
17 |    0      2187    G   Xorg
      85MiB |
18 +-----------------------------------------------------------------------------+
```


Vérifier que le pilote graphique NVIDIA GRID est correctement installé

Pour vérifier si le pilote graphique NVIDIA GRID est correctement installé, exécutez **nvidia-smi**. Le résultat se présente comme suit :

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

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

Définissez la configuration correcte pour la carte :

```
etc/X11/ctx-nvidia.sh
```

Problèmes d'actualisation des multi-écrans HDX 3D Pro

Si vous rencontrez des problèmes d'actualisation des écrans autres que l'écran principal, vérifiez que la licence NVIDIA GRID est disponible.

Vérifier les journaux d'erreurs Xorg

Le nom du fichier journal Xorg est similaire à **Xorg.{DISPLAY}.log** dans le dossier **/var/log/**.

Problèmes connus et limitations

Pour vGPU, la console locale XenServer affiche l'écran de la session de bureau ICA

Solution : désactivez la console VGA locale de la machine virtuelle en exécutant la commande suivante :

```
xe vm-param-set uuid=<vm-uuid> platform:vgpu_extra_args="disable_vnc=1"
```

L'API NVENC n'est pas prise en charge dans les profils vGPU autres que 8Q

Les profils vGPU de la carte NVIDIA Tesla M60 autres que 8Q ne prennent pas en charge cuda ; par conséquent, les encodages matériels API NVENC et Citrix 3D Pro ne sont pas disponibles.

Les cartes graphiques NVIDIA K2 ne prennent pas en charge le codage matériel YUV444 en mode passthrough

Il s'agit d'une limitation des cartes graphiques NVIDIA K2.

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 la fenêtre de Citrix Receiver

Si vous redimensionnez la fenêtre Citrix Receiver, 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)` ».

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.

```
/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.

```
/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 :

```
sudo yum -y install openldap

sudo yum -y install libxml2

sudo yum -y install cyrus-sasl

sudo yum -y install cyrus-sasl-gssapi
```

SLES/SELD :

```
sudo zypper install openldap2

sudo zypper install libxml2

sudo zypper install cyrus-sasl

sudo zypper install cyrus-sasl-gssapi
```

Ubuntu :

```
sudo apt-get install -y libldap-2.4-2

sudo apt-get install -y libsasl2-2

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. Ce paramètre est requis par le service de stratégie pour effectuer une recherche LDAP dans ces environnements.

Après l'installation du package Linux VDA, exécutez la commande suivante :

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

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 :

```
/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
```

Les stratégies suivantes s'appliquent uniquement au VDA Linux et peuvent uniquement être configurées dans Citrix Studio 7.12 et versions ultérieures :

- ClipboardSelectionUpdateMode
- PrimarySelectionUpdateMode
- MaxSpeexQuality

Ces stratégies sont décrites dans la liste des stratégies prises en charge. Si vous utilisez Citrix Studio version 7.11 ou une version ultérieure, vous devez configurer ces stratégies localement sur le VDA Linux à l'aide de la commande **ctxreg**.

> **Remarque :**
>
> Des plages de valeurs doivent être respectées. Pour des descriptions détaillées, consultez la liste

> des stratégies prises en charge.

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
Persistances ICA	SendICAKeepAlives	Ordinateur	ICA/Persistance	Ne pas envoyer de messages de persistance ICA (0)
Délai d'expiration de persistance ICA	ICAKeepAliveTimeout	Ordinateur	ICA/Persistance	60 secondes
Numéro de port de l'écouteur ICA	IcaListenerPortNumber	Ordinateur	ICA	1494
Limite de bande passante de redirection audio	LimitAudioBw	Utilisateur	Audio	0 kbps
Redirection audio cliente	AllowAudioRedirection	Utilisateur	Audio	Autorisé (1)
Redirection d'imprimante cliente	AllowPrinterRedir	Utilisateur	Impression	Autorisé (1)
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"

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Compression d'images en mouvement	MovingImageCompressionConfiguration	Utilisateur	Thinwire	Activé (1)
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)
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)
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	AllowMicrophoneRedir	Utilisateur	Audio	Autorisé (1)
Nombre maximum de sessions	MaximumNumberOfSessions	Ordinateur	Gestion de la charge	250
Tolérance d'ouvertures de session simultanées	ConcurrentLogonsTolerance	Ordinateur	Gestion de la charge	2
Activer la mise à jour automatique des contrôleurs	EnableAutoUpdateOfControllers	Ordinateur	Paramètres Virtual Delivery Agent	Autorisé (1)

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Mode de mise à jour de la sélection du Presse-papiers	ClipboardSelectionUpdateMode	Utilisateur	Presse-papiers	3
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	ICA/Redirection de fichier	Activé (1)
Lecteurs optiques clients	AllowCdromDrives	Utilisateur	ICA/Redirection de fichier	Autorisé (1)
Lecteurs fixes clients	AllowFixedDrives	Utilisateur	ICA/Redirection de fichier	Autorisé (1)
Lecteurs de disquette clients	AllowFloppyDrives	Utilisateur	ICA/Redirection de fichier	Autorisé (1)
Lecteurs réseau clients	AllowNetworkDrives	Utilisateur	ICA/Redirection de fichier	Autorisé (1)
Lecteurs amovibles clients	AllowRemoveableDrives	Utilisateur	ICA/Redirection de fichier	Autorisé (1)
Redirection de lecteur client	AllowDriveRedir	Utilisateur	ICA/Redirection de fichier	Autorisé (1)
Accès en lecture unique sur le lecteur client	ReadOnlyMappedDrive	Utilisateur	ICA/Redirection de fichier	Désactivé (0)

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

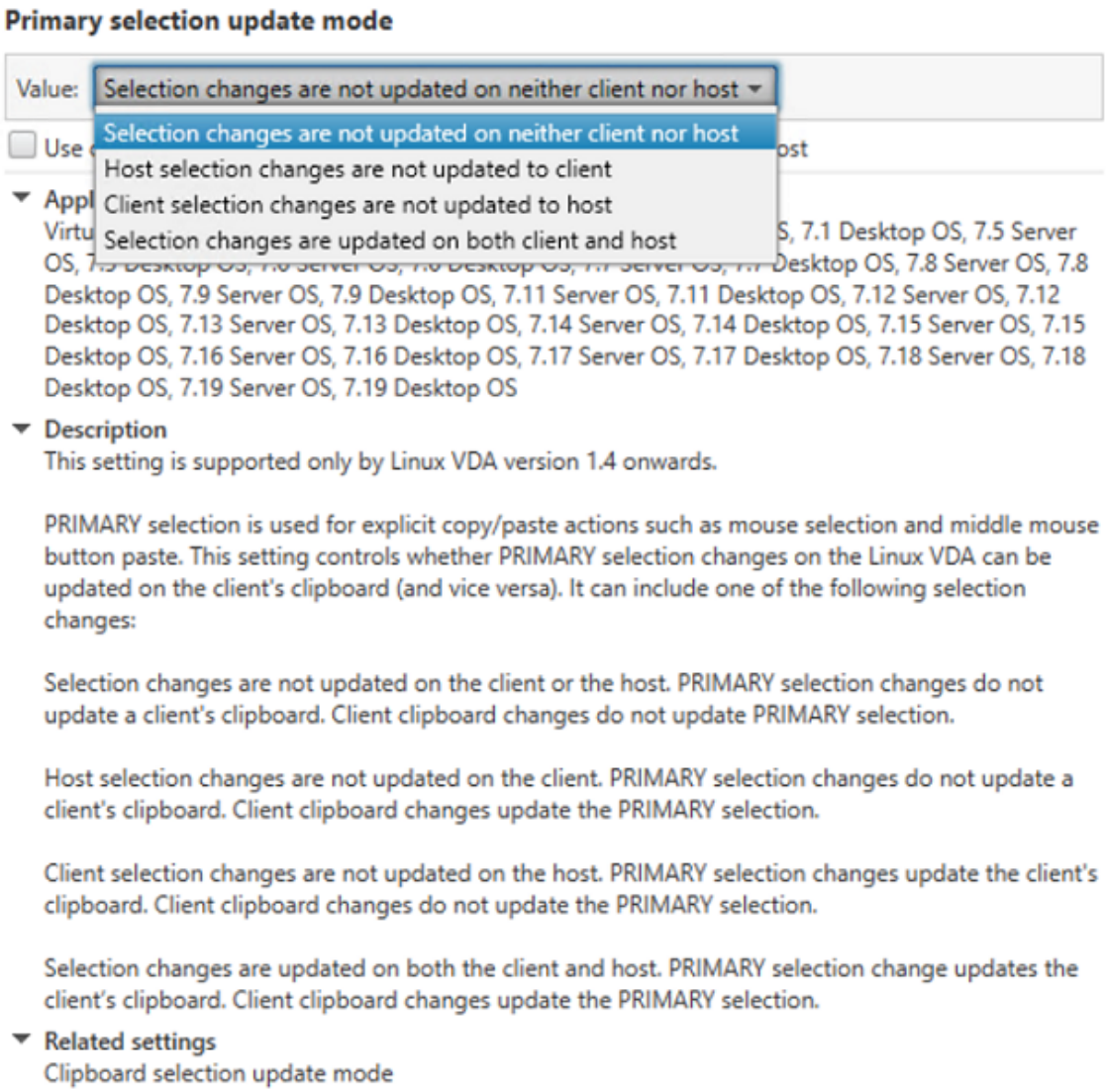
  Valeur (enum) : [0, 1, 2, 3]

  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 :



- **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

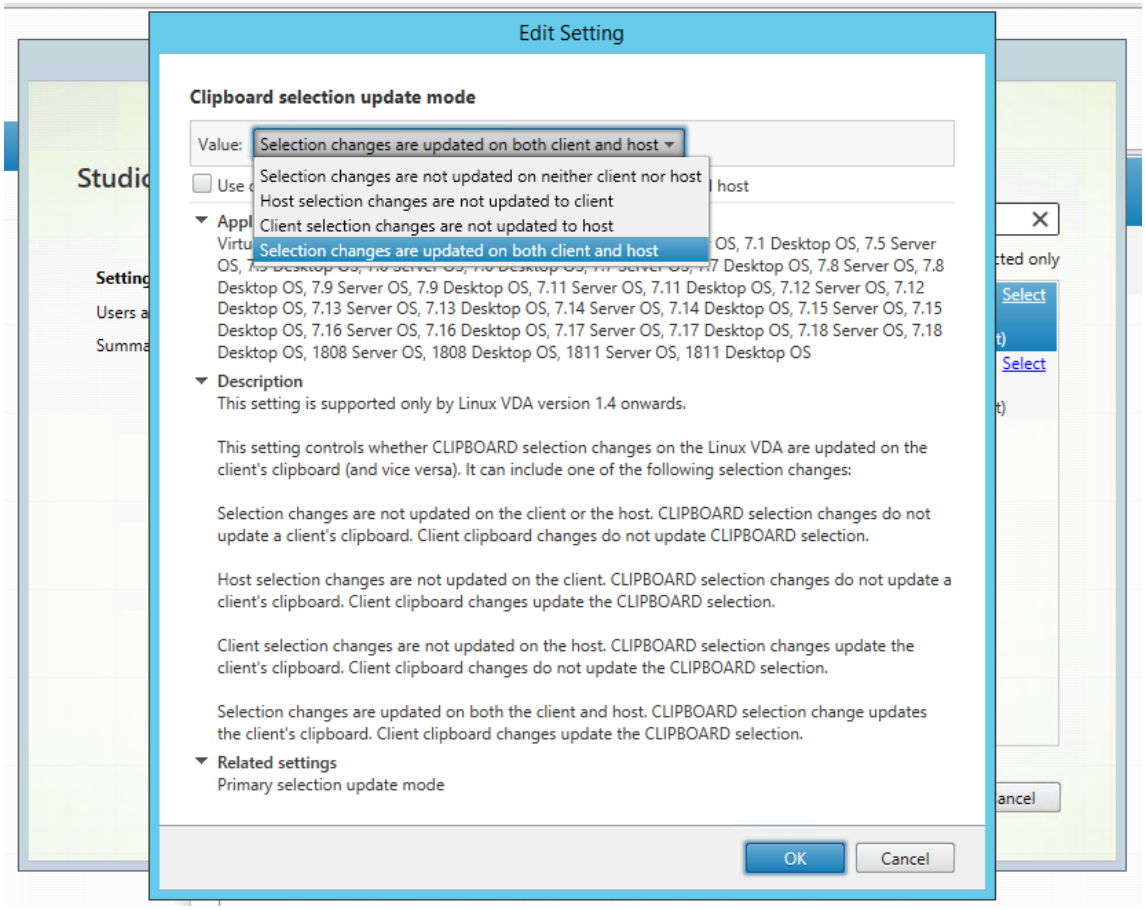
  Valeur (énumération) : [0, 1, 2, 3]

  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 VDA Linux prend en charge IPv6 pour s'aligner avec XenApp et XenDesktop. Lors de l'utilisation de cette fonctionnalité, considérez ce qui suit :

- Pour les environnements double pile, IPv4 est utilisé sauf si le protocole IPv6 est explicitement activé.
- Si le protocole IPv6 est activé dans un environnement IPv4, le Linux VDA ne fonctionnera pas.

> **Important :**
>
> - L'environnement réseau entier doit être IPv6, et pas uniquement pour le Linux VDA.
> - Centrify ne prend pas en charge IPv6 pur.

Aucune tâche de configuration spéciale n'est requise pour IPv6 lors de l'installation du Linux VDA.

Configurer le protocole IPv6 pour le Linux VDA

Avant de modifier la configuration du Linux VDA, assurez-vous que votre machine virtuelle Linux a précédemment fonctionné dans un réseau IPv6. Deux clés de registre sont associées à la configuration d'IPv6 :

```
1  " HKLM\Software\Policies\Citrix\VirtualDesktopAgent "  -t  " REG_DWORD "
     -v  " OnlyUseIPv6ControllerRegistration "
2
3  " HKLM\Software\Policies\Citrix\VirtualDesktopAgent "  -t  " REG_DWORD "
     -v  " ControllerRegistrationIPv6Netmask "
```


OnlyUseIPv6ControllerRegistration doit être défini sur 1 pour activer IPv6 sur Linux VDA :

```
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 :

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Policies\
    Citrix\VirtualDesktopAgent" -t "REG_SZ" -v "
    ControllerRegistrationIPv6Netmask " -d "{
 IPv6 netmask }
 " --force
```

Remplacez **{IPv6 netmask}** par le masque réseau réel (par exemple, 2000::/64).

Pour de plus amples informations sur le déploiement d'IPv6 dans XenApp et XenDesktop, consultez 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)

February 11, 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.

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.

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
    Citrix\CEIP" -v "CEIPSwitch" -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 :

```
/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

Point de données	Nom de la clé	Description
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
Dernière heure de redémarrage des services LVDA principaux	ctxhdx ctxvda	Dernière heure de redémarrage des services `ctxhdx` et `ctxvda`, au format jj-hh:mm:ss, par exemple, 10-17:22:19
Type de GPU	gpu_type	Indique le type de processeur graphique de la machine
Cœurs d'UC	cpu_cores	Entier indiquant le nombre de cœurs d'UC de la machine
Fréquence du processeur	cpu_frequency	Nombre flottant indiquant la fréquence du processeur en MHz
Taille de la mémoire physique	memory_size	Entier indiquant la taille de la mémoire physique en Ko
Nombre de sessions actives	active_session_number	Entier indiquant le nombre de sessions actives 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

Point de données	Nom de la clé	Description
Clé de session	session_key	Identification de la session d'où les données proviennent
Coût de reconnexion	econnect_time_cost	Utilisé pour enregistrer le coût en temps de reconnexion de la session. La taille du tableau est de 5. Il assure le suivi de la valeur courante, la valeur minimale, la valeur maximale, le cumul et le nombre de mises à jour de ce point de données.
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 de Citrix Receiver utilisé pour lancer la session
Version du client Receiver	receiver_version	Chaîne de texte indiquant la version de Citrix Receiver utilisée pour lancer la session
Nombre d'impressions	printing_count	Entier indiquant le nombre de fois que la session utilise la fonction d'impression
Nombre de redirections USB	usb_redirecting_count	Entier indiquant le nombre de fois que la session utilise un périphérique USB

Configurer la redirection USB

September 23, 2024

Les périphériques USB sont partagés entre Citrix Receiver et le bureau VDA Linux. Lorsqu'un périphérique USB a été redirigé sur le bureau, l'utilisateur peut utiliser le périphérique USB comme s'il était connecté localement.

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 VDA Linux et Citrix Receiver 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 :

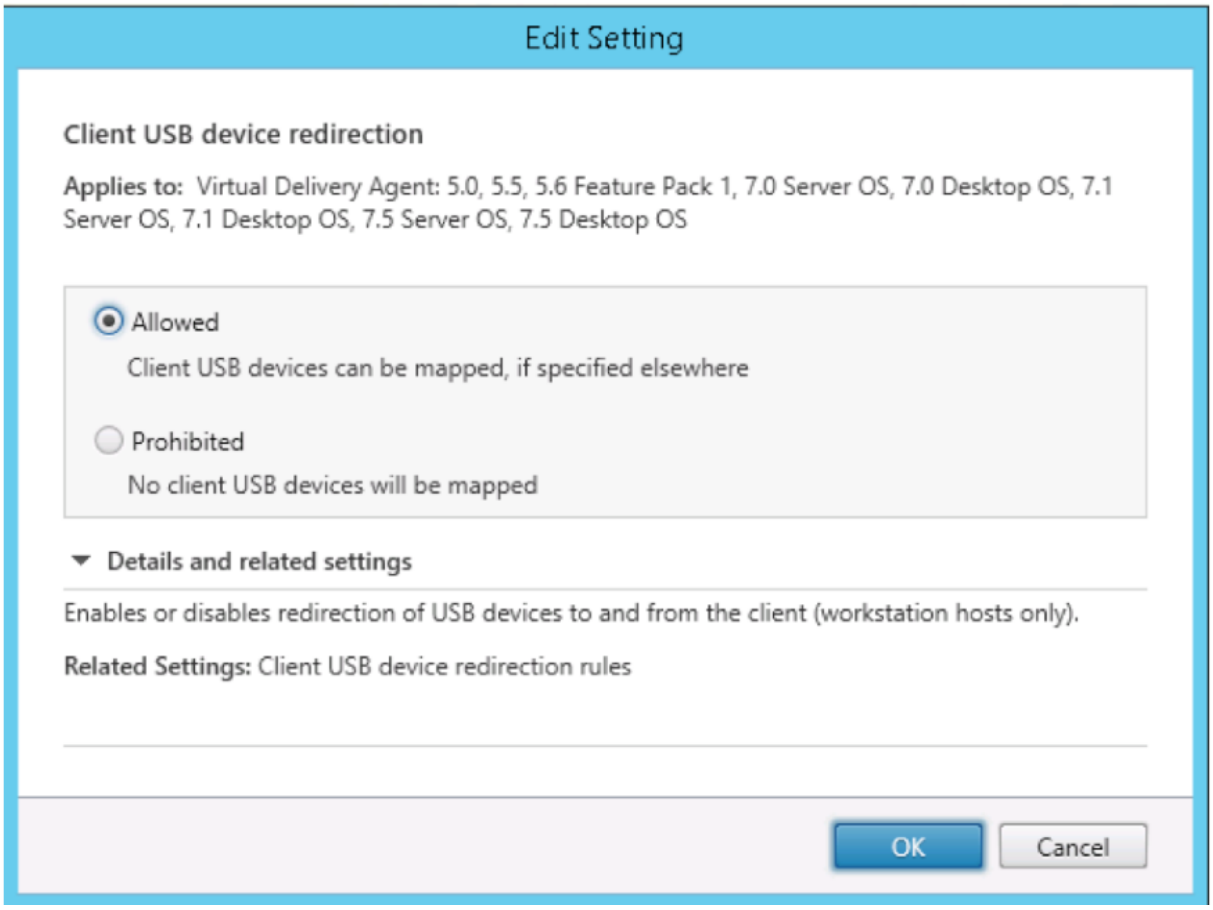
- Stratégie de redirection de périphérique USB client
- Règles de redirection de périphérique USB client

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**.

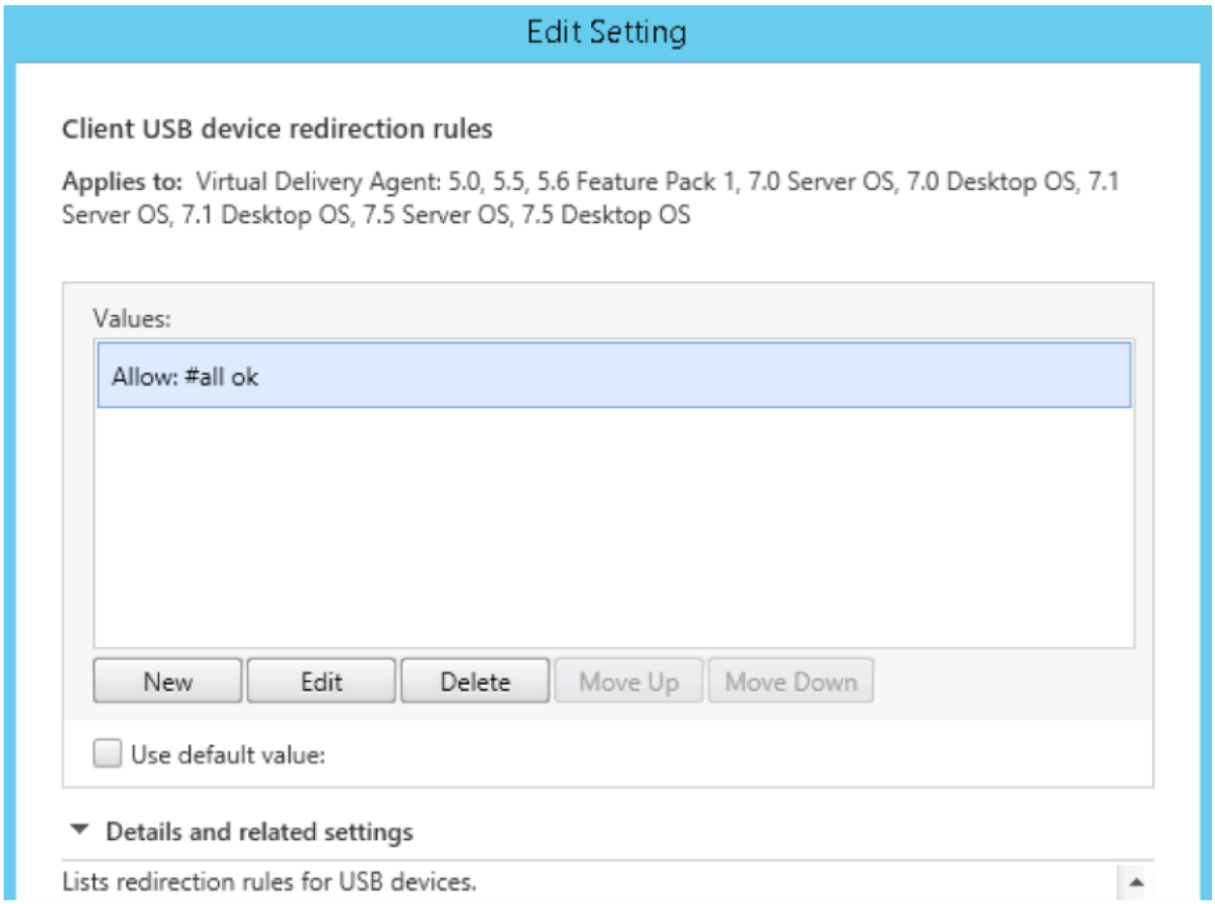


Définir des règles de redirection USB

Après activation de la stratégie de redirection USB, définissez les règles de redirection à l'aide de Citrix Studio en spécifiant les périphériques qui sont autorisés (ou interdits) sur le Linux VDA.

Dans la boîte de dialogue Règles de redirection de périphérique USB client :

1. Cliquez sur **Nouveau** pour ajouter une règle de redirection, ou cliquez sur **Modifier** pour vérifier une règle existante.
2. Après avoir créé (ou modifié) une règle, cliquez sur **OK**.



Pour de plus amples informations sur la configuration de la redirection USB générique, reportez-vous au Guide de configuration de la redirection USB générique Citrix.

Créer le module noyau VHCI

La redirection USB dépend des modules du noyau VHCI (**usb-vhci-hcd.ko** et **usb-vhci-iocif.ko**). Ces modules font partie de la distribution de Linux VDA (inclus dans le package RPM). Ils sont compilés selon les noyaux de distribution Linux officiels et sont indiqués dans le tableau suivant :

Distribution Linux prise en charge	Version du noyau
RHEL 7.3	3.10.0-514.el7.x86_64
RHEL 6.6	2.6.32-504.el6.x86_64
SUSE 12.2	4.4.49-92.11-default
SUSE 11.4	3.0.101-0.47.55-default
Ubuntu 16.04	4.4.0-45-generic

> **Important :**
>
> Si le noyau de votre machine n'est pas compatible avec le pilote créé par Citrix pour les Linux VDA, le service USB peut ne pas parvenir à démarrer. Dans ce cas, vous pouvez utiliser la fonctionnalité de redirection USB uniquement si vous créez vos propres modules noyau VHCI.

Vérifier que votre noyau est cohérent avec les modules créés par Citrix

Sur la ligne de commande, exécutez la commande suivante pour vérifier si le noyau est cohérent :

```
insmod /opt/Citrix/VDA/lib64/usb-vhci-hcd.ko
```

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. Restaurez les fichiers depuis le fichier citrix-linux-vda-sources.zip ; les fichiers source VHCI sont disponibles dans **linux-vda-souces/vhci-hcd-1.15.tar.bz2** ; vous pouvez restaurer les fichiers 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 7.3/RHEL 6.9/RHEL 6.6 :

   ```
   yum install kernel-devel
   ```

   SUSE 12.2 :

   ```
   zypper install kernel-devel

   zypper install kernel-source
   ```

   SUSE 11.4 :

   ```
   zypper install kernel-source
   ```


Ubuntu 16.04 :

```
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 lez noyau pour obtenir ce fichier (par exemple, `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. Dans le fichier **vhci-hcd-1.15/Makefile**, modifiez le fichier Makefile de VCHI et définissez KDIR sur le répertoire du noyau :

```
#KDIR = $(BUILD_PREFIX)/lib/modules/$(KVERSION)/build

KDIR = /usr/src/kernels/3.10.0-327.10.1.el7.x86_64
```

6. 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/**.

7. Remplacez le module du noyau par celui qui vient d'être créé : **cp -f usb-vhci-*.ko /opt/Citrix/VDA/lib64/**
8. Redémarrez le service USB : **service ctxusbsd restart**
9. Fermez, puis rouvrez la session. Vérifiez si la redirection USB fonctionne.

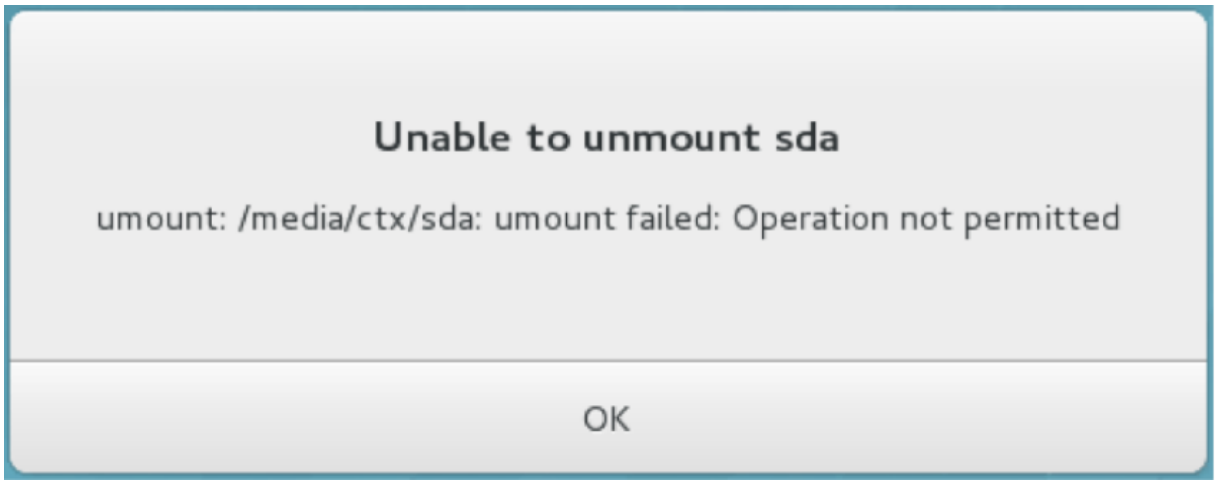
Résolution des problèmes de redirection USB

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

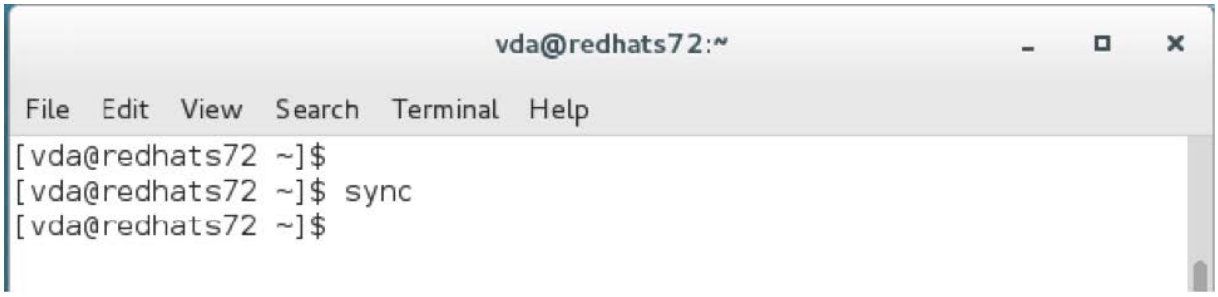
Pour le contrôle d'accès de tous les disques USB redirigés à partir de Citrix Receiver, le VDA Linux gère tous ces périphériques sous privilèges d'administrateur afin de garantir que seul le propriétaire peut

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

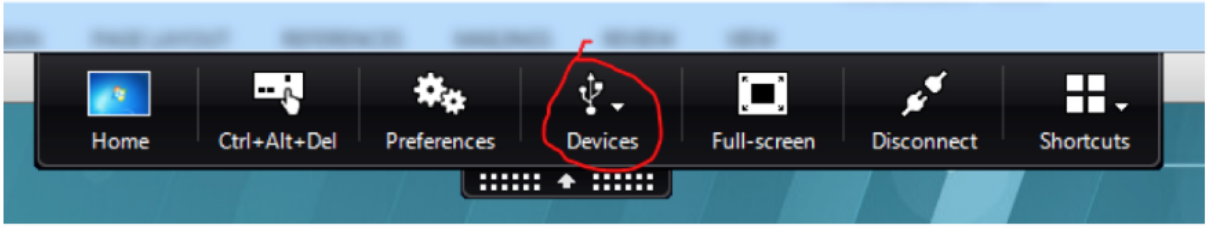
Si vous redirigez un disque USB dans une session, essayez de le modifier (par exemple, en créant des fichiers sur le disque), puis arrêtez de le rediriger immédiatement à l'aide de la barre d'outils de Citrix Receiver, le fichier que vous avez modifié ou créé peut être perdu. Ce problème se produit car, 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 Citrix Receiver, 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 syncdans un terminal pour purger les données vers le disque avant d'arrêter la redirection USB.



Aucun périphérique dans la barre d'outils de Citrix Receiver

Dans certains cas, vous ne pouvez pas voir les périphériques figurant sur la barre d'outils de Citrix Receiver, 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 Citrix Receiver pour Linux.

Affichage des périphériques USB dans la barre d'outils de Citrix Receiver, mais avec la mention *Limité par une stratégie*, ce qui entraîne l'échec de la redirection

Ce problème se produit en raison de la configuration de la stratégie du périphérique. Dans ce cas, 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 Citrix Receiver. Un périphérique peut être bloqué par le paramètre de registre de Citrix Receiver. 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. Parfois, cependant, d'autres types de périphériques peuvent être redirigés vers une session Linux VDA active. Dans ce cas, pour chaque périphérique redirigé, 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 Linux VDA configure et monte le disque. L'utilisateur (et seul l'utilisateur qui l'a installé) peut accéder au disque sans aucune configuration supplémentaire.

> Cela peut ne pas être possible avec les périphériques qui ne se trouvent pas dans la liste des périphériques pris en charge.

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 XenDesktop ou XenApp comme vous le faites d'habitude.

Modifiez votre méthode d'entrée conformément à ce qui est requis sur le client pour commencer à utiliser à l'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.
- L'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.
- L'éditeur IME client n'est pas pris en charge dans une distribution SUSE 11.

HDX Insight

February 9, 2024

Vue d'ensemble

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 NVIDIA ou Citrix SD-WAN.

Dans cette version, le VDA Linux prend partiellement en charge la fonctionnalité HDX Insight. Étant donné que la fonctionnalité EUEM (Gestion de l'expérience des utilisateurs) n'est pas implémentée, les points de données liés à la durée ne sont pas disponibles.

Installation

Aucun package dépendant ne doit être installé.

Utilisation

HDX Insight analyse les messages ICA transmis via NetScaler entre l'application Citrix Workspace et le VDA Linux.

Vous devez configurer un déploiement NetScaler Insight Center avec le Linux VDA et activer la fonctionnalité HDX Insight. Vous pouvez migrer votre déploiement de NetScaler Insight Center vers Citrix ADM sans perdre la configuration, les paramètres ou les données existants. Pour plus d'informations, consultez Migrer de NetScaler Insight Center vers Citrix ADM.

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 activée sur NetScaler, ou une instance incorrecte de NetScaler est configurée sur Insight Center.

- 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.

Problème connu

Impossible d'afficher les points de données liés à la durée. Étant donné que la fonctionnalité de suivi de l'expérience utilisateur n'est pas implémentée, les points de données liés à la durée (tels que la durée des boucles ICA) ne sont pas disponibles et s'affichent comme S/O.

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 :


```
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 :

```
setlog values

log_path (Log Output Path) = /var/log/xdl/hdx.log

log_size (Max Log Size (MiB)) = 200

log_count (Max Old Log Files) = 2
```

Afficher ou définir une valeur `setlog` unique :

```
setlog value <name> [<value>]
```

Par exemple :

```
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 :

```
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 :

```
setlog level <class> [<level>]
```

La variable **<class>** spécifie un composant de l'agent Linux VDA. Pour couvrir tous les composants, définissez-la sur tous :

```
setlog level all error

Setting log class ALL to ERROR.
```

Indicateurs Par défaut, les indicateurs sont définis comme suit :

```
setlog flags

DATE = true

```



```
TIME = true

NAME = true

PID = true

TID = false

SID = true

UID = false

GID = false

CLASS = false

LEVEL = false

FUNC = true

FILE = false
```

Afficher les indicateurs actuels :

```
setlog flags
```

Afficher ou définir un indicateur de journalisation unique :

```
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 :

```
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. Citrix recommande aux utilisateurs root de ne pas accorder l'accès en écriture à d'autres utilisateurs. Si cette consigne n'est pas respectée, `ctxlogd` peut être configuré de manière arbitraire ou malveillante, ce qui peut affecter les performances des serveurs et par conséquent l'expérience utilisateur.

Résolution des problèmes

Le démon `ctxlogd` échoue et vous ne pouvez pas redémarrer le service `ctxlogd` lorsque le fichier **/var/xdl/.ctxlog** est manquant (s'il a été supprimé accidentellement par exemple).

/var/log/messages :

```
Apr 1 02:28:21 RH72 citrix-ctxlogd[17881]: Failed to open logging configuration file.

Apr 1 02:28:21 RH72 systemd: ctxlogd.service: main process exited, code=exited, status=1/FAILURE

Apr 1 02:28:21 RH72 systemd: Unit ctxlogd.service entered failed state.

Apr 1 02:28:21 RH72 systemd: ctxlogd.service failed.
```

Pour résoudre ce problème, exécutez `setlog` en tant qu'utilisateur racine pour créer le fichier **/var/xdl/.ctxlog**. Redémarrez le service `ctxlogd` dont dépendent d'autres services.

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 prélancement de session n'est pas non plus pris en charge sur Citrix Receiver 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 XenApp et XenDesktop.

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 :

```
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 :

```
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):

```
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** :

```
ps uax | grep nscd
cat /etc/nscd.conf | grep 'passwd' | grep 'enable-cache'
```


Définissez la variable du cache **passwd** sur **no** s'il est activé, puis redémarrez le service **ncsd**. Vous devrez peut-être réinstaller le Linux VDA après la modification de cette configuration.

- **Le bouton de l'écran de verrouillage est affiché dans une session non authentifiée avec KDE**.

Le bouton et le menu de l'écran de verrouillage sont désactivés par défaut dans une session non authentifiée. Toutefois, ils peuvent toujours être visibles dans KDE. Dans KDE, pour désactiver le bouton et le menu de l'écran de verrouillage pour un utilisateur spécifique, ajoutez les lignes suivantes au fichier de configuration **$Home/.kde/share/config/kdeglobals**. Par exemple :

```
[KDE Action Restrictions]
action/lock_screen=false
```

Toutefois, si le paramètre **KDE Action Restrictions** est configuré comme non modifiable dans un fichier **kdeglobals** global 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** global pour supprimer la balise **\$i]** dans la section **KDE Action Restrictions** ou utilisez directement la configuration 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/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 pour Linux VDA, exécutez le script suivant (vous devez être connecté en tant qu'administrateur) :

La syntaxe de cette commande comprend les éléments suivants :

- Activer LDAP sur SSL/TLS avec le certificat d'autorité de certification racine fourni :

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enable pathToRootCA
```

- Retour à LDAP sans SSL/TLS

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Disable
```

Le keystore Java dédié à LDAPS se trouve dans **/etc/xdl/.keystore**. Clés de registre affectées :

```
HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServers

HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServersForPolicy

HKLM\Software\Citrix\VirtualDesktopAgent\UseLDAPS

HKLM\Software\Policies\Citrix\VirtualDesktopAgent\Keystore
```

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 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** et **smb.conf**. Modifiez les fichiers comme suit :


```
ldap.conf:

TLS_REQCERT never

smb.conf:

ldap ssl = start tls

ldap ssl ads = yes

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** :

```
smb.conf:

ldap ssl = off

ldap ssl ads = no

client ldap sasl wrapping = seal
```

Centrify

Centrify ne prend pas en charge LDAPS sur le port 636. Toutefois, il fournit un cryptage sécurisé sur le port 389. Pour de plus amples informations, consultez le site Centrify.

Quest

Quest Authentication Service ne prend pas en charge LDAPS sur le port 636, mais il offre un cryptage sécurisé sur le port 389 à l'aide d'une autre méthode.

Résolution des problèmes

Les problèmes suivants peuvent se produire lors de l'utilisation de cette fonctionnalité :

- **Disponibilité du service LDAPS**

  Vérifiez que la connexion LDAPS est disponible sur le serveur AD/LDAP. Le port par défaut est 636.

- **Échec de l'enregistrement du Linux VDA lorsque LDAPS est activé**

Vérifiez que le serveur LDAP et les ports sont configurés correctement. Vérifiez le certificat d'autorité de certification racine et assurez-vous qu'il correspond au serveur AD/LDAP.

- **Modification incorrecte du registre effectuée accidentellement**

  Si 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. En général, 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. Citrix recommande le format PEM codé en base64 si vous rencontrez un problème avec le format du certificat.

- **Impossible d'afficher le certificat d'autorité de certification racine avec la commande -list de Keytool**

  Lorsque vous activez LDAPS en exécutant **/opt/Citrix/VDA/sbin/enable_ldaps.sh**, le certificat est importé sur /etc/xdl/.keystore, et le mot de passe est défini pour protéger le keystore. Si vous avez oublié le mot de passe, vous pouvez réexécuter le script pour créer un keystore.

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 :

```
# xauth -f ~/.Xauthority

# > list

# > 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 :

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "
    XauthEnabled" -d "0x00000001" --force

sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "ListenTCP"
     -d "0x00000001" --force
```


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 à Xauthority. Pour un exemple, reportez-vous à la commande suivante :

  ```
  export DISPLAY={
  Display number stored in the Xauthority file }


  export XAUTHORITY={
  the file path of .Xauthority }
  ```

  > **Remarque :**
  >
  > Si la variable d'environnement `XAUTHORITY` n'est pas définie, le fichier `~/.Xauthority` est utilisé par défaut.

- Transmettre le fichier `.Xauthority` à XClient en montant un répertoire de base partagé

  La façon la plus pratique consiste à monter un répertoire de base partagé pour la session utilisateur. Lorsque le Linux VDA démarre une session ICA, le fichier `.Xauthority` est créé dans le répertoire de base de la session utilisateur. Si ce répertoire de base est partagé avec le XClient, l'utilisateur n'a pas besoin de transmettre manuellement ce fichier `.Xauthority` à XClient. Après avoir correctement défini les variables d'environnement DISPLAY et XAUTHORITY, l'interface utilisateur est affichée dans le bureau XServer automatiquement.

Résolution des problèmes

Si Xauthority ne fonctionne pas, suivez la procédure de dépannage ci-dessous :

1. En tant qu'administrateur avec privilège root, récupérez tous les cookies Xorg :

   ```
   ps aux | grep -i xorg
   ```

   Cette commande affiche le processus Xorg et les paramètres transmis à Xorg lors du démarrage. Un autre paramètre affiche le fichier `.Xauthority` utilisé. Par exemple :

   ```
   /var/xdl/xauth/.Xauthority110
   ```

   Affichez les cookies à l'aide de la commande **Xauth** :


```
Xauth -f /var/xdl/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 :

   ```
   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.