CITRIX

Linux Virtual Delivery Agent 1811

Contents

Nouveautés

February 15, 2019

Nouveautés dans la version 1811

La version 1811 du VDA Linux comprend les nouvelles fonctionnalités et améliorations suivantes :

Codage matériel HDX 3D Pro

Auparavant disponible en tant que fonctionnalité expérimentale, l'ajustement des débits moyens en fonction des estimations de bande passante est désormais entièrement pris en charge. En outre, l'amélioration de la netteté est également prise en charge désormais. Pour plus d'informations, voir Configurer les graphiques.

Transfert de fichiers

Cette version prend en charge les transferts de fichiers entre le VDA Linux et le périphérique client. Cette fonctionnalité est disponible lorsque le périphérique client exécute un navigateur Web qui prend en charge l'attribut sandbox HTML5. L'attribut sandbox HTML5 permet aux utilisateurs d'accéder à des bureaux virtuels ou à des applications de navigateur Web à l'aide de l'application Citrix Workspace pour HTML5 ou de l'application Citrix Workspace pour Chrome. Pour plus d'informations, consultez la section Transfert de fichiers.

Clavier logiciel

À compter de cette version, la fonctionnalité de clavier logiciel est disponible dans une session d'application ou de bureau virtuel Linux. Le clavier logiciel s'affiche ou se masque automatiquement lorsque vous accédez à un champ de saisie ou le quittez. Pour plus d'informations, consultez la section Clavier logiciel.

Authentification Single Sign-On double-hop

À compter de cette version, vous pouvez utiliser l'application Citrix Workspace pour Linux et Citrix Receiver pour Linux 13.10 pour accéder à des bureaux et applications virtuels à partir d'une session de bureau virtuel Linux, sans entrer les informations d'identification de l'utilisateur une deuxième fois. Pour plus d'informations, consultez la section Authentification Single Sign-On double-hop.

Modifications apportées à la configuration système requise

- Dans cette version, RHEL6.10 et CentOS 6.10 sont pris en charge. Pour plus d'informations, consultez la section Configuration système requise.
- La nouvelle dépendance suivante a été ajoutée pour SUSE 12 :

```
ibus >= 1.5
```

> **Remarque :**
>
> pour empêcher la mise à jour de vos packages logiciels vers les versions correspondantes dans RHEL 7.6 et CentOS 7.6, exécutez la commande `echo '7.5' > /etc/yum/vars/releasever` avant d'installer le package VDA Linux.

Problèmes résolus

January 11, 2019

Par rapport à : Linux Virtual Delivery Agent 1808

Linux Virtual Delivery Agent 1811 contient les correctifs suivants :

- Les processus de bureau tiers peuvent écraser et provoquer ainsi des paramètres de clavier incorrects sur le VDA Linux. [LC9906]
- Les processus de canal virtuel ne peuvent pas démarrer lorsque le démon CTXLog (ctxlogd) déclenche un signal SIGPIPE. [LC8760]
- Les processus de canal virtuel ne peuvent pas démarrer lorsque le numéro DISPLAY d'une session est 0. [LD0353]
- IME ne fonctionne pas sur les plates-formes Ubuntu. [LD0598]

Problèmes connus

January 11, 2019

Les problèmes suivants ont été identifiés dans cette version :

- Une fenêtre inattendue apparaît lors du téléchargement de fichier. La fenêtre n'affecte pas la fonctionnalité de téléchargement de fichier et disparaît automatiquement après un certain temps. [LNXVDA-5646]

- Les paramètres par défaut de PulseAudio provoquent la fermeture du programme du serveur audio après 20 secondes d'inactivité. Lorsque PulseAudio se termine, le son ne fonctionne pas. Pour contourner ce problème, définissez exit-idle-time=-1 dans le fichier /etc/pulse/daemon.conf. [LNXVDA-5464]
- libtcmalloc 4.3.0 dans SUSE 12.3 peut provoquer la fermeture inattendue des processus.
- Le service ctxhdx peut se fermer de manière inattendue sur les VDA Ubuntu 16.04 et SUSE 12.3. Le problème se produit avec les versions 2.22 à 2.24 de la bibliothèque GNU C (glibc). Le problème est résolu dans la glibc 2.25. Si vous utilisez la distribution SUSE 12.3, vous pouvez installer le correctif fourni par SUSE pour résoudre le problème. Aucune correction n'est disponible pour Ubuntu 16.04 au moment de la publication de Linux VDA 7.17. [LNXVDA-4481]
- Les sessions ne peuvent pas être lancées dans l'application Citrix Workspace pour Linux lorsque le cryptage SSL est activé. [RFLNX-1557]
- Le processus indicator-datetime-service n'utilise pas la variable d'environnement $TZ. Lorsque le client et la session se trouvent dans des fuseaux horaires différents, le panneau Unity sur un bureau Unity Ubuntu 16.04 n'affiche pas l'heure du client. [LNXVDA-2128]
- Graphiques Ubuntu : dans HDX 3D Pro, un cadre noir peut apparaître autour des applications après le redimensionnement de Desktop Viewer, ou dans certains cas, l'arrière-plan peut s'afficher en noir.
- Il est possible que les imprimantes créées par la redirection d'impression de Linux VDA ne puissent pas être supprimées après la fermeture d'une session.
- Les fichiers CDM sont absents lorsqu'un répertoire contient de nombreux fichiers et sous-répertoires. Ce problème peut se produire si le client a trop de fichiers ou de répertoires.
- Dans cette version, seul l'encodage UTF-8 est pris en charge pour les langues autres que l'anglais.
- L'état du verrouillage des majuscules de l'application Citrix Workspace pour Android peut être inversé lors de l'itinérance de session. L'état de CAPS VERR peut être perdu lors de l'itinérance d'une connexion existante à l'application Citrix Workspace pour Android. Pour résoudre le problème, utilisez la touche MAJ sur le clavier étendu pour basculer entre les majuscules et les minuscules.
- Les raccourcis ALT ne fonctionnent pas toujours lors d'une connexion à un VDA Linux à l'aide de l'application Citrix Workspace pour Mac. L'application Citrix Workspace pour Mac envoie AltGr pour les touches Options/Alt droite et gauche par défaut. Vous pouvez modifier ce comportement dans les paramètres de l'application Citrix Workspace, mais les résultats varient selon les applications .
- L'enregistrement échoue lorsque le VDA Linux 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.
- L'application Citrix Workspace pour Windows peut rencontrer une distorsion audio lors de l'enregistrement audio.

Avis de tiers

January 11, 2019

Linux Virtual Desktop version 1811 (PDF)

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

Configuration système requise

January 11, 2019

Distributions Linux

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

Linux VDA prend en charge les distributions Linux suivantes :

- SUSE Linux Enterprise :
  - Desktop 12 Service Pack 3
  - Server 12 Service Pack 3
- Red Hat Enterprise Linux
  - Workstation 7.5
  - Workstation 6.10
  - Workstation 6.9
  - Server 7.5
  - Server 6.10
  - Server 6.9
- CentOS Linux
  - CentOS 7.5
  - CentOS 6.10
  - CentOS 6.9
- Ubuntu Linux
  - Ubuntu Desktop 16.04
  - Serveur Ubuntu 16.04
- Pardus Linux
  - Pardus 17 (pour plus d'informations sur l'étendue des fonctionnalités prises en charge, consultez l'article CTX238492 du centre de connaissances).

> **Remarque :**
>
> pour empêcher la mise à jour de vos packages logiciels vers les versions correspondantes dans RHEL 7.6 et CentOS 7.6, exécutez la commande `echo '7.5' > /etc/yum/vars/releasever` avant d'installer le package VDA Linux.

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

Distribution Linux	Version Xorg
RHEL 7.5, CentOS 7.5	1.19 (1.19.3-11.el7_4.1 et versions ultérieures)
RHEL 6.10/6 .9, CentOS 6.10/6 .9	1.17

Distribution Linux	Version Xorg
Ubuntu 16.04	1.18
SUSE 12.3	1.18

N'utilisez pas le serveur hwe xorg 1.19 sur Ubuntu.

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

Citrix Virtual Desktops

Le VDA Linux est compatible avec toutes les versions actuellement prises en charge de Citrix Virtual Desktops. Pour de plus amples informations sur le cycle de vie des produits Citrix Virtual Desktops et savoir quand Citrix arrête la prise en charge de versions spécifiques des produits, consultez le tableau du cycle de vie des produits Citrix.

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

Environnements de virtualisation et plates-formes hôte pris en charge

- XenServer
- VMware ESX et ESXi
- Microsoft Hyper-V
- Nutanix AHV
- Microsoft Azure Resource Manager
- services Web Amazon (AWS)

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

Hyperviseurs

- XenServer
- VMware ESX et ESXi
- Nutanix AHV

> **Remarque** les hyperviseurs sont compatibles avec certaines distributions Linux.

Processeur graphique

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

- NVIDI GTX750Ti
- NVIDIA GRID™ 3.0 - Tesla M60
- NVIDIA GRID™ - K2
- NVIDIA GRID™ - Tesla P40

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

- NVIDIA GRID™ 3.0 - Tesla M60
- NVIDIA GRID™ 3.0 - Tesla M10
- NVIDIA GRID™ - Tesla P40

Configurer Delivery Controller

February 15, 2019

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

Mettre à jour la configuration d'un Delivery Controller

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

- CTX142438 : correctif Update 2 - pour Delivery Controller 7.6 (32 bits) – Anglais
- CTX142439 : correctif 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 VDA Linux 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\BrokerServic**

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
```

Présentation de l'installation

January 11, 2019

> **Remarque :**
>
> pour empêcher la mise à jour de vos packages logiciels vers les versions correspondantes dans RHEL 7.6 et CentOS 7.6, exécutez la commande `echo '7.5' > /etc/yum/vars/releasever` avant d'installer le package VDA Linux.

Il existe trois options pour installer le VDA Linux :

- Easy Install. Après l'installation du package VDA Linux sur une machine, vous pouvez configurer l'environnement d'exécution à l'aide du script ctxinstall.sh. Pour de plus amples informations, consultez la section Easy Install.
- MCS. Vous pouvez utiliser MCS pour créer des machines virtuelles Linux par lots où le package VDA Linux est également installé. Pour plus d'informations, consultez la section Utiliser MCS pour créer des machines virtuelles Linux.

  > **Remarque :** n'utilisez pas Easy Install sur la VM modèle lorsque vous utilisez MCS pour créer des machines virtuelles Linux.

- Installation manuelle. Vous pouvez suivre les étapes générales suivantes pour installer le VDA Linux. Les variantes et commandes spécifiques sont documentées par la distribution. Pour plus d'informations, voir Installer Virtual Delivery Agent Linux pour RHEL/CentOS, Installer Virtual Delivery Agent Linux pour SUSE et Installer Virtual Delivery Agent Linux pour Ubuntu.

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

Easy Install

February 15, 2019

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

> **Remarque :**
>
> n'utilisez pas Easy Install sur la VM modèle lorsque vous utilisez MCS pour créer des machines virtuelles Linux.

Distributions prises en charge

	Winbind	SSSD	Centrify
RHEL 7.5	Oui	Oui	Oui
RHEL 6.10	Oui	Oui	Oui
RHEL 6.9	Oui	Oui	Oui
CentOS 7.5	Oui	Oui	Oui
CentOS 6.10	Oui	Oui	Oui
CentOS 6.9	Oui	Oui	Oui
Ubuntu 16.04	Oui	Oui	Oui
SUSE 12.3	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 VDA Linux
   Accédez au site Web Citrix et téléchargez le package VDA Linux en fonction de la distribution Linux appropriée.
3. Définissez l'environnement d'exécution afin de terminer l'installation du VDA Linux.

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 VDA Linux 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 VDA Linux, 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 Window sont installés.

Notions importantes

- 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 VDA Linux.
  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.

  Journal :

```
1  ADSITE    : Check that this machine's subnet is in a site known by
       AD    : Failed
2            : This machine's subnet is not known by AD.
```



```
3            : We guess you should be in the site Site1.
```

Ce problème est 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**.

- Easy Install prend en charge IPv6 pur à partir de la version 7.16 de Linux VDA. Cette amélioration dispose de la condition préalable et de la limite suivantes :
  - Vous devez configurer votre référentiel Linux pour vous assurer que votre machine peut télécharger les packages requis dans des environnements IPv6 purs.
  - Centrify n'est pas pris en charge dans les réseaux IPv6 purs.

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

- Si vous choisissez Centrify comme méthode pour rejoindre un domaine, le script ctxinstall.sh 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 VDA Linux, 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
```

Étape 3 : installer le package VDA Linux

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

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 VDA Linux, 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 du VDA Linux.
- **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 VDA Linux 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 VDA Linux requiert une liste séparée par des espaces de noms de domaines complets. 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 VDA Linux 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 (par défaut, les ports 80 et 1494) dans le pare-feu du système pour Linux Virtual Desktop.
- **CTX_XDL_HDX_3D_PRO**=Y | N : Linux Virtual Desktop prend en charge HDX 3D Pro, un ensemble de technologies d'accélération des graphiques conçues pour optimiser la virtualisation des applications riches en graphiques. HDX 3D Pro nécessite l'installation d'une carte graphique NVIDIA GRID compatible. 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. HDX 3D Pro n'est pas pris en charge sur SUSE. Assurez-vous que la valeur est définie sur N pour une plate-forme SUSE.
- **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 VDA Linux détecte 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, la valeur peut être définie sur **<none>**.
- **CTX_XDL_LDAP_LIST**=list-ldap-servers : le VDA Linux envoie une requête au 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, la valeur peut être définie sur **<none>**.
- **CTX_XDL_SEARCH_BASE**=search-base-set : le VDA Linux 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, la valeur peut être définie sur **<none>**.
- **CTX_XDL_FAS_LIST** = list-fas-servers : les serveurs du service d'authentification fédérée (FAS) sont configurés via la stratégie de groupe AD. Comme le VDA Linux ne prend pas en charge la stratégie de groupe AD, vous pouvez fournir une liste de serveurs FAS séparés par des points-virgules. La séquence doit être la même que celle configurée dans la stratégie de groupe AD. Si une adresse de serveur est supprimée, remplissez son espace vide avec la chaîne de texte **<none>** et conservez la séquence d'adresses du serveur sans effectuer de modification.
- **CTX_XDL_START_SERVICE**=Y | N : indique si les services VDA Linux 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_FAS_LIST = list-fas-servers | '<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.

Éventuellement, vous pouvez spécifier les paramètres en utilisant 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_FAS_LIST = list-fas-servers \

CTX_XDL_START_SERVICE=Y|N \

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

Résolution des problèmes

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

Impossible de joindre un domaine en utilisant SSSD

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

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

/var/log/xdl/vda.log :

```
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. sudo apt-get update
2. 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.

```

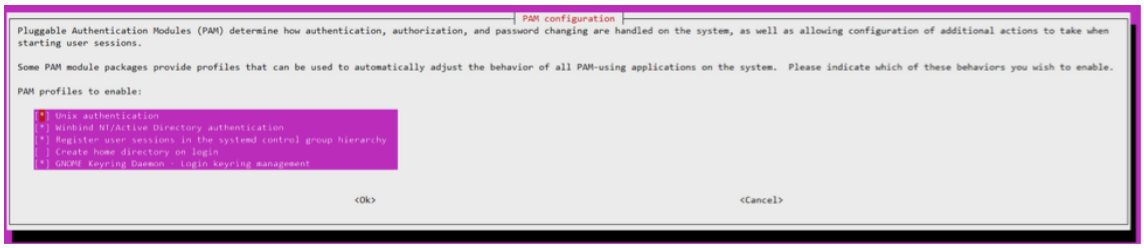


```
2016-11-02 13:21:59.217 <P22449:S1> citrix-ctxgfx: main: Exiting
    normally.
```

> **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.

```



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

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

```
1  Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] pid.c:
       Stale PID file, overwriting.
2
3  Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] bluez5-
       util.c: Failed to get D-Bus connection: Did not receive a reply.
       Possible causes include: the remote application did not send a reply
       , the message bus security policy blocked the reply, the reply
       timeout expired, or the network connection was broken.
4
5  Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] hashmap
       .c: Assertion 'h' failed at pulsecore/hashmap.c:116, function
       pa_hashmap_free(). Aborting.
6
7  Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: [pulseaudio] core-
       util.c: Failed to connect to system bus: Did not receive a reply.
       Possible causes include: the remote application did not send a reply
       , the message bus security policy blocked the reply, the reply
       timeout expired, or the network connection was broken.
8
9  Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: message repeated 10
       times: [ [pulseaudio] core-util.c: Failed to connect to system bus:
       Did not receive a reply. Possible causes include: the remote
       application did not send a reply, the message bus security policy
       blocked the reply, the reply timeout expired, or the network
       connection was broken.]
10
11 Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: [pulseaudio] pid.c:
       Daemon already running.Nov  3 11:03:58 user01-HVM-domU citrix-ctxgfx
       [24693]: Exiting normally
```

Certains des groupes ou des modules ne prennent effet qu'après un redémarrage. Si les messages d'erreur **dbus** s'affichent dans le journal, 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.

Utiliser MCS pour créer des machines virtuelles Linux

January 11, 2019

À partir de la version 7.18, vous pouvez utiliser Citrix Machine Creation Services (MCS) pour créer des machines virtuelles Linux.

> **Remarque :**
>
> n'utilisez pas Easy Install sur la VM modèle lorsque vous utilisez MCS pour créer des machines virtuelles Linux.

Pour utiliser MCS afin de créer des machines virtuelles Linux, préparez une image principale sur votre hyperviseur XenServer, Microsoft Azure ou VMware vSphere (la prise en charge des autres hyperviseurs n'est actuellement pas disponible). Ce processus implique l'installation du VDA sur la VM modèle, la création d'un catalogue de machines dans Citrix Studio, la création d'un groupe de mise à disposition et l'exécution de certaines tâches de configuration.

> **Remarque :**
>
> les résultats inattendus peuvent se produire si vous essayez de préparer une image principale sur des hyperviseurs autres que XenServer.

Utiliser MCS pour créer des machines virtuelles Linux sur XenServer

Étape 1 : préparer une image principale

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

Étape 1a : installer les outils XenServer Tools

Les outils XenServer Tools doivent être installés sur la VM modèle pour que chaque VM puisse utiliser l'interface de ligne de commande xe ou XenCenter. Les performances de la VM peuvent être lentes à moins que les outils ne soient installés. Sans les outils, vous ne pouvez pas effectuer les opérations suivantes :

- Arrêter, redémarrer ou suspendre une VM correctement
- Afficher les données de performances de la VM dans XenCenter
- Migrer une VM en cours d'exécution (via XenMotfion)

- Créer des instantanés ou des instantanés avec de la mémoire (points de contrôle) et revenir aux instantanés
- Régler le nombre de vCPU sur une VM Linux en cours d'exécution

> **Important :**
>
> L'exécution d'une VM sans l'installation des outils XenServer Tools n'est pas une configuration prise en charge.

1. Exécutez la commande suivante pour monter les outils XenServer Tools nommés guest-tools.iso.

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

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

   PourRHEL/CentOS :

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

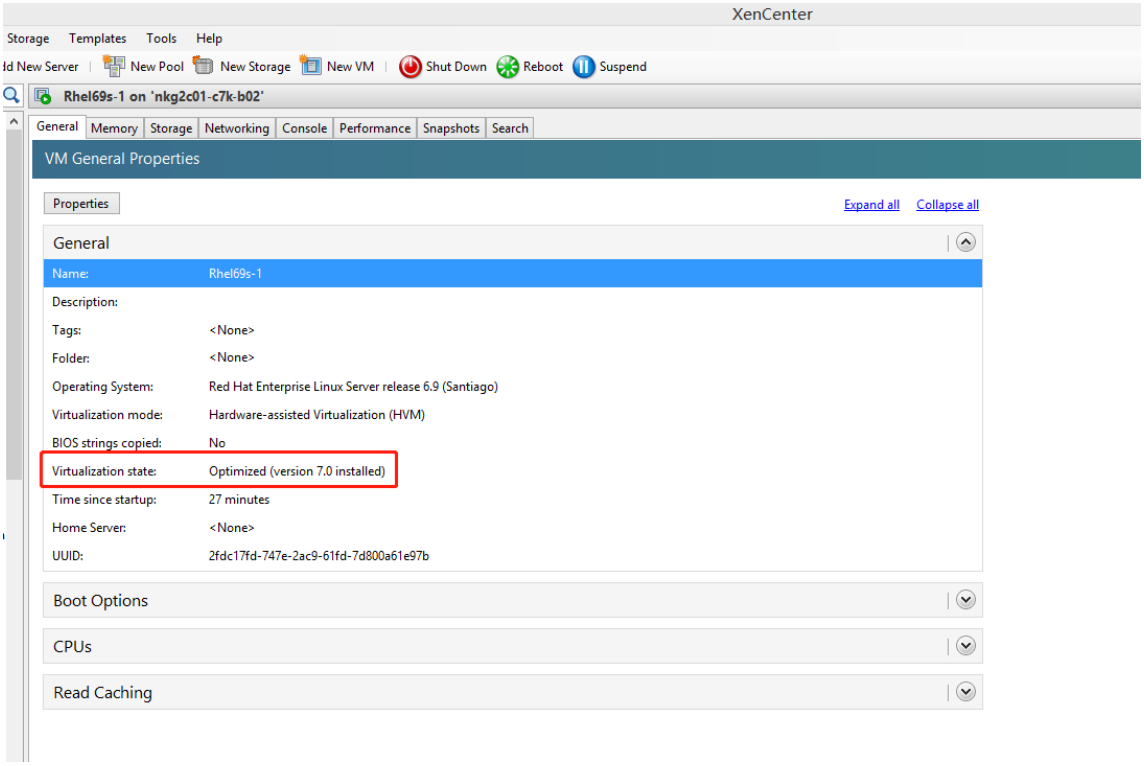
   Pour Ubuntu :

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

   Pour SUSE 12 :

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

3. Vérifiez l'état de la virtualisation de la VM modèle dans l'onglet **General** de XenCenter. Si les outils XenServer sont correctement installés, l'état de la virtualisation est défini sur**Optimized** comme indiqué ci-dessous :



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

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

PourRHEL/CentOS :

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

Pour Ubuntu :

```
sudo dpkg  -i  <PATH>/<Linux VDA DEB>

apt-get install -f
```

Pour SUSE 12 :

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

Étape 1c : activer les référentiels pour installer le package tdb-tools

Pour un serveur RHEL 7 :

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


Pour un poste de travail RHEL 7 :

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

Étape 1d : activer le référentiel EPEL pour installer ntfs-3g

Pour RHEL 6/CentOS 6 :

```
sudo rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest
    -6.noarch.rpm
```

Pour RHEL 7/CentOS 7 :

```
sudo rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest
    -7.noarch.rpm
```

Étape 1e : installer ntfs-3g pour SUSE 12

Sur la plate-forme SUSE 12, aucun référentiel ne fournit ntfs-3g. Vous devez télécharger le code source et compiler puis installer ntfs-3g manuellement :

1. Installez le système de compilation GCC (GNU Compiler Collection) et le package de création :

   ```
   sudo zypper install gcc
   sudo zypper install make
   ```

2. Téléchargez le package ntfs-3g depuis https://www.tuxera.com/community/open-source-ntfs-3g/.
3. Décompressez le package ntfs-3g :

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

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

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

5. Installez ntfs-3g :

   ```
   ./configure
   make
   make install
   ```


Étape 1f : configurer l'environnement d'exécution

Avant d'exécuter **deployymcs.sh**, procédez comme suit :

- Modifiez les variables dans **/var/xdl/mcs/mcs.conf**. Le fichier de configuration **mcs.conf** contient des variables pour la configuration de MCS et du VDA Linux. Vous pouvez définir les variables suivantes si nécessaire :
  - dns : définit l'adresse IP du DNS.
  - AD_INTEGRATION : définit Winbind ou SSSD (SSSD n'est pas pris en charge sur SUSE).
  - WORKGROUP : définit le nom du groupe de travail (sensible à la casse) s'il est configuré dans AD.
- Sur la machine modèle, ajoutez des lignes de commande au fichier **/var/xdl/mcs/mcs_local_setting.reg** pour écrire ou mettre à jour les valeurs de registre selon les besoins. Cette action empêche la perte de données et de paramètres chaque fois qu'une machine provisionnée par MCS redémarre.

  Chaque ligne du fichier **/var/xdl/mcs/mcs_local_setting.reg** est une commande permettant de définir ou de modifier une valeur de registre.

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

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

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

Étape 1g : créer une image principale

1. Exécutez **/opt/Citrix/VDA/sbin/deploymcs.sh**.
2. Sur XenServer, arrêtez le VM modèle. Créez et nommez un instantané de l'image principale.

Étape 2 : créer un catalogue de machines

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

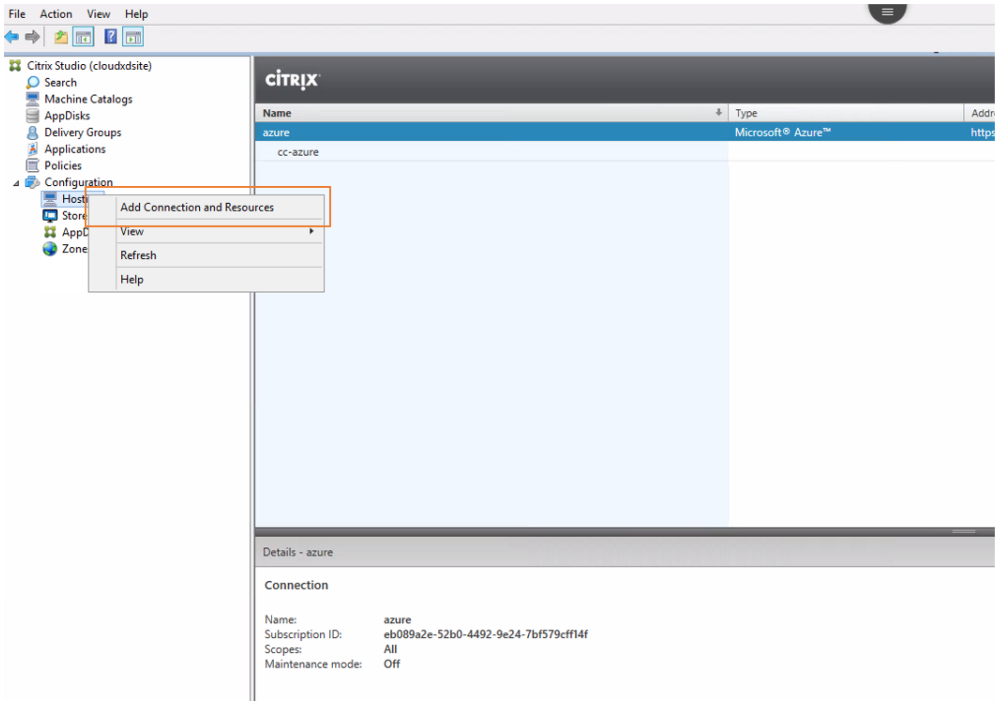
Étape 3 : créer un groupe de mise à disposition

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

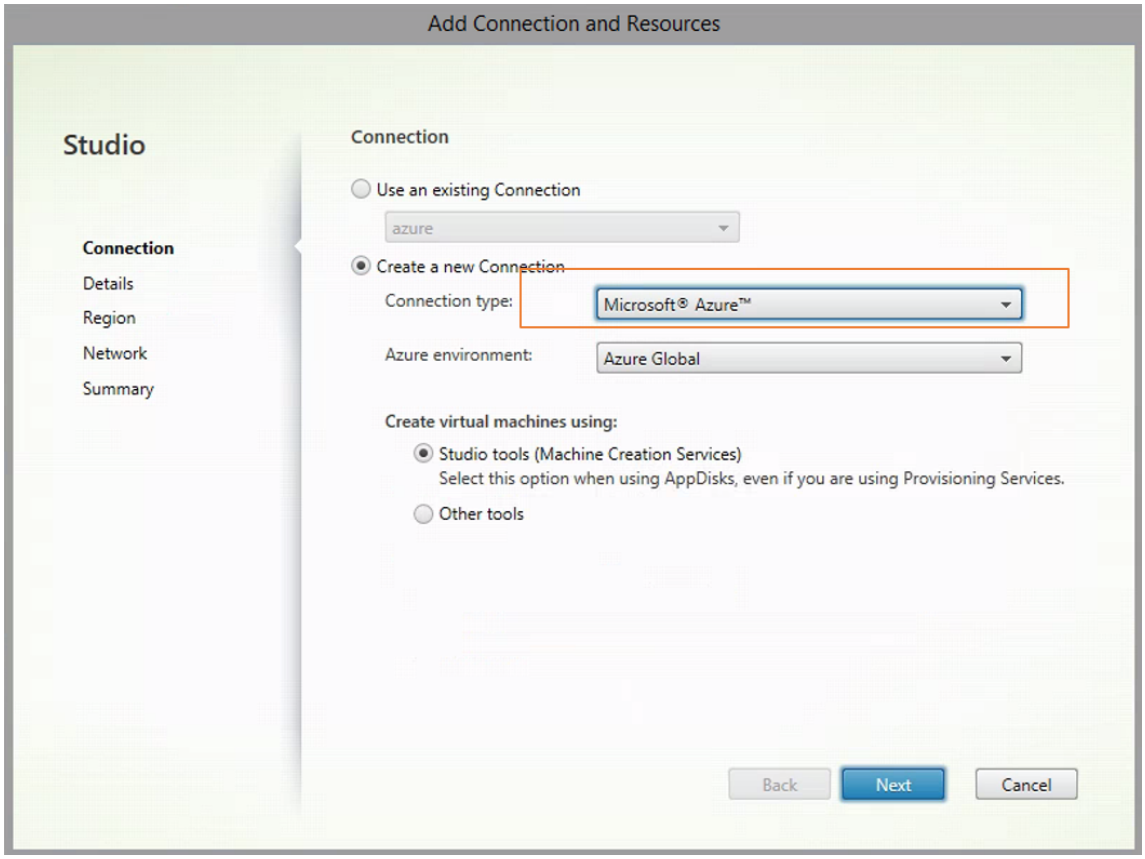
Utiliser MCS pour créer des machines virtuelles Linux sur Azure

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

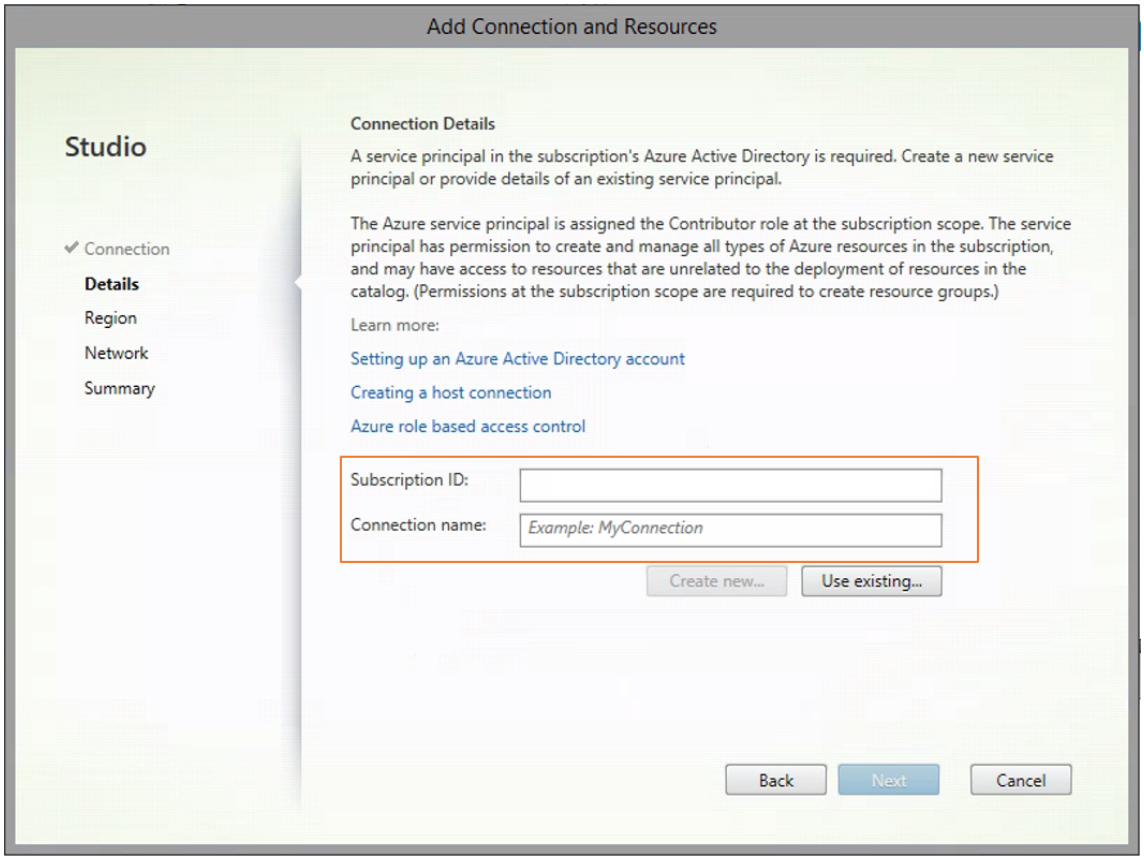
1. Dans Citrix Studio, sélectionnez **Configuration** > **Hébergement** > **Ajouter une connexion et des ressources** pour créer une connexion à Azure.



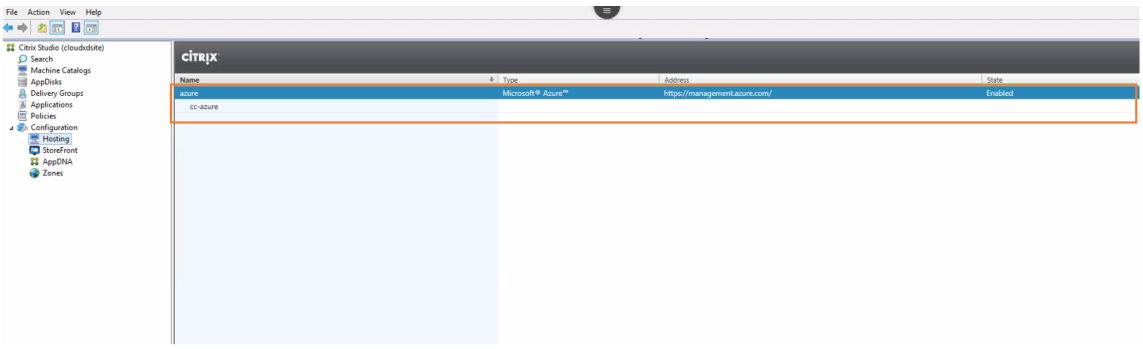
2. Sélectionnez le type de connexion Microsoft Azure.



3. Entrez l'ID d'abonnement de votre compte Azure et saisissez votre nom de connexion.



Une nouvelle connexion apparaît dans le panneau d'hébergement.

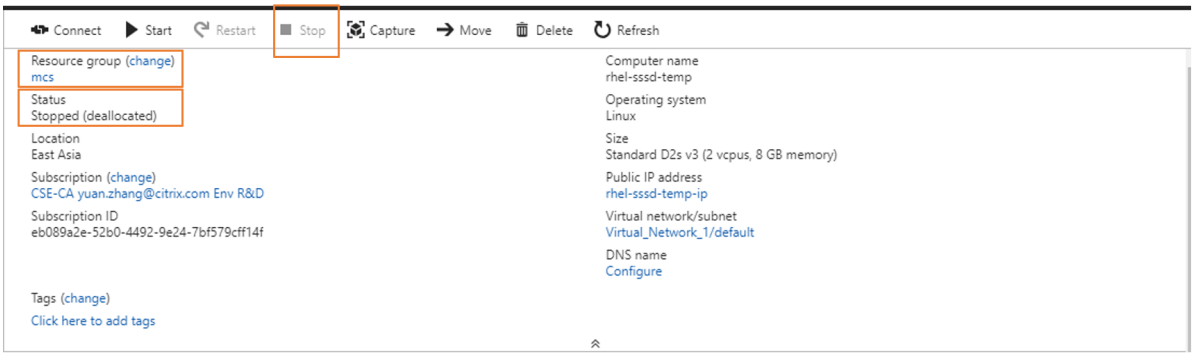


Étape 2 : préparer une image principale

Suivez l'étape 1 (à l'exception des étapes 1a et 1c) de la section précédente **Utiliser MCS pour créer des machines virtuelles Linux sur XenServer** afin de préparer une image principale.

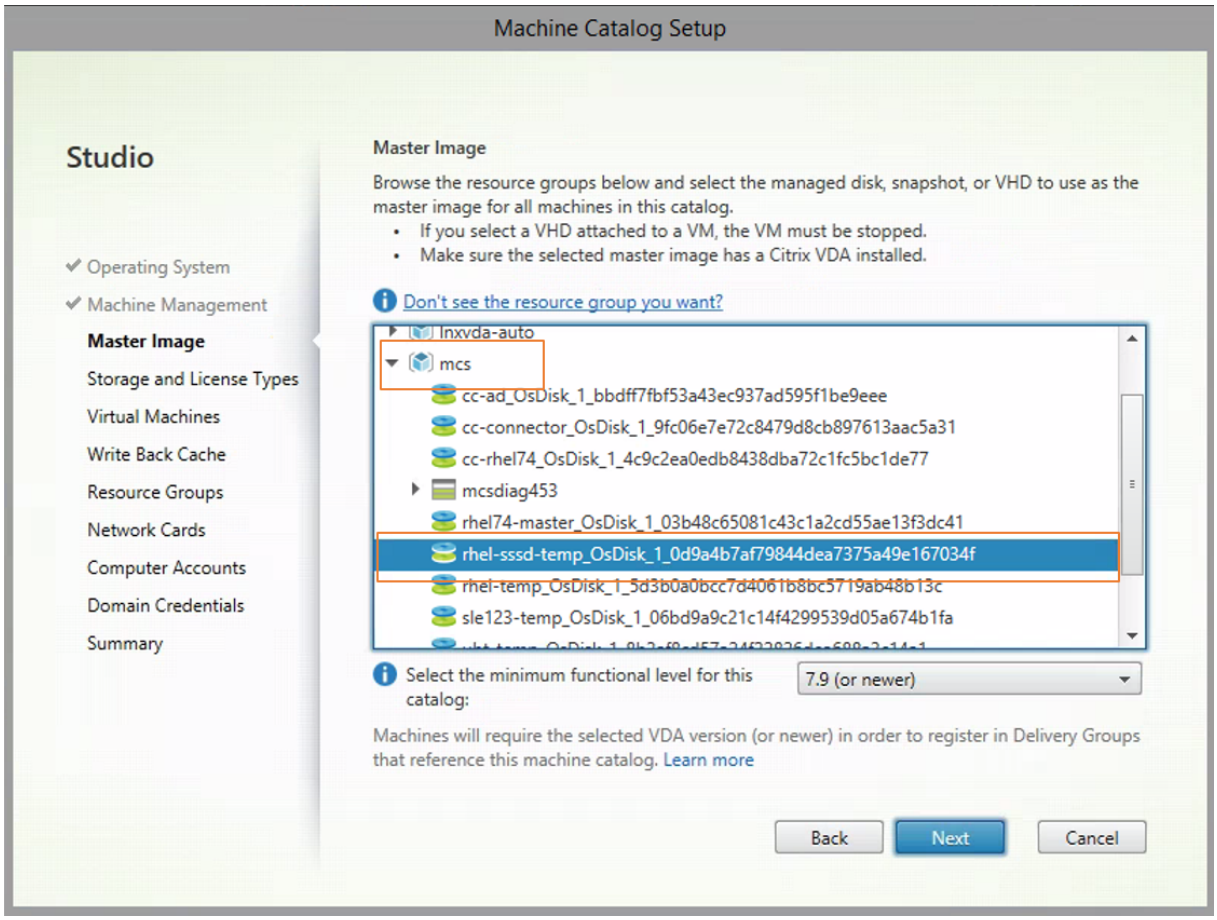
Après avoir installé les applications sur la VM modèle, fermez la VM modèle à partir du portail Azure. Assurez-vous que l'état de l'alimentation de la VM modèle est défini sur **Arrêté (libéré)**.

Mémorisez le nom du groupe de ressources. Vous avez besoin du nom pour localiser votre image principale sur Azure.



Étape 3 : créer un catalogue de machines

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



Effectuez d'autres tâches de configuration si nécessaire. Pour plus d'informations, consultez l'article CTX219270 du centre de connaissances et la section Créer un catalogue de machines à l'aide de Studio.

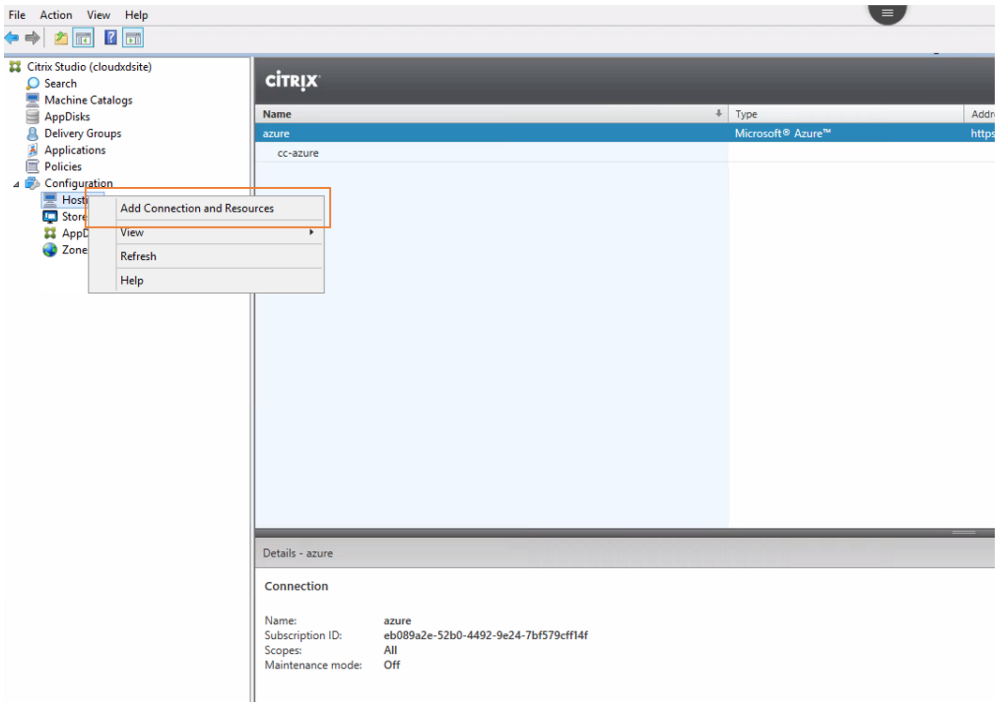
Étape 4 : créer un groupe de mise à disposition

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

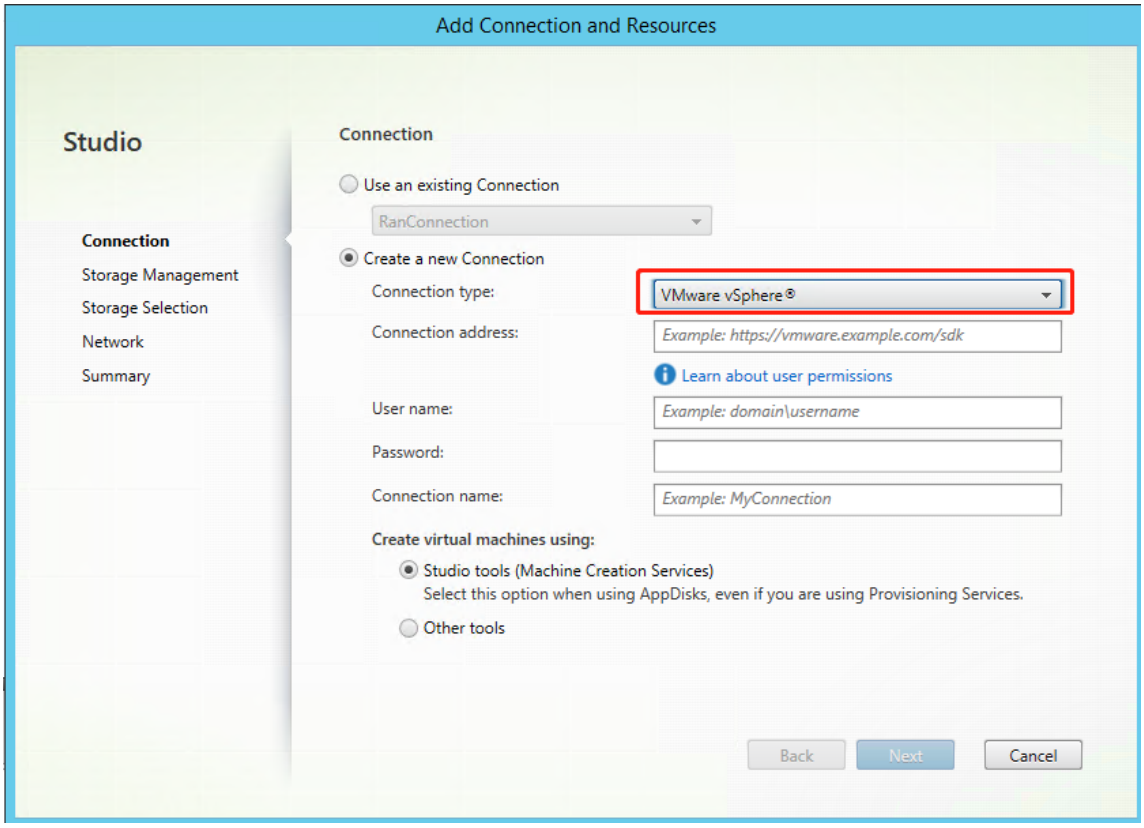
Utiliser MCS pour créer des machines virtuelles Linux sur VMware vSphere

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

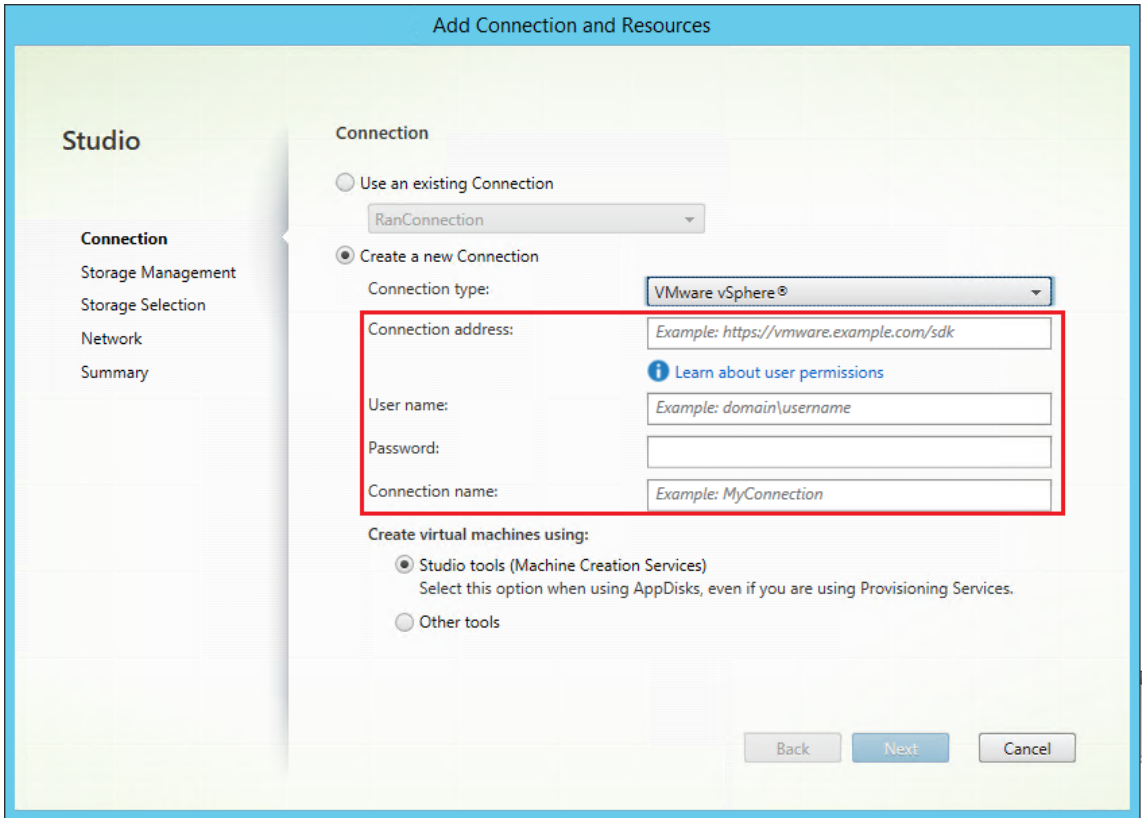
1. Installez vCenter Server dans l'environnement vSphere. Pour plus d'informations, consultez la section VMware vSphere.
2. Dans Citrix Studio, sélectionnez **Configuration** > **Hébergement** > **Ajouter une connexion et des ressources** pour créer une connexion à VMware vSphere.



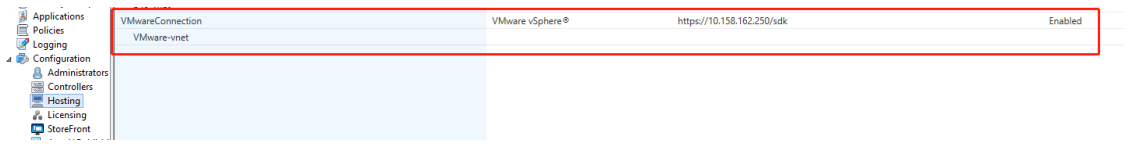
3. Sélectionnez le type de connexion VMware vSphere.



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



Une nouvelle connexion apparaît dans le panneau d'hébergement.



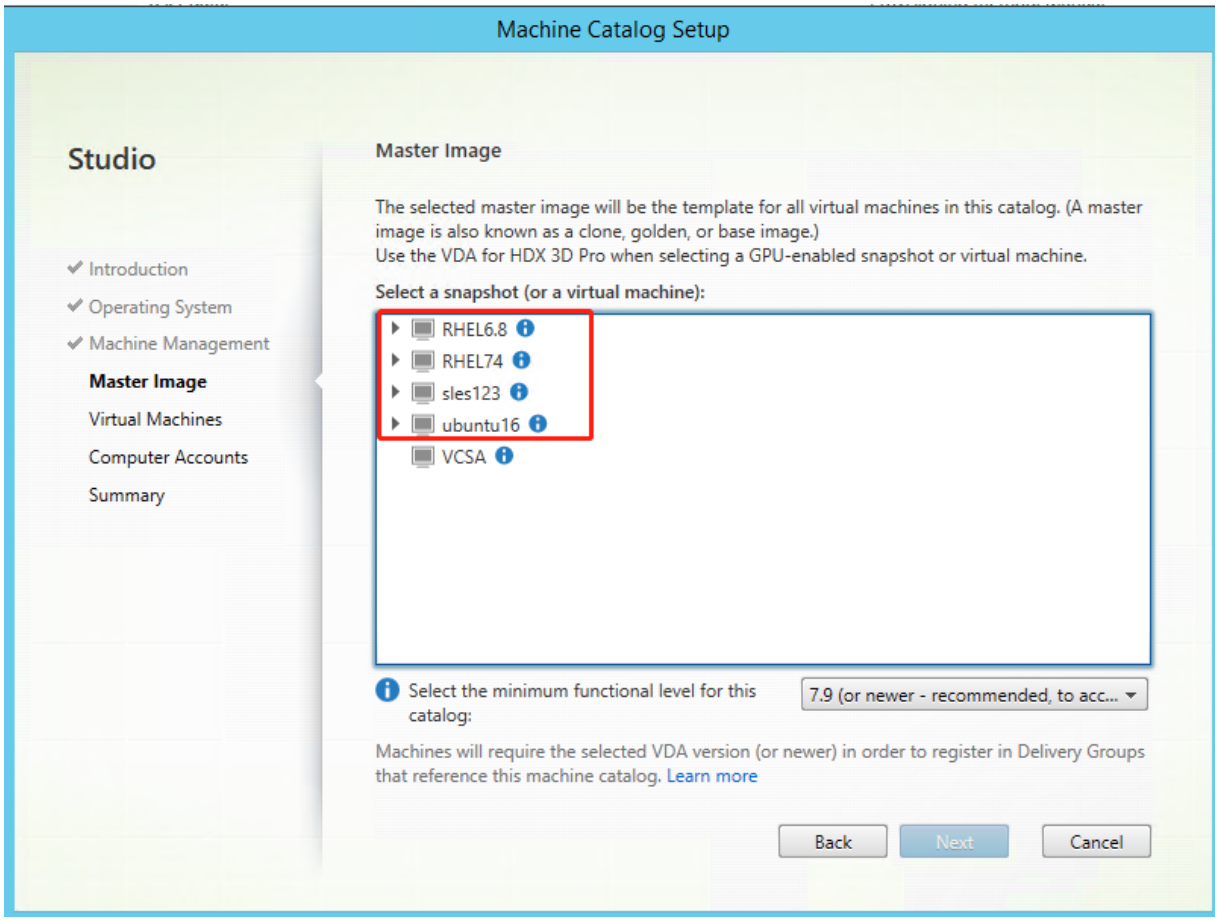
Étape 2 : préparer une image principale

Suivez l'étape 1 (à l'exception des étapes 1a et 1c) de la section précédente **Utiliser MCS pour créer des machines virtuelles Linux sur XenServer** afin de préparer une image principale.

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

Étape 3 : créer un catalogue de machines

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



Effectuez d'autres tâches de configuration si nécessaire. Pour plus d'informations, consultez l'article CTX219270 du centre de connaissances et la section Créer un catalogue de machines à l'aide de Studio.

Étape 4 : créer un groupe de mise à disposition

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

(Non recommandé) Utiliser MCS pour effectuer la mise à niveau de votre VDA Linux

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

1. Mettez à niveau votre VDA Linux sur la machine modèle :

   Pour RHEL 7/CentOS 7 :

   ```
   1 sudo rpm -U LinuxVDA-1811.el7_x.rpm
   ```


Pour RHEL 6/CentOS 6 :

```
sudo rpm -U LinuxVDA-1811.el6_x.rpm
```

Pour SUSE 12 :

```
sudo rpm -U LinuxVDA-1811.sle12_x.rpm
```

Pour Ubuntu :

```
sudo dpkg -i LinuxVDA-1811.ubuntu16.04.deb
```

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

Installer Virtual Delivery Agent Linux pour RHEL/CentOS

February 15, 2019

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 Esay Install uniquement pour les nouvelles installations. N'utilisez pas Easy Install pour mettre à jour une installation existante.[](/fr-fr/linux-virtual-delivery-agent/current-release/installation-overview/easy-install.html)

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

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=**nom d'hôte**

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

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

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

Par exemple :

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

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

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

Étape 1d : vérifier le nom d'hôte

Vérifiez que le nom d'hôte est correctement configuré :

```
1 hostname
```

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

Vérifiez que le nom de domaine complet est correctement configuré :

```
1 hostname -f
```

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

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

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


```
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 VDA Linux 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 **server** 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 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 VDA Linux 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
```

> **Conseil :**
>
> 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 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 :

- RHEL 7 uniquement : PostgreSQL 9


```
sudo systemctl enable postgresql

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 VDA Linux.

Étape 2 : préparer l'hyperviseur

Certaines modifications sont requises pour l'exécution du VDA Linux 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 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 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 pour éviter tout conflit avec NTP. La synchronisation de l'heure Hyper-V peut co-exister avec la synchronisation de l'heure NTP.

Corriger la synchronisation de l'heure sur ESX et ESXi

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

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

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

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

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

- Samba Winbind
- Service d'authentification Quest
- 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 :

```
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 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 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 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.

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 VDA Linux

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

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 VDA Linux

Solution à l'application forcée de la stratégie SELinux

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

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


```
SELINUX=permissive
```

Cette modification nécessite le redémarrage de la machine :

```
1 reboot
```

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

Configurer le démon VAS

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

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

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

Configuration de PAM et de NSS

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

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

Rejoindre un domaine Windows

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

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


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

Vérifier l'appartenance à un domaine

Le 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.

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 adjoin Centrify :

```
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
```

Pour tester la connectivité avec les différents services Active Directory et Kerberos :

```
adinfo --test
```

SSSD

Utilisez les informations suivantes pour configurer SSSD. Cette section comprend des instructions permettant de connecter une machine VDA Linux à un domaine Windows et des indications sur la configuration de l'authentification Kerberos.

> **Remarque :** si vous utilisez SSSD, suivez les instructions de cette section.

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 utilisateurs locaux ainsi que les données utilisateur supplémentaires.

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 7.5 ou version ultérieure
- CentOS 7.5 ou version ultérieure

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. 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

# 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 service sssd start

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 :

```
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

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 VDA Linux. 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 :

```
klist
```

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 4 : installer le VDA Linux

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

Pour effectuer une nouvelle installation

1. (Facultatif) Désinstaller l'ancienne version

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

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

2. Télécharger le package VDA Linux

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

3. Installer le VDA Linux

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

    **Pour RHEL 7/CentOS 7 :**

```



```
    ```
    sudo yum install -y LinuxVDA-1811.el7_x.rpm
    ```

    **Pour RHEL 6/CentOS 6 :**

    ```
    sudo yum install -y LinuxVDA-1811.el6_x.rpm
    ```

- Installez le logiciel VDA Linux 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 LinuxVDA-1811.el7_x.rpm
    ```

    Pour RHEL 6/CentOS 6 :

    ```
    sudo rpm -i LinuxVDA-1811.el6_x.rpm
    ```

    Liste des dépendances RPM pour RHEL 7/CentOS 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
```


```

```
48   xorg-x11-server-utils >= 7.7
49
50   xorg-x11-xinit >= 1.3.2
51
52   libXpm >= 3.5.10
53
54   libXrandr >= 1.4.1
55
56   libXtst >= 1.2.2
57
58   motif >= 2.3.4
59
60   pam >= 1.1.8
61
62   util-linux >= 2.23.2
63
64   bash >= 4.2
65
66   findutils >= 4.5
67
68   gawk >= 4.0
69
70   sed >= 4.2
71
72   cups >= 1.6.0
73
74   foomatic-filters >= 4.0.9
75
76   openldap >= 2.4
77
78   cyrus-sasl >= 2.1
79
80   cyrus-sasl-gssapi >= 2.1
81
82   libxml2 >= 2.9
83
84   python-requests >= 2.6.0
85
86   gperftools-libs >= 2.4
87
88   rpmlib(FileDigests) <= 4.6.0-1
89
90   rpmlib(PayloadFilesHavePrefix) <= 4.0-1
91
92   pmlib(CompressedFileNames) <= 3.0.4-1
```


```
93
94      rpmlib(PayloadIsXz) <= 5.2-1
95      ‘‘‘
96
97  > **Remarque :**
98  >
99  >Pour une matrice des distributions Linux et des versions Xorg que
        cette version du VDA Linux prend en charge, consultez la section [
        Configuration systéme requise](/fr-fr/linux-virtual-delivery-agent/
        current-release/system-requirements.html).
100
101     **Liste des dépendances RPM pour RHEL 6/CentOS 6 :**
102
103     ‘‘ ‘
104     postgresql-jdbc >= 8.4
105
106     postgresql-server >= 8.4
107
108     java-1.7.0-openjdk >= 1.7.0
109
110     ImageMagick >= 6.5.4.7
111
112     GConf2 >= 2.28.0
113
114     system-config-firewall-base >= 1.2.27
115
116     policycoreutils-python >= 2.0.83
117
118     xorg-x11-server-utils >= 7.7
119
120     xorg-x11-xinit >= 1.0.9
121
122     ConsoleKit >= 0.4.1
123
124     dbus >= 1.2.24
125
126     dbus-x11 >= 1.2.24
127
128     libXpm >= 3.5.10
129
130     libXrandr >= 1.4.1
131
132     libXtst >= 1.2.2
133
134     openmotif >= 2.3.3
```



```
135
136     pam >=1.1.1
137
138     util-linux-ng >= 2.17.2
139
140     bash >= 4.1
141
142     findutils >= 4.4
143
144     gawk >= 3.1
145
146     sed >=4.2
147
148     cups >= 1.4.0
149
150     foomatic >= 4.0.0
151
152     openldap >= 2.4
153
154     cyrus-sasl >= 2.1
155
156     cyrus-sasl-gssapi >= 2.1
157
158     libxml2 >= 2.7
159
160     python-requests >= 2.6.0
161
162     gperftools-libs >= 2.0
163
164     rpmlib(FileDigests) <= 4.6.0-1
165
166     rpmlib(PayloadFilesHavePrefix) <= 4.0-1
167
168     rpmlib(CompressedFileNames) <= 3.0.4-1
169
170     rpmlib(PayloadIsXz) <= 5.2-1
171     ‘‘ ‘
```

> **Remarque :**
>
> Après avoir installé Linux VDA sur RHEL 7.x, exécutez la commande **sudo yum install -y python-websockify x11vnc**. Le but est d’installer python-websockify et x11vnc manuellement pour utiliser la fonctionnalité d’observation de session. Pour plus d’informations, consultez la section Observer des sessions.

Pour effectuer une mise à niveau d'une installation existante

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

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

  Pour RHEL 7/CentOS 7 :

  ```
  sudo yum install -y LinuxVDA-1811.el7_x.rpm
  ```

  Pour RHEL 6/CentOS 6 :

  ```
  sudo yum  install -y LinuxVDA-1811.el6_x.rpm
  ```

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

  Pour RHEL 7/CentOS 7 :

  ```
  sudo rpm -U LinuxVDA-1811.el7_x.rpm
  ```

  Pour RHEL 6/CentOS 6 :

  ```
  sudo rpm -U LinuxVDA-1811.el6_x.rpm
  ```

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

Étape 5 : configurer le VDA Linux

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 :

```
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** : 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** : Linux VDA requiert une liste séparée par des espaces de noms de domaines complets. 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** : 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** : 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 Virtual Desktop prend en charge HDX 3D Pro, un ensemble de technologies d'accélération des graphiques conçues pour optimiser la virtualisation des applications riches en graphiques HDX 3D Pro nécessite l'installation d'une carte graphique NVIDIA GRID compatible. 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). HDX 3D Pro n'est pas pris en charge sur SUSE. Assurez-vous que la valeur est définie sur N pour une plate-forme SUSE.

- **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** : 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** : 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 VDA Linux envoie une requête à LDAP via une base de recherche définie sur la racine du domaine (Active Directory (par exemple, D, DC=mycompany,DC=com). Pour améliorer les performances de recherche, vous pouvez spécifier une base de recherche (par exemple, OU=VDI,DC=mycompany,DC=com). Cette variable est définie sur **<none>** par défaut.
- **CTX_XDL_FAS_LIST = list-fas-servers** : les serveurs du service d'authentification fédérée (FAS) sont configurés via la stratégie de groupe AD. Comme le VDA Linux ne prend pas en charge la stratégie de groupe AD, vous pouvez fournir une liste de serveurs FAS séparés par des points-virgules. La séquence doit être la même que celle configurée dans la stratégie de groupe AD. Si une adresse de serveur est supprimée, remplissez son espace vide avec la chaîne de texte **<none>** et conservez la séquence d'adresses du serveur sans effectuer de modification.
- **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-site-name | '<none>'

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

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

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

export CTX_XDL_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.

Éventuellement, vous pouvez spécifier les paramètres en utilisant 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_FAS_LIST = list-fas-servers \

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 VDA Linux 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 VDA Linux pour que les modifications prennent effet.

Étape 6 : exécuter le VDA Linux

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 VDA Linux :

```
sudo /sbin/service ctxhdx start

sudo /sbin/service ctxvda start
```

Arrêter Linux VDA :

Pour arrêter les services VDA Linux :


```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
```

Redémarrer Linux VDA :

Pour redémarrer les services VDA Linux :

```
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 du VDA Linux :

```
sudo /sbin/service ctxvda status

sudo /sbin/service ctxhdx status
```

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

Le processus de création de catalogues de machines et d'ajout de machines VDA Linux 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 VDA Linux, 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.
- Ne combinez pas de machines VDA Linux 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 d'OS de serveur Windows ou d'OS de

> serveur implique un modèle de mise à disposition équivalent de bureaux partagés hébergés. La sélection de l'option Système d'exploitation 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 la rejoignez au domaine Active Directory, vous devez supprimer et rajouter la machine au catalogue de machines.

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

Le processus de création d'un groupe de mise à disposition et d'ajout de catalogues de machines contenant des machines VDA Linux 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 VDA Linux, 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 VDA Linux.
- 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 VDA Linux ne prend pas en charge la mise à disposition de bureaux et d'applications sur la même machine.

Pour plus d'informations sur la création de catalogues de machines et de groupes de mise à disposition, consultez Citrix Virtual Apps and Desktops 7 1811.

Installer Virtual Delivery Agent Linux pour SUSE

February 15, 2019

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 Esay 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 VDA Linux. 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**.
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 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.
>
> **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 modifiez également la ligne suivante :

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

et remplacez-la avec ce qui suit :

```
hosts: files dns
```

Vérifier le nom d'hôte

Vérifiez que le nom d'hôte est correctement configuré :

```
1 hostname
```

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

Vérifiez que le nom de domaine complet est correctement configuré :

```
1 hostname -f
```

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

Vérifier la résolution de nom et l'accessibilité du service

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

```
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 VDA Linux 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 VDA Linux

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

- PostgreSQL
  - SLED/SLES 12 : version 9.3 ou ultérieure
- OpenJDK 1.7.0
- OpenMotif Runtime Environment 2.3.1 ou version ultérieure
- Cups
  - SLED/SLES 12 : version 1.6.0 ou ultérieure
- Filtres Foomatic
  - SLED/SLES 12 : version 1.0.0 ou ultérieure
- ImageMagick
  - 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 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 12, exécutez les commandes :

```
1 sudo mkdir -p /mnt/sles
2
3 sudo mount -t iso9660 path-to-iso/SLES-12-SP3-DVD-x86_64-GM-DVD1.iso /
     mnt/sles
4
5 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 VDA Linux 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 VDA Linux 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 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 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/sdk
```

Étape 2 : préparer une VM Linux pour l'hyperviseur

Certaines modifications sont requises pour l'exécution du VDA Linux 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 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 co-exister avec la synchronisation de l'heure NTP.

Corriger la synchronisation de l'heure sur ESX et ESXi

Si la fonctionnalité de synchronisation de l'heure de VMware est activée, vous rencontrerez des problèmes dans chaque VM Linux paravirtualisée car l'hyperviseur et NTP tenteront de gérer l'horloge du système. Pour éviter que l'horloge ne soit plus synchronisée avec d'autres serveurs, 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
- Service d'authentification Quest
- Centrify DirectControl

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

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 VDA Linux.
3. Cliquez sur **OK**. Si vous êtes invité(e) à installer des packages, cliquez sur **Install**.
4. Si un contrôleur de domaine est trouvé, vous êtes invité à joindre le domaine. Cliquez sur **Yes**.

5. Lorsque vous y êtes invité(e), saisissez les informations d'identification d'un utilisateur de domaine avec les autorisations nécessaires pour ajouter des ordinateurs au domaine, et cliquez sur **OK**.
6. Un message indiquant si le processus a réussi s'affiche.
7. Si vous êtes invité(e) à installer des packages samba et krb5, cliquez sur **Install**.

YaST peut avoir indiqué que ces modifications nécessitent le redémarrage de certains services ou de la machine. Il est conseillé 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 VDA Linux 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 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
```

Quitter la session

```
exit
```

Le même test peut être réalisé en ouvrant une session directement sur la console KDE ou Gnome.

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 VDA Linux

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

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 VDA Linux

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 le NSS :

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

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

Rejoindre un domaine Windows

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

```
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.

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

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

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

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

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

Quittez la session :

```
1 exit
```

Le même test peut être réalisé en ouvrant une session directement sur la console KDE ou Gnome.

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 **adjoin** Centrify :

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

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

Vérifier l'appartenance à un domaine

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

```
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
```

Pour tester la connectivité avec les différents services Active Directory et Kerberos :

```
adinfo --test
```

Étape 4 : installer le VDA Linux

Étape 4a : désinstaller l'ancienne version

Si vous avez déjà installé une version de VDA Linux antérieure à la version 1.1, 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 dernières versions est prise en charge.

> **Remarque :**
>
> À compter de la version 1.3, le chemin d'accès 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 aussi ajouter **/opt/Citrix/VDA/sbin** et **/opt/Citrix/VDA/bin** au chemin d'accès système.

Étape 4b : télécharger le package VDA Linux

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

Étape 4c : installer le VDA Linux

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

Pour SUSE 12 :

```
sudo zypper install LinuxVDA-1811.sle12_x.rpm
```

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

Pour SUSE 12 :

```
sudo rpm -i LinuxVDA-1811.sle12_x.rpm
```

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

Vous pouvez mettre à niveau les versions précédentes du logiciel Linux VDA à l'aide du gestionnaire de packages RPM :

Pour SUSE 12 :

```
sudo rpm -U LinuxVDA-1811.sle12_x.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
```



```
50
51 libtcmalloc4 >= 2.5
52
53 libcap-progs >= 2.22
54
55 xorg-x11-server >= 7.6_1.18.3-76.15
56
57 ibus >= 1.5
```

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

Étape 5 : configurer le VDA Linux

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 :

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

Configuration automatique

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

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

- **CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N** : 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** : Linux VDA requiert une liste séparée par des espaces de noms de domaines complets. 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** : 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** : 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 Virtual Desktop prend en charge HDX 3D Pro, un ensemble de technologies d'accélération des graphiques conçues pour optimiser la virtualisation des applications riches en graphiques. HDX 3D Pro nécessite l'installation d'une carte graphique NVIDIA GRID compatible. 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). HDX 3D Pro n'est pas pris en charge sur SUSE. Assurez-vous que la valeur est définie sur N pour une plate-forme SUSE.
- **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** : 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** : 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 VDA Linux envoie une requête à LDAP via

une base de recherche définie sur la racine du domaine (Active Directory (par exemple, D, DC=mycompany,DC=com). Pour améliorer les performances de recherche, vous pouvez spécifier une base de recherche (par exemple, OU=VDI,DC=mycompany,DC=com). Cette variable est définie sur **<none>** par défaut.

- **CTX_XDL_FAS_LIST = list-fas-servers** : les serveurs du service d'authentification fédérée (FAS) sont configurés via la stratégie de groupe AD. Comme le VDA Linux ne prend pas en charge la stratégie de groupe AD, vous pouvez fournir une liste de serveurs FAS séparés par des points-virgules. La séquence doit être la même que celle configurée dans la stratégie de groupe AD. Si une adresse de serveur est supprimée, remplissez son espace vide avec la chaîne de texte **<none>** et conservez la séquence d'adresses du serveur sans effectuer de modification.
- **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.

> **Remarque :**
>
> HDX 3D Pro n'est actuellement pas disponible sur SUSE.

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-site-name | '<none>'

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

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

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

export CTX_XDL_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.

Éventuellement, vous pouvez spécifier les paramètres en utilisant 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_FAS_LIST = list-fas-servers \

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 VDA Linux 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 VDA Linux pour que les modifications prennent effet.

Étape 6 : exécuter le VDA Linux

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 VDA Linux :

```
sudo /sbin/service ctxhdx start

sudo /sbin/service ctxvda start
```

Arrêter Linux VDA :

Pour arrêter les services VDA Linux :

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
```

Redémarrer Linux VDA :

Pour redémarrer les services VDA Linux :

```
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 du VDA Linux :

```
sudo /sbin/service ctxvda status

sudo /sbin/service ctxhdx status
```

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

Le processus de création de catalogues de machines et d'ajout de machines VDA Linux 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 VDA Linux, 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.
- Ne combinez pas de machines VDA Linux 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 d'OS de serveur Windows ou d'OS de serveur implique un modèle de mise à disposition équivalent de bureaux partagés hébergés. La sélection de l'option Système d'exploitation 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 la rejoignez au domaine Active Directory, vous devez supprimer et rajouter la machine au catalogue de machines.

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

Le processus de création d'un groupe de mise à disposition et d'ajout de catalogues de machines contenant des machines VDA Linux 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 VDA Linux, 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 VDA Linux.
- 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 VDA Linux ne prend pas en charge la mise à disposition de bureaux et d'applications sur la même machine.

Pour plus d'informations sur la création de catalogues de machines et de groupes de mise à disposition, consultez Citrix Virtual Apps and Desktops 7 1811.

Installer Virtual Delivery Agent Linux pour Ubuntu

February 15, 2019

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 Esay 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

Citrix recommande que le réseau soit 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 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.
>
> **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 :

```
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**. Modifiez également la ligne suivante :

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

et remplacez-la avec ce qui suit :

```
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 VDA Linux 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 VDA Linux 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 VDA Linux 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 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 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'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
- Service d'authentification Quest
- 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

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**. La propriété **REALM** est le nom du domaine Kerberos en majuscules, tel que **EXAMPLE.COM**.

Configurer l'authentification Winbind

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

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

```
[global]

workgroup = WORKGROUP

security = ADS

```



```
realm = REALM

encrypt passwords = yes

idmap config *:range = 16777216-33554431

winbind trusted domains only = no

kerberos method = secrets and keytab

winbind refresh tickets = yes

template shell = /bin/bash
```

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

Configurer nsswitch

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

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

Rejoindre un domaine Windows

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

```
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.

> **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 VDA Linux

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

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 VDA Linux

Solution à l'application forcée de la stratégie SELinux

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

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

```
SELINUX=disabled
```

Cette modification nécessite le redémarrage de la machine :

```
1 reboot
```

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

> racine et d'autres utilisateurs locaux.

Configurer le démon VAS

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

```
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 le NSS :

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

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

Rejoindre un domaine Windows

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

```
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
```

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 adjoin Centrify :

```
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
```

Pour tester la connectivité avec les différents services Active Directory et Kerberos :

```
adinfo --test
```

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
```



```
6
7  [realms]
8
9   REALM = {
10
11
12    admin_server = domain-controller-fqdn
13
14    kdc = domain-controller-fqdn
15
16    }
17
18
19  [domain_realm]
20
21   domain-dns-name = REALM
22
23   .domain-dns-name = REALM
```

La propriété domain-dns-name dans ce contexte est le nom de domaine DNS, tel que example.com. La propriété **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. Il existe plusieurs méthodes de jonction du domaine :

- adcli
- samba
- realmd

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

Utilisez adcli pour rejoindre le domaine :

Installer adcli :

Installez les packages requis :

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

Rejoindre le domaine avec adcli :

Supprimez l'ancien fichier keytab du système et rejoignez le domaine à l'aide de :

```
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 configurez les paramètres suivants :

```
[global]

   workgroup = WORKGROUP

   security = ADS

   realm = REALM

   client signing = yes

   client use spnego = yes

   kerberos method = secrets and keytab
```


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

Rejoindre le domaine avec samba :

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

```
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]

services = nss, pam

config_file_version = 2

domains = domain-dns-name

[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. Le 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 VDA Linux. 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.

Étape 4 : installer le VDA Linux

Étape 4a : télécharger le package VDA Linux

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

Étape 4b : installer le VDA Linux

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

```
sudo dpkg -i LinuxVDA-1811.ubuntu16.04.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
```



```
18
19 util-linux >= 2.27.1
20
21 bash >= 4.3
22
23 findutils >= 4.6.0
24
25 sed >= 4.2.2
26
27 cups >= 2.1
28
29 libldap-2.4-2 >= 2.4.42
30
31 libsasl2-modules-gssapi-mit >= 2.1.~
32
33 python-requests >= 2.9.1
34
35 libgoogle-perftools4 >= 2.4~
36
37 xserver-xorg-core >= 2:1.18
38
39 xserver-xorg-core << 2:1.19
40
41 x11vnc>=0.9.13
42
43 python-websockify >= 0.6.1
```

> **Remarque :**
>
> pour une matrice des distributions Linux et des versions Xorg que cette version du VDA Linux prend en charge, consultez la section Configuration système requise.

Étape 4c : configurer le VDA Linux

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, 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** : 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** : Linux VDA requiert une liste séparée par des espaces de noms de domaines complets. 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** : 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** : 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 Virtual Desktop prend en charge HDX 3D Pro, un ensemble de technologies d'accélération des graphiques conçues pour optimiser la virtualisation des applications riches en graphiques HDX 3D Pro nécessite l'installation d'une carte graphique

NVIDIA GRID compatible. 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** : 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** : 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 VDA Linux envoie une requête à LDAP via une base de recherche définie sur la racine du domaine (Active Directory (par exemple, D, DC=mycompany,DC=com). Toutefois, pour améliorer les performances de recherche, vous pouvez spécifier une base de recherche (par exemple, OU=VDI,DC=mycompany,DC=com). Cette variable est définie sur **<none>** par défaut.
- **CTX_XDL_FAS_LIST = list-fas-servers** : les serveurs du service d'authentification fédérée (FAS) sont configurés via la stratégie de groupe AD. Comme le VDA Linux ne prend pas en charge la stratégie de groupe AD, vous pouvez fournir une liste de serveurs FAS séparés par des points-virgules. La séquence doit être la même que celle configurée dans la stratégie de groupe AD. Si une adresse de serveur est supprimée, remplissez son espace vide avec la chaîne de texte **<none>** et conservez la séquence d'adresses du serveur sans effectuer de modification.
- **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
```



```
14
15 export CTX_XDL_VDI_MODE=Y|N
16
17 export CTX_XDL_SITE_NAME=dns-site-name | '<none>'
18
19 export CTX_XDL_LDAP_LIST=list-ldap-servers | '<none>'
20
21 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
22
23 export CTX_XDL_FAS_LIST = list-fas-servers | '<none>'
24
25 export CTX_XDL_START_SERVICE=Y|N
26
27 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.

Éventuellement, vous pouvez spécifier les paramètres en utilisant une seule commande :

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



```
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 VDA Linux 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 VDA Linux pour que les modifications prennent effet.

Désinstaller le logiciel VDA Linux

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

```
dpkg -l xendesktopvda
```

Pour afficher des informations plus détaillées :

```
apt-cache show xendesktopvda
```

> **Remarque :**
>
> La désinstallation du logiciel VDA Linux 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 VDA Linux 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 VDA Linux

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

Démarrer Linux VDA :

Pour démarrer les services VDA Linux :

```
sudo systemctl start ctxhdx

sudo systemctl start ctxvda
```

Arrêter Linux VDA :

Pour arrêter les services VDA Linux :

```
sudo systemctl stop ctxvda

sudo systemctl stop ctxhdx
```

Redémarrer Linux VDA :

Pour redémarrer les services VDA Linux :

```
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 du VDA Linux :

```
sudo systemctl status ctxvda

sudo systemctl status ctxhdx
```


Étape 6 : créer le catalogue de machines dans Citrix Virtual Apps ou Citrix Virtual Desktops

Le processus de création de catalogues de machines et d'ajout de machines VDA Linux 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 VDA Linux, 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.
- Ne combinez pas de machines VDA Linux 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 d'OS de serveur Windows ou d'OS de serveur implique un modèle de mise à disposition équivalent de bureaux partagés hébergés. La sélection de l'option Système d'exploitation 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 la rejoignez au domaine Active Directory, vous devez supprimer et rajouter la machine au catalogue de machines.

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

Le processus de création d'un groupe de mise à disposition et d'ajout de catalogues de machines contenant des machines VDA Linux 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 VDA Linux, 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 VDA Linux.
- N'autorisez pas l'ouverture de session d'utilisateurs non authentifiés (anonymes).
- Ne combinez pas le groupe de mise à disposition avec des catalogues de machines contenant des machines Windows.

Pour plus d'informations sur la création de catalogues de machines et de groupes de mise à disposition, consultez Citrix Virtual Apps and Desktops 7 1811.

Configurer le VDA Linux

January 11, 2019

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

> **Conseil :**
>
> le script Bash xdlcollect utilisé pour collecter les journaux est intégré dans le logiciel VDA Linux et se trouve dans /opt/Citrix/VDA/bin. Après avoir installé Linux VDA, vous pouvez exécuter la commande **bash /opt/Citrix/VDA/bin/xdlcollect.sh** pour collecter les journaux.
>
> Une fois la collecte de journaux terminée, un fichier journal compressé est généré dans le même dossier que le script. Xdlcollect peut vous demander de télécharger ou non le fichier journal compressé dans Citrix Insight Services (CIS). Si vous acceptez, xdlcollect renvoie upload_ID une fois le téléchargement terminé. Le téléchargement ne supprime pas le fichier journal compressé de votre machine locale. Les autres utilisateurs peuvent utiliser upload_ID pour accéder au fichier journal dans CIS.

Intégrer NIS avec Active Directory

February 15, 2019

Cet article décrit comment intégrer NIS avec Windows Active Directory (AD) sur le VDA Linux à l'aide de SSSD. Le VDA Linux est considéré comme un composant de Citrix Virtual Apps and Desktops. Par conséquent, il s'intègre sans problème à l'environnement Windows Active Directory.

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

> **Remarque :**
>
> L'authentification est toujours effectuée par le serveur Active Directory. NIS+ n'est pas pris en

> charge. Si vous utilisez NIS comme fournisseur d'UID et de GID, les attributs POSIX du serveur Windows ne sont plus utilisés.
>
> **Conseil :**
>
> Cette méthode de déploiement de Linux VDA est obsolète et n'est utilisée que pour des scénarios particuliers. Pour une distribution RHEL/CentOS, suivez les instructions indiquées dans la section Installer Linux Virtual Delivery Agent pour RHEL/CentOS. Pour une distribution Ubuntu, suivez les instructions indiquées dans la section Installer Linux Virtual Delivery Agent pour Ubuntu.

Présentation de SSSD

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

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 7.5 ou version ultérieure
- CentOS 7.5 ou version ultérieure

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.

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

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

Configurer SSSD

La configuration de SSSD comprend les étapes suivantes :

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

- Démarrez le service **sssd**.

/etc/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 :

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

> **Conseil :**
>
> Lors de la configuration des paramètres de VDA Linux, n'oubliez pas qu'il n'y a aucun paramètre spécial pour le client VDA Linux 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 le VDA Linux, vérifiez que le fichier **keytab** système a été créé et contient des clés valides :

```
1 sudo klist -ke
```

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

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

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

February 15, 2019

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 VDA Linux.

Publier des applications à l'aide de Citrix Studio

Vous pouvez publier des applications installées sur un VDA Linux 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 VDA Linux 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 VDA Linux et StoreFront.

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


```
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 VDA Linux. Activez ou désactivez le mode transparent sur le VDA Linux 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 : Mutter, Metacity et Compiz (Ubuntu 16.04). Kwin et les autres gestionnaires de fenêtres ne sont pas pris en charge. Assurez-vous que votre gestionnaire de fenêtres est pris en charge.
- Lorsque vous exécutez plusieurs applications LibreOffice, seule celle lancée en premier s'affiche sur Citrix Studio, car ces applications partagent le processus.
- Il est possible que les applications publiées basées sur Qt5, telles que « Dolphin », n'affichent pas d'icônes. Pour remédier à ce problème, reportez-vous à l'article https://wiki.archlinux.org/index.php/Qt#Configuration_of_Qt5_apps_under_environments_other_than_KDE_Plasma.
- 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

February 15, 2019

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 un certain nombre d'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=
```



```
4
5 model=
6
7 ppdpath=
8
9 drivertype=
```

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

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

```
1 lpinfo -m
2
3 ...
4
5 xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
6
7 xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
8
9 xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
```

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

```
1 Model=xerox/ph3115.ppd.gz
```

Si le pilote d'imprimante universel n'est pas compatible avec l'imprimante cliente, configurez le chemin de fichier ppd du pilote d'imprimante natif. La valeur de **ppdpath** est le chemin d'accès absolu du fichier du pilote d'imprimante natif.

Par exemple, il existe un **pilote ppd** sous /home/tester/NATIVE_PRINTER_DRIVER.ppd :

```
1 ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
```

Il existe trois types de pilote d'imprimante universel fournis par Citrix (postscript, pcl5 et pcl6). Vous pouvez configurer le type de pilote si aucun pilote d'imprimante natif n'est disponible.

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

```
1 drivertype=pcl5
```


La taille de sortie est définie sur zéro

Essayez différents types d'imprimantes. Essayez également avec une imprimante virtuelle comme CutePDF et PDFCreator pour savoir si ce problème est lié au pilote d'imprimante.

La tâche d'impression dépend du pilote de l'imprimante par défaut du client. Il est important d'identifier le type de pilote actif. Si l'imprimante cliente utilise un pilote PCL5 mais que le VDA Linux 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 VDA Linux :

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

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

Impression lente avec les documents volumineux

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

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

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

Recherchez le nom de stratégie configuré dans le fichier.

```
DefaultPolicy default
```

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

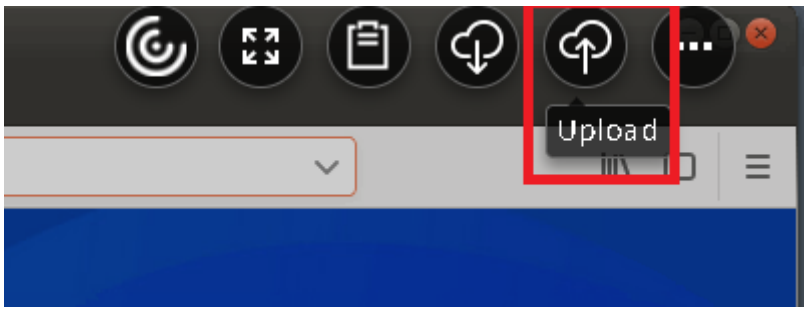

```
<Policy default>

     # Job/subscription privacy...

     JobPrivateAccess default

     JobPrivateValues default

     SubscriptionPrivateAccess default

     SubscriptionPrivateValues default

     … …

     <Limit Create-Printer-Subscription>

          Require user @OWNER

          Order deny,allow

     </Limit>

     <Limit All>

          Order deny,allow

     </Limit>

</Policy>
```

Transfert de fichiers

January 15, 2019

Le transfert de fichiers est pris en charge entre le VDA Linux et le périphérique client. Cette fonctionnalité est disponible lorsque le périphérique client exécute un navigateur Web qui prend en charge l'attribut sandbox HTML5. L'attribut sandbox HTML5 permet aux utilisateurs d'accéder à des bureaux virtuels ou à des applications de navigateur Web à l'aide de l'application Citrix Workspace pour HTML5 ou de l'application Citrix Workspace pour Chrome. Dans le bureau publié ou les sessions d'application de navigateur Web, vous pouvez utiliser la barre d'outils de l'application Citrix Workspace pour charger et télécharger des fichiers entre le VDA Linux et le périphérique client. Par exemple, vous pouvez cli-

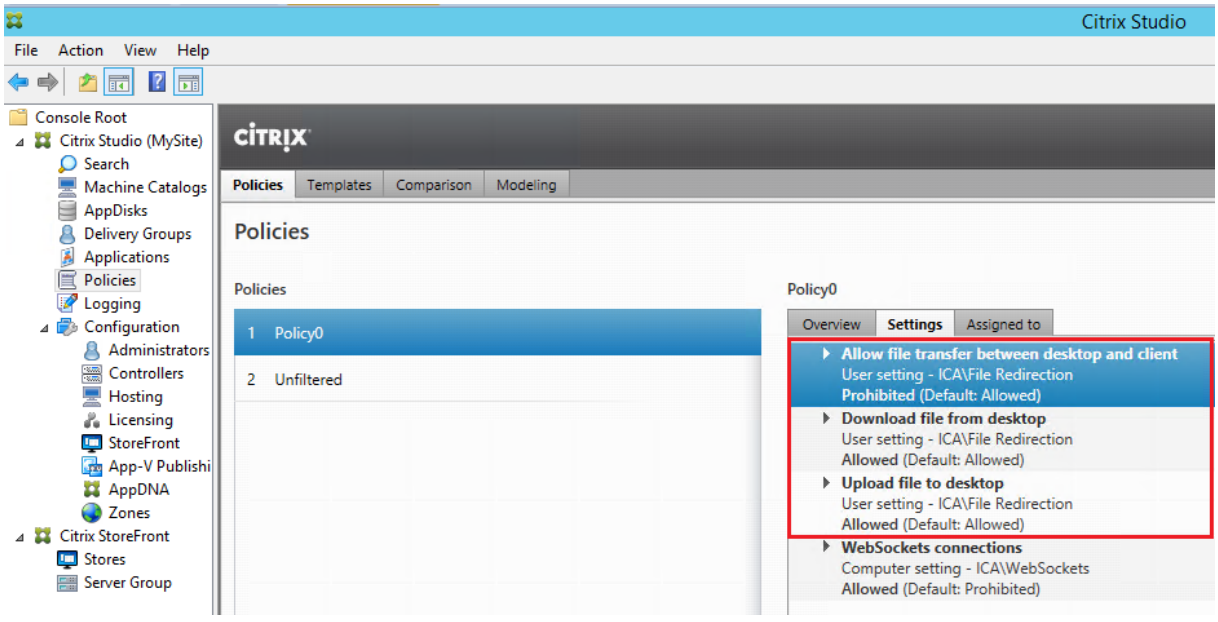
quer sur l'icône **Charger** dans la barre d'outils, choisir un fichier sur le périphérique client et charger le fichier sur le VDA Linux.



> **Remarque :**
>
> cette fonctionnalité est disponible pour RedHat7.5, CentOS7.5, SUSE12.3 et Ubuntu16.04. Pour utiliser cette fonctionnalité, assurez-vous que la barre d'outils de l'application Citrix Workspace est activée.

Stratégies de transfert de fichiers

Vous pouvez utiliser Citrix Studio pour définir les stratégies de transfert de fichiers. Par défaut, le transfert de fichiers est activé.



Descriptions des stratégies :

- **Autoriser le transfert de fichiers entre le bureau et le client.** Autorise ou empêche les utilisateurs de transférer des fichiers entre une session Citrix Virtual Apps and Desktops et leurs appareils.

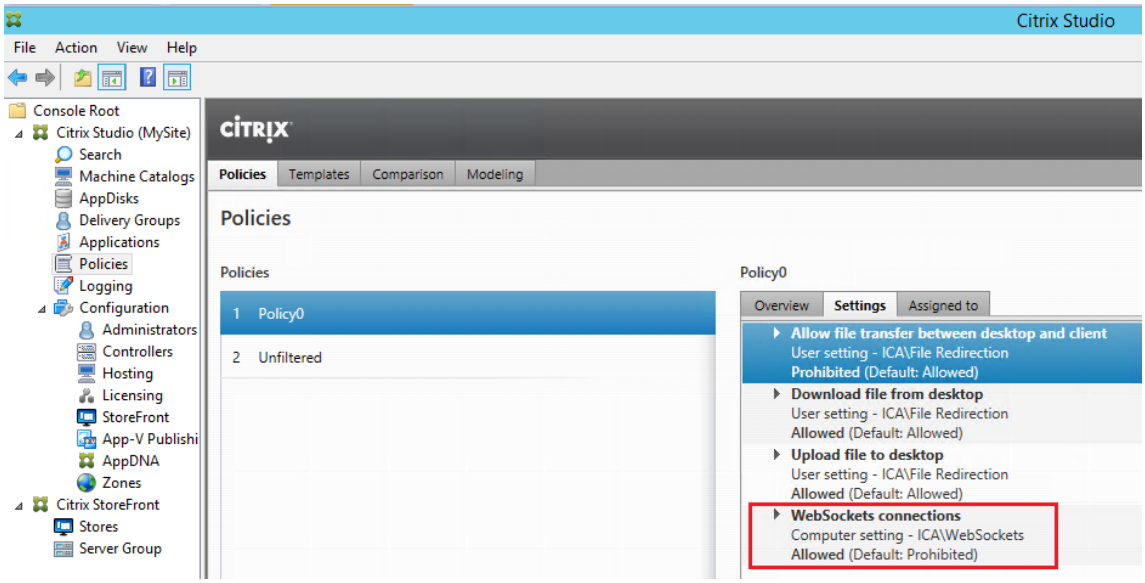
- **Télécharger des fichiers depuis le bureau.** Autorise ou empêche les utilisateurs de télécharger des fichiers depuis une session Citrix Virtual Apps and Desktops vers leurs appareils.
- **Charger des fichiers sur le bureau.** Autorise ou empêche les utilisateurs de charger des fichiers depuis leurs appareils sur une session Citrix Virtual Apps and Desktops.

> **Remarque :**
>
> pour vous assurer que les stratégies **Télécharger des fichiers depuis le bureau** et **Charger des fichiers sur le bureau** prennent effet, définissez l'option **Autoriser le transfert de fichiers entre le bureau et le client** sur **Autorisé**.

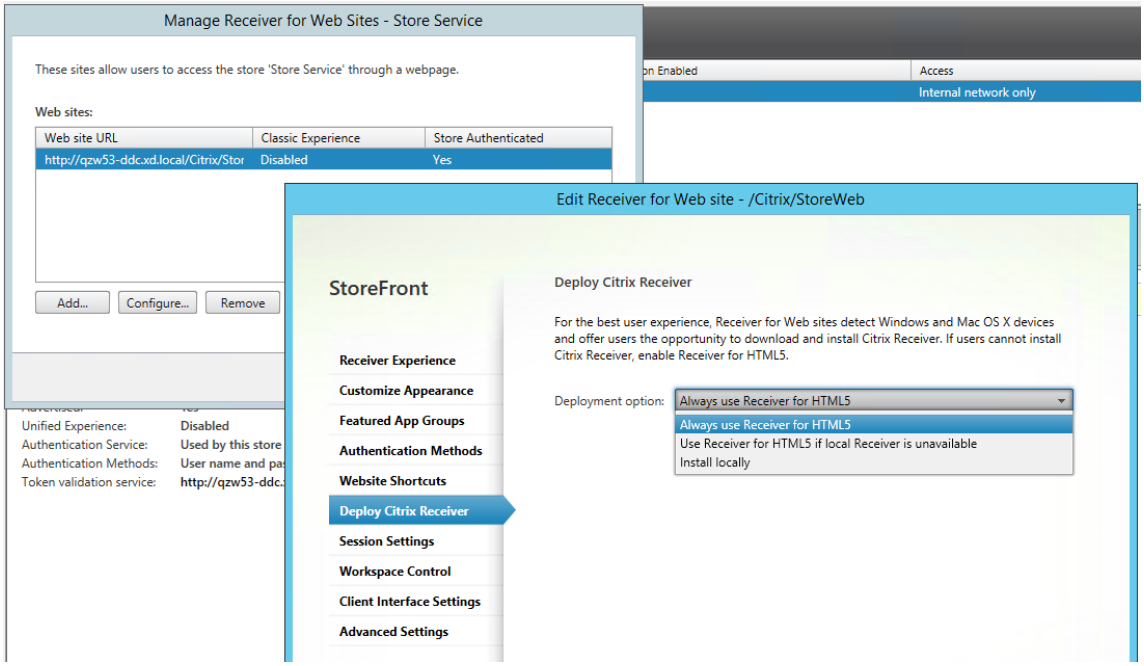
Utilisation

Pour utiliser la fonctionnalité de transfert de fichiers via l'application Citrix Workspace pour HTML5 :

1. Dans Citrix Studio, définissez la stratégie **Connexions WebSockets** sur **Autorisé**.



2. Dans Citrix Studio, activez le transfert de fichiers via les stratégies de transfert de fichiers décrites ci-dessus.
3. Dans la console de gestion Citrix StoreFront, cliquez sur **Magasins**, sélectionnez le nœud **Gérer les sites Receiver pour Web** et activez Citrix Receiver pour HTML5 en sélectionnant l'option **Toujours utiliser Receiver pour HTML5**.



4. Lancez une session de bureau virtuel ou d'application de navigateur Web. Chargez et téléchargez des fichiers entre le VDA Linux et votre périphérique client.

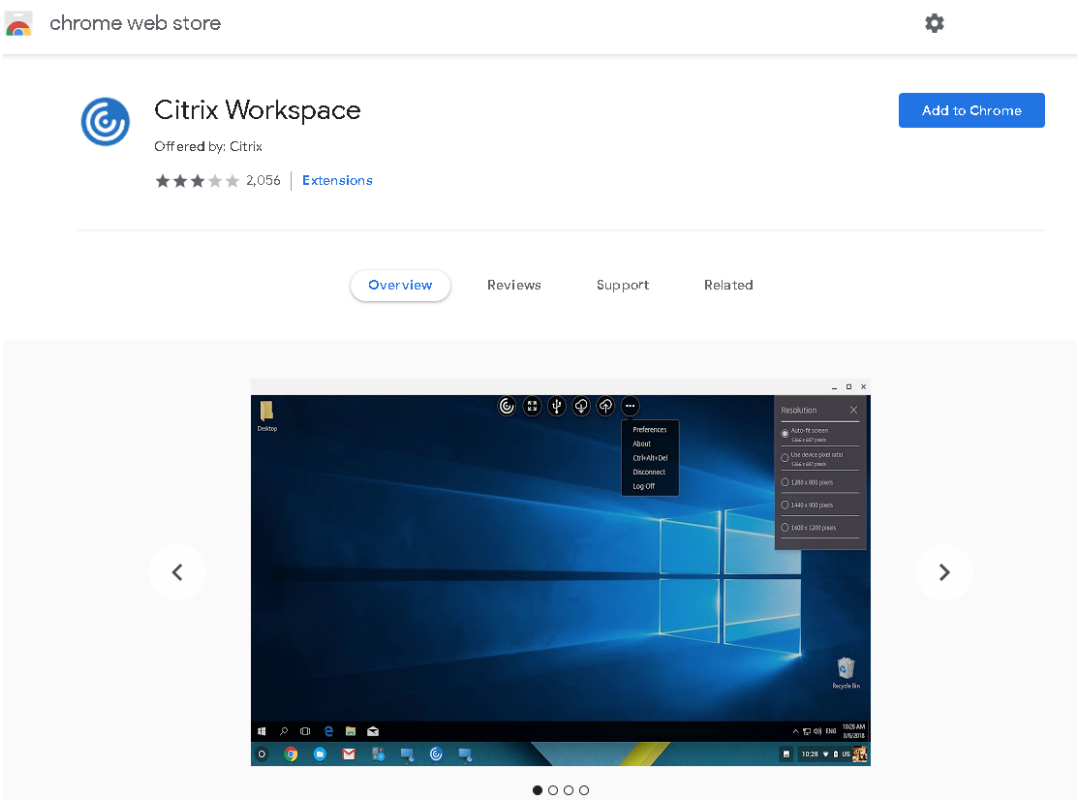
Pour utiliser la fonctionnalité de transfert de fichiers via l'application Citrix Workspace pour Chrome :

1. Activez le transfert de fichiers via les stratégies de transfert de fichiers décrites ci-dessus.
2. Obtenez l'application Citrix Workspace à partir de Chrome Web Store.

   Ignorez cette étape si vous avez déjà ajouté l'application Citrix Workspace pour Chrome à la page des applications Chrome.

   a) Tapez **Citrix Workspace for Chrome** dans la zone de recherche de Google Chrome. Cliquez sur l'icône de recherche.

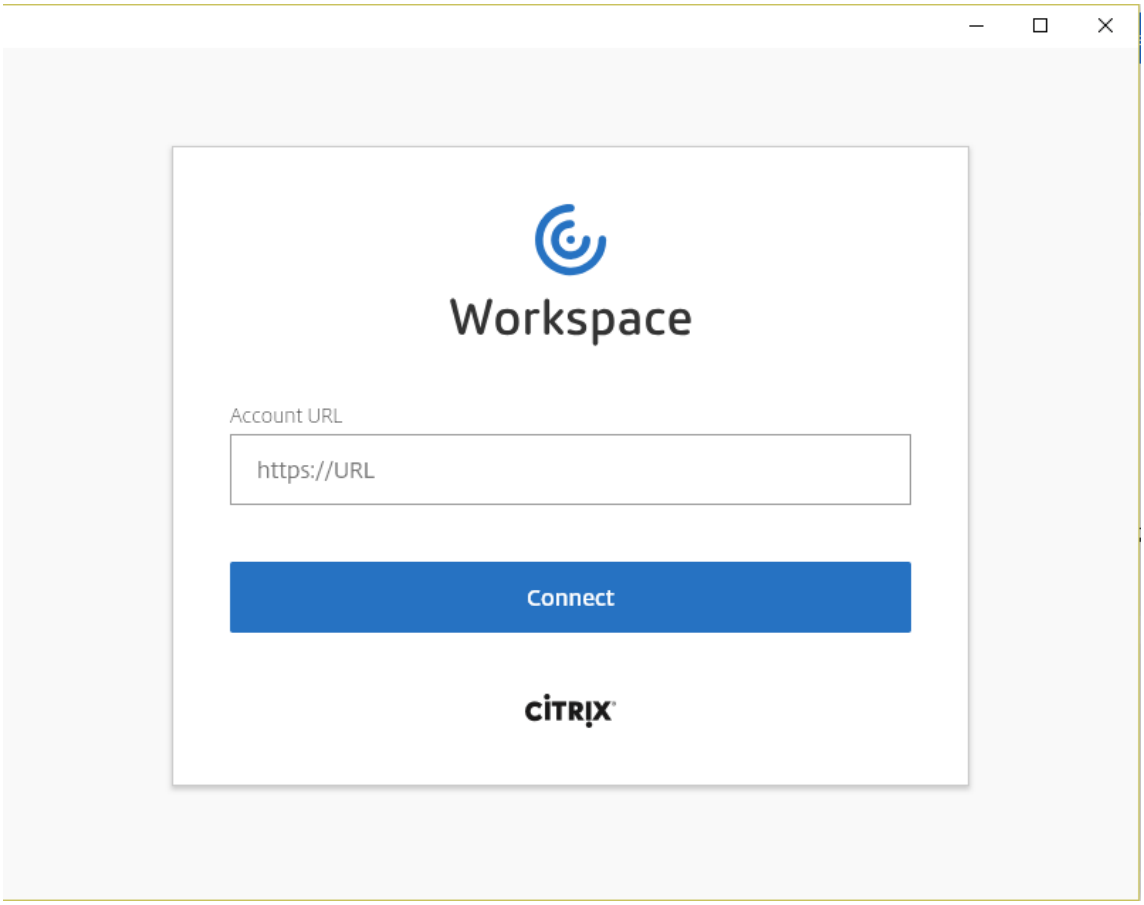
   b) Parmi les résultats de la recherche, cliquez sur l'URL du Chrome Web Store où l'application Citrix Workspace est disponible.



c) Cliquez sur **Ajouter à Chrome** pour ajouter l'application Citrix Workspace à Google Chrome.

3. Cliquez sur l'application Citrix Workspace pour Chrome sur la page des applications Chrome.
4. Tapez l'URL de votre magasin StoreFront pour la connexion.

   Ignorez cette étape si vous avez déjà saisi l'URL.



5. Lancez une session de bureau virtuel ou d'application de navigateur Web. Chargez et téléchargez des fichiers entre le VDA Linux et votre périphérique client.

Impression PDF

February 15, 2019

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 VDA Linux. 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 VDA Linux 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

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

February 15, 2019

Cet article fournit des instructions pour configurer et ajuster les graphiques du VDA Linux.

Pour de plus amples informations, consultez les sections Configuration système requise et Présentation de l'installation.

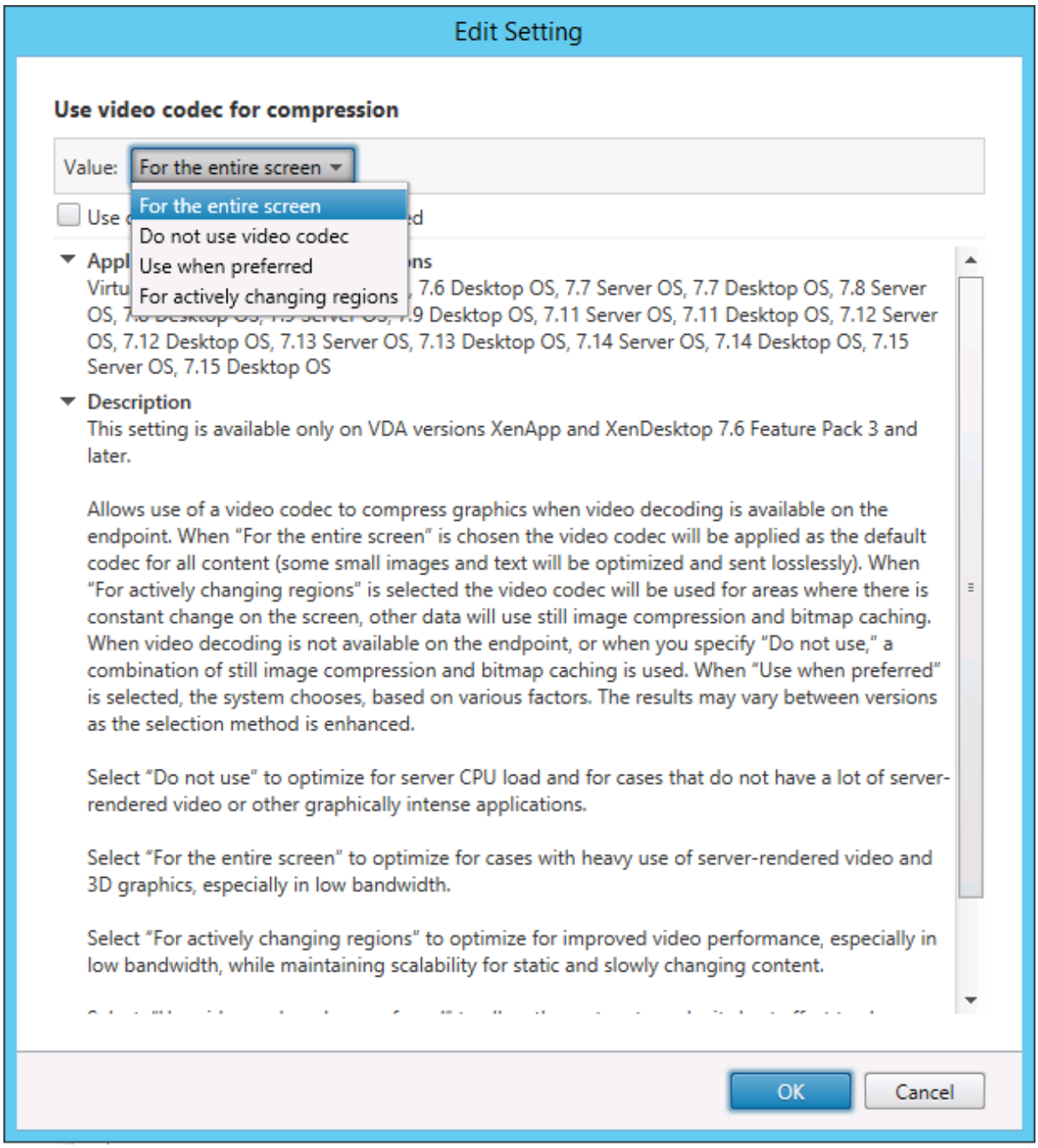
Configuration

Thinwire est la technologie de communication à distance d'écran utilisée dans le VDA Linux. Cette technologie permet aux graphiques générés sur une machine d'être transmis, généralement via un réseau, vers une autre machine.

La stratégie de graphiques **Utiliser codec vidéo pour la compression** définit le mode graphique par défaut et fournit les options suivantes pour différents cas d'utilisation :

- **Utiliser au choix**. il s'agit du réglage par défaut. Aucune configuration supplémentaire n'est requise. Le maintien de ce paramètre assure que Thinwire est sélectionné pour toutes les connexions Citrix, et est optimisé pour la capacité à monter en charge, la bande passante et une qualité d'image supérieure pour les charges de travail de bureau standard.
- **Pour l'écran entier**. ce paramètre permet de mettre à disposition Thinwire avec H.264 ou H.265 plein écran pour optimiser l'expérience utilisateur et la bande passante, particulièrement dans les cas dans lesquels les graphiques 3D sont fortement sollicités.

- **Pour les zones changeant constamment**. la technologie d'affichage adaptatif dans Thinwire identifie les images en mouvement (vidéo, 3D en mouvement) et utilise H.264 uniquement dans la partie de l'écran sur laquelle l'image est en mouvement. L'***utilisation sélective du codec vidéo H.264*** permet à HDX Thinwire de détecter et de coder des parties de l'écran qui sont fréquemment mises à jour à l'aide du codec vidéo H.264, par exemple du contenu vidéo. La compression d'images immobiles (JPEG, RLE) et la mise en cache de bitmaps continuent à être utilisées pour le reste de l'écran, y compris le texte et l'imagerie photographique. Les utilisateurs bénéficient d'une bande passante plus faible et d'une meilleure qualité pour le contenu vidéo, conjointement avec du texte sans perte ou à des images de haute qualité. Pour activer cette fonctionnalité, remplacez le paramètre de stratégie **Utiliser codec vidéo pour la compression** par **Utiliser au choix** (valeur par défaut) ou **Pour les zones changeant constamment**. Pour plus d'informations, veuillez consulter la section Paramètres de stratégie des graphiques.



D'autres paramètres de stratégie, y compris les paramètres de stratégie Affichage visuel suivants, peuvent être utilisés pour optimiser les performances de la communication à distance d'écran :

- **Nombre de couleurs préféré pour les graphiques simples**
- **Taux de trames cible**
- **Qualité visuelle**

Utilisation de H.264 pour l'option Sans perte si possible dans Thinwire

Par défaut, la préférence **Sans perte si possible** du paramètre de stratégie **Qualité visuelle** est désormais H.264 au lieu de JPEG pour les images en mouvement.

L'encodage H.264 offre une qualité d'image supérieure. La stratégie **Utiliser codec vidéo pour la compression** contrôle cette préférence avec la valeur par défaut **Utiliser au choix**. Pour forcer l'option **Sans perte si possible** à utiliser JPEG, définissez la stratégie **Utiliser codec vidéo pour la compression** sur **Ne pas utiliser de codec vidéo**. Si votre client ne prend pas en charge le mode sélectif H.264, l'option **Sans perte si possible** revient au format JPEG, quels que soient les paramètres de stratégie. Citrix Receiver pour Windows 4.9 à 4.12, Citrix Receiver pour Linux 13.5 à 13.10, l'application Citrix Workspace 1808 pour Windows et versions ultérieures, et Citrix Workspace application 1808 pour Linux et versions ultérieures prennent en charge Sélectif H.264. Pour plus d'informations sur les paramètres de stratégie **Qualité visuelle** et **Utiliser codec vidéo pour la compression**, consultez la section Paramètres de stratégie Affichage visuel et Paramètres de stratégie Graphiques.

Prise en charge du codec vidéo H.265

À compter de la version 7.18, le VDA Linux prend en charge le codec vidéo H.265 pour l'accélération matérielle des graphiques et vidéos distants. Vous pouvez utiliser cette fonctionnalité sur Citrix Receiver pour Windows 4.10 à 4.12 et sur l'application Citrix Workspace 1808 pour Windows et versions ultérieures. Pour bénéficier de cette fonctionnalité, activez-la à la fois sur le VDA Linux et sur votre client. Si le GPU de votre client ne prend pas en charge le décodage H.265 à l'aide de l'interface DXVA, le paramètre de stratégie de décodage H265 pour les graphiques est ignoré et la session utilise le codec vidéo H.264. Pour plus d'informations, consultez la section Codage vidéo H.265.

Pour activer le codage matériel H.265 sur le VDA :

1. Activez la stratégie **Utiliser le codage matériel pour le codec vidéo**.
2. Activez la stratégie **Optimiser pour la charge des graphiques 3D**.
3. Assurez-vous que la stratégie **Utiliser codec vidéo pour la compression** est définie par défaut ou définie sur **Pour l'écran entier**.
4. Assurez-vous que la stratégie **Qualité visuelle** n'est **PAS** définie sur **Sans perte si possible** ni sur **Toujours sans perte**.

Pour activer le codage matériel H.265 sur votre client, consultez la section Codage vidéo H.265.

Prise en charge du codage logiciel YUV444

Le VDA Linux prend en charge le codage logiciel YUV444. Le schéma de codage YUV attribue à chaque pixel des valeurs de luminosité et de couleur. En YUV, ' Y 'représente la luminosité, ou' luma 'valeur, et' UV 'représente la couleur ou les valeurs de' chroma '. Vous pouvez utiliser cette fonctionnalité du

VDA Linux sur Citrix Receiver pour Windows 4.10 à 4.12 et sur l'application Citrix Workspace 1808 pour Windows et versions ultérieures.

Chaque valeur unique Y, U et V comprend 8 bits, ou un octet, de données. Le format de données YUV444 transmet 24 bits par pixel. Le format de données YUV422 partage les valeurs U et V entre deux pixels, ce qui permet un taux de transmission moyen de 16 bits par pixel. Le tableau suivant contient une comparaison intuitive entre YUV444 et YUV420.

YUV444

	A	B	C
1	Citrix	Citrix	Citrix
2	Citrix	Citrix	Citrix
3	Citrix	Citrix	Citrix
4	Citrix	Citrix	Citrix
5	Citrix	Citrix	Citrix
6	Citrix	Citrix	Citrix

YUV420

	A	B	C
1	Citrix	Citrix	Citrix
2	Citrix	Citrix	Citrix
3	Citrix	Citrix	Citrix
4	Citrix	Citrix	Citrix
5	Citrix	Citrix	Citrix
6	Citrix	Citrix	Citrix

Pour activer le codage logiciel YUV444 sur le VDA :

1. Activez la stratégie **Autoriser la compression visuelle sans perte**.
2. Assurez-vous que la stratégie **Utiliser codec vidéo pour la compression** est définie sur **Pour l'écran entier**.
3. Assurez-vous que la stratégie **Qualité visuelle** est définie sur **Toujours sans perte** ou **Sans perte si possible**

Ajuster les débits moyens en fonction des estimations de bande passante

Citrix améliore le codage matériel HDX 3D Pro en ajustant les débits binaires moyens en fonction des estimations de bande passante.

Lorsque le codage matériel HDX 3D Pro est utilisé, le VDA peut estimer par intermittence la bande passante du réseau et ajuster les débits des images codées en fonction des estimations de bande passante. Cette nouvelle fonctionnalité fournit un mécanisme pour équilibrer la netteté et la fluidité.

Par défaut, cette fonction est activée. Pour le désactiver, exécutez la commande suivante :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
     CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
     DisableReconfigureEncoder" -d "0x00000001" --force
```

Outre l'utilisation de cette fonctionnalité, vous pouvez également exécuter les commandes suivantes pour régler la netteté et la fluidité. Les paramètres **AverageBitRatePercent** et **MaxBitRatePercent** définissent le pourcentage d'utilisation de la bande passante. Les valeurs les plus élevées que vous

définissez, les graphiques plus nets et la fluidité moindre que vous obtenez. La plage de réglages recommandée est de 50 à 100.

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    AverageBitRatePercent" -d "90" --force

sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    MaxBitRatePercent" -d "100" --force
```

Avec le réglage de débit binaire moyen, lorsque votre écran reste immobile, l'image la plus récente reste dans un état de mauvaise qualité car aucune nouvelle image n'est envoyée. L'amélioration de la netteté peut résoudre ce problème en reconfigurant et en envoyant immédiatement l'image la plus récente avec la plus haute qualité.

Pour une liste complète des stratégies prises en charge par Linux VDA Thinwire, consultez la Liste des stratégies prises en charge.

Pour plus d'informations sur la configuration de la prise en charge de moniteurs multiples sur Linux VDA, consultez CTX220128.

Résolution des problèmes

Vérifier quel mode graphique est utilisé

Exécutez la commande suivante pour vérifier quel mode graphique est utilisé (**0** signifie TW+ ; **1** signifie codec vidéo plein écran) :

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep GraphicsMode
```

Le résultat ressemble à:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"-v "
GraphicsMode"-d "0x00000000"--force
```

Vérifier si H.264 est utilisé

Exécutez la commande suivante pour vérifier si H.264 est en cours d'utilisation (**0** signifie pas en cours d'utilisation ; **1** signifie en cours d'utilisation) :

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H264
```


Le résultat ressemble à:

```
create -k ”HKLM\Software\Citrix\Ica\Session\4\Graphics”-t ”REG_DWORD”-v ”
H264”-d ”0x00000000”--force
```

Vérifier si H.265 est utilisé

Exécutez la commande suivante pour vérifier si H.265 plein écran est en cours d'utilisation (**0** signifie pas en cours d'utilisation ; **1** signifie en cours d'utilisation) :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H265
```

Le résultat ressemble à:

```
create -k ”HKLM\Software\Citrix\Ica\Session\4\Graphics”-t ”REG_DWORD”-v ”
H265”-d ”0x00000000”--force
```

Vérifier quel schéma de codage YUV est utilisé

Exécutez la commande suivante pour vérifier quel schéma de codage YUV est utilisé (**0** signifie YUV420 ; **1** signifie YUV422 ; **2** signifie YUV444) :

Remarque : la valeur de YuvFormat n'a de sens que lorsqu'un codec vidéo est utilisé.

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep YUVFormat
```

Le résultat ressemble à:

```
create -k ”HKLM\Software\Citrix\Ica\Session\4\Graphics”-t ”REG_DWORD”-v ”
YUVFormat”-d ”0x00000000”--force
```

Vérifier si le codage logiciel YUV444 est utilisé

Exécutez la commande suivante pour vérifier si le codage logiciel YUV444 est utilisé :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep Graphics
```

Lorsque YUV444 est utilisé, le résultat ressemble à cela :

```
create -k ”HKLM\Software\Citrix\Ica\Session\4\Graphics”-t ”REG_DWORD”-v ”
GraphicsMode”-d ”0x00000001”--force
create -k ”HKLM\Software\Citrix\Ica\Session\4\Graphics”-t ”REG_DWORD”-v ”
H264”-d ”0x00000001”--force
```



```
create -k ”HKLM\Software\Citrix\Ica\Session\4\Graphics”-t ”REG_DWORD”-v ”
HardwareEncoding”-d ”0x00000000”--force
create -k ”HKLM\Software\Citrix\Ica\Session\4\Graphics”-t ”REG_DWORD”-v ”
YUVFormat”-d ”0x00000002”--force
```

Vérifier si le codage matériel est utilisé pour 3D Pro

Exécutez la commande suivante (**0** signifie qu'il n'est pas utilisé, **1** signifie qu'il est utilisé) :

```
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 :

```
Tue Apr 12 10:42:03 2016
+-----------------------------------------------------+
| NVIDIA-SMI 361.28     Driver Version: 361.28        |
|-------------------------------+----------------------+----------------------+

| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
   Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
   Compute M. |
|===============================+======================+======================|

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


+-----------------------------------------------------------------------------+

| Processes:                                                       GPU
   Memory |
|  GPU       PID  Type  Process name
   Usage      |
|=============================================================================|
```



```
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 :

```
1  +-----------------------------------------------------+
2  | NVIDIA-SMI 352.70     Driver Version: 352.70        |
3  |-------------------------------+----------------------+----------------------+

4  | GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
      Uncorr. ECC |
5  | Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
      Compute M. |
6  |===============================+======================+======================|

7  |   0  Tesla M60           Off  | 0000:00:05.0     Off |
                       Off |
8  | N/A   20C    P0    37W / 150W |     19MiB /  8191MiB |      0%
      Default |
9  +-------------------------------+----------------------+----------------------+

10
11 +-----------------------------------------------------------------------------+

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

15 |  No running processes found
                                    |
16 +-----------------------------------------------------------------------------+
```

Définissez la configuration correcte pour la carte :

`etc/X11/ctx-nvidia.sh`

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

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

Vérifier les journaux d'erreurs Xorg

Le nom du fichier journal Xorg est similaire à **Xorg.{DISPLAY}.log** idans 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 :

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

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

Si le paramètre de stratégie **Sans perte si possible** est activé, un écran noir ou gris apparaît lorsque les utilisateurs lancent une application ou une session de bureau avec une carte graphique NVIDIA K2. Ce problème se produit car les cartes graphiques NVIDIA K2 ne prennent pas en charge le codage matériel YUV444 en mode passthrough. Pour plus d'informations, consultez la page Video Encode and Decode GPU Support Matrix.

Les fenêtres contextuelles du bureau Gnome 3 sont lentes lors de l'ouverture de session

Il s'agit d'une limitation du démarrage de session de bureau Gnome 3.

Certaines applications OpenGL/WebGL ne s'affichent pas correctement après le redimensionnement de l'application Citrix Workspace

Si vous redimensionnez la fenêtre de l'application Citrix Workspace, la résolution de l'écran est modifiée. Le pilote propriétaire NVIDIA modifie certains états internes et peut attendre des applications une

réponse adaptée. Par exemple, l'élément de bibliothèque WebGL **lightgl.js** peut générer une erreur « `Rendering to this texture is not supported (incomplete frame buffer)` ».

Affichage progressif Thinwire

January 11, 2019

L'interactivité de session peut se dégrader sur des connections à faible bande passante ou à latence élevée. Par exemple, sur les connexions avec une bande passante inférieure à 2 Mbits/s ou une latence de plus de 200 ms, le défilement sur une page Web peut devenir lent, ne pas répondre ou être saccadé. Les opérations clavier et souris peuvent être décalées par rapport aux mises à jour graphiques.

Jusqu'à la version 7.17, vous pouviez utiliser les paramètres de stratégie pour réduire la consommation de bande passante en configurant la session sur une **faible** qualité visuelle ou en définissant une profondeur de couleur inférieure (graphiques 16 ou 8 bits). Cependant, vous aviez besoin de savoir qu'un utilisateur était sur une connexion faible. HDX Thinwire ne pouvait pas ajuster dynamiquement la qualité des images statiques en fonction des conditions du réseau.

À compter de la version 7.18, HDX Thinwire bascule par défaut en mode de mise à jour progressive lorsque la bande passante disponible tombe en dessous de 2 Mbits/s, ou que la latence du réseau dépasse 200 ms. Dans ce mode :

- Toutes les images statiques sont fortement compressées.
- La qualité du texte est réduite.

Par exemple, dans le graphique suivant où le mode de mise à jour progressive est actif, les lettres **F** et **e** disposent d'artefacts bleus et l'image est fortement compressée. Cette approche réduit considérablement la consommation de bande passante, ce qui permet de recevoir les images et le texte plus rapidement et améliore l'interactivité de la session.

Lorsque vous arrêtez d'interagir avec la session, les images et le texte dégradés sont progressivement affinés sans perte. Par exemple, dans le graphique suivant, les lettres ne contiennent plus d'artefacts bleus et la qualité de l'image est restaurée.

Features

Pour les images, l'amélioration de la netteté utilise une méthode aléatoire de type bloc. Pour le texte, des lettres individuelles ou des parties de mots sont affinées. Le processus d'amélioration de la netteté se produit sur plusieurs trames. Cette approche évite d'introduire un retard avec une trame importante unique d'amélioration de la netteté.

Les images transitoires (vidéo) sont toujours gérées avec l'affichage adaptatif ou sélectif H.264.

Utilisation du mode progressif

Par défaut, le mode progressif attend les paramètres de la stratégie **Qualité visuelle** : **Élevé**, **Moyen** (par défaut) et **Faible**.

Le mode progressif est désactivé (non utilisé) lorsque :

- **Qualité visuelle** = **Toujours sans perte** ou **Sans perte si possible**
- **Nombre de couleurs préféré pour les graphiques simples** = 8 bits
- **Utiliser codec vidéo pour la compression** = **Pour l'écran entier** (lorsque le mode H.264 en plein écran est souhaité)

Lorsque le mode progressif est en veille, il est activé par défaut lorsque l'une des conditions suivantes se présente :

- La bande passante disponible est inférieure à 2 Mbits/s.
- La latence du réseau est supérieure à 200 ms.

Après un changement de mode, un minimum de 10 s est passé dans ce mode, même si les conditions de réseau défavorables sont momentanées.

Changement du comportement du mode progressif

Vous pouvez modifier le comportement du mode progressif en exécutant la commande suivante :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    ProgressiveDisplay" -d "<value>" --force
```


où <la valeur> est :

0 = Toujours désactivé (ne jamais utiliser)

1 = Automatique (bascule en fonction des conditions du réseau, valeur par défaut)

2 = Toujours activé

En mode automatique (1), vous pouvez exécuter les commandes suivantes pour modifier les seuils de basculement du mode progressif :

```
sudo /opt/Citrix/VDA/bin/ctxreg  create -k "HKEY_LOCAL_MACHINE\SYSTEM\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    ProgressiveDisplayBandwidthThreshold" -d "<value>" --force
```

où <la valeur> est <le seuil en Kbits/s> (par défaut = 2 048)

Exemple : 4096 = bascule en mode progressif si la bande passante descend sous 4 Mbits/s

```
sudo /opt/Citrix/VDA/bin/ctxreg  create -k "HKEY_LOCAL_MACHINE\SOFTWARE
    \CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    ProgressiveDisplayLatencyThreshold" -d "<value>" --force
```

où la valeur est <le seuil en Kbits/s> (par défaut = 200)

Exemple : 100 = bascule en mode progressif si le réseau descend sous 100 ms.

Graphiques 3D non-GRID

January 11, 2019

Généralités

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.

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 en utilisant « 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 VDA Linux.

   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 VDA Linux de reconnaître le nom du fichier de configuration défini à l'étape 1.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\System\
    CurrentControlSet\Control\Citrix\XDamage" -t "REG_SZ" -v "
    DriverName" -d "intel" --force
```


Activer la fonctionnalité de graphiques 3D non-GRID

Cette fonctionnalité est désactivée par défaut. Vous pouvez exécuter la commande suivante pour l'activer en définissant XDamageEnabled sur 1.

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\System\
    CurrentControlSet\Control\Citrix\XDamage" -t "REG_DWORD" -v "
    XDamageEnabled" -d "0x00000001" --force
```

Résolution des problèmes

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 afin de collecter les informations de traçage à des fins de débogage.

Le codage matériel ne fonctionne pas

Cette fonctionnalité prend uniquement en charge le codage logiciel.

Configurer les stratégies

February 15, 2019

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 VDA Linux.

RHEL/CentOS :

```
sudo yum -y install openldap

sudo yum -y install libxml2
```



```
4
5 sudo yum -y install cyrus-sasl
6
7 sudo yum -y install cyrus-sasl-gssapi
```

SLES/SELD :

```
1 sudo zypper install openldap2
2
3 sudo zypper install libxml2
4
5 sudo zypper install cyrus-sasl
6
7 sudo zypper install cyrus-sasl-gssapi
```

Ubuntu :

```
1 sudo apt-get install -y libldap-2.4-2
2
3 sudo apt-get install -y libsasl2-2
4
5 sudo apt-get install -y libsasl2-modules-gssapi-mit
```

Configuration

Paramètres de stratégie dans Citrix Studio

Pour configurer des stratégies dans Citrix Studio, procédez comme suit :

1. Ouvrez **Citrix Studio**.
2. Sélectionnez le panneau **Stratégies**.
3. Cliquez sur **Créer une stratégie**.
4. Définissez la stratégie en fonction de la liste de stratégies prises en charge.

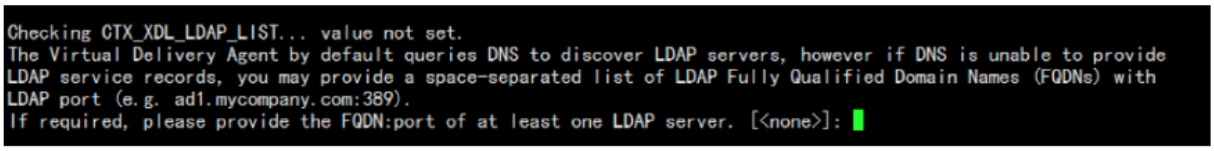
Paramètre du serveur LDAP sur le VDA

Le paramètre du serveur LDAP sur le VDA Linux 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 VDA Linux, 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).



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
```

Liste des stratégies prises en charge

February 15, 2019

Liste des stratégies prises en charge avec le VDA Linux

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Limite de bande passante globale de session	LimitOverallBw	User	ICA\Bande passante	0
Limite de bande passante de redirection audio	LimitAudioBw	User	ICA\Bande passante	0
Pourcentage de limite de bande passante de la redirection audio	LimitAudioBwPerc	User	ICA\Bande passante	0

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Limite de bande passante de redirection du périphérique USB client	LimitUSBBw	User	ICA\Bande passante	0
Pourcentage de bande passante de redirection du périphérique USB client	LimitUSBBwPerce	User	ICA\Bande passante	0
Limite de bande passante de redirection du Presse-papiers	LimitClipbdBW	User	ICA\Bande passante	0
Pourcentage de la limite de la bande passante de redirection du Presse-papiers	LimitClipbdBWPer	User	ICA\Bande passante	0
Limite de bande passante de redirection de fichier	LimitCdmBw	User	ICA\Bande passante	0
Pourcentage de limite de bande passante de redirection de fichier	LimitCdmBwPerce	User	ICA\Bande passante	0
Limite de bande passante de redirection d'imprimante	LimitPrinterBw	User	ICA\Bande passante	0

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Pourcentage de limite de bande passante de redirection de l'imprimante	LimitPrinterBwPer	User	ICA\Bande passante	0
Connexions WebSockets	AcceptWebSocketsC	Ordinateur	ICA\WebSockets	Interdit
Numéro de port WebSockets	WebSocketsPort	Ordinateur	ICA\WebSockets	8008
Liste de serveurs d'origine approuvés WebSockets	WSTrustedOriginSe	Ordinateur	ICA\WebSockets	*
Persistances ICA	SendICAKeepAlive	Ordinateur	Persistance ICA	Ne pas envoyer de messages de persistance ICA (0)
Délai d'expiration de persistance ICA	ICAKeepAliveTimeo	Ordinateur	Persistance ICA	60 secondes
Numéro de port de l'écouteur ICA	IcaListenerPortNu	Ordinateur	ICA	1494
Transport adaptatif HDX	HDXoverUDP	Ordinateur	ICA	Préféré (2)
Connexions de fiabilité de session	AcceptSessionReli	Ordinateur	ICA\Fiabilité de session	Autorisé (1)
Niveau de transparence de l'interface durant la reconnexion	ReconnectionUiTra	Ordinateur	ICA\Reconnexion automatique des clients	80 %
Numéro de port de la fiabilité de session	SessionReliabilityP	Ordinateur	ICA\Fiabilité de session	2598

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Expiration de délai de la fiabilité de session	SessionReliabilityTimeout	Ordinateur	ICA\Fiabilité de session	180 s
Reconnexion automatique des clients	AllowAutoClientRe	User	ICA\Reconnexion automatique des clients	Autorisé (1)
Redirection audio cliente	AllowAudioRedirection	User	Audio	Autorisé (1)
Redirection d'imprimante cliente	AllowPrinterRedir	User	Impression	Autorisé (1)
Créer automatiquement l'imprimante universelle PDF	AutoCreatePDFPrinter	User	Impression	Désactivé (0)
Redirection de Presse-papiers client	AllowClipboardRe	User	Presse-papiers	Autorisé (1)
Redirection de périphérique USB client	AllowUSBRedir	User	USB	Interdit (0)
Règles de redirection des périphériques USB clients	USBDeviceRules	User	USB	« \{0} »
Compression d'images en mouvement	MovingImageCompressi	SessionConfiguration	ThinWire	Activé (1)
Compression couleur supplémentaire	ExtraColorCompre	User	ThinWire	Désactivé (0)
Taux de trame minimum cible	TargetedMinimumFramesPerSecond		ThinWire	10 fps

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Taux de trames cible	FramesPerSecond	User	ThinWire	30 fps
Qualité visuelle	VisualQuality	User	ThinWire	Moyenne (3)
Utiliser codec vidéo pour la compression	VideoCodec	User	ThinWire	Utiliser au choix (3)
Utiliser le codage matériel pour le codec vidéo	UseHardwareEncodingF	UserForVideoCodec	ThinWire	Activé (1)
Autoriser la compression visuelle sans perte	AllowVisuallyLossl	User	ThinWire	Désactivé (0)
Optimiser pour la charge des graphiques 3D	OptimizeFor3dWorkload	User	ThinWire	Désactivé (0)
Nombre de couleurs préféré pour les graphiques simples	PreferredColorDep	User	ThinWire	24 bits par pixel (1)
Qualité audio	SoundQuality	User	Audio	Élevée : audio à définition élevée (2)
Redirection du microphone client	AllowMicrophoneF	User	Audio	Autorisé (1)
Nombre maximum de sessions	MaximumNumberOfSessions	Ordinateur	Gestion de la charge	250
Tolérance d'ouvertures de session simultanées	ConcurrentLogons	Ordinateur	Gestion de la charge	2.

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Activer la mise à jour automatique des contrôleurs	EnableAutoUpdateOfControllers	Computer	Paramètres Virtual Delivery Agent	Autorisé (1)
Mode de mise à jour de la sélection du Presse-papiers	ClipboardSelectionUpdateMode	User	Presse-papiers	3
Mode de mise à jour de la sélection principale	PrimarySelectionUpdateMode	User	Presse-papiers	3
Qualité speex maximale	MaxSpeexQuality	User	Audio	5
Connecter automatiquement les lecteurs clients	AutoConnectDrives	User	Redirection de fichier/CDM	Activé (1)
Lecteurs optiques clients	AllowCdromDrives	User	Redirection de fichier/CDM	Autorisé (1)
Lecteurs fixes clients	AllowFixedDrives	User	Redirection de fichier/CDM	Autorisé (1)
Lecteurs de disquette clients	AllowFloppyDrives	User	Redirection de fichier/CDM	Autorisé (1)
Lecteurs réseau clients	AllowNetworkDrives	User	Redirection de fichier/CDM	Autorisé (1)
Lecteurs amovibles clients	AllowRemoveableDrives	User	Redirection de fichier/CDM	Autorisé (1)
Redirection de lecteur client	AllowDriveRedir	User	Redirection de fichier/CDM	Autorisé (1)
Accès en lecture unique sur le lecteur client	ReadOnlyMappedDrive	User	Redirection de fichier/CDM	Désactivé (0)

Stratégie Studio	Nom de la clé	Type	Module	Valeur par défaut
Affichage de clavier automatique	AllowAutoKeyboardPopUp	User	MRVC	Désactivé (0)
Autoriser le transfert de fichiers entre le bureau et le client	AllowFileTransfer	User	Transfert de fichiers	Autorisé
Télécharger des fichiers depuis le bureau	AllowFileDownload	User	Transfert de fichiers	Autorisé
Charger des fichiers sur le bureau	AllowFileUpload	User	Transfert de fichiers	Autorisé

Configurer IPv6

January 11, 2019

Le VDA Linux prend en charge IPv6 pour s'aligner avec Citrix Virtual Apps and Desktops. Lors de l'utilisation de cette fonctionnalité, considérez ce qui suit :

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

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

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

Configurer le protocole IPv6 pour le VDA Linux

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


```
1 “HKLM\Software\Policies\Citrix\VirtualDesktopAgent” -t “REG_DWORD”
    -v “OnlyUseIPv6ControllerRegistration”
2 “HKLM\Software\Policies\Citrix\VirtualDesktopAgent” -t “REG_DWORD”
    -v “ControllerRegistrationIPv6Netmask”
```

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

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k ”HKLM\Software\Policies\
    Citrix\VirtualDesktopAgent” -t ”REG_DWORD” -v ”
    OnlyUseIPv6ControllerRegistration” -d ”0x00000001” --force
```

Si l’agent Linux VDA comporte plusieurs interfaces réseau, **ControllerRegistrationIPv6Netmask** peut être utilisé pour spécifier l’interface à utiliser pour l’enregistrement de Linux VDA :

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

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

Pour plus d’ informations sur le déploiement IPv6 dans Citrix Virtual Apps and Desktops, consultez la section Prise en charge d’IPv4/IPv6.

Résolution des problèmes

Vérifiez l’environnement réseau IPv6 de base et utilisez ping6 pour vérifier si AD et Delivery Controller sont accessibles.

Configurer CEIP

January 11, 2019

Lorsque vous choisissez de participer au Programme d’amélioration de l’expérience utilisateur (CEIP), des informations d’utilisation et des statistiques anonymes sont envoyées à Citrix pour nous aider à améliorer la qualité et les performances des produits Citrix. En outre, une copie des données anonymes est envoyée à Google Analytics (GA) pour une analyse rapide et efficace.

Paramètres de registre

Par défaut, vous participez automatiquement au programme CEIP lorsque vous installez le VDA Linux. Le premier chargement de données se produit approximativement sept jours après l'installation du VDA Linux. Vous pouvez modifier ce paramètre par défaut dans le registre.

- **CEIPSwitch**

Paramètre de Registre qui active ou désactive le programme CEIP (valeur par défaut = 0) :

Emplacement : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Nom : CEIPSwitch

Valeur : 1 = désactivé, 0 = activé

Si elle n'est pas spécifiée, le programme CEIP est activé.

Vous pouvez exécuter la commande suivante sur un client pour désactiver le programme CEIP.

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\ SOFTWARE\
     Citrix\CEIP" -v "CEIPSwitch" -d "1"
```

- **GASwitch**

Paramètre de Registre qui active ou désactive GA (valeur par défaut = 0) :

Emplacement : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Nom : GASwitch

Valeur : 1 = désactivé, 0 = activé

Si elle n'est pas spécifiée, GA est activé.

Vous pouvez exécuter la commande suivante sur un client pour désactiver GA :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\ SOFTWARE\
     Citrix\CEIP" -v "GASwitch" -d "1"
```

- **DataPersistPath**

Paramètre de Registre qui contrôle le chemin d'accès des données persistantes (défaut = /var/xdl/-ceip) :

Emplacement : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Nom : DataPersistPath

Valeur : chaîne

Vous pouvez exécuter la commande suivante pour définir ce chemin d'accès :


```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\ SOFTWARE\
    Citrix\CEIP" -v "DataPersistPath" -d "your_path"
```

Si le chemin d'accès que vous avez 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 VDA Linux

Le tableau suivant présente un exemple de types d'informations anonymes collectées. Les données ne contiennent aucun détail permettant d'identifier le client.

Point de données	Nom de la clé	Description
GUID de machine	machine_guid	Identification de la machine d'où les données proviennent
Solution Active Directory	ad_solution	Chaîne de texte indiquant la méthode de jonction du domaine de la machine
Version du noyau Linux	kernel_version	Chaîne de texte indiquant la version du noyau de la machine
Version LVDA	vda_version	Chaîne de texte indiquant la version installée du VDA Linux
Mise à jour LVDA ou nouvelle installation	update_or_fresh_install	Chaîne de texte indiquant que le package VDA Linux 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

Point de données	Nom de la clé	Description
Paramètres régionaux système	system_locale	Chaîne de texte indiquant les paramètres régionaux de cette machine
Dernière heure de redémarrage des services LVDA principaux	ctxhdx ctxvda	Dernière heure de redémarrage des services ctxhdx et ctxvda, au format jj-hh:mm:ss, par exemple, 10-17:22:19
Type de GPU	gpu_type	Indique le type de processeur graphique de la machine
Cœurs d'UC	cpu_cores	Entier indiquant le nombre de cœurs d'UC de la machine
Fréquence du processeur	cpu_frequency	Nombre flottant indiquant la fréquence du processeur en MHz
Taille de la mémoire physique	memory_size	Entier indiquant la taille de la mémoire physique en Ko
Nombre de sessions lancées	session_launch	Entier indiquant le nombre de sessions lancées (connexions ou reconnexions) sur la machine au moment où ce point de données est collecté
Version et nom du système d'exploitation Linux	os_name_version	Chaîne de texte indiquant le nom et la version du système d'exploitation Linux de la machine
Clé de session	session_key	Identification de la session d'où les données proviennent
Type de ressource	resource_type	Chaîne de texte indiquant le type de ressource de la session lancée : bureau ou <appname>

Point de données	Nom de la clé	Description
Période active de session	active_session_time	Utilisé pour enregistrer les périodes actives de la session. Une session peut contenir plusieurs périodes actives car la session peut se déconnecter/se reconnecter.
Durée de session	session_duration_time	Utilisé pour enregistrer la durée de la session de l'ouverture à la fermeture de session
Type de client Receiver	receiver_type	Entier indiquant le type d'application Citrix Workspace utilisé pour lancer la session
Version du client Receiver	receiver_version	Chaîne de texte indiquant la version de l'application Citrix Workspace utilisée pour lancer la session
Nombre d'impressions	printing_count	Entier indiquant le nombre de fois que la session utilise la fonction d'impression
Nombre de redirections USB	usb_redirecting_count	Entier indiquant le nombre de fois que la session utilise un périphérique USB
Type de fournisseur Gfx	gfx_provider_type	Chaîne de texte indiquant le type de fournisseur de graphiques de la session
Nombre d'observations	shadow_count	Entier indiquant le nombre de fois que la session a été observée
Langue sélectionnée par l'utilisateur	ctxism_select	Chaîne longue composée qui contient toutes les langues sélectionnées par les utilisateurs

Point de données	Nom de la clé	Description
Nombre de redirections de carte à puce	scard_redirecting_count	Entier indiquant le nombre de fois que la session utilise la redirection de carte à puce, y compris pour l'ouverture de session et l'utilisation de cartes à puce pendant la session

Configurer la redirection USB

February 15, 2019

Les périphériques USB sont partagés entre l'application Citrix Workspace 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 VDA Linux, Citrix réutilise le pilote noyau de VHCI. Toutefois tous les transferts de données USB entre le VDA Linux et l'application Citrix Workspace sont encapsulés dans le protocole ICA de Citrix.

Service VHCI :

Le service VHCI est un service open source fourni par Citrix pour communiquer avec le module noyau VHCI. Ce service fonctionne en tant que passerelle entre VHCI et le service USB Citrix.

Service USB :

Le service USB représente un module Citrix qui gère tous les transferts de données et de virtualisation sur le périphérique USB.

Fonctionnement de la redirection USB

En général, si un périphérique USB n'est pas redirigé correctement vers Linux VDA, un ou plusieurs nœuds de périphérique sont créés dans le chemin d'accès system/dev. Parfois, cependant, le périphérique redirigé ne peut pas être utilisé par une session Linux VDA active. Les périphériques USB s'appuient sur les pilotes pour fonctionner correctement et certains périphériques nécessitent des pilotes spéciaux. Si les pilotes ne sont pas fournis, les périphériques USB redirigés sont inaccessibles à la session VDA Linux active. Pour assurer la connectivité du périphérique USB, installez les pilotes et configurez le système correctement.

Le VDA Linux 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.

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 VDA Linux, configurez les stratégies et règles suivantes :

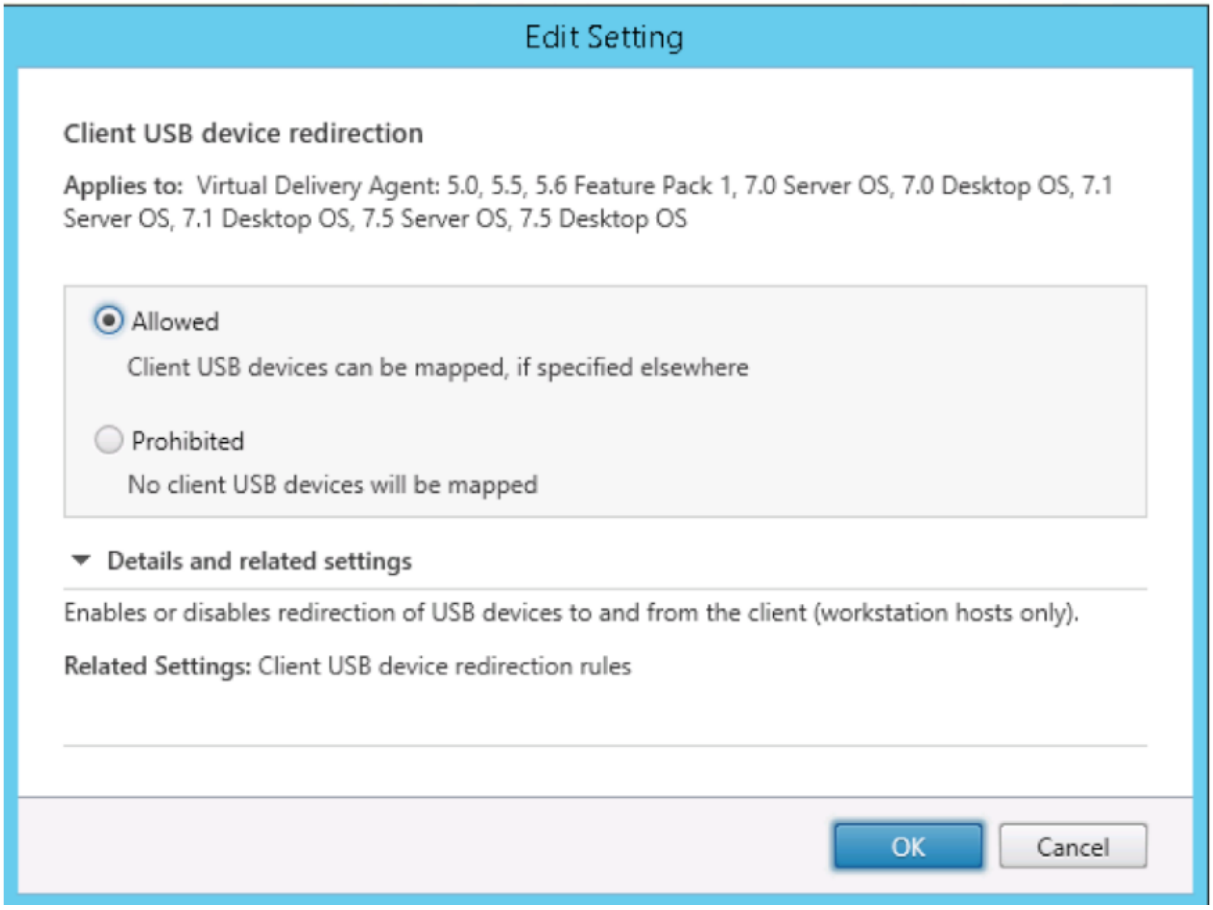
- Stratégie de redirection de périphérique USB client
- Règles de redirection des périphériques USB clients

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**.

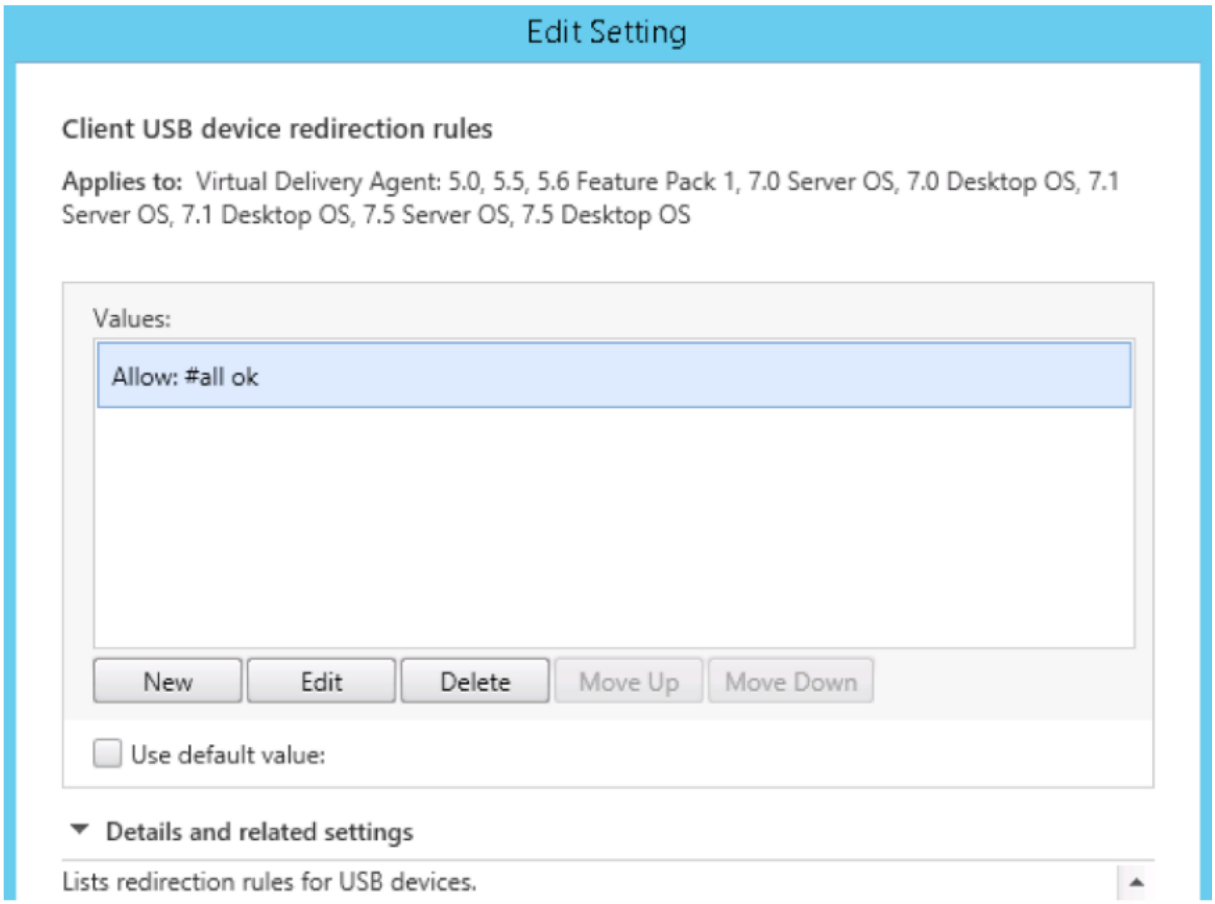


Définir des règles de redirection USB

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 VDA Linux.

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.

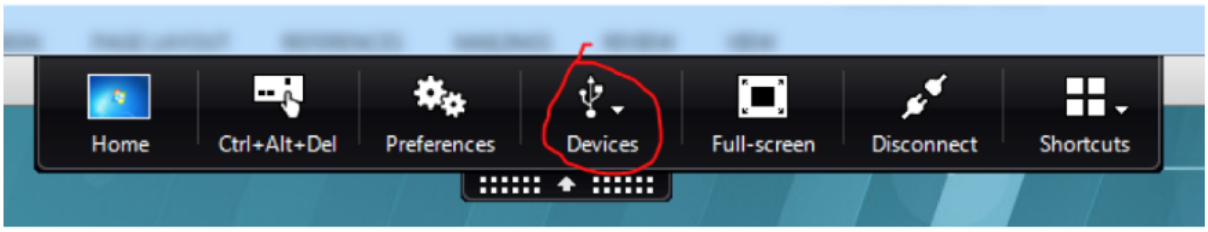
Résolution des problèmes de redirection USB

Utilisez les informations de cette section pour résoudre les problèmes que vous pourriez rencontrer lors de l'utilisation du VDA Linux.

Aucun périphérique dans la barre d'outils de l'application Citrix Workspace

Dans certains cas, vous ne pouvez pas voir les périphériques figurant sur la barre d'outils de l'application Citrix Workspace, ce qui indique qu'aucune redirection USB n'est en cours. Si vous rencontrez ce problème, vérifiez les éléments suivants :

- La stratégie est configurée pour permettre la redirection USB.
- Le module du noyau est compatible avec votre noyau



> **Remarque :**
>
> l'onglet **Périphériques** n'est pas disponible dans l'application Citrix Workspace pour Linux.

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

Ce problème se produit en raison de la configuration de la stratégie du périphérique. Dans ce cas, procédez comme suit :

- Configurez la stratégie du VDA Linux pour activer la redirection.
- Vérifiez si des restrictions de stratégie supplémentaires sont configurées dans le registre de l'application Citrix Workspace. Un périphérique peut être bloqué par le paramètre de registre de l'application Citrix Workspace. Vérifiez **DeviceRules** dans le chemin d'accès du registre pour vous assurer que ce paramètre n'interdit pas l'accès au périphérique :

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB

Pour de plus amples informations, consultez la section Comment configurer la redirection automatique des périphériques USB sur le site de support de Citrix.

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 VDA Linux configure et monte le disque. L'utilisateur (et seul l'utilisateur qui l'a installé) peut accéder au disque sans aucune configuration supplémentaire. Cela peut ne pas être possible avec les périphériques qui ne se trouvent pas dans la liste des périphériques pris en charge.

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 VDA Linux (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 6.9	2.6.32-696.10.3.el6.x86_64
RHEL 7.5	3.10.0-862.9.1.el7.x86_64
SUSE 12.3	4.4.73-5-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 VDA Linux, le service USB peut ne pas parvenir à démarrer. Dans ce cas, vous pouvez utiliser la fonctionnalité de redirection USB uniquement si vous créez vos propres modules noyau VHCI.

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

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

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

Si la commande s'exécute correctement, le module noyau a été chargé avec succès et la version est cohérente avec celle installée par Citrix.

Si la commande s'exécute avec des erreurs, le noyau n'est pas cohérent avec le module 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/CentOS :

   ```
   yum install kernel-devel
   ```

   SUSE 12 :

   ```
   zypper install kernel-devel

   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.

Périphériques USB pris en charge

Les périphériques suivants ont été testés pour prendre en charge cette version de VDA Linux. D'autres périphériques peuvent être utilisés, avec des résultats imprévisibles :

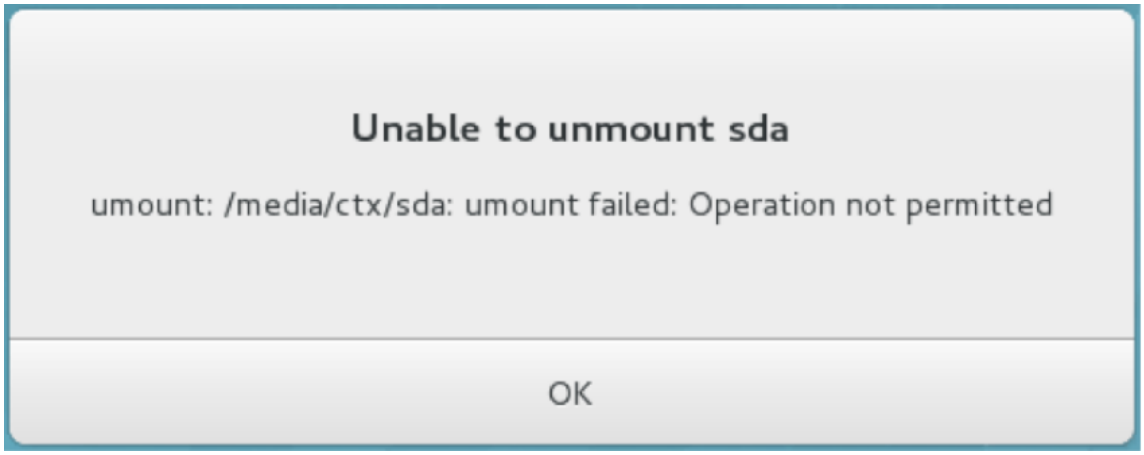
Périphérique de stockage de masse USB	VID:PID	Système de fichiers
Netac Technology Co., Ltd	0dd8:173c	FAT32
Kingston Datatraveler 101 II	0951:1625	FAT32
Kingston Datatraveler GT101 G2	1567:8902	FAT32
Lecteur Flash SanDisk SDCZ80	0781:5580	FAT32
SanDisk Cruzer 16GB	1058:10B8	FAT32
Disque dur HDD WD	0781:5567	FAT32

Souris 3D USB	VID:PID
3DConnexion SpaceMouse Pro	046d: c62b

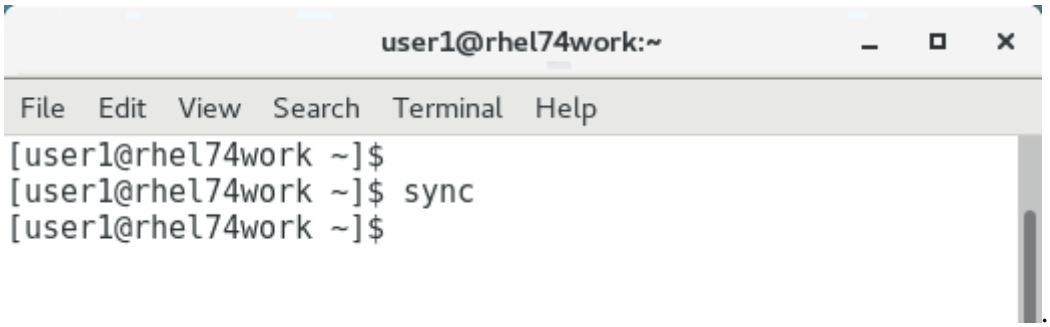
Scanner USB	VID:PID
Photo Epson Perfection V330	04B8: 0142

Problèmes connus

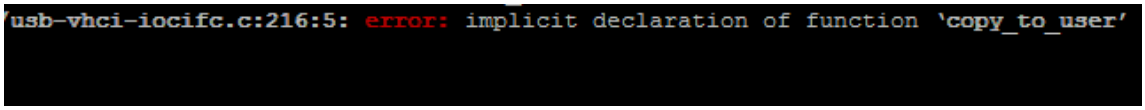
- **Impossible de démonter le disque USB redirigé**. Pour le contrôle d'accès de tous les disques USB redirigés à partir de l'application Citrix Workspace, le VDA Linux gère tous ces périphériques sous privilèges d'administrateur afin de garantir que seul le propriétaire peut accéder au périphérique 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 l'application Citrix Workspace, le fichier que vous avez modifié ou créé peut être perdu. Ce problème se produit car, lors de l'écriture de données dans un système de fichiers, le système monte le cache mémoire dans le système de fichiers. Les données ne sont pas écrites sur le disque lui-même. Si vous arrêtez la redirection à l'aide de la barre d'outils de l'application Citrix Workspace, les données n'ont pas le temps d'être purgées vers le disque, ce qui entraîne une perte de données. Pour résoudre ce problème, utilisez la commande de synchronisation dans un terminal pour purger les données vers le disque avant d'arrêter la redirection USB.



- **Une erreur de compilation du noyau peut se produire pour des noyaux spécifiques d'Ubuntu 16**. Le message d'erreur indique **déclaration implicite de la fonction copy_to_user** comme indiqué ci-dessous :



L'erreur se produit en raison des modifications du fichier d'en-tête dans les noyaux. Pour résoudre ce problème, ajoutez la ligne **#include <linux/uaccess.h>** au fichier`vhci-hcd-1.15/usb-vhci-iocifc.c`.


```
#include <linux/fs.h>
#include <linux/uaccess.h>

#include "usb-vhci-hcd.h"
```

- **Une erreur de compilation du noyau peut se produire pour le noyau 4.15.0-29-generic d'Ubuntu 16**. Le message d'erreur est **'driver_attr_debug_output' undeclared** comme indiqué ci-dessous :

```
error: 'driver_attr_debug_output' undeclared (first use in this function)
```

  L'erreur se produit lorsque des symboles sont manquants sur le noyau. Pour contourner le problème, désactivez la définition de macro pour DEBUG dans les fichiers `vhci-hcd-1.15/usb-vhci-iocifc.c` et `vhci-hcd-1.15/usb-vhci-hcd.c`.

```
22
23 //#define DEBUG
24
25 #include <linux/module.h>
```

Configurer la fiabilité de session

February 15, 2019

Citrix introduit la fonction de fiabilité de session sur toutes les plates-formes Linux prises en charge. L'option de fiabilité de session est activée par défaut.

La fiabilité de session reconnecte les sessions ICA en toute transparence pour toutes les interruptions réseau. Pour de plus amples informations sur la fiabilité de session, consultez la section Reconnexion automatique des clients et fiabilité de session.

Remarque : les données transmises via une connexion de fiabilité de session sont en texte brut par défaut. Pour des raisons de sécurité, Citrix vous recommande d'activer le cryptage SSL. Pour de plus amples informations sur le cryptage SSL, consultez la section Gérer les sessions utilisateur.

Configuration

Paramètres de stratégie dans Citrix Studio

Vous pouvez définir les stratégies suivantes pour la fiabilité de session dans Citrix Studio :

- Connexions de fiabilité de session
- Expiration de délai de la fiabilité de session
- Numéro de port de la fiabilité de session

- Niveau de transparence de l'interface durant la reconnexion

Pour obtenir des informations supplémentaires, reportez-vous à Paramètres de stratégie Fiabilité de session et Paramètres de stratégie Reconnexion automatique des clients.

Remarque : après avoir défini la stratégie **Connexions de fiabilité de session** ou **Numéro de port de la fiabilité de session**, redémarrez le service VDA et le service HDX, dans cet ordre, pour que vos paramètres soient pris en compte.

Paramètres sur le VDA Linux

- **Activer/désactiver l'écouteur TCP de fiabilité de session**

Par défaut, l'écouteur TCP de fiabilité de session est activé et écoute sur le port 2598. Pour désactiver l'écouteur, exécutez la commande suivante.

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
     CurrentControlSet\Control\Citrix\WinStations\cgp"   -v  "
     fEnableWinStation" -d "0x00000000"
```

Remarque : redémarrez le service HDX pour que vos paramètres soient pris en compte. La désactivation de l'écouteur TCP ne désactive pas la fiabilité de session. La fiabilité de session est toujours disponible au travers d'autres écouteurs (par exemple, SSL) si la fonctionnalité est activée via la stratégie **Connexions de fiabilité de session**.

- **Numéro de port de la fiabilité de session**

Vous pouvez également définir le numéro de port de fiabilité de session à l'aide de la commande suivante (qui utilise le numéro de port 2599 à titre d'exemple).

```
1 /opt/Citrix/VDA/bin/ctxreg update -k  "HKEY_LOCAL_MACHINE\SYSTEM\
     CurrentControlSet\Control\Citrix\WinStations\cgp"   -v  "PortNumber"
      -d  "2599"
```

Remarque : vous devez redémarrer le service HDX pour que ce paramètre soit pris en compte. Si le numéro de port a été défini via le paramètre de stratégie dans Citrix Studio, votre paramètre sur le VDA Linux est ignoré. Assurez-vous que le pare-feu sur le VDA est configuré pour ne pas interdire le trafic réseau via le port défini.

- **Intervalle de persistance serveur vers client**

Les messages de persistance de fiabilité de session sont envoyés entre le VDA Linux et le client ICA lorsqu'il n'y a aucune activité dans la session (par exemple, aucun mouvement de souris, aucune mise à jour d'écran). Les messages de persistance sont utilisés pour détecter si le client est toujours réactif. S'il n'y a pas de réponse du client, la session est suspendue jusqu'à ce que le client se reconnecte. Ce paramètre spécifie le nombre de secondes entre les messages de persistance successifs.

Ce paramètre n'est pas configuré par défaut. Pour le configurer, exécutez la commande suivante (qui utilise 10 secondes à titre d'exemple).

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\
    Citrix\XTEConfig" -t "REG_DWORD" -v "CgpServerToClientKeepAlive"
     -d "10" --force
```

- **Intervalle de persistance client vers serveur**

Ce paramètre spécifie le nombre de secondes entre les messages de persistance successifs envoyés depuis le client ICA vers le VDA Linux. Ce paramètre n'est pas configuré par défaut. Pour le configurer, exécutez la commande suivante (qui utilise 10 secondes à titre d'exemple).

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\
    Citrix\XTEConfig" -t "REG_DWORD" -v "CgpClientToServerKeepAlive"
     -d "10" --force
```

Résolution des problèmes

Impossible de lancer des sessions après avoir activé la fiabilité de session via le paramètre de stratégie.

Pour contourner ce problème, procédez comme suit :

1. Assurez-vous que le service VDA et le service HDX sont redémarrés, dans cet ordre, après avoir activé la fiabilité de session via le paramètre de stratégie dans Citrix Studio.
2. Utilisez la commande suivante pour vérifier que l'écouteur TCP de fiabilité de session est en cours d'exécution (utilise le port 2598 à titre d'exemple).

   ```
   netstat -an | grep 2598
   ```

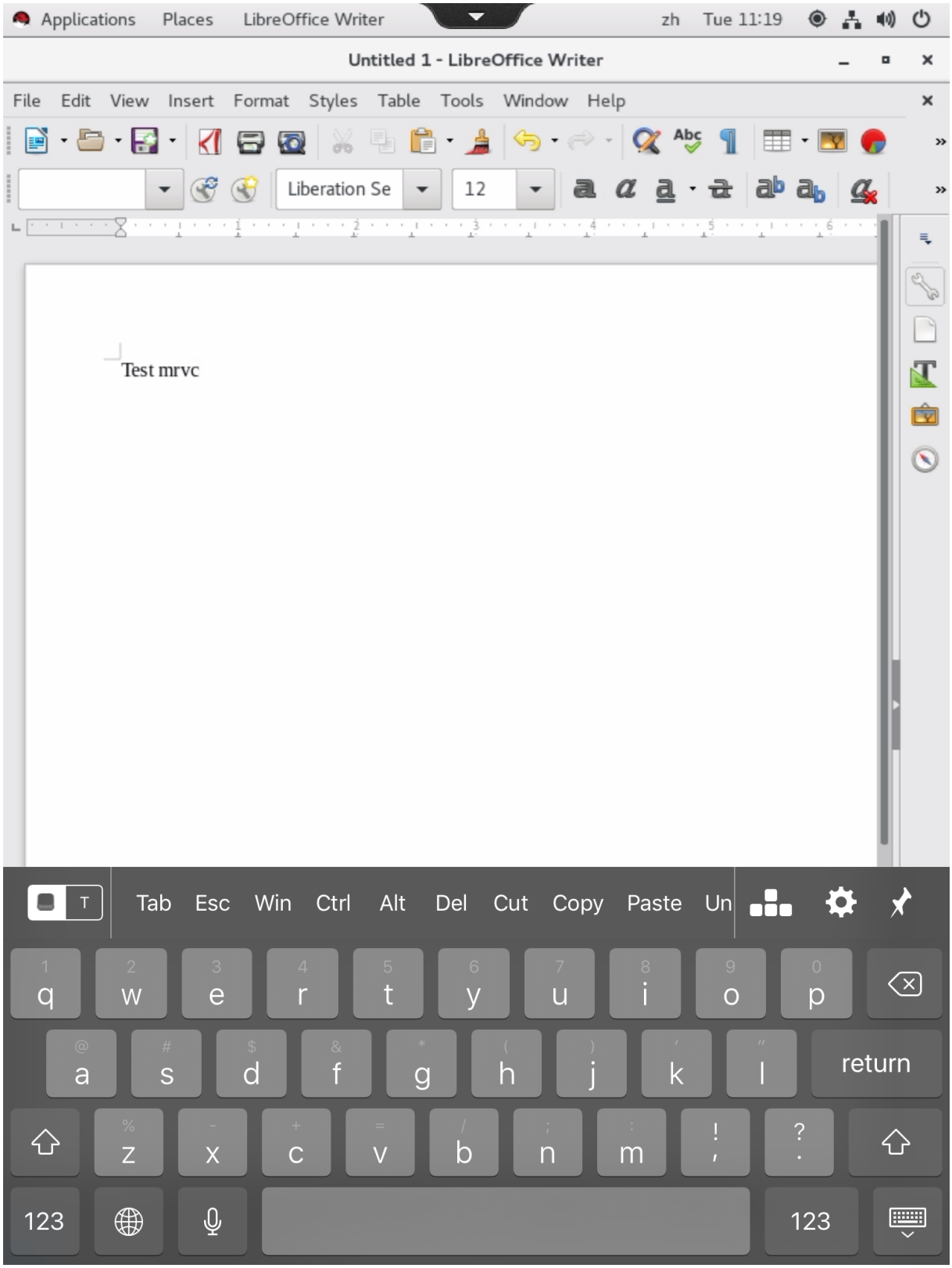
   S'il n'y a pas d'écouteur TCP sur le port de fiabilité de session, activez l'écouteur en utilisant la commande suivante.

   ```
   /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
       CurrentControlSet\Control\Citrix\WinStations\cgp" -v "
       fEnableWinStation" -d "0x00000001"
   ```

Clavier logiciel

January 11, 2019

La fonctionnalité de clavier logiciel est disponible dans une session d'application ou de bureau virtuel Linux. Le clavier logiciel s'affiche ou se masque automatiquement lorsque vous accédez à un champ de saisie ou le quittez.



> **Remarque :**
>
> la fonctionnalité est disponible pour RHEL 7.5, RHEL 6.9, CentOS 7.5, CentOS 6.9, SUSE 12.3 et Ubuntu 16.04. Elle est prise en charge sur l'application Citrix Workspace pour iOS et Android.

Activer et désactiver la fonctionnalité

Cette fonction est désactivée par défaut. Utilisez l'utilitaire **ctxreg** pour activer ou désactiver cette fonctionnalité. La configuration de la fonctionnalité sur un VDA Linux donné s'applique à toutes les sessions sur ce VDA.

Pour mettre la fonctionnalité en service :

1. Exécutez la commande :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
    CurrentControlSet\Control\Citrix\VirtualChannels\MrVc"  -v "
    Enabled" -d "0x00000001"
```

2. Dans Citrix Studio, définissez la stratégie **Affichage automatique du clavier** sur **Autorisé**.
3. (Facultatif) Pour RHEL 7 et CentOS 7, exécutez la commande suivante pour configurer Intelligent Input Bus (IBus) en tant que service de messagerie instantanée par défaut :

```
1 echo "GTK_IM_MODULE=ibus" >>/etc/bashrc
```

Pour désactiver cette fonctionnalité, exécutez la commande suivante :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\
    Control\Citrix\VirtualChannels\MrVc"  -v "Enabled" -d "0x00000000"
```

> **Remarque :**
>
> les paramètres précédents prennent effet lorsque vous vous connectez à une nouvelle session ou que vous fermez une session et que vous vous reconnectez à la session en cours.

Limitations

- La fonctionnalité peut ne pas fonctionner comme prévu avec Google Chrome, LibreOffice et d'autres applications.
- Pour afficher à nouveau le clavier logiciel après l'avoir masqué manuellement, cliquez sur un champ sans saisie, puis de nouveau sur le champ de saisie actuel.

- Le clavier logiciel peut ne pas apparaître lorsque vous cliquez depuis un champ de saisie vers un autre dans un navigateur Web. Pour contourner ce problème, cliquez sur un champ sans saisie, puis sur le champ de saisie cible.
- La fonctionnalité ne prend pas en charge les caractères Unicode et les caractères codés sur deux octets (tels que les caractères chinois, japonais et coréen).
- Le clavier logiciel n'est pas disponible pour les champs de saisie de mot de passe.
- Le clavier logiciel peut chevaucher le champ de saisie actuel. Dans ce cas, déplacez la fenêtre de l'application ou faites défiler l'écran vers le haut pour déplacer le champ de saisie vers une position accessible.
- En raison de problèmes de compatibilité entre l'application Citrix Workspace et les tablettes Huawei, le clavier logiciel apparaît sur les tablettes Huawei même si un clavier physique est connecté.

Éditeur IME client

January 11, 2019

Généralités

Les caractères codés sur deux octets (tels que les caractères chinois, japonais et coréen) doivent être saisis via un éditeur de méthode d'entrée (IME). L'éditeur IME client permet de saisir de tels 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 VDA Linux.

Utilisation

Ouvrez une session Citrix Virtual Apps ou Citrix Virtual Desktops comme d'habitude.

Modifiez votre méthode d'entrée conformément à ce qui est requis sur le client pour commencer à utiliser à l'éditeur IME client.

Problèmes connus

- Vous devez double-cliquer sur une cellule dans une feuille de calcul Google avant de pouvoir utiliser l'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.

Prise en charge des entrées en plusieurs langues

January 15, 2019

Depuis la version 1.4 du VDA Linux, Citrix a ajouté la prise en charge des applications publiées. Les utilisateurs peuvent accéder à une application Linux souhaitée sans l'environnement de bureau Linux.

Toutefois, la barre de langue sur le VDA Linux n'était pas disponible pour l'application publiée, car elle est étroitement intégrée à l'environnement de bureau Linux. Par conséquent, les utilisateurs ne pouvaient pas saisir de texte dans une langue nécessitant un éditeur IME tel que le chinois, le japonais ou le coréen. En outre, les utilisateurs ne pouvaient pas non plus basculer entre les dispositions de clavier pendant une session d'application.

Pour résoudre ces problèmes, cette fonctionnalité fournit une barre de langue pour les applications publiées acceptant la saisie de texte. La barre de langue permet aux utilisateurs de sélectionner un IME côté serveur et de basculer entre les dispositions de clavier durant une session d'application.

Configuration

Vous pouvez utiliser l'utilitaire**ctxreg** pour activer ou désactiver cette fonctionnalité (désactivée par défaut). La configuration de la fonctionnalité sur un serveur VDA Linux donné s'applique à toutes les applications publiées sur ce VDA.

La clé de configuration est «HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlS et\Control\Citrix\LanguageBar » et le type est DWORD.

Pour activer cette fonctionnalité, exécutez la commande :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE \SYSTEM\
    CurrentControlSet\Control\Citrix\LanguageBar" -v "Enabled" -d "0
    x00000001"
```

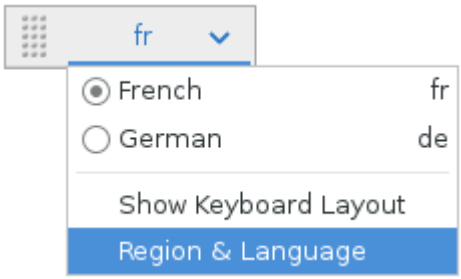
Pour désactiver cette fonctionnalité, exécutez la commande :


```
/opt/Citrix/VDA/bin/ctxreg update -k ”HKEY_LOCAL_MACHINE \SYSTEM\
   CurrentControlSet\Control\Citrix\LanguageBar” -v ”Enabled” -d ”0
   x00000000”
```

Utilisation

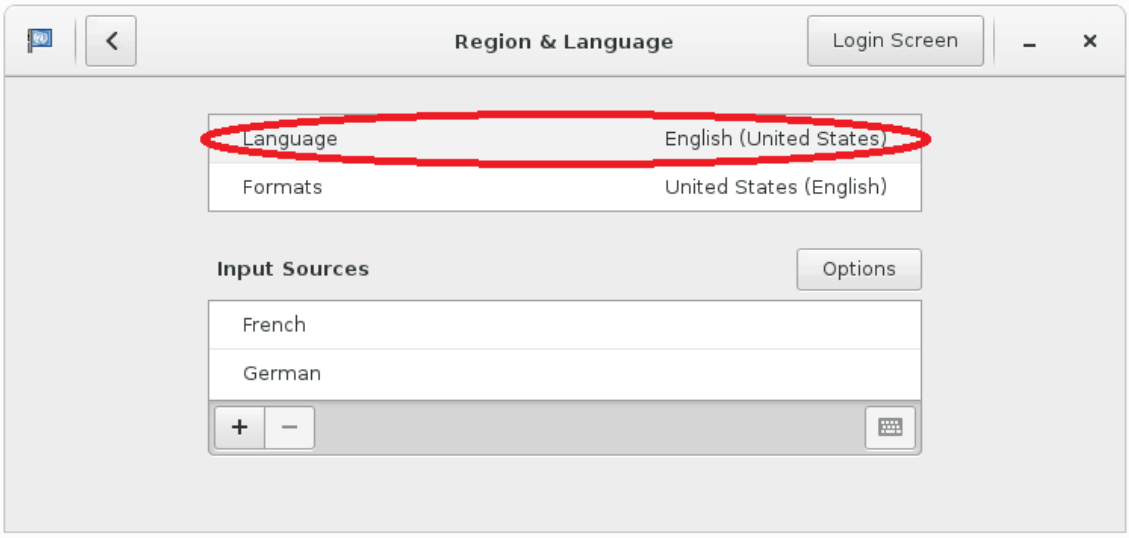
Son utilisation est simple.

1. Activez la fonctionnalité.
2. Accédez à une application publiée pouvant accepter la saisie de texte. Une barre de langue s’affiche dans la session, à côté de l’application.
3. Dans le menu déroulant, sélectionnez **Région et langue** pour ajouter la langue souhaitée (source d’entrée).



4. Sélectionnez l’IME ou la disposition du clavier dans le menu déroulant.
5. Saisissez une langue à l’aide de l’IME ou de la disposition du clavier sélectionné(e).

> **Remarque :**
>
> - Lorsque vous modifiez une disposition de clavier sur la barre de langue côté VDA, vérifiez que la même disposition de clavier est utilisée côté client (application Citrix Workspace).
> - Le package **accountsservice** doit être mis à niveau vers la version 0.6.37 ou ultérieure avant la configuration dans la boîte de dialogue **Région et langue**.



Synchronisation dynamique de la disposition du clavier

February 15, 2019

Auparavant, les dispositions de clavier sur le VDA Linux et sur la machine cliente devaient être les mêmes. Par exemple, lorsque la disposition du clavier passait de l'anglais au français sur la machine cliente mais pas sur le VDA, des problèmes de mappage de touches pouvaient se produire et persister jusqu'à ce que le VDA passe également au français.

À partir de cette version, Citrix résout le problème en synchronisant automatiquement la disposition du clavier du VDA avec celle de la machine cliente. Chaque fois que la disposition du clavier de la machine cliente change, la disposition sur le VDA change en conséquence.

> **Conseil :**
>
> Cette fonctionnalité est prise en charge sur l'application Citrix Workspace pour Windows et est compatible avec les applications et les bureaux publiés.

Configuration

Cette fonction est désactivée par défaut. Utilisez l'utilitaire **ctxreg** pour activer ou désactiver cette fonctionnalité. La configuration de la fonctionnalité sur un VDA Linux donné s'applique à toutes les sessions sur ce VDA.

La clé de configuration est « HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\SyncKeyboardLay
» et le type est DWORD.

Pour activer cette fonctionnalité, exécutez la commande :


```
/opt/Citrix/VDA/bin/ctxreg update -k ”HKEY_LOCAL_MACHINE\System\
    CurrentControlSet\Control\Citrix\LanguageBar” -v ”SyncKeyboardLayout
    ” -d ”0x00000001”
```

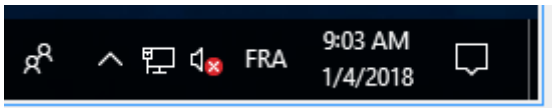
Pour désactiver cette fonctionnalité, exécutez la commande :

```
/opt/Citrix/VDA/bin/ctxreg update -k ”HKEY_LOCAL_MACHINE\System\
    CurrentControlSet\Control\Citrix\LanguageBar” -v ”SyncKeyboardLayout
    ” -d ”0x00000000”
```

Utilisation

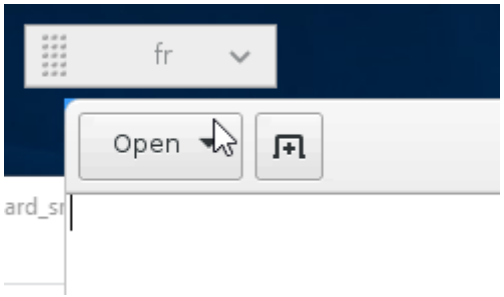
Lorsque cette fonctionnalité est activée, si la disposition du clavier change sur la machine cliente pendant une session, la disposition du clavier de la session change en conséquence.

Par exemple, si vous changez la disposition du clavier sur une machine cliente vers le français (FR) :

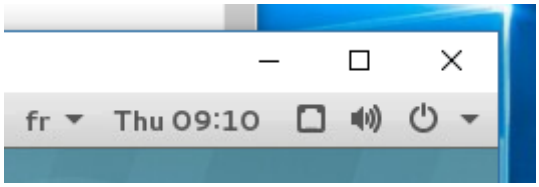


La disposition du clavier de la session Linux VDA devient également « fr ».

Dans une session d’application, ce changement automatique est visible si vous avez activé la barre de langue :



Dans une session de bureau, cette modification automatique est affichée dans la barre des tâches :

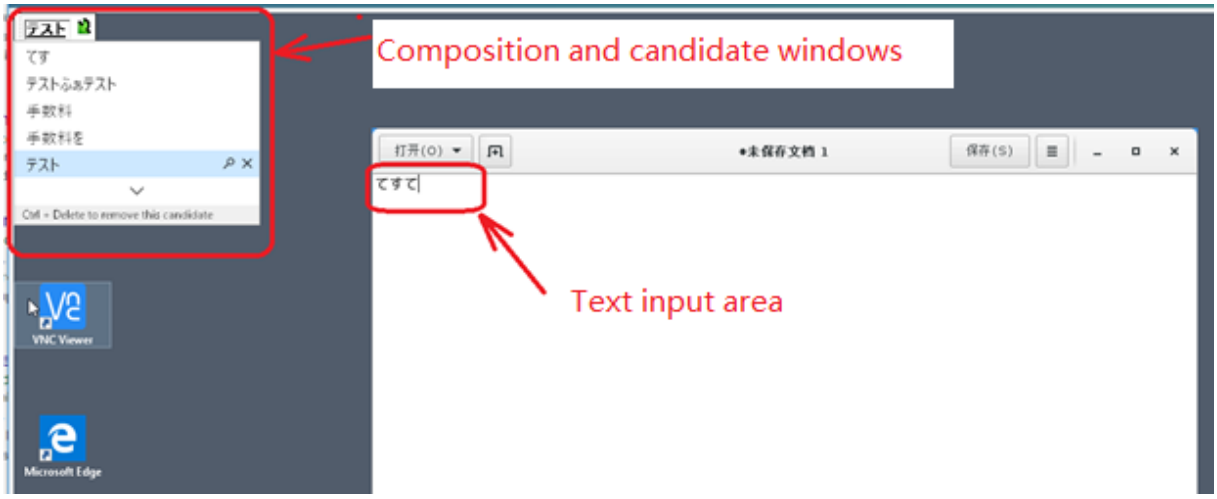


Synchronisation de l’interface utilisateur de l’éditeur IME client

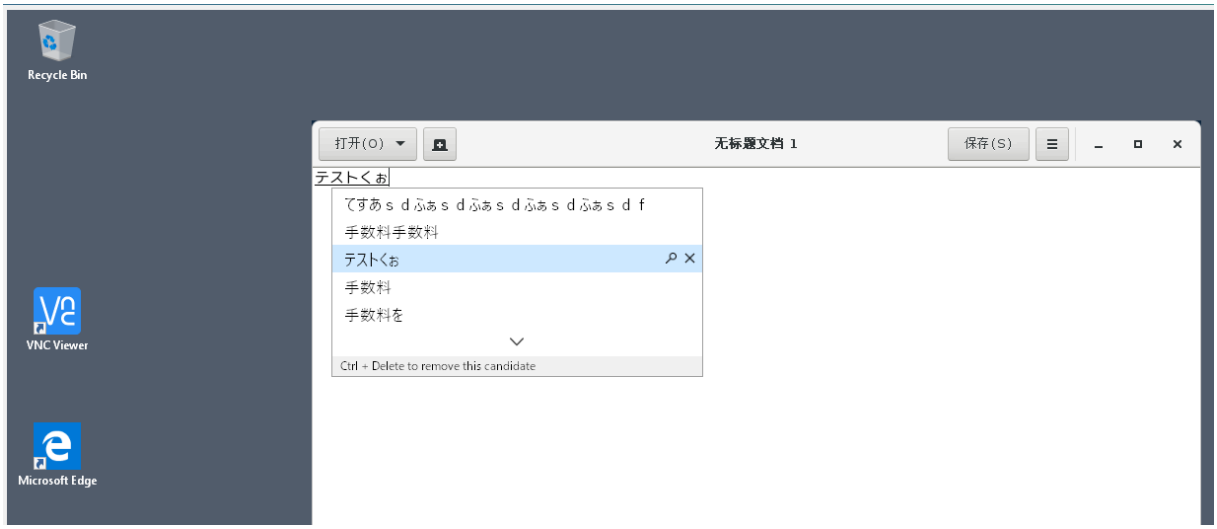
January 11, 2019

Généralités

Jusqu'à présent, l'interface utilisateur de l'éditeur IME client (y compris la fenêtre de composition et la fenêtre candidate) était positionnée dans le coin supérieur gauche de l'écran. Celle-ci ne suivait pas le curseur et était parfois située loin du curseur dans la zone de saisie de texte.



À partir de cette version, Citrix améliore la convivialité et optimise davantage l'expérience transparente avec l'éditeur IME client comme suit :



> **Remarque :**
>
> La fonctionnalité est disponible pour RHEL7.x, SUSE 12.x, Ubuntu 16.04 et CentOS 7.x. Elle est prise en charge sur l'application Citrix Workspace pour Windows et pour Mac.
>
> La fonctionnalité s'installe automatiquement, mais vous devez l'activer avant de pouvoir l'utiliser.

Activer et désactiver la fonctionnalité

Cette fonction est désactivée par défaut. Utilisez l'utilitaire **ctxreg** pour activer ou désactiver cette fonctionnalité. La configuration de la fonctionnalité sur un VDA Linux donné s'applique à toutes les sessions sur ce VDA.

Pour activer cette fonctionnalité, exécutez la commande suivante :

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

Pour désactiver cette fonctionnalité, exécutez la commande suivante :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
     CurrentControlSet\Control\Citrix\LanguageBar" -v "SyncClientIME" -d
     "0x00000000"
```

HDX Insight

January 11, 2019

Généralités

HDX Insight fait partie de NetScaler Insight Center. Il est basé sur la norme standard AppFlow. 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 NetScaler ou CloudBridge.

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 environnement Insight Center avec le VDA Linux et activer la fonctionnalité HDX Insight. Pour plus d'informations sur l'utilisation de la fonctionnalité HDX Insight, consultez la section Cas d'utilisation : HDX Insight.

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 VDA Linux.

  ```
  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.

Transport adaptatif

January 11, 2019

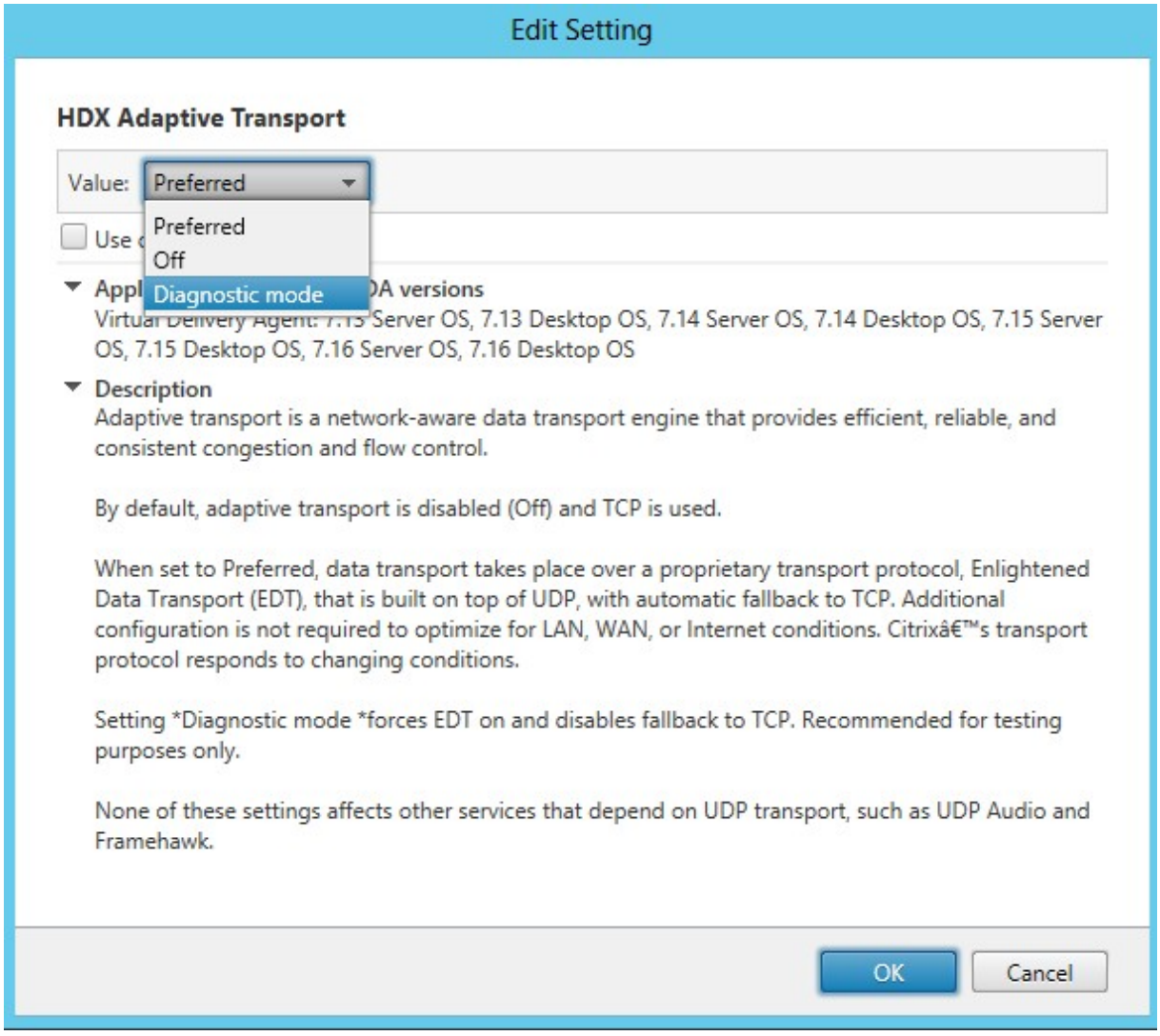
Préalablement disponible en tant que fonctionnalité expérimentale, le transport adaptatif est une fonctionnalité entièrement prise en charge dans cette version.

Le transport adaptatif est un mécanisme de transport de données pour Citrix Virtual Apps and Desktops. Plus rapide et plus évolutif, il améliore l'interactivité avec les applications et il est plus adapté aux connexions WAN et Internet longue distance difficiles. Pour plus d'informations sur le transport adaptatif, consultez la section Transport adaptatif.

Activer le transport adaptatif

Dans Citrix Studio, vérifiez que la stratégie **HDX Adaptive Transport** est définie sur le mode **Préféré** ou **Diagnostic**. Le paramètre **Préféré** est sélectionné par défaut.

- **Préféré** : le transport adaptatif via EDT (Enlightened Data Transport) est utilisé autant que possible, avec retour vers TCP.
- **Mode Diagnostic** : EDT est activé de force et le retour vers TCP est désactivé.



Désactiver le transport adaptatif

Pour désactiver le transport adaptatif, définissez la stratégie **HDX Adaptive Transport** sur **Off** dans Citrix Studio.

Résolution des problèmes

Vérifier si le transport adaptatif est activé

Exécutez la commande suivante pour vérifier si les écouteurs UDP sont en cours d'exécution.

```
netstat -an | grep "1494|2598"
```

Dans des circonstances normales, la sortie est similaire à ce qui suit.

```
udp        0      0 0.0.0.0:2598            0.0.0.0:*

udp       0      0 :::1494                 :::*
```

Traçage activé

February 15, 2019

Généralités

La collecte de journaux et la reproduction des problèmes ralentissent les diagnostics et dégradent l'expérience utilisateur. Cette version offre une fonctionnalité de traçage afin de faciliter ces tâches. Par défaut, le traçage est activé pour le VDA Linux.

Configuration

Le démon ctxlogd et l'utilitaire setlog sont maintenant inclus dans le package du VDA Linux. Par défaut, le démon ctxlogd démarre après l'installation et la configuration du VDA Linux.

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 VDA Linux 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 root 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 root pour créer le fichier **/var/xdl/.ctxlog**. Redémarrez le service ctxlogd dont dépendent d'autres services.

Observer des sessions

February 15, 2019

La fonctionnalité d'observation de session permet aux administrateurs de domaine d'afficher les sessions ICA d'utilisateurs dans un intranet. La fonctionnalité utilise noVNC pour se connecter aux sessions ICA et est prise en charge uniquement avec RHEL 7.x et Ubuntu 16.04.

> **Remarque :**
>
> Pour utiliser la fonctionnalité d'observation de session, la version de Citrix Director doit être 7.16 ou ultérieure.

Installation et configuration

Dépendances

Deux nouvelles dépendances, python-websockify et x11vnc, sont requises pour l'observation de session. Les dépendances python-websockify et x11vnc sont automatiquement installées lorsque vous installez le VDA Linux sur Ubuntu 16.04. Sur RHEL 7.x, vous devez installer manuellement python-websockify et x11vnc après avoir installé le VDA Linux.

Exécutez la commande suivante sur RHEL 7.x pour installer python-websockify et x11vnc (x11vnc version 0.9.13 ou version ultérieure).

```
1 sudo yum install -y python-websockify x11vnc
```

Pour résoudre python-websockify et x11vnc, activez les référentiels suivants sur RHEL 7.x :

- EPEL

  Le référentiel EPEL (Extra Packages for Enterprise Linux) est requis pour python-websockify et x11vnc. Pour activer le référentiel EPEL, exécutez la commande suivante :

  ```
  1 sudo yum install https://dl.fedoraproject.org/pub/epel/epel-
      release-latest-$(rpm -E '%{
  2 rhel }
  3 ').noarch.rpm
  ```

- RPM facultatifs

  Exécutez l'une des commandes suivantes pour activer le référentiel de RPM facultatifs pour l'installation de certains packages de dépendances de x11vnc :

  Pour un poste de travail :

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

  Pour un serveur :

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

Port

La fonctionnalité d'observation de session sélectionne automatiquement les ports disponibles entre 6001 et 6099 pour établir des connexions entre le VDA Linux et Citrix Director. Par conséquent, le nombre de sessions ICA que vous pouvez observer simultanément est limité à 99. Assurez-vous que

suffisamment de ports sont disponibles pour répondre à vos besoins, en particulier pour l'observation multi-sessions.

Registre

Le tableau suivant répertorie les registres associés :

Registre	Description	Valeur par défaut
EnableSessionShadowing	Active ou désactive l'observation de session	1 (activé)
ShadowingUseSSL	Détermine si vous souhaitez crypter la connexion entre le VDA Linux et Citrix Director	0 (désactivé)

Exécutez la commande ctxreg sur le VDA Linux pour modifier les valeurs de Registre. Par exemple, pour désactiver l'observation de session, exécutez la commande suivante :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
     VirtualDesktopAgent" -v "EnableSessionShadowing" -d 0x00000000
```

SSL

La connexion noVNC entre le VDA Linux et Citrix Director utilise le protocole WebSocket. Pour l'observation de session, le choix entre ws:// et wss:// est déterminé par le registre « ShadowingUseSSL » mentionné précédemment. Par défaut, ws:// est choisi. Toutefois, pour des raisons de sécurité, Citrix vous recommande d'utiliser wss:// et d'installer des certificats sur chaque client Citrix Director et sur chaque serveur VDA Linux. Citrix décline toute responsabilité en matière de sécurité en ce qui concerne l'observation de session de VDA Linux avec l'utilisation de ws://.

Obtenir des certificats SSL serveur et racine

Les certificats doivent être signés par une autorité de certification (AC).

Un certificat de serveur distinct (y compris la clé) est requis pour chaque serveur VDA Linux sur lequel vous souhaitez configurer SSL. Un certificat de serveur identifie une machine. Vous devez donc connaître le nom de domaine complet (FQDN) de chaque serveur. Pour des raisons pratiques, vous pouvez utiliser un certificat générique pour la totalité du domaine. Dans ce cas, vous devez connaître au moins le nom de domaine.

Outre l'installation d'un certificat de serveur sur chaque serveur, vous devez installer un certificat racine de la même autorité de certification (CA) sur chaque client Citrix Director qui communique avec le serveur VDA Linux. Les autorités de certification émettant des certificats de serveur émettent aussi les certificats racines. Vous pouvez installer les certificats de serveurs et racines à partir d'une autorité de certification (CA) intégrés à votre système d'exploitation, d'une CA d'entreprise (soit une CA à laquelle votre organisation vous donne accès) ou d'une CA non intégrée à votre système d'exploitation. Consultez l'équipe des experts en sécurité de votre organisation afin de trouver parmi les méthodes celle requise pour l'obtention des certificats.

Important :

- Le nom commun d'un certificat de serveur doit être le nom de domaine complet exact du serveur VDA Linux ou, au moins, les caractères générique + domaine corrects. Par exemple, vda1.basedomain.com ou * .basedomain.com.
- Les algorithmes de hachage, y compris SHA1 et MD5, sont trop faibles pour les signatures dans les certificats numériques pour certains navigateurs. SHA-256 est donc spécifié comme standard minimum.

Installer un certificat racine sur chaque client Citrix Director

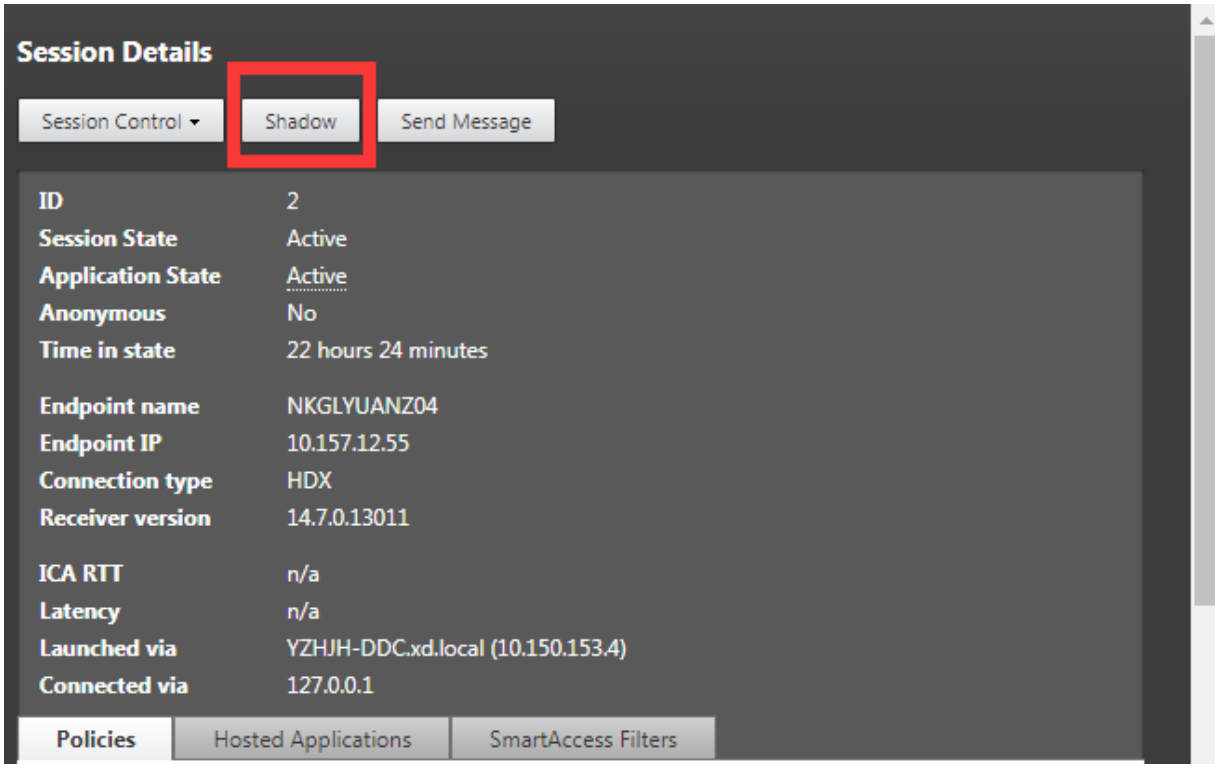
L'observation de session utilise le même magasin de certificats qu'IIS (reposant sur le registre). Par conséquent, vous pouvez installer les certificats à l'aide d'IIS ou du composant logiciel enfichable MMC (Microsoft Management Console). Après avoir reçu un certificat d'une autorité de certification, vous pouvez redémarrer l'assistant Certificat de serveur Web d'IIS. L'assistant installe alors le certificat. Vous pouvez également afficher et importer des certificats sur l'ordinateur en utilisant la console MMC et ajouter le certificat en tant que composant logiciel enfichable autonome. Internet Explorer et Google Chrome importent les certificats installés sur votre système d'exploitation par défaut. Pour Mozilla Firefox, vous devez importer vos certificats SSL racine dans l'onglet **Autorités** du gestionnaire de certificats.

Installer un certificat de serveur et sa clé sur chaque serveur VDA Linux

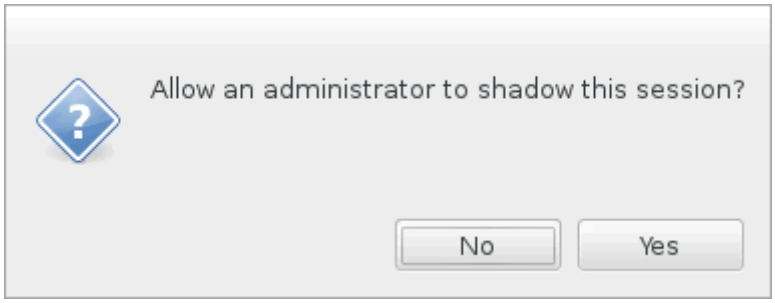
Appelez les certificats de serveur « shadowingcert.* » et le fichier de clé « shadowingkey.* » (* peut indiquer le format, par exemple, shadowingcert.csr et shadowingkey.key). Placez les certificats de serveur et les fichiers de clés sous le chemin d'accès **/etc/xdl/shadowingss** et protégez-les correctement avec des autorisations restreintes. Si le nom ou le chemin est incorrect, le VDA Linux est incapable de trouver un certificat ou un fichier de clé spécifique et, par conséquent, cela entraîne une défaillance de la connexion avec Citrix Director.

Utilisation

Dans Citrix Director, recherchez la session cible et cliquez sur **Observer** dans la vue **Détails de la session** pour envoyer une demande d'observation à l'agent Linux VDA.



Une fois que la connexion s'initialise, une confirmation s'affiche sur le client de session ICA (pas le client Citrix Director) pour demander l'autorisation d'observer la session.



Si l'utilisateur clique sur **Oui**, une fenêtre s'affiche du côté Citrix Director, indiquant que la session ICA est en cours d'observation.

Pour de plus amples informations sur l'utilisation, veuillez consulter la documentation de Citrix Director.

Limitations

- L'observation de session est conçue pour une utilisation dans un intranet uniquement. Elle ne fonctionne pas pour les réseaux externes même en se connectant via NetScaler. Citrix décline toute responsabilité en ce qui concerne l'observation de session de VDA Linux dans un réseau externe.
- Lorsque l'observation de session est activée, un administrateur de domaine peut uniquement afficher les sessions ICA, et n'a pas l'autorisation d'écrire dessus ou de le contrôler.
- Une fois qu'un administrateur a cliqué sur **Observer** depuis Citrix Director, une confirmation s'affiche pour demander l'autorisation à l'utilisateur d'observer la session. Une session peut être observée uniquement lorsque l'utilisateur de la session en donne l'autorisation.
- La confirmation mentionnée précédemment a un délai d'expiration, qui est de 20 secondes. Une demande d'observation échoue lorsque ce délai est écoulé.
- Une session ICA peut être observée par un seul administrateur dans une seule fenêtre Citrix Director. Si une session ICA a été observée par l'administrateur A et pendant ce temps, l'administrateur B envoie une demande d'observation, la confirmation d'obtention de l'autorisation de l'utilisateur réapparaît sur la machine utilisateur. Si l'utilisateur accepte, la connexion d'observation pour l'administrateur A s'arrête et une nouvelle connexion d'observation est créée pour l'administrateur B. Il en est de même si une autre demande d'observation pour la même session ICA est envoyée par le même administrateur.
- Pour utiliser l'observation de session, installez Citrix Director 7.16 ou version ultérieure.
- Un client Citrix Director utilise un nom de domaine complet plutôt qu'une adresse IP pour se connecter au serveur VDA Linux cible. Par conséquent, le client Citrix Director doit pouvoir résoudre le nom de domaine complet du serveur VDA Linux.

Résolution des problèmes

Si l'observation de session échoue, effectuez le débogage à la fois sur le client Citrix Director et sur le VDA Linux.

Sur le client Citrix Director

À l'aide des outils de développement du navigateur, vérifiez les journaux de sortie dans l'onglet **Console**. Ou vérifiez la réponse de l'API ShadowLinuxSession dans l'onglet **Réseau**. Si la confirmation de l'obtention de l'autorisation de l'utilisateur s'affiche mais que la connexion ne parvient pas à être établie, envoyez une commande ping au nom de domaine complet du VDA Linux pour vérifier que Citrix Director peut résoudre le nom de domaine complet. En cas de problème avec la connexion wss://, vérifiez vos certificats.

Sur le VDA Linux

Vérifiez que la confirmation d'obtention de l'autorisation de l'utilisateur s'affiche en réponse à une requête d'observation. Si ce n'est pas le cas, vérifiez les fichiers vda.log et hdx.log à la recherche d'indices. Pour obtenir le fichier vda.log, procédez comme suit :

1. Recherchez le fichier /etc/xdl/ctx-vda.conf. Supprimez les marques de commentaire sur la ligne suivante pour activer la configuration vda.log :

   ```
   Log4jConfig=" /etc/xdl/log4j.xml"
   ```

2. Ouvrez le fichier /etc/xdl/log4j.xml, localisez la partie com.citrix.dmc et rempmlacez « info » par « trace » comme suit :

   ```
   <!-- Broker Agent Plugin - Director VDA plugin Logger -->

    <logger name="com.citrix.dmc">

      <level value="trace"/>

    </logger>
   ```

3. Exécutez la commande **service ctxvda restart** pour redémarrer le service ctxvda.

En cas d'erreur lors de l'établissement de la connexion, procédez comme suit :

1. Recherchez toute limitation de pare-feu qui empêche l'observation de session d'ouvrir le port.
2. Vérifiez que les certificats et les fichiers de clés sont correctement nommés et placés sous le bon chemin pour un scénario SSL.
3. Vérifiez qu'il reste suffisamment de ports entre 6001 et 6099 pour les nouvelles demandes d'observation.

Prise en charge de l'application Citrix Workspace pour HTML5

January 11, 2019

À partir de cette version, vous pouvez utiliser l'application Citrix Workspace pour HTML5 pour accéder directement aux applications et aux bureaux virtuels Linux sans connecter votre client à Citrix Gateway. Pour plus d'informations sur l'application Citrix Workspace pour HTML5, consultez la documentation Citrix.

Activer cette fonctionnalité

Cette fonction est désactivée par défaut. Pour l'activer, procédez comme suit :

1. Dans Citrix StoreFront, activez l'application Citrix Workspace pour HTML5.

   Pour obtenir la procédure détaillée, reportez-vous à l'étape 1 de l'article CTX208163 du centre de connaissances.

2. Activez les connexions WebSocket.

   a) Dans Citrix Studio, définissez la stratégie **Connexions WebSockets** sur **Autorisé**.

   Vous pouvez également définir les autres stratégies WebSocket. Pour obtenir la liste complète des stratégies WebSocket, consultez Paramètres de stratégie WebSockets.

   b) Sur le VDA, redémarrez le service ctxvda et le service ctxhdx, dans cet ordre, pour que votre paramètre prenne effet.

   c) Sur le VDA, exécutez la commande suivante pour vérifier si l'écouteur WebSocket est en cours d'exécution.

   ```
   netstat -an | grep 8008
   ```

   Lorsque l'écouteur WebSocket est en cours d'exécution, le résultat de la commande est similaire au suivant :

   ```
   tcp 0 0 :::8008 :::* LISTEN
   ```

Remarque : vous pouvez également activer le chiffrement TLS pour sécuriser les connexions WebSocket. Pour de plus amples informations sur l'activation du cryptage TLS, consultez la section Gérer les sessions utilisateur.

Sécuriser les sessions utilisateur en utilisant SSL

January 15, 2019

À compter de la version 7.16, le VDA Linux prend en charge le chiffrement SSL pour des sessions utilisateur sécurisées Le chiffrement SSL est désactivé par défaut.

Activer le chiffrement SSL

Pour activer le chiffrement SSL pour des sessions utilisateur sécurisées, obtenez des certificats et activez le cryptage SSL sur le VDA Linux et le Delivery Controller (le Controller).

Obtenir des certificats

Procurez-vous des certificats de serveur au format PEM et des certificats racine au format CRT auprès d'une autorité de certification (CA) de confiance. Un certificat de serveur contient les sections suivantes :

- Certificat
- Clé privée non chiffrée
- Certificats intermédiaires (facultatif)

Exemple de certificat de serveur

```
-----BEGIN CERTIFICATE-----

MIIDTTCCAragAwIBAgIJALluncpiqGXCMA0GCSqGSIb3DQEBBQUAMGcxCzAJBgNV

BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU

MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0

MB4XDTA4MDkzMDEwNTk1M1oXDTI4MDkyNTEwNTk1M1owgYoxCzAJBgNVBAYTAlVL

MRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEUMBIGA1UE

ChMLQ2l0cml4IFRlc3QxGzAZBgNVBAsTElNlcnZlciBDZXJ0aWZpY2F0ZTEgMB4G

A1UEAxMXY2EwMDEtc2MwMDEuY2l0cml0ZS5uZXQwgZ8wDQYJKoZIhvcNAQEBBQAD

gY0AMIGJAoGBALCTTOdxcivbI0L0F66xgO5gkNeIGKVP+37pSKV8B66lWCVzr6p9

t72Fa+9oCcf2x/ue274NXFcg4fqGRDsrEw13YxM6COyBf7L6psrsCDNnBP1q8TJH

4xoPIXUeaW4MVk/3PVyfhHKs4fz8yy1I4VDnXVHhw+0FQ2Bq3NhwsRhnAgMBAAGj

gdwwgdkwCQYDVR0TBAIwADAdBgNVHQ4EFgQUrLidzYot+CUXSh9xMfp1M+/O8y0w

gZkGA1UdIwSBkTCBjoAU85kN1EPJ0cVhcOss1slseDQwGsKha6RpMGcxCzAJBgNV

BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU

MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0

ggkAy8nC8dcB32EwEQYJYIZIAYb4QgEBBAQDAgVgMA0GCSqGSIb3DQEBBQUAA4GB

AD5axBYHwIxJCJzNt2zdXnbp200yUToWElBwQe/9cGaP6CpjoxJ7FJa2/8IpaT68

VelBu1SEYY1GKCGCw93pc7sPKqb8pGBRI5/dygb+geFk1Q7KyVbu0IjOtr3pkxAe

b6CFJtNLudHUrwF6l0rB72zbyz3PiIx+HEwt1j0j8z4K

-----END CERTIFICATE-----
```



```
40
41      -----BEGIN RSA PRIVATE KEY-----
42
43      MIICXgIBAAKBgQCwk0zncXIr2yNC9BeusYDuYJDXiBilT/t+6UilfAeupVglc6+q
44
45      fbe9hWvvaAnH9sf7ntu+DVxXIOH6hkQ7KxMNd2MTOgjsgX+y+qbK7AgzZwT9avEy
46
47      R+MaDyF1HmluDFZP9z1cn4RyrOH8/MstSOFQ511R4cPtBUNgatzYcLEYZwIDAQAB
48
49      AoGBAKwBgZu/bkl8edgB8YPyU7diiBX89I0s4b/aPjM+JDmjxb8N96RsPO24p9Ea
50
51      FtUc9+iL8mEroLUbSicCXjsJFc+cxg9vVaNa6EEkkBj735oCUERqSx0Yb/lAdck/
52
53      FXzU0tqytUe/KHgcSgjtjrSeqLJqMm+yxzBAatVRTTzGdwAhAkEA3l1KRZjIN5uz
54
55      Enmi2RTI3ngBhBP/S3GEbvJfKsD5n2Ri90+OoEPxclvvp5ne8Q0zUpshbjFEPb0C
56
57      ykZ6UassFwJBAMtI5yPnV9ewPzJoaNjZIJcMtNXDchSlxXiJiyzv+Qmr8RuQz9Pv
58
59      fIenmTrfZ+Wo4DaKg+8ar2OvOnKF0HFAmDECQQDEwR1H6cE3WyCfN1u942M9XkhR
60
61      GvSpR7+b///vL6Nwwv3CwPV9n8DTpL+wuDkJZ9nCvRteil9MlaMTYjs3alNvAkEA
62
63      qy5JzZcbBnrYzMbVO32jju7ZPISnhTGO1xDjzMSLLpTGpNLN34b0k3sTclr8L42E
64
65      uQjtTqRm+wdsrVF3lFazkQJANudmsUVv3gZKhMGaV2hzIdXIfHyOIYv+3leZhQY6
66
67      h5eEmxSZS50TvyNGt2e6m2ZgaZmjTagH59TCBHvR5nof2g==
68
69      -----END RSA PRIVATE KEY-----
70
71      -----BEGIN CERTIFICATE-----
72
73      MIIDGTCCAoKgAwIBAgIJAMvJwvHXAd9hMA0GCSqGSIb3DQEBBQUAMGcxCzAJBgNV
74
75      BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU
76
77      MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0
78
79      MB4XDTA4MDkzMDEwNDExMVoXDTI4MDkyNTEwNDExMVowZzELMAkGA1UEBhMCVUsx
80
81      EjAQBgNVBAgTCUNhbWJyaWRnZTESMBAGA1UEBxMJQ2FtYm91cm5lMRQwEgYDVQQK
82
83      EwtDaXRyaXggVGVzdDEaMBgGA1UEAxMRY2EwMDEuY2l0cml0ZS5uZXQwgZ8wDQYJ
84
```



```
KoZIhvcNAQEBBQADgY0AMIGJAoGBAKVZmF7Uj7u0nvO3Qwdfi0nr3QkNH2DXpWrZ

Zh8cI9Vv+UFRUiC6oB7izLtBMFn3fOUP7i2CfkHN3ZGJ17p89pdyjket1MslVeJw

acOqrYvD+fNNSvJjunTbaCywVtALjmFSfMHeZJXVSckrpEhnk0nkMS16tcrya/K/

osSlzvI3AgMBAAGjgcwwgckwDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQU85kN1EPJ

0cVhcOss1slseDQwGsIwgZkGA1UdIwSBkTCBjoAU85kN1EPJ0cVhcOss1slseDQw

GsKha6RpMGcxCzAJBgNVBAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNV

BAcTCUNhbWJvdXJuZTEUMBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNh

MDAxLmNpdHJpdGUubmV0ggkAy8nC8dcB32EwDQYJKoZIhvcNAQEFBQADgYEAIZ4Z

gXLLXf12RNqh/awtSbd41Ugv8BIKAsg5zhNAiTiXbzz8Cl3ec53Fb6nigMWc5Tli

UNCLXwnxRUiD400tESLX9ACUNH3I94yxOgujkSOSBni21jjZTvfBB32Rmr5DByJg

UmKORn/hdqMlcqpe5wO6as6+HN4WUOi+hEtUMME=

-----END CERTIFICATE-----
```

Activer le chiffrement SSL

Activer le chiffrement SSL sur l'agent Linux VDA

Sur Linux VDA, utilisez l'outil **enable_vdassl.sh** pour activer (ou désactiver) le chiffrement SSL. L'outil est situé dans le répertoire **/opt/Citrix/VDA/sbin**. Pour plus d'informations sur les options disponibles dans l'outil, exécutez la commande **/opt/Citrix/VDA/sbin/enable_vdassl.sh -help**.

Conseil : un certificat de serveur doit être installé sur chaque serveur Linux VDA et des certificats racine doivent être installés sur chaque serveur et client Linux VDA.

Activer le chiffrement SSL sur le Controller

> **Remarque :**
>
> - Le Controller doit utiliser le nom de domaine complet (FQDN) du VDA Linux. Il ne peut pas utiliser l'adresse IP (utilisée par défaut) pour se connecter au VDA Linux cible.
> - Vous pouvez activer le chiffrement SSL uniquement pour les groupes de mise à disposition entiers. Vous ne pouvez pas activer le chiffrement SSL pour des applications spécifiques.

Dans une fenêtre PowerShell sur le Controller, exécutez les commandes suivantes dans l'ordre pour activer le chiffrement SSL pour le groupe de mise à disposition cible et pour que le Controller utilise le nom de domaine complet du VDA Linux.

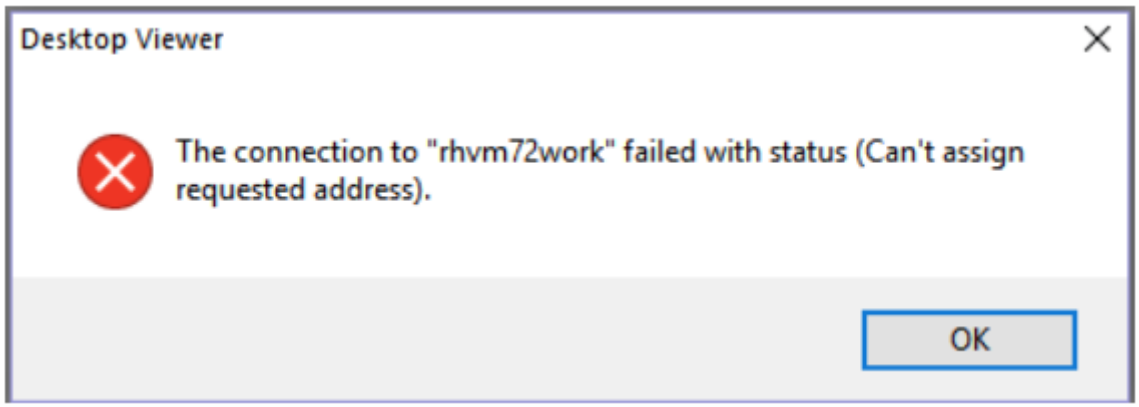
1. Asnp citrix.*
2. Get-BrokerAccessPolicyRule -DesktopGroupName 'NOMGROUPE' | Set-BrokerAccessPolicyRule -HdxSslEnabled $true.
3. Set-BrokerSite –DnsResolutionEnabled $true

Pour désactiver le chiffrement SSL sur le Controller, exécutez les commandes suivantes dans l'ordre :

1. Asnp citrix.*
2. Get-BrokerAccessPolicyRule -DesktopGroupName 'NOMGROUPE' | Set-BrokerAccessPolicyRule -HdxSslEnabled $false.
3. Set-BrokerSite –DnsResolutionEnabled $false

Résolution des problèmes

Le message d'erreur « Can't assign requested address » (Impossible d'attribuer l'adresse demandée) peut s'afficher dans l'application Citrix Workspace pour Windows lorsque vous tentez d'accéder à une session de bureau publié :



Pour résoudre ce problème, ajoutez une entrée au fichier**hosts**, comme :

10.108.13.180 rhvm72work.citrixlab.local

Où

- **10.108.13.180** est l'adresse IP de l'agent Linux VDA.
- **rhvm72work.citrixlab.local** est le nom de domaine complet de l'agent Linux VDA.

Sur les machines Windows, le fichier **hosts** est généralement situé dans **C:\Windows\System32\drivers\etc\hosts**

Sécuriser les sessions utilisateur en utilisant DTLS

January 11, 2019

Le cryptage DTLS est une fonctionnalité entièrement prise en charge à partir de la version 7.18. Par défaut, cette fonction est activée sur le VDA Linux. Pour plus d'informations, consultez la section Transport Layer Security.

Activer le chiffrement DTLS

Vérifier que le transport adaptatif est activé

Dans Citrix Studio, vérifiez que la stratégie **HDX Adaptive Transport** est définie sur le mode **Préféré** ou **Diagnostic**.

Activer le chiffrement SSL sur l'agent Linux VDA

Sur Linux VDA, utilisez l'outil **enable_vdassl.sh** pour activer (ou désactiver) le chiffrement SSL. L'outil se trouve dans **/opt/Citrix/VDA/sbin**. Pour plus d'informations sur les options disponibles dans l'outil, exécutez la commande **/opt/Citrix/VDA/sbin/enable_vdassl.sh –h**.

> **Remarque :**
>
> Le VDA Linux prend actuellement en charge DTLS 1.0 et DTLS 1.2. DTLS 1.2 nécessite Citrix Receiver pour Windows 4.12 ou l'application Citrix Workspace 1808 pour Windows ou version ultérieure. Si votre client prend en charge uniquement DTLS 1.0 (par exemple, Citrix Receiver pour Windows 4.11), définissez **SSLMinVersion** to **TLS_1.0** et **SSLCipherSuite** sur **COM** ou **ALL** à l'aide de l'outil **enable_vdassl.sh**.

Authentification unique avec des cartes à puce

January 11, 2019

Les utilisateurs peuvent utiliser une carte à puce connectée à la machine cliente pour s'authentifier lors de la connexion à une session de bureau virtuel Linux. Cette fonctionnalité est implémentée via la redirection de carte à puce sur le canal virtuel de la carte à puce ICA. Les utilisateurs peuvent également utiliser la carte à puce dans la session. Les cas d'utilisation incluent l'ajout d'une signature numérique à un document, le cryptage ou le décryptage d'un e-mail ou l'authentification sur un site Web nécessitant l'authentification par carte à puce.

Le VDA Linux utilise la même configuration que le VDA Windows pour cette fonctionnalité. Pour plus d'informations, consultez la section Configurer l'environnement de carte à puce.

La disponibilité de l'authentification pass-through avec des cartes à puce dépend des facteurs suivants :

- Le VDA Linux est installé sur RHEL 7.5.
- Des cartes à puce prises en charge par CoolKey sont utilisées.
- L'application Citrix Workspace pour Windows est utilisée.

> **Remarque :**
>
> L'authentification par carte à puce auprès de Citrix n'est pas officiellement prise en charge.

S'assurer que CoolKey prend en charge votre carte à puce

CoolKey est un pilote de carte à puce largement utilisé sur RHEL. CoolKey prend en charge quatre types de cartes à puce, à savoir les cartes CoolKey, CAC, PIV et PKCS#15. Cependant, le nombre de cartes officiellement prises en charge et validées reste limité (consultez la page Smart Card Support in Red Hat Enterprise Linux).

Dans cet article, la carte à puce Yubikey 4 est utilisée comme exemple pour illustrer la configuration. Yubikey 4 est un périphérique USB CCID PIV tout-en-un qui peut facilement être acheté auprès d'Amazon ou d'autres revendeurs. Le pilote CoolKey prend en charge Yubikey 4.

Si votre organisation a besoin d'une autre carte à puce plus avancée, préparez une machine physique avec les packages RHEL 7.5 et CoolKey installés. Pour plus d'informations sur l'installation de CoolKey, consultez la section Installer le pilote de la carte à puce. Insérez votre carte à puce et exécutez la commande suivante pour vérifier que CoolKey prend en charge votre carte à puce :

```
1 pkcs11-tool --module libcoolkeypk11.so --list-slots
```

Si CoolKey prend en charge votre carte à puce, les résultats de la commande sont similaires aux suivants avec informations sur le logement de la carte.


```
[root@rhphy ~]# pkcs11-tool --module libcoolkeypk11.so --list-slots
Available slots:
Slot 0 (0x1): Yubico Yubikey 4 CCID 00 00
  token label        : user1
  token manufacturer :
  token model        :
  token flags        : login required, token initialized, PIN initialized, readonly
  hardware version   : 0.0
  firmware version   : 0.0
  serial num         :
[root@rhphy ~]#
```

Configuration

Configurer l'environnement de la carte à puce

Le VDA Linux utilise le même environnement de carte à puce que le VDA Windows. Dans l'environnement, plusieurs composants doivent être configurés, notamment le contrôleur de domaine, l'autorité de certification Microsoft (CA), Internet Information Services, Citrix StoreFront et l'application Citrix Workspace. Pour plus d'informations sur la configuration basée sur la carte à puce Yubikey 4, consultez l'article Citrix CTX206156.

Avant de passer à l'étape suivante, vérifiez que tous les composants sont correctement configurés, que la clé privée et le certificat utilisateur sont téléchargés sur la carte à puce et que vous pouvez ouvrir une session sur le VDA Windows à l'aide de la carte à puce.

Installer les packages PC/SC Lite

PCSC Lite est une mise en œuvre de la spécification PC/SC (Personal Computer/Smart Card) sous Linux. Il fournit une interface de carte à puce Windows pour communiquer avec les cartes à puce et les lecteurs. La redirection de carte à puce dans le VDA Linux est implémentée au niveau PC/SC.

Exécutez la commande suivante pour installer les packages PC/SC Lite.

```
1 yum install pcsc-lite pcsc-lite-ccid pcsc-lite-libs
```

Installer le pilote de la carte à puce

CoolKey est un pilote de carte à puce largement utilisé sur RHEL. Si CoolKey n'est pas installé, exécutez la commande suivante pour l'installer.

```
1 yum install coolkey
```


Installer les modules PAM pour l'authentification par carte à puce

Exécutez la commande suivante pour installer les modules pam_krb5 et krb5-pkinit.

```
yum install pam_krb5 krb5-pkinit
```

Le module pam_krb5 est un module d'authentification enfichable que les applications prenant en charge PAM peuvent utiliser pour vérifier les mots de passe et obtenir des tickets d'octroi de tickets depuis le centre de distribution de clés (KDC). Le module krb5-pkinit contient le plugin PKINIT qui permet aux clients d'obtenir les informations d'identification initiales depuis le KDC à l'aide d'une clé privée et d'un certificat.

Installer le logiciel VDA Linux sur RHEL 7.5

Installez le logiciel Linux VDA à l'aide du gestionnaire de packages RPM ou de l'installation easy install. Consultez la section Présentation de l'installation.

Une fois l'installation du VDA terminée, vérifiez que le VDA peut s'enregistrer auprès du Delivery Controller et que les sessions de bureau Linux publiées peuvent être lancées avec succès à l'aide de l'authentification par mot de passe.

Préparer un certificat racine

Un certificat racine est utilisé pour vérifier le certificat dans la carte à puce. Procédez comme suit pour télécharger et installer un certificat racine.

1. Procurez-vous un certificat racine au format PEM, généralement auprès de votre serveur d'autorité de certification.

   Vous pouvez exécuter une commande similaire à la suivante pour convertir un fichier DER (*.crt, *.cer, *.der) en PEM. Dans l'exemple de commande suivant, **certnew.cer** est un fichier DER.

   ```
   openssl x509 -inform der -in certnew.cer -out certnew.pem
   ```

2. Installez le certificat racine dans le répertoire openssl. Le fichier **certnew.pem** est utilisé à titre d'exemple.

   ```
   cp certnew.pem /etc/pki/CA/certs/
   ```

Configurer la base de données NSS

Le module de connexion au VDA Linux utilise la base de données NSS pour accéder aux cartes à puce et aux certificats. Procédez comme suit pour configurer la base de données NSS.

1. Ajoutez le certificat racine mentionné précédemment à la base de données NSS.

```
certutil -A -n "My Corp Root" -t "CT,C,C" -a -d /etc/pki/nssdb -i
    /etc/pki/CA/certs/certnew.pem
```

2. Exécutez la commande suivante pour vérifier que le certificat racine est correctement ajouté à la base de données NSS.

```
certutil -L -d /etc/pki/nssdb
```

Les résultats de la commande sont similaires aux suivants si le certificat racine est ajouté avec succès.

```
[root@rh73ws LVDA]# certutil -L -d /etc/pki/nssdb

Certificate Nickname                                         Trust Attributes
                                                             SSL,S/MIME,JAR/XPI

My Corp Root                                                 CT,C,C
```

3. Vérifiez si CoolKey est installé dans la bibliothèque NSS PKCS # 11.

```
modutil -list -dbdir /etc/pki/nssdb
```

Les résultats de la commande sont similaires aux suivants si le module CoolKey est installé.

```
[root@rh73demo ~]# modutil -list -dbdir /etc/pki/nssdb

Listing of PKCS #11 Modules
-----------------------------------------------------------
  1. NSS Internal PKCS #11 Module
         slots: 2 slots attached
        status: loaded

         slot: NSS Internal Cryptographic Services
        token: NSS Generic Crypto Services

         slot: NSS User Private Key and Certificate Services
        token: NSS Certificate DB

  2. CoolKey PKCS #11 Module
        library name: libcoolkeypk11.so
         slots: There are no slots attached to this module
        status: loaded
-----------------------------------------------------------
```

Si le module CoolKey n'est pas installé, exécutez la commande suivante pour l'installer manuellement et vérifiez à nouveau l'installation.

```
modutil -add "CoolKey PKCS #11 Module" -libfile libcoolkeypk11.so
    -dbdir /etc/pki/nssdb
```


Configurer le module pam_krb5

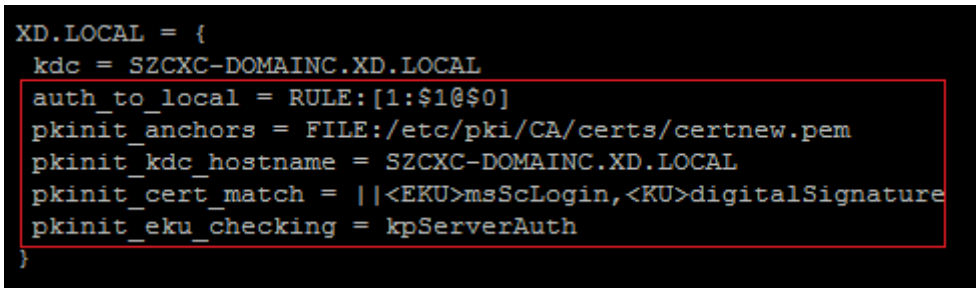
Le module pam_krb5 interagit avec le KDC pour obtenir des tickets Kerberos à l'aide des certificats de la carte à puce. Pour activer l'authentification pam_krb5 dans PAM, exécutez la commande suivante :

```
authconfig --enablekrb5 --update
```

Dans le fichier de configuration **/etc/krb5.conf**, ajoutez des informations pkinit en fonction du domaine réel.

```
EXAMPLE.COM = {


    kdc = KDC. EXAMPLE.COM

    auth_to_local = RULE:[1:$1@$0]

    pkinit_anchors = FILE:/etc/pki/CA/certs/certnew.pem

    pkinit_kdc_hostname = KDC.EXAMPLE.COM

    pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature

    pkinit_eku_checking = kpServerAuth

  }
```

Le fichier de configuration ressemble à ce qui suit une fois que vous avez ajouté les informations pkinit.



Configurer l'authentification PAM

Les fichiers de configuration PAM indiquent les modules qui sont utilisés pour l'authentification PAM. Pour ajouter pam_krb5 en tant que module d'authentification, ajoutez la ligne suivante au fichier **/etc/pam.d/smartcard-auth** :


```
auth [success=done ignore=ignore default=die] pam_krb5.so preauth_options=
X509_user_identity=PKCS11:/usr/lib64/pkcs11/libcoolkeypk11.so
```

Le fichier de configuration ressemble à ce qui suit après les modifications si SSSD est utilisé.

```
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        [success=done ignore=ignore default=die] pam_krb5.so preauth_options=X509_user_identity=PKCS11:/usr/lib64/pkcs11/libcoolkeypk11.so
auth        sufficient    pam_permit.so
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     [default=bad success=ok auth_err=ignore user_unknown=ignore ignore=ignore] pam_krb5.so
account     required      pam_permit.so

password    required      pam_pkcs11.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
session     optional      pam_oddjob_mkhomedir.so umask=0077
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
session     optional      pam_sss.so
session     optional      pam_krb5.so
```

Le fichier de configuration ressemble à ce qui suit après les modifications si Winbind est utilisé.

```
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        [success=done ignore=ignore default=die] pam_krb5.so preauth_options=X509_user_identity=PKCS11:/usr/lib64/libiidp11.so
auth        sufficient    pam_permit.so
auth        required      pam_deny.so

account     required      pam_unix.so broken_shadow
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     [default=bad success=ok user_unknown=ignore] pam_winbind.so
account     [default=bad success=ok auth_err=ignore user_unknown=ignore ignore=ignore] pam_krb5.so
account     required      pam_permit.so

password    required      pam_pkcs11.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
session     optional      pam_oddjob_mkhomedir.so umask=0077
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
session     optional      pam_winbind.so
session     optional      pam_krb5.so
```

Le fichier de configuration ressemble à ce qui suit après les modifications si Centrify est utilisé.

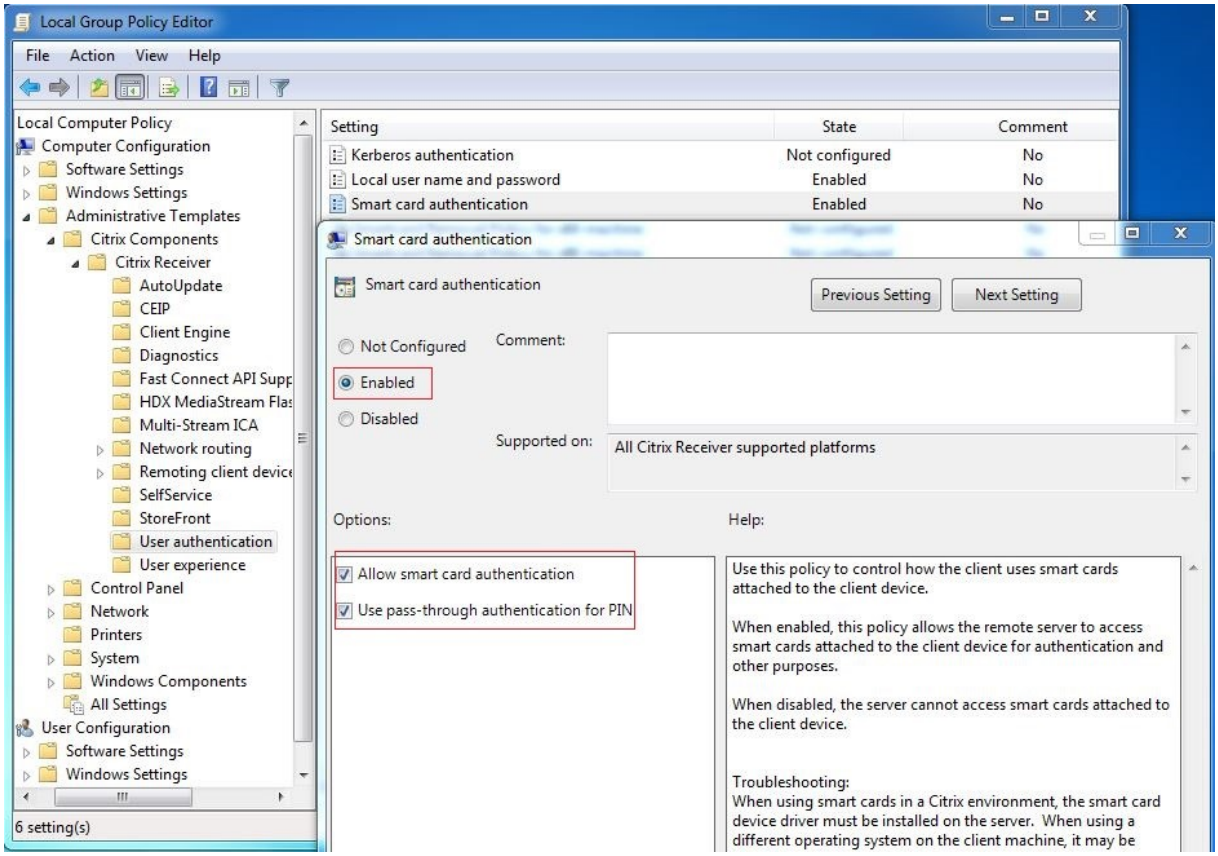
```
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        [success=done ignore=ignore default=die] pam_krb5.so preauth_options=X509_user_identity=PKCS11:/usr/lib64/pkcs11/libcoolkeypk11.so
auth        sufficient    pam_permit.so
auth        required      pam_deny.so

account     required      pam_nologin.so
account     required      pam_krb5.so
account     required      pam_permit.so

password    required      pam_pkcs11.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional     pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
session     optional      pam_krb5.so
```

(Facultatif) Single Sign-On avec cartes à puce

Citrix Single Sign-On (SSO) est une fonctionnalité qui implémente l'authentification unique lors du lancement de bureaux virtuels et d'applications. Cette fonctionnalité réduit le nombre de fois que

les utilisateurs entrent leur code PIN. Pour utiliser l'authentification SSO avec le VDA Linux, configurez l'application Citrix Workspace. La configuration est la même avec le VDA Windows. Pour plus d'informations, consultez l'article CTX133982 du centre de connaissances.

Activez l'authentification par carte à puce comme suit lors de la configuration de la stratégie de groupe dans l'application Citrix Workspace.

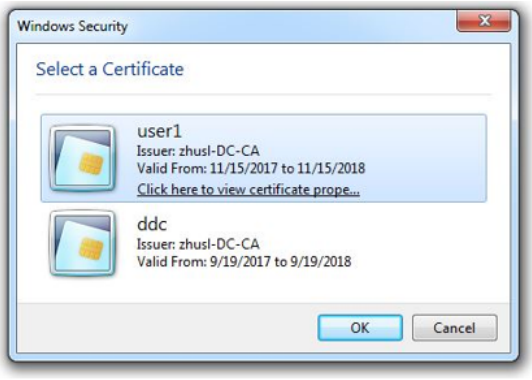


Utilisation

Se connecter au VDA Linux en utilisant une carte à puce

Les utilisateurs peuvent utiliser une carte à puce pour se connecter au VDA Linux dans les scénarios SSO et non SSO.

- Dans le scénario SSO, les utilisateurs sont automatiquement connectés à StoreFront avec le certificat et le code PIN de la carte à puce mis en cache. Lorsque les utilisateurs lancent une session de bureau virtuel Linux dans StoreFront, le code PIN est transmis au VDA Linux pour l'authentification par carte à puce.
- Dans le scénario non SSO, les utilisateurs sont invités à sélectionner un certificat et à entrer un code PIN pour se connecter à StoreFront.



Lorsque les utilisateurs lancent une session de bureau virtuel Linux dans StoreFront, une boîte de dialogue de connexion au VDA Linux apparaît comme suit. Le nom d'utilisateur est extrait du certificat dans la carte à puce et les utilisateurs doivent le saisir de nouveau pour l'authentification de connexion.

Le comportement est le même avec le VDA Windows.

Se reconnecter à une session en utilisant une carte à puce

Pour vous reconnecter à une session, assurez-vous que la carte à puce est connectée à la machine cliente. Sinon, une fenêtre de mise en cache grise apparaît du côté du VDA Linux et se ferme rapidement car la ré-authentification échoue si la carte à puce n'est pas connectée. Aucune autre invite ne s'affiche dans ce cas pour vous rappeler de connecter la carte à puce.

Du côté de StoreFront, cependant, si une carte à puce n'est pas connectée lorsque vous essayez de vous reconnecter à une session, le site Web StoreFront peut afficher une alerte comme suit.

Limitation

Stratégie de retrait de carte à puce

Actuellement, le VDA Linux utilise uniquement le comportement par défaut pour le retrait de la carte à puce. Lorsque vous retirez la carte à puce après vous être connecté au VDA Linux, la session reste connectée et l'écran de session n'est pas verrouillé.

Prise en charge des autres cartes à puce et de la bibliothèque PKCS#11

Bien que seule la carte à puce CoolKey soit répertoriée dans notre liste de prise en charge, vous pouvez essayer d'utiliser d'autres cartes à puce et la bibliothèque PKCS #11 car Citrix fournit une solution générique de redirection de carte à puce. Pour passer à votre carte à puce spécifique ou à la bibliothèque PKCS#11 :

1. Remplacez toutes les instances `libcoolkeypk11.so` par votre bibliothèque PKCS#11.
2. Pour définir le chemin d'accès de votre bibliothèque PKCS#11 sur le Registre, exécutez la commande suivante :

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
     CurrentControlSet\Control\Citrix\VirtualChannels\Scard" -v "
     PKCS11LibPath" -d "PATH"
```

où **PATH** pointe vers votre bibliothèque PKCS#11 comme /usr/lib64/pkcs11/libcoolkeypk11.so

Authentification Single Sign-On double-hop

January 11, 2019

La fonctionnalité injecte les informations d'identification utilisateur entrées pour accéder à un magasin StoreFront dans le module AuthManager de l'application Citrix Workspace pour Linux et Citrix Receiver pour Linux 13.10. Après l'injection, vous pouvez utiliser le client pour accéder à des bureaux et applications virtuels à partir d'une session de bureau virtuel Linux, sans entrer les informations d'identification de l'utilisateur une deuxième fois.

> **Remarque :**
>
> cette fonctionnalité est prise en charge sur l'application Citrix Workspace pour Linux et Citrix Receiver pour Linux 13.10.

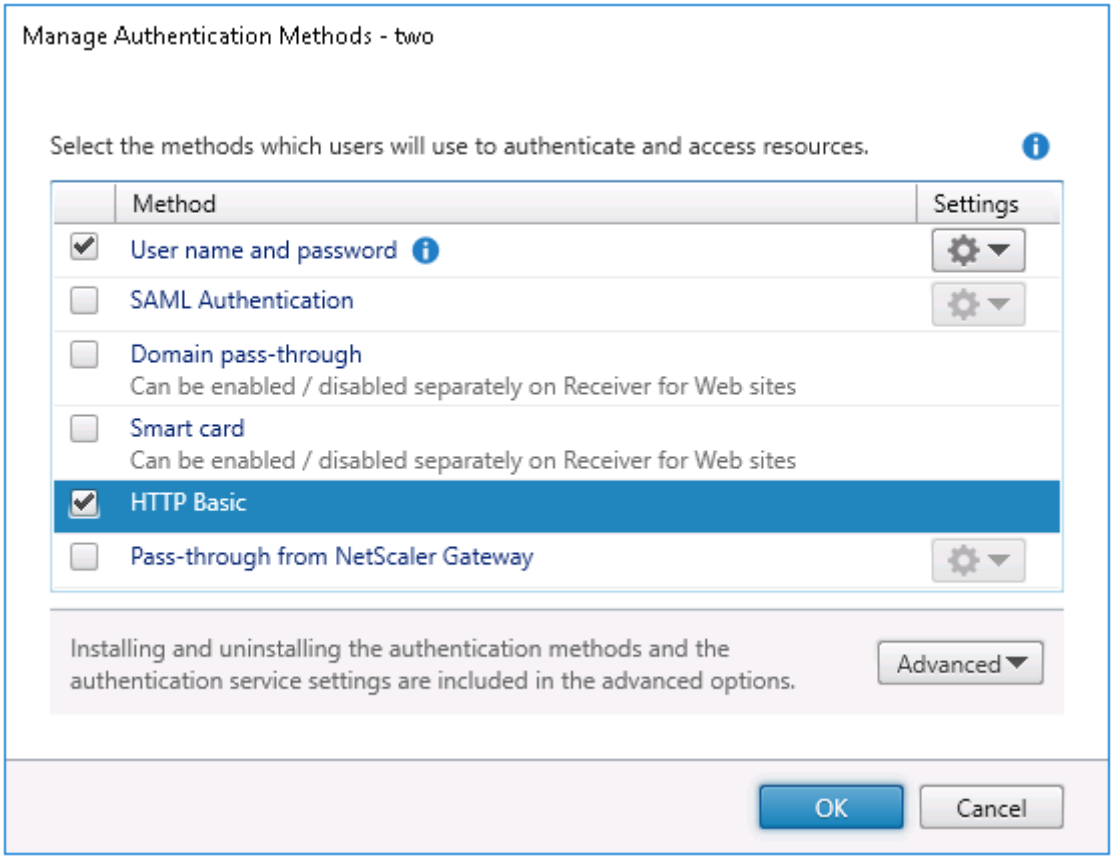
Pour mettre la fonctionnalité en service :

1. Sur le VDA Linux, installez l'application Citrix Workspace pour Linux ou Citrix Receiver pour Linux 13.10.

   Téléchargez l'application depuis la page de téléchargement Citrix pour l'application Citrix Workspace ou pour Citrix Receiver.

   Le chemin d'installation par défaut est /opt/Citrix/Icaclient/. Si vous installez l'application sur un chemin d'accès différent, définissez la variable d'environnement ICAROOT pour qu'elle pointe vers le chemin d'installation réel.

2. Dans la console de gestion Citrix StoreFront, ajoutez la méthode d'authentification **HTTP basique** pour le magasin cible.



3. Ajoutez la clé suivante au fichier de configuration AuthManager ($ICAROOT/config/AuthManConfig.xml) pour autoriser l'authentification HTTP basique :

```
<Protocols>
     <HTTPBasic>
         <Enabled>True</Enabled>
    </HTTPBasic>
</Protocols>
```

4. Exécutez les commandes suivantes pour installer le certificat racine dans le répertoire spécifié.

```
cp rootcert.pem $ICAROOT/keystore/cacerts/
$ICAROOT/util/ctx_rehash  $ICAROOT/keystore/cacerts/
```

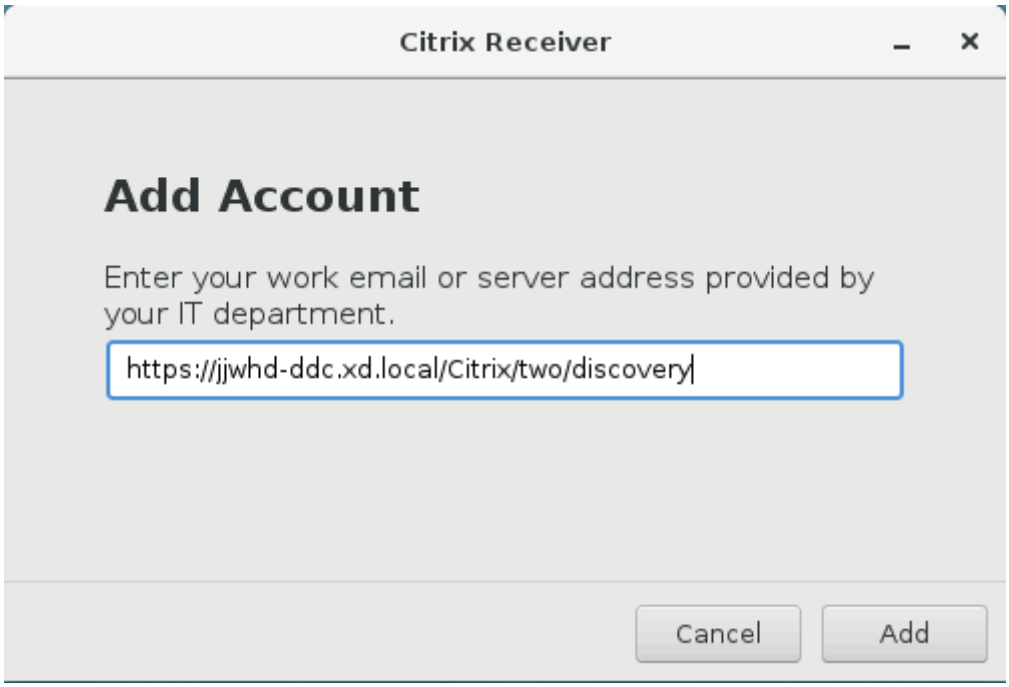
5. Exécutez la commande suivante pour activer la fonctionnalité :

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
   CurrentControlSet\Control\Citrix" -v "LurSsonEnabled" -d "0
   x00000001"
```


6. Lancez une session de bureau virtuel Linux et démarrez l'application Citrix Workspace pour Linux ou Citrix Receiver pour Linux 13.10 dans cette session.

   Vous êtes invité à entrer un compte de magasin la première fois que vous démarrez l'application Citrix Workspace pour Linux ou Citrix Receiver pour Linux 13.10 dans une session de bureau virtuel Linux. Ensuite, vous serez automatiquement connecté au magasin que vous avez spécifié précédemment.

   > **Remarque :**
   >
   > entrez une URL HTTPS comme compte de magasin.



Configurer des sessions non authentifiées

February 15, 2019

Utilisez les informations de cet article pour configurer des sessions non authentifiées. Aucun paramètre spécial n'est requis lors de l'installation de Linux VDA pour utiliser cette fonctionnalité.

> **Remarque :**
>
> Lorsque vous configurez des sessions non authentifiées, n'oubliez pas que le pré-lancement de session n'est pas pris en charge. Le prélancement de session n'est pas non plus pris en charge sur l'application Citrix Workspace pour Android.

Créer un magasin non authentifié

Vous devez créer un magasin non authentifié à l'aide de StoreFront pour prendre en charge une session non authentifiée sur l'agent Linux VDA.

Activer les utilisateurs non authentifiés dans un groupe de mise à disposition

Après la création d'un magasin non authentifié, activez les utilisateurs non authentifiés dans un groupe de mise à disposition pour prendre en charge une session non authentifiée. Pour activer les utilisateurs non authentifiés dans un groupe de mise à disposition, suivez les instructions de la documentation Citrix Virtual Apps and Desktops.

Définir le délai d'inactivité de sessions non authentifiées

Une session non authentifiée a un délai d'inactivité par défaut de 10 minutes. Cette valeur est configurée avec le paramètre de registre **AnonymousUserIdleTime**. Utilisez l'outil **ctxreg** pour modifier cette valeur. Par exemple, pour définir ce paramètre de registre sur cinq minutes, procédez comme suit :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
    CurrentControlSet\Control\Citrix" -v AnonymousUserIdleTime -d 0
    x00000005
```

Définir le nombre maximal d'utilisateurs non authentifiés

Pour définir le nombre maximal d'utilisateurs non authentifiés, utilisez la clé de registre **MaxAnonymousUserNumber**. Ce paramètre limite le nombre de sessions non authentifiées s'exécutant simultanément sur un seul agent Linux VDA. Utilisez l'outil **ctxreg** pour configurer ce paramètre de registre. Par exemple, pour définir la valeur sur 32 bits :

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
    CurrentControlSet\Control\Citrix" -v MaxAnonymousUserNumber -d 0
    x00000020
```

> **Important :**
>
> Il est essentiel de limiter 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 VDA Linux 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, essayez de modifier 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

February 15, 2019

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 VDA Linux et les serveurs LDAP.

Les composants VDA Linux 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 VDA Linux
- 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 VDA Linux

Pour activer ou désactiver LDAPS pour VDA Linux, 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 VDA Linux, 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 VDA Linux 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 VDA Linux 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

February 15, 2019

Les environnements qui utilisent le déport d'affichage X11 interactif (y compris xterm et gvim) sont pris en charge par le VDA Linux. 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 VDA Linux 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 VDA Linux 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 VDA Linux (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.

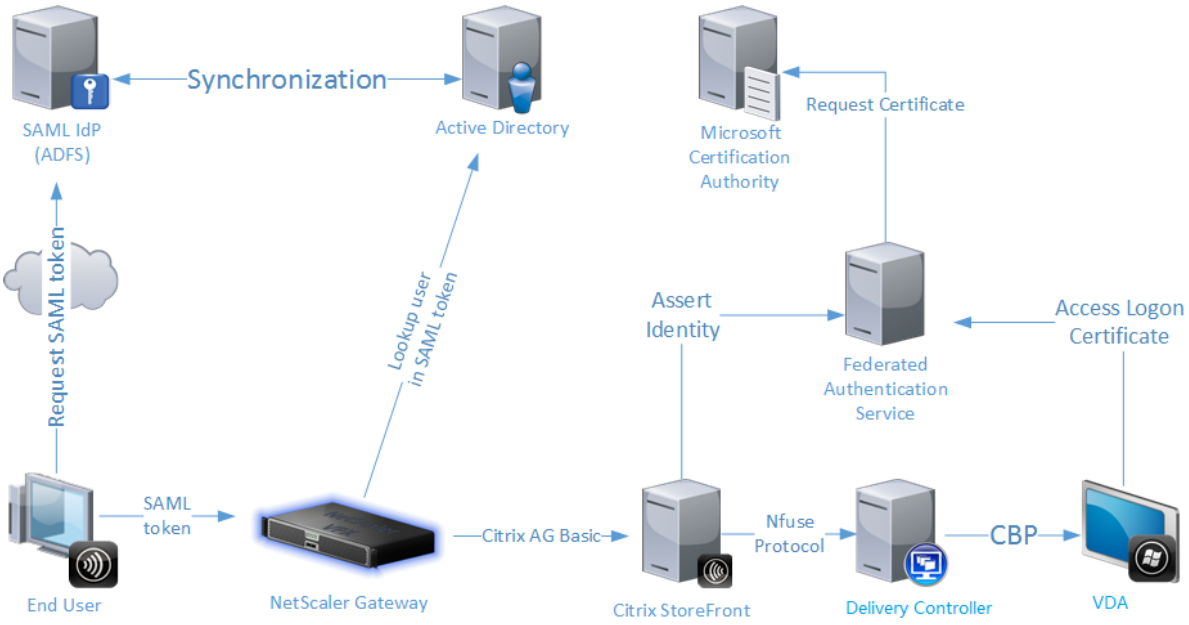
Service d'authentification fédérée

February 15, 2019

Généralités

Le Service d'authentification fédérée (FAS) de Citrix est un composant doté de privilèges conçu pour s'intégrer avec les Services de certificats Active Directory. Il émet des certificats pour les utilisateurs de manière dynamique, ce qui leur permet de se connecter à un environnement Active Directory comme s'ils avaient une carte à puce. Cette fonctionnalité permet à StoreFront d'utiliser une gamme plus large d'options d'authentification, telles que les assertions SAML (Security Assertion Markup Language). SAML est généralement utilisé comme une alternative aux comptes utilisateur Windows traditionnels sur Internet.

Le diagramme suivant illustre l'intégration du Service d'authentification fédérée avec une autorité de certification Microsoft, ainsi que la fourniture de services de support à StoreFront et aux VDA.



Les serveurs StoreFront de confiance contactent le FAS lorsque les utilisateurs demandent accès à l'environnement Citrix. Le FAS accorde un ticket qui permet à une seule session Citrix Virtual Apps ou Citrix Virtual Desktops de s'authentifier avec un certificat pour cette session. Lorsqu'un VDA doit authentifier un utilisateur, il se connecte au FAS utilise le ticket. Seul le FAS a accès à la clé privée du certificat utilisateur. Le VDA doit envoyer au FAS chaque opération de signature et de décryptage qu'il doit effectuer avec le certificat.

Exigences

Le Service d'authentification fédérée est pris en charge sur les serveurs Windows (Windows Server 2008 R2 ou version supérieure).

- Citrix vous recommande d'installer le FAS sur un serveur qui ne contient pas d'autres composants Citrix.
- Le serveur Windows doit être sécurisé. Il aura accès à un certificat d'autorité d'inscription et à une clé privée qui lui permettent d'émettre automatiquement des certificats pour les utilisateurs du domaine, et il aura accès à ces certificats utilisateur et clés privées.

Dans le site Citrix Virtual Apps ou Citrix Virtual Desktops :

- Les Delivery Controller doivent être à la version minimale 7.9.
- Le serveur StoreFront doit être à la version minimale 3.6 (il s'agit de la version fournie avec l'ISO XenApp et XenDesktop 7.9).
- Les VDA Linux doivent être à la version minimale 7.18. Vérifiez que la configuration de la stratégie de groupe Service d'authentification fédérée a été correctement appliquée aux VDA avant de créer le catalogue de machines de la manière habituelle. Pour plus d'informations, consultez la section **Configurer une stratégie de groupe** dans cet article.

Références :

- Services de certificats Active Directory
  https://technet.microsoft.com/en-us/library/hh831740.aspx
- Configuration de Windows pour l'ouverture de session par certificat
  http://support.citrix.com/article/CTX206156
- Installation du Service d'authentification fédérée
  Service d'authentification fédérée

Configurer Windows pour l'ouverture de session par certificat

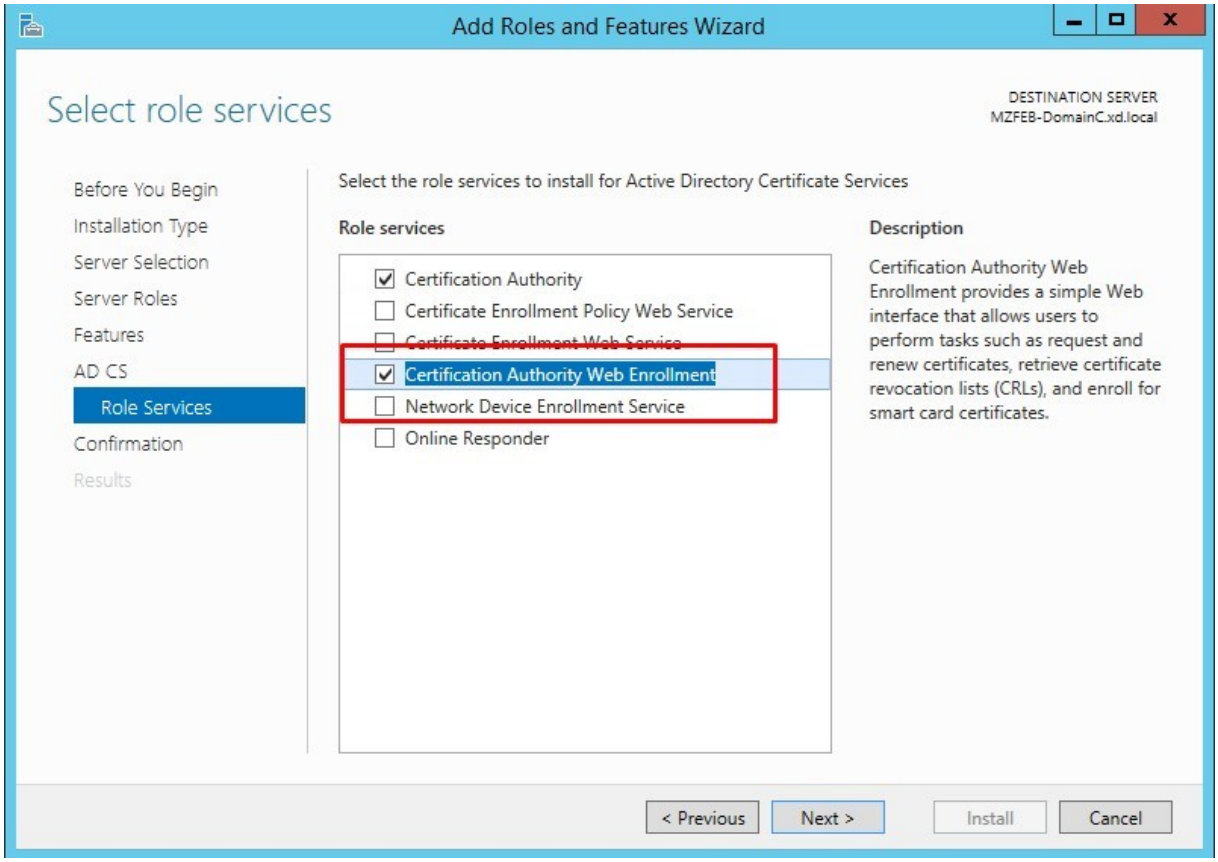
Pour plus d'informations sur la configuration de Windows pour l'ouverture de session par certificat, consultez l'article CTX206156 du centre de connaissances pour télécharger et lire le fichier **Smart_card_config_Citrix_Env.pdf** (nommé ci-après « fichier PDF »). Effectuez les étapes suivantes selon le fichier PDF tout en notant les différences ou les compléments qui sont donnés à chaque étape. Prêtez une attention particulière à la machine cible sur laquelle vous travaillez, par exemple AD, Delivery Controller ou StoreFront.

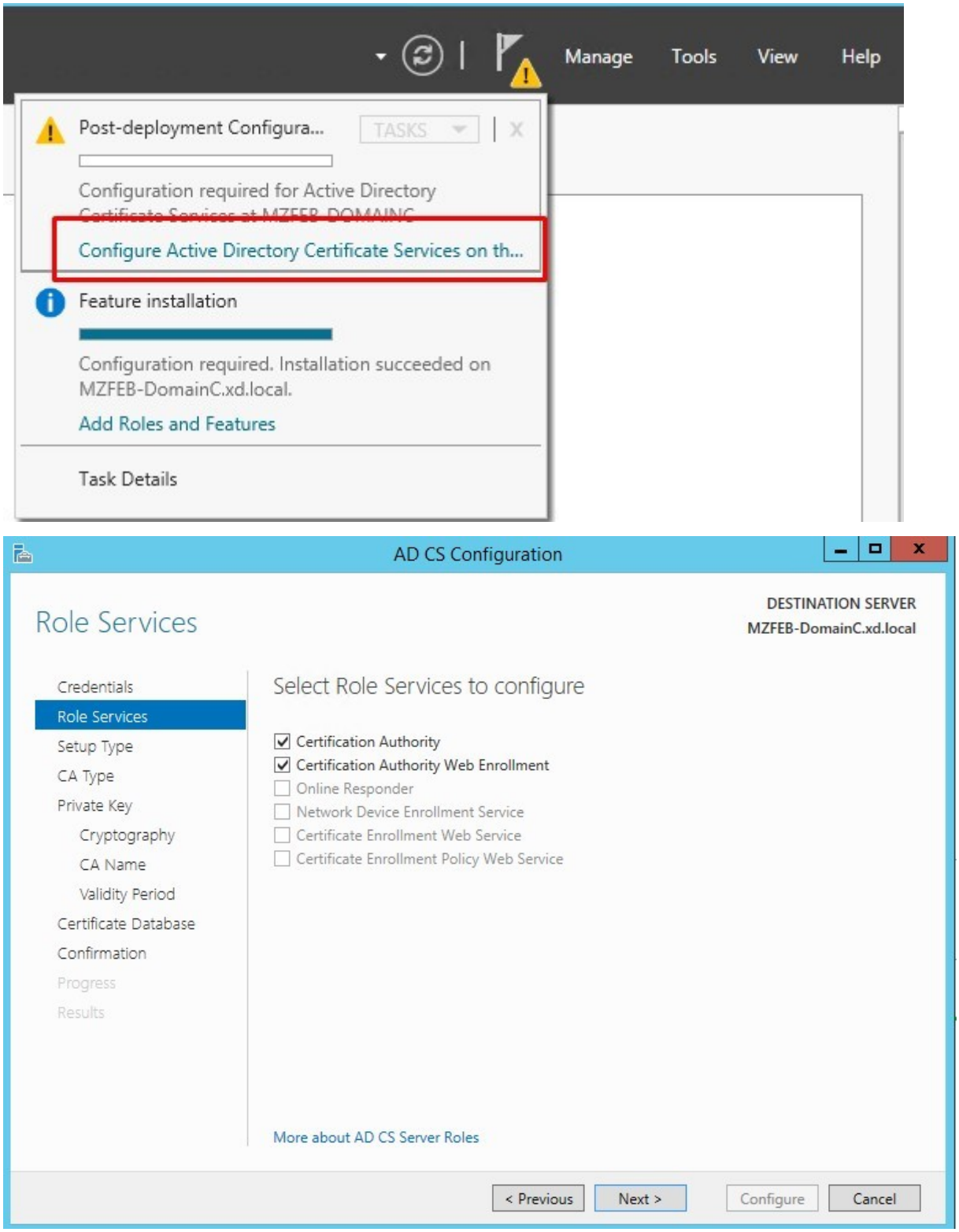
Configurer un domaine Windows (sur AD)

Installer les rôles de contrôleur de domaine

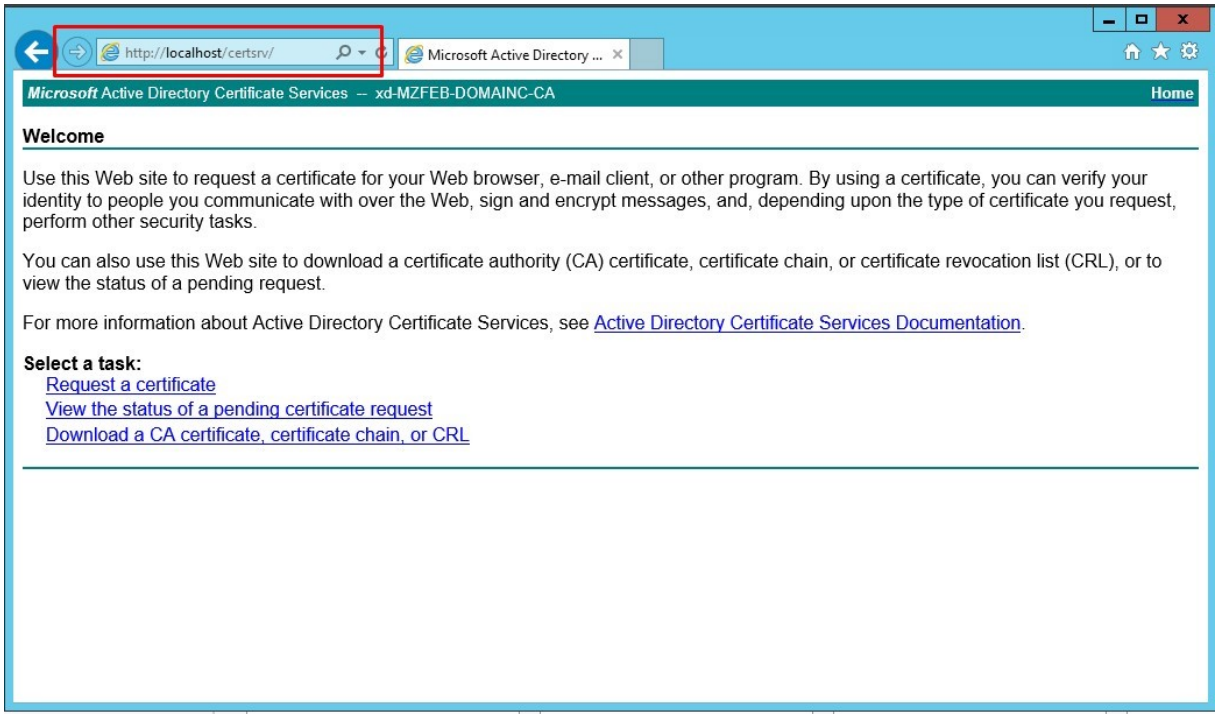
Consultez la section **Installing Domain Controller Roles** (Installer les rôles de contrôleur de domaine) du fichier PDF.

Lors de l'installation des services de certificats Active Directory, assurez-vous que les options suivantes sont sélectionnées comme indiqué ci-dessous :





Ouvrez `http://localhost/certsrv/` pour vérifier si la page d'accueil suivante est affichée. Si elle est affichée, les services de certificats Active Directory ont bien été installés.



Préparer l'autorité de certification pour l'utilisation de la carte à puce

Pas de complément. Consultez la section **Preparing the Certificate Authority for Smart card usage** (Préparer l'autorité de certification pour l'utilisation de la carte à puce) du fichier PDF.

Émettre un certificat de contrôleur de domaine

Pas de complément. Consultez la section **Issuing a Domain Controller Certificate** (Émettre un certificat de contrôleur de domaine) du fichier PDF.

Configurer Microsoft IIS pour HTTPS (sur StoreFront)

Configurer HTTPS sur Microsoft IIS

Pas de complément. Consultez la section **Configuring HTTPS on Microsoft IIS** (Configurer HTTPS sur Microsoft IIS) du fichier PDF.

Ordinateurs n'appartenant pas au domaine

Consultez la section **Non-Domain Joined Computers** (Ordinateurs n'appartenant pas au domaine) du fichier PDF.

Récupérer le certificat CA à partir de l'autorité de certification Microsoft (sur AD)

Pas de complément. Consultez la section **Retrieving the CA Certificate from the Microsoft CA** (Récupérer le certificat CA à partir de l'autorité de certification Microsoft) du fichier PDF.

Installer le certificat CA de confiance sur Windows

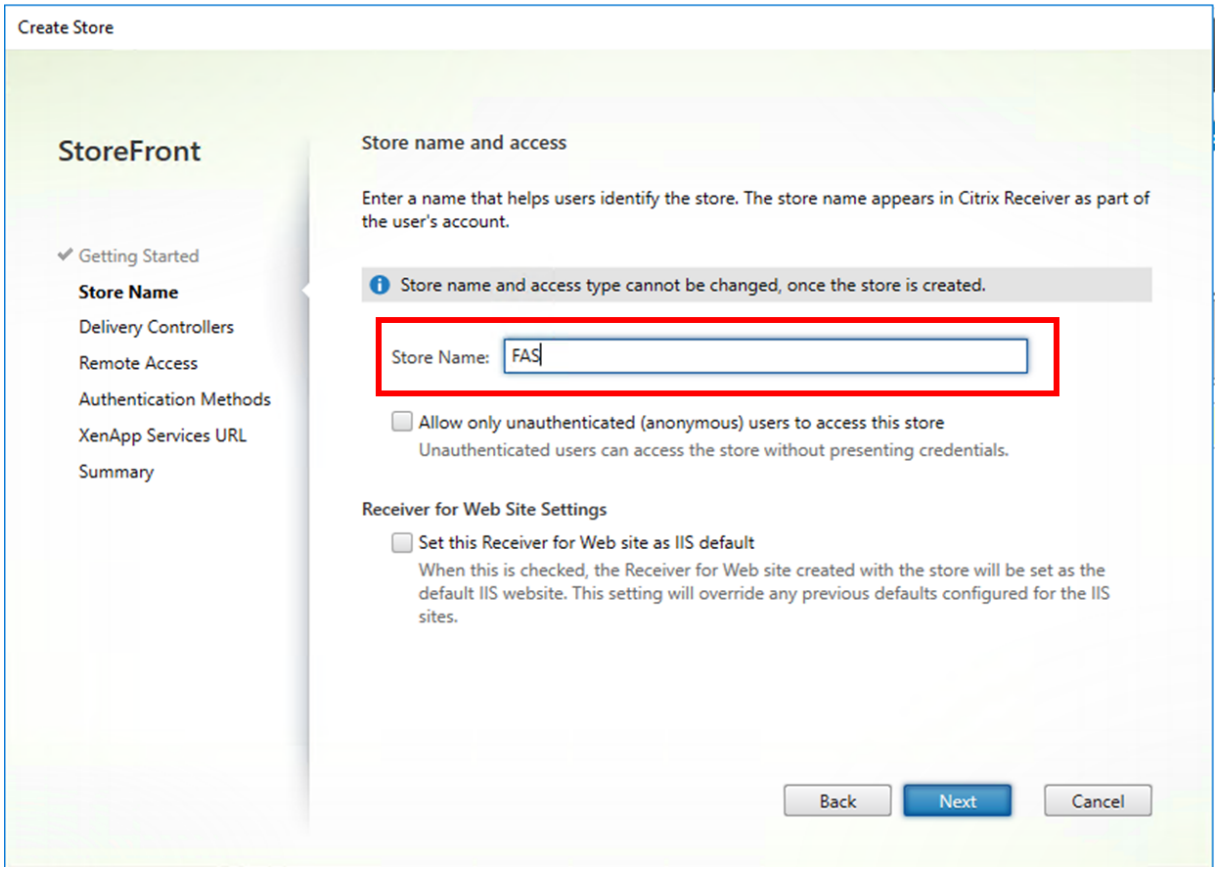
Pas de complément. Consultez la section **Installing the Trusted CA Certificate on Windows** (Installer le certificat CA de confiance sur Windows) du fichier PDF.

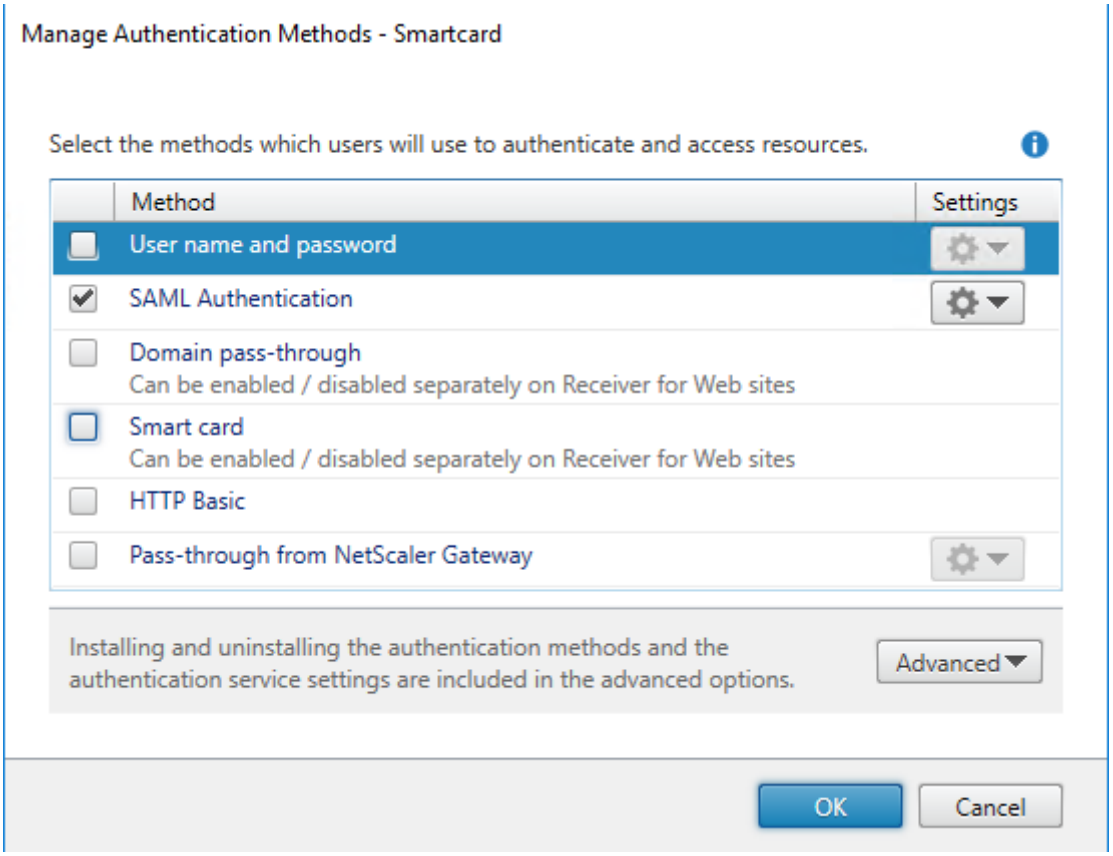
Configurer Citrix StoreFront (sur StoreFront)

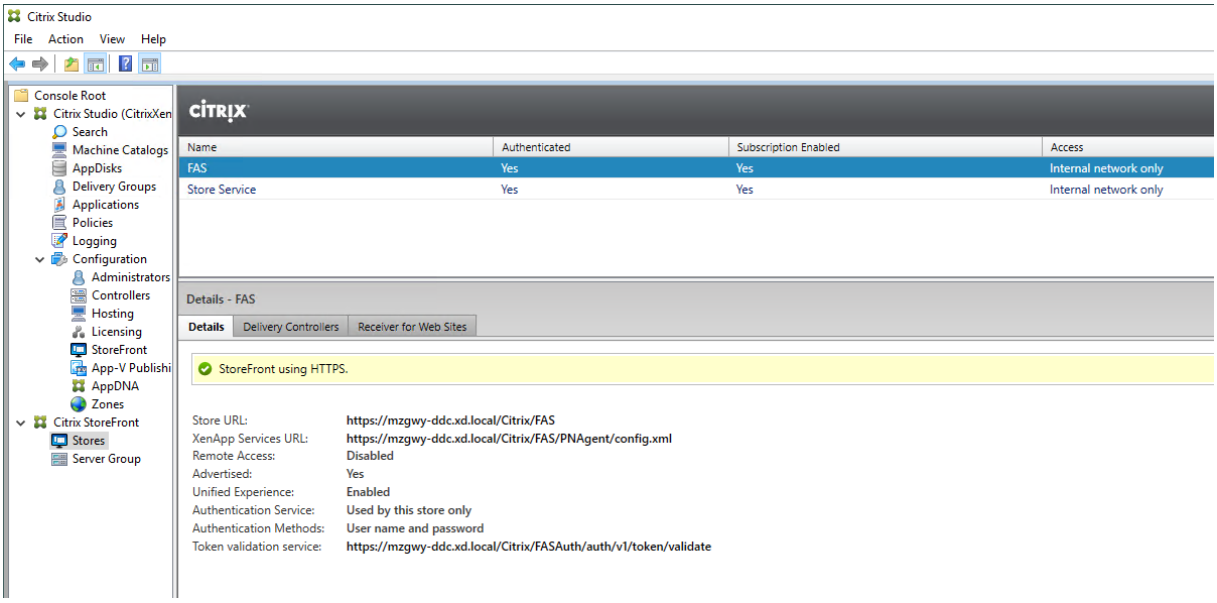
Créer un magasin

Consultez la section **Creating the Store** (Créer un magasin) du fichier PDF.

Après la configuration IIS précédente, l'URL de base du magasin commun est définie de manière forcée sur `https://` plutôt que `http://`. FAS ne partageant pas le magasin avec les cartes à puce, un nouveau magasin est donc requis pour FAS. Le FAS du VDA Linux est compatible avec toutes les méthodes d'authentification StoreFront. Par exemple, le magasin FAS peut être configuré pour utiliser des mots de passe ou SAML, mais ne peut pas utiliser les deux en même temps. Lorsque SAML est sélectionné, l'URL de StoreFront est automatiquement redirigée vers le fournisseur d'identité et la méthode d'authentification par mot de passe est ignorée.







Démarrez Internet Explorer et ouvrez l'URL du magasin FAS (par exemple, `https://mzgwy-ddc.xd.local/Citrix/FASWeb`).

Remarque : l'URL du magasin FAS doit disposer d'un lien **Web**.

Installer et configurer FAS

Le processus d'installation et de configuration comprend les étapes suivantes :

1. Installer le Service d'authentification fédérée
2. Activer le plug-in Service d'authentification fédérée sur les serveurs StoreFront
3. Configurer une stratégie de groupe
4. Utilisez la console d'administration Service d'authentification fédérée pour : (a) Déployer les modèles fournis, (b) Définir des autorités de certification, et (c) Autoriser le Service d'authentification fédérée à utiliser votre autorité de certification
5. Configurer des règles d'utilisateur

Pour obtenir des instructions sur chacune des étapes, consultez la section Service d'authentification fédérée. Notez les différences ou les compléments suivants dans chacune des étapes. Prêtez une attention particulière à la machine cible sur laquelle vous travaillez, par exemple AD, Delivery Controller, StoreFront ou le serveur FAS.

Installer le Service d'authentification fédérée (sur le serveur FAS)

Pour des raisons de sécurité, Citrix recommande d'installer le FAS sur un serveur dédié qui est sécurisé de la même manière qu'un contrôleur de domaine ou une autorité de certification.

Activer le plug-in Service d'authentification fédérée sur un magasin StoreFront (sur StoreFront)

Assurez-vous que la commande suivante utilise le même nom de magasin FAS que celui que vous avez saisi lors de la configuration de StoreFront. Par exemple, FAS est le nom du magasin dans cet exemple :

$StoreVirtualPath = "/Citrix/**FAS**"

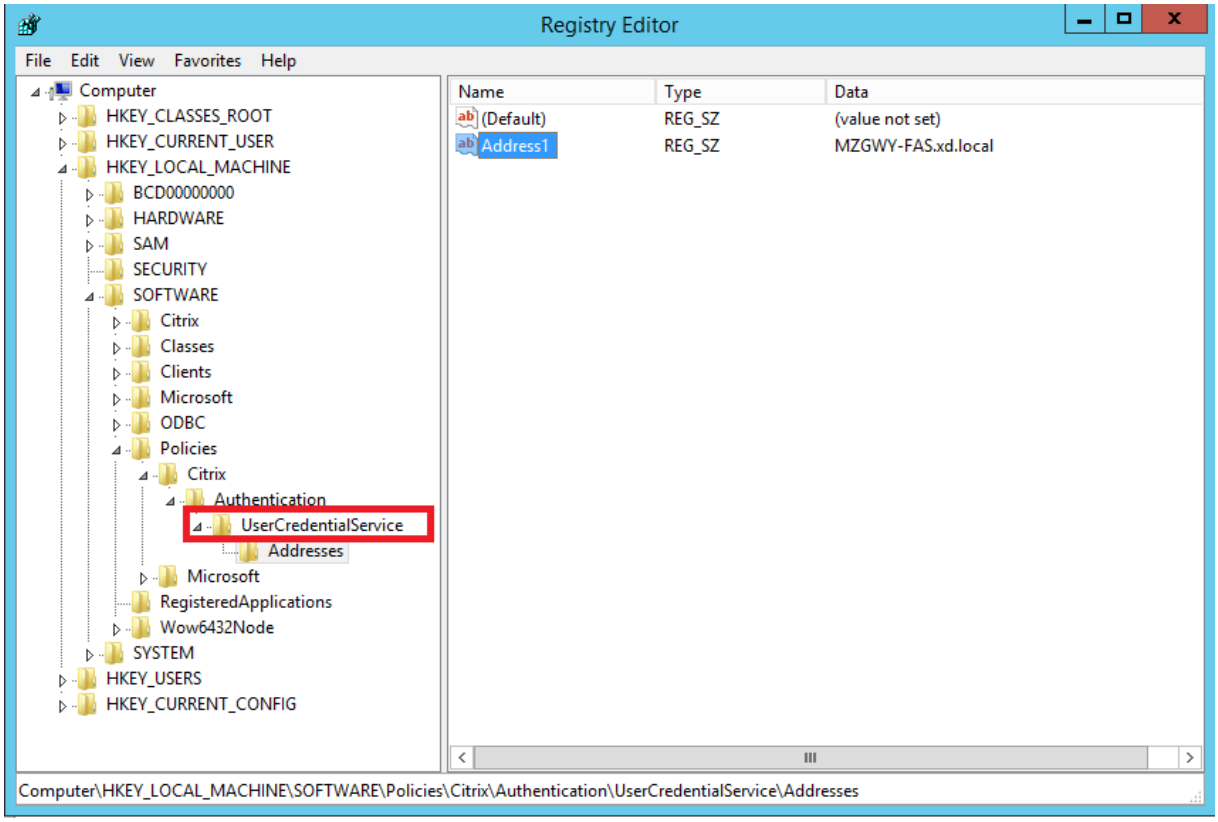
Configurer le Delivery Controller (sur Delivery Controller)

Pour utiliser le Service d'authentification fédérée, configurez le Delivery Controller de manière à approuver les serveurs StoreFront qui peuvent s'y connecter : exécutez l'applet de commande PowerShell **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true**. Vous devrez peut-être parfois lancer **asnp citrix*** en premier.

Configurer la stratégie de groupe (sur le serveur FAS et sur l'AD)

Vous devez être administrateur pour pouvoir effectuer les étapes 1 à 7 dans cette section. L'étape 1 doit être effectuée sur le serveur FAS et les étapes 2 à 7 doivent être effectuées sur l'AD.

Après avoir effectué les étapes 1 à 7, vérifiez que la stratégie FAS a été définie dans l'Éditeur du Registre du serveur FAS.



Activer la prise en charge du certificat dans la session

Le VDA Linux ne prend pas en charge les certificats dans la session.

Utiliser la console d'administration du Service d'authentification fédérée (sur le serveur FAS)

Pas de complément. Consultez l'article Service d'authentification fédérée.

Déployer des modèles de certificat (sur le serveur FAS)

Pas de complément. Consultez l'article Service d'authentification fédérée.

Configurer des services de certificats Active Directory (sur le serveur FAS)

Pas de complément. Consultez l'article Service d'authentification fédérée.

Autoriser le Service d'authentification fédérée (sur le serveur FAS)

Pas de complément. Consultez l'article Service d'authentification fédérée.

Configurer les règles d'utilisateur (sur le serveur FAS)

Pas de complément. Consultez l'article Service d'authentification fédérée.

Pour plus d'informations, consultez également les parties **Agents d'inscription délégués** et **Configuration de la liste de contrôle d'accès** dans la section **Considérations de sécurité** de l'article Service d'authentification fédérée.

Déploiement ADFS du Service d'authentification fédérée

Pour plus d'informations sur le déploiement du fournisseur d'identité ADFS pour le Service d'authentification fédérée, consultez la section Déploiement ADFS du Service d'authentification fédérée.

Configurer le VDA Linux

Définir les serveurs FAS

Dans le cadre d'une nouvelle installation VDA Linux, pour utiliser FAS, tapez le nom de domaine complet de chaque serveur FAS lorsque CTX_XDL_FAS_LIST vous est demandé lors de l'exécution de ctxinstall.sh ou de ctxsetup.sh. Comme le VDA Linux ne prend pas en charge la stratégie de groupe AD, vous pouvez fournir une liste de serveurs FAS séparés par des points-virgules. Si une adresse de serveur est supprimée, remplissez son espace vide avec la chaîne de texte **<none>** et conservez la séquence d'adresses du serveur sans effectuer de modification.

Pour mettre à niveau une installation VDA Linux existante, vous pouvez réexécuter ctxsetup.sh pour définir les serveurs FAS. Vous pouvez également exécuter les commandes suivantes pour définir les serveurs FAS et redémarrer le service ctxvda pour que vos paramètres prennent effet.

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent\Authentication\UserCredentialService" -t "REG_SZ
     " -v "Addresses" -d "<Your-FAS-Server-List>"  - force
2
3 service ctxvda restart
```

Pour mettre à jour les serveurs FAS via ctxreg, exécutez les commandes suivantes :


```
sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
    VirtualDesktopAgent\Authentication\UserCredentialService" -v "
    Addresses" -d "<Your-FAS-Server-List>"

service ctxvda restart
```

Installer un certificat d'autorité de certification racine

Pour la vérification des certificats des utilisateurs, installez le certificat d'autorité de certification racine sur le VDA. Vous pouvez obtenir le certificat racine AD depuis l'étape précédente **Récupérer le certificat CA à partir de l'autorité de certification Microsoft (sur AD)** ou télécharger son format DER à partir du serveur de l'autorité de certification racine `http://CA-SERVER/certsrv`.

Vous pouvez exécuter une commande similaire à la suivante pour convertir un fichier DER (.crt, *.cer, *.der) en PEM.

```
sudo openssl x509 -inform der -in root.cer -out root.pem
```

Installez ensuite le certificat d'autorité de certification racine dans le répertoire openssl en exécutant la commande suivante :

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

> **Remarque :**
>
> ne placez pas le certificat d'autorité de certification racine sous le chemin d'accès **/root**. Sinon, FAS n'a pas l'autorisation de lecture sur le certificat d'autorité de certification racine.

Configurer FAS

Exécutez la commande suivant pour configurer les paramètres du service FAS :

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

Deux variables d'environnement sont ajoutées pour pouvoir exécuter `ctxfascfg.sh` en mode silencieux :

- **CTX_FAS_ADINTEGRATIONWAY=winbind | sssd | centrify** : indique la méthode d'intégration d'Active Directory, qui est `CTX_EASYINSTALL_ADINTEGRATIONWAY` lorsque `CTX_EASYINSTALL_ADINTEGR` est spécifié. Si `CTX_EASYINSTALL_ADINTEGRATIONWAY` n'est pas spécifié, `CTX_FAS_ADINTEGRATIONWAY` utilise son propre paramètre de valeur.

- **CTX_FAS_ROOT_CA_PATH - <root_CA_certificate>** : spécifie le chemin complet du certificat d'autorité de certification racine.

Choisissez la méthode d'intégration Active Directory correcte, puis tapez le chemin correct du certificat d'autorité de certification racine (par exemple, `/etc/pki/CA/certs/root.pem`).

Le script installe ensuite les packages krb5-pkinit et pam_krb5 et définit les fichiers de configuration pertinents.

Limitation

- FAS prend en charge des plateformes et des méthodes d'intégration AD limitées. Reportez-vous à la matrice suivante :

	Winbind	SSSD	Centrify
RHEL 7.5	√	√	√
Ubuntu 16.04 (noyau 4.13)	√	×	√
SLES 12.3	√	×	√

- FAS ne prend pas encore en charge l'écran de verrouillage. Si vous cliquez sur le bouton de verrouillage dans une session, vous ne pouvez plus vous reconnecter à la session en utilisant FAS.
- Cette version ne prend en charge que les déploiements FAS courants décrits dans l'article Vue d'ensemble des architectures du Service d'authentification fédérée, dont **Windows 10 Azure AD Join** est exclu.

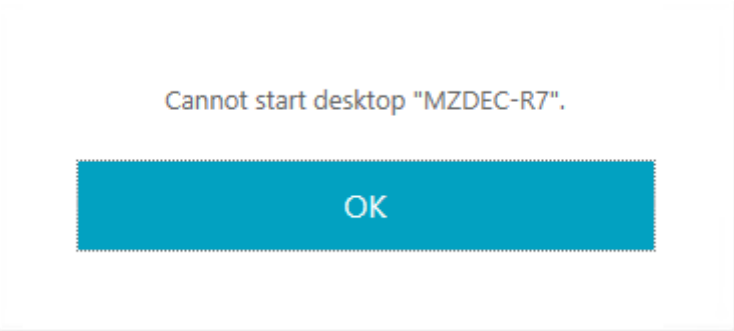
Résolution des problèmes

Avant de résoudre les problèmes dans FAS, assurez-vous que le VDA Linux est installé et configuré correctement afin qu'une session non FAS puisse être lancée dans le magasin commun en utilisant l'authentification par mot de passe.

S'il n'y a aucun problème avec les sessions non FAS, définissez le niveau de journalisation HDX de la classe **Login** sur VERBOSE et le niveau de journalisation VDA sur TRACE. Pour plus d'informations sur l'activation de la consignation de trace pour Linux VDA, consultez l'article du centre de connaissances CTX220130.

Erreur de configuration du serveur FAS

Le lancement d'une session depuis le magasin FAS échoue et la fenêtre suivante s'affiche :



Vérifiez /var/log/xdl/hdx.log et recherchez le journal des erreurs similaire au suivant :

```
2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin: query2fas: failed
    to retrieve data: No such file or directory.

2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin:
    sayhello2fas_internal: Failed to query.

2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin:
    sayhello2fas_convertcredential: exit.

2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin: LoginFasValidate:
    Failed to start FAS.

2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin: receive_data:
    LoginFASValidate - parameters check error.

2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin: receive_data: Exit
     FAILURE

2018-03-27 10:17:56.722 <P10122:S2> citrix-ctxlogin: main: EXITING
    login process..., FAILURE
```

Solution

Exécutez la commande suivante pour vérifier que la valeur de Registre Citrix « HKEY_LOCAL_MACHINE\SOFTWARE\C
» est définie sur <Your-FAS-Server-List>.

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep "UserCredentialService"
```

Si le paramètre existant est incorrect, suivez l'étape précédente Définir les serveurs FAS pour le définir à nouveau.

Configuration du certificat d'autorité de certification racine incorrecte

Le lancement d'une session à partir du magasin FAS échoue. Une fenêtre grise apparaît et disparaît quelques secondes plus tard.

Vérifiez /var/log/xdl/hdx.log et recherchez le journal des erreurs similaire au suivant :

```
2018-03-27 10:15:52.227 <P9099:S3> citrix-ctxlogin: validate_user:
    pam_authenticate err,can retry for user user1@CTXFAS.LAB

2018-03-27 10:15:52.228 <P9099:S3> citrix-ctxlogin: logout_user:
    closing session and pam transaction

2018-03-27 10:15:52.228 <P9099:S3> citrix-ctxlogin: validate_user: Exit
     (user=user1@CTXFAS.LAB)=INVALID_PASSWORD

2018-03-27 10:15:52.228 <P9099:S3> citrix-ctxlogin: LoginBoxValidate:
    failed validation of user 'user1@CTXFAS.LAB', INVALID_PASSWORD

2018-03-27 10:15:52.228 <P9099:S3> citrix-ctxlogin: Audit_login_failure
    : Not yet implemented
```

Solution

Vérifiez que le chemin d'accès complet du certificat d'autorité de certification racine est correctement défini dans /etc/krb5.conf. Le chemin d'accès complet est similaire au suivant :

```
 [realms]

EXAMPLE.COM = {


    ......

    pkinit_anchors = FILE:/etc/pki/CA/certs/root.pem
```



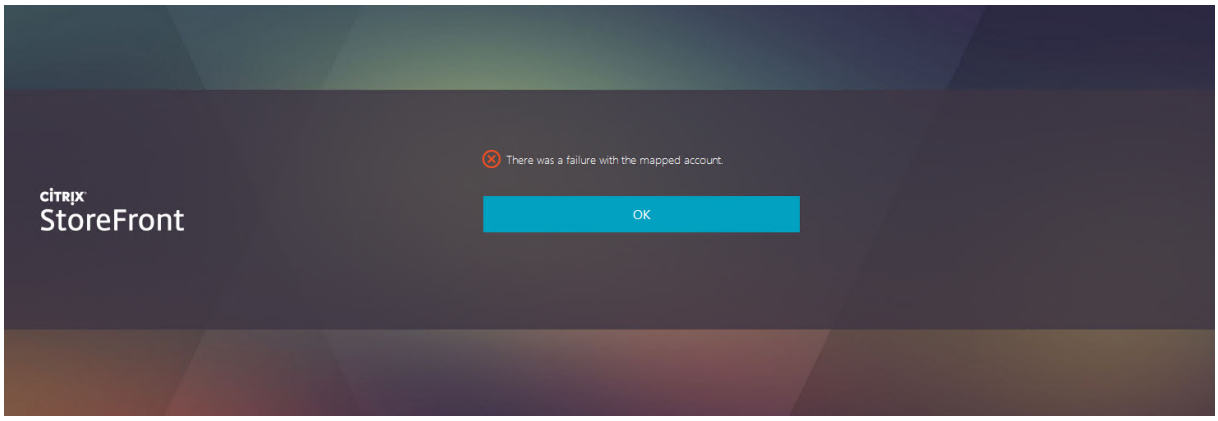
```
9
10      ......
11
12  }
```

Si le paramètre existant est incorrect, suivez l'étape précédente Installer un certificat d'autorité de certification racine pour le définir à nouveau.

Vous pouvez également vérifier si le certificat d'autorité de certification racine est valide.

Erreur de mappage du compte fictif

FAS est configuré par l'authentification SAML. L'erreur suivante peut apparaître après qu'un utilisateur ADFS a tapé le nom d'utilisateur et le mot de passe sur la page de connexion ADFS.



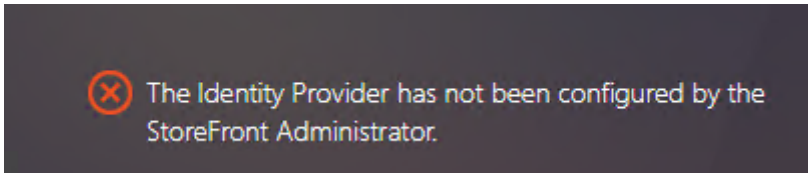
Cette erreur indique que l'utilisateur ADFS a été vérifié, mais qu'aucun utilisateur fictif n'est configuré sur AD.

Solution

Définissez le compte fictif sur AD.

ADFS non configuré

L'erreur suivante apparaît lors de l'ouverture de session sur le magasin FAS :



Cette erreur apparaît car le magasin FAS est configuré pour utiliser l'authentification SAML alors que le déploiement ADFS est manquant.

Solution

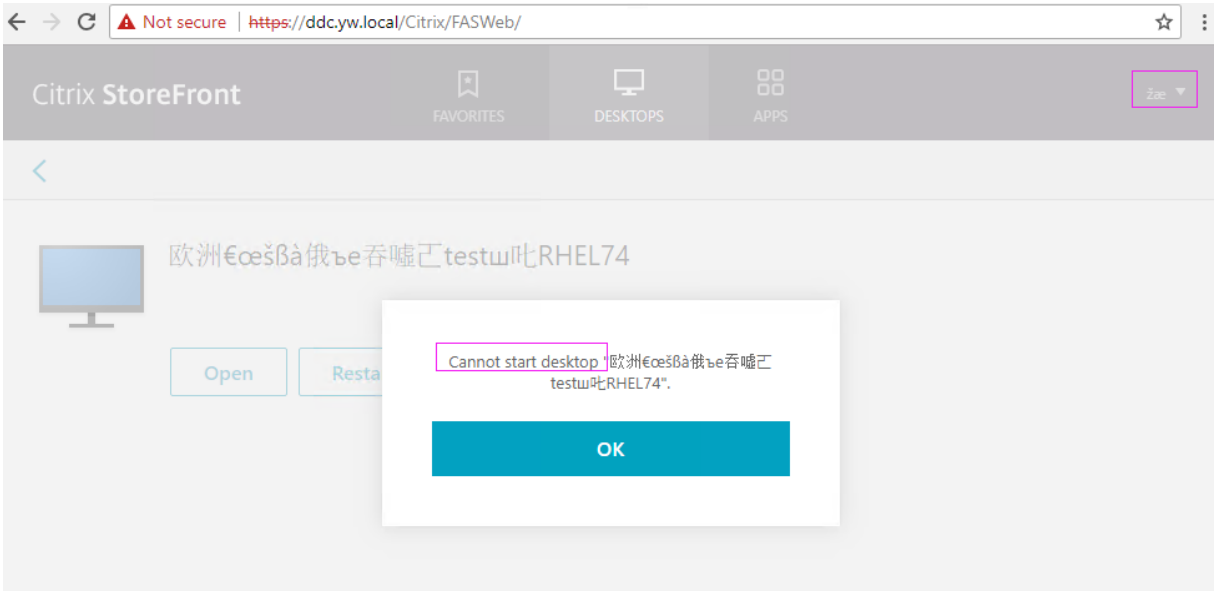
Déployez le fournisseur d'identité ADFS du Service d'authentification fédérée. Pour plus d'informations, consultez la section Déploiement ADFS du Service d'authentification fédérée.

Informations connexes

- Les déploiements FAS courants sont décrits dans l'article Vue d'ensemble des architectures du Service d'authentification fédérée.
- Des informations pratiques sont disponibles dans l'article Configuration et gestion du Service d'authentification fédérée.

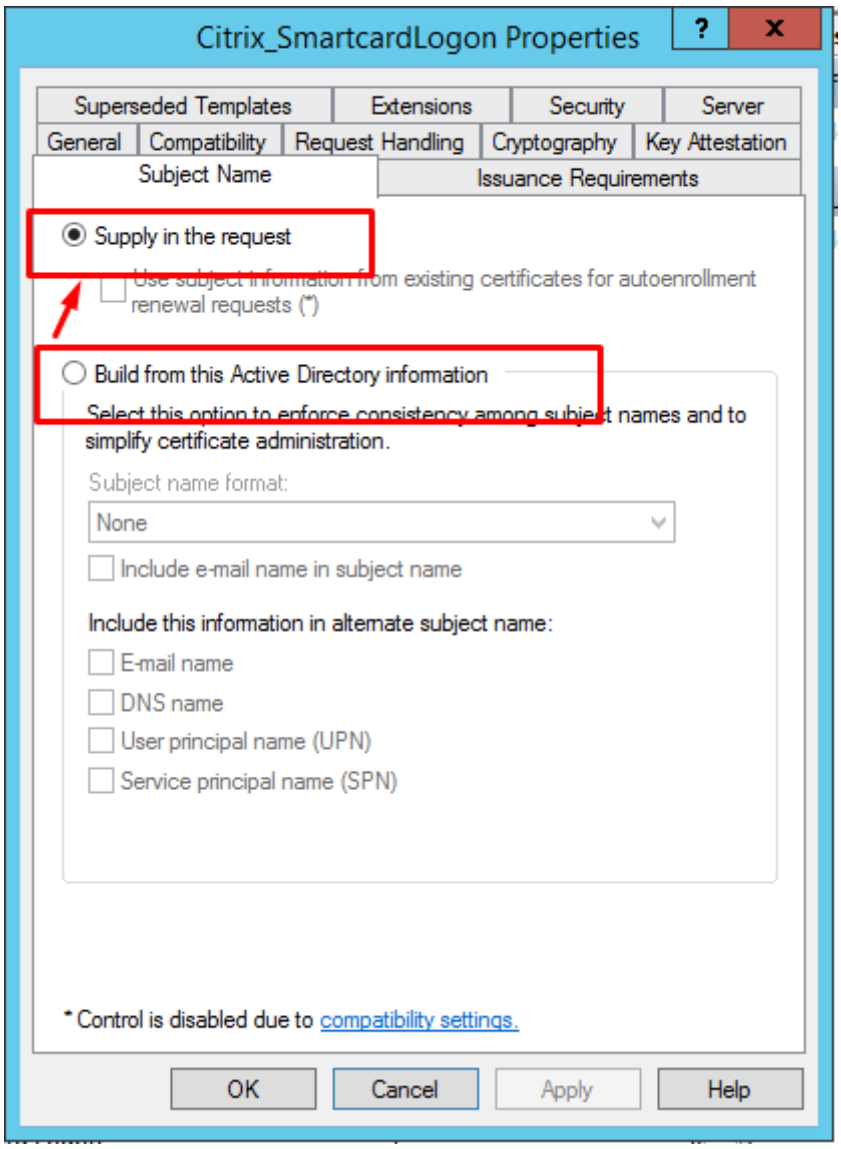
Problème connu

Lorsque FAS est utilisé, la tentative de lancement d'une session de bureau ou d'application publiée avec des caractères non anglais peut échouée.



Solution

Cliquez avec le bouton droit sur **Manage Templates** dans l'outil d'autorité de certification pour modifier le modèle **Citrix_SmartcardLogon** à partir de **Build from this Active Directory information** vers **Supply in the request** comme indiqué ci-dessous :



Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States