

Configuration des postes de travail Horizon 7 for Linux

Dernière modification le 15 septembre 2017
VMware Horizon 7 7.2



vmware®

Vous trouverez la documentation technique la plus récente sur le site Web de VMware, à l'adresse :

<https://docs.vmware.com/fr/>

Si vous avez des commentaires à propos de cette documentation, envoyez-les à l'adresse suivante :

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware France SAS.
Tour Franklin
100-101 Terrasse Boieldieu
92042 Paris La Défense 8 Cedex
France
www.vmware.com/fr

Copyright © 2016, 2017 VMware, Inc. Tous droits réservés. [Informations relatives aux copyrights et marques commerciales.](#)

Table des matières

| | |
|---|-----------|
| Configuration des postes de travail Horizon 7 for Linux | 5 |
| 1 Fonctionnalités et configuration système requise | 6 |
| Fonctionnalités des postes de travail Horizon Linux | 6 |
| Présentation des étapes de configuration des postes de travail Horizon 7 for Linux | 10 |
| Configuration système requise pour Horizon 7 for Linux | 11 |
| Paramètres de machine virtuelle pour les graphiques 2D et vSGA | 17 |
| 2 Préparation d'une machine virtuelle Linux pour un déploiement de postes de travail | 21 |
| Créer une machine virtuelle et installer Linux | 21 |
| Préparer une machine Linux pour un déploiement de postes de travail distants | 22 |
| Installer des modules de dépendance pour Horizon Agent | 24 |
| 3 Configuration de l'intégration Active Directory pour les postes de travail Linux | 27 |
| Intégration de Linux à Active Directory | 27 |
| Configuration de l'authentification unique et de la redirection de carte à puce | 28 |
| 4 Configuration des graphiques pour les postes de travail Linux | 31 |
| Configurer des distributions RHEL prises en charge pour vGPU | 31 |
| Installer le VIB pour la carte graphique NVIDIA GRID vGPU sur l'hôte ESXi | 32 |
| Configurer un périphérique PCI partagé pour vGPU sur la machine virtuelle Linux | 33 |
| Installer le pilote d'affichage NVIDIA GRID vGPU | 35 |
| Vérifier que le pilote d'affichage NVIDIA est installé | 36 |
| Configurer RHEL 6 pour vDGA | 37 |
| Activer DirectPath I/O pour NVIDIA GRID sur un hôte | 38 |
| Ajouter un périphérique de relais vDGA à une machine virtuelle RHEL 6 | 38 |
| Installer le pilote d'affichage NVIDIA pour vDGA | 39 |
| Vérifier que le pilote d'affichage NVIDIA est installé | 41 |
| Configurer RHEL 7 pour vSGA | 42 |
| Installer le VIB pour la carte graphique NVIDIA pour vSGA sur l'hôte ESXi | 42 |
| Configurer des capacités 3D pour vSGA sur la machine virtuelle Linux | 43 |
| Vérifier que vSGA est en cours d'exécution sur une machine virtuelle Linux | 44 |
| 5 Installation d'Horizon Agent | 45 |
| Installer Horizon Agent sur une machine virtuelle Linux | 45 |
| Options de ligne de commande install_viewagent.sh | 46 |
| Configurer le certificat de Linux Agent | 48 |
| Mise à niveau d'Horizon Agent sur une machine virtuelle Linux | 49 |

| | |
|---|------------|
| Mettre à niveau Horizon Agent sur une machine virtuelle Linux | 50 |
| Désinstaller Horizon 7 pour les machines Linux | 51 |
| 6 Options de configuration pour les postes de travail Linux | 52 |
| Définir des options dans des fichiers de configuration sur un poste de travail Linux | 52 |
| Exemples de paramètres Blast pour des postes de travail Linux | 61 |
| Exemples d'options de la redirection du lecteur client pour des postes de travail Linux | 62 |
| Supprimer l'affichage de la console vSphere d'un poste de travail Linux | 63 |
| 7 Créer et gérer des pools de postes de travail Linux | 64 |
| Créer un pool de postes de travail manuel pour Linux | 64 |
| Gérer un pool de postes de travail pour Linux | 65 |
| Créer un pool de postes de travail de clone complet automatisé pour Linux | 67 |
| Commandes PowerCLI Broker | 69 |
| 8 Déploiement en bloc de pools de postes de travail manuels Horizon 7 | 72 |
| Présentation du déploiement en bloc de postes de travail Linux | 72 |
| Présentation de la mise à niveau en bloc de postes de travail Linux | 74 |
| Créer un modèle de machine virtuelle pour cloner des machines de poste de travail Linux | 75 |
| Fichier d'entrée des exemples de scripts PowerCLI pour déployer des postes de travail Linux | 77 |
| Exemple de script pour cloner des machines virtuelles Linux | 78 |
| Exemple de script pour joindre des machines virtuelles clonées à un domaine AD | 82 |
| Exemple de script pour joindre des machines virtuelles clonées à un domaine AD avec SSH | 85 |
| Exemple de script pour télécharger des fichiers de configuration sur des machines virtuelles Linux | 88 |
| Exemple de script pour télécharger des fichiers de configuration sur des machines virtuelles Linux avec SSH | 92 |
| Exemple de script pour mettre à niveau Horizon Agent sur des machines de poste de travail Linux | 96 |
| Exemple de script pour mettre à niveau Horizon Agent sur des machines virtuelles Linux avec SSH | 101 |
| Exemple de script pour effectuer des opérations sur des machines virtuelles Linux | 106 |
| 9 Dépannage des postes de travail Linux | 111 |
| Collecter des informations de diagnostic pour une machine Horizon 7 for Linux | 111 |
| Dépannage du copier/coller entre un poste de travail distant et un hôte client | 112 |
| Configuration du pare-feu Linux pour autoriser les connexions TCP entrantes | 112 |
| View Agent ne se déconnecte pas d'Horizon Client sur iPad Pro | 112 |
| Le poste de travail SLES 12 SP1 ne s'actualise pas automatiquement après un glisser-déplacer | 113 |
| L'authentification unique (SSO) ne peut pas se connecter à un agent de mise hors tension | 113 |
| Machine virtuelle inaccessible après la création d'un pool de postes de travail manuel pour Linux | 114 |

Configuration des postes de travail Horizon 7 for Linux

Le document *Configuration des postes de travail Horizon 7 for Linux* contient des informations sur la configuration d'une machine virtuelle Linux afin de l'utiliser en tant que poste de travail VMware Horizon[®] 7. Il décrit également la préparation du système d'exploitation invité Linux, l'installation d'Horizon Agent sur la machine virtuelle et la configuration de la machine dans View Administrator pour l'utiliser dans un déploiement d'Horizon 7.

Public cible

Ces informations sont conçues pour toute personne souhaitant configurer et utiliser des postes de travail distants exécutés sur des systèmes d'exploitation invités Linux. Les informations sont rédigées pour des administrateurs système Linux expérimentés qui connaissent parfaitement la technologie des machines virtuelles et les opérations de datacenter.

Fonctionnalités et configuration système requise

1

Avec Horizon 6 ou version ultérieure, les utilisateurs peuvent se connecter à des postes de travail distants qui exécutent le système d'exploitation Linux.

Ce chapitre contient les rubriques suivantes :

- [Fonctionnalités des postes de travail Horizon Linux](#)
- [Présentation des étapes de configuration des postes de travail Horizon 7 for Linux](#)
- [Configuration système requise pour Horizon 7 for Linux](#)

Fonctionnalités des postes de travail Horizon Linux

Horizon 7 version 7.2 introduit plusieurs nouvelles fonctionnalités pour les postes de travail Linux.

Les nouvelles fonctionnalités suivantes sont prises en charge pour Horizon 7 version 7.2.

- Redirection de lecteur client (CDR)
- Prise en charge de la redirection USB
- Prise en charge de la sortie audio pour HTML Access
- Prise en charge de l'authentification unique sur RHEL 7 Workstation x64 et CentOS 7 x64
- Prise en charge de K Desktop Environment (KDE) sur CentOS 6 x64 et RHEL 6 x64
- Prise en charge de RHEL 6.9 x64 et CentOS 6.9 x64

La liste suivante présente les principales fonctionnalités des postes de travail Linux Horizon.

| | |
|--|---|
| Pool de postes de travail de clone complet automatisé | À partir d'Horizon 7 version 7.0.2, vous pouvez créer des pools de postes de travail de clone complet automatisés pour des postes de travail Linux. |
| Pool de postes de travail manuel. | Source de machines. <ul style="list-style-type: none">■ Machine virtuelle gérée - Source de la machine virtuelle vCenter. Une machine virtuelle gérée est prise en charge pour les déploiements de mises à niveau et les nouveaux déploiements. |

- Machine virtuelle non gérée - Source de machine d'autres sources. Les machines virtuelles non gérées sont uniquement prises en charge lorsque la mise à niveau concerne un déploiement de machines virtuelles non gérées.

Note Pour garantir les meilleures performances possibles, n'utilisez pas de machine virtuelle non gérée.

Plusieurs moniteurs

- Le poste de travail vDGA/vGPU prend en charge une résolution maximale de 2 560 x 1 600 sur quatre moniteurs.
- Le poste de travail 2D/vSGA sur vSphere 6.0 ou version ultérieure prend en charge une résolution maximale de 2 048 x 1 536 sur quatre moniteurs ou de 2 560 x 1 600 sur trois moniteurs.

Pour Ubuntu 14.04 et 16.04, vous devez désactiver Compiz pour prendre en charge plusieurs moniteurs. Pour plus d'informations, reportez-vous à <http://kb.vmware.com/kb/2114809>.

Pour SLES 12 SP1, vous devez utiliser le package par défaut avec un noyau de niveau kernel-default-3.12.49-11.1. Si vous avez mis le package à niveau, la fonctionnalité multimoniteur échoue et le poste de travail apparaît sur un seul moniteur.

VMware Horizon HTML Access ne prend pas en charge la fonction multimoniteur dans Horizon 7 for Linux.

PNG sans perte

Les images et les vidéos générées sur un poste de travail sont rendues sur le périphérique client en respectant le nombre de pixels.

Codeur logiciel H.264

H.264 peut améliorer les performances de Blast Extreme pour le poste de travail Horizon, en particulier sous des réseaux disposant d'une bande passante faible. Si le client a désactivé H.264, Blast Extreme revient automatiquement à un codage JPEG/PNG.

À partir d'Horizon 7 version 7.0.3, plusieurs moniteurs sont pris en charge.

Graphiques 3D

Les graphiques 3D sont pris en charge avec les combinaisons suivantes de versions Linux et de cartes graphiques :

- vSGA est pris en charge sur RHEL 7 Workstation x64 avec des cartes graphiques NVIDIA GRID K1 ou K2.
- vDGA est pris en charge sur RHEL 6 Workstation x64 avec des cartes graphiques NVIDIA GRID K1 ou K2.
- vGPU est pris en charge sur RHEL 6 Workstation x64 avec des cartes graphiques NVIDIA Maxwell M60.

- vGPU est pris en charge sur RHEL 7 Workstation x64 avec des cartes graphiques NVIDIA Maxwell M60.
- vGPU est pris en charge sur RHEL 6 Workstation x64 avec des cartes graphiques NVIDIA M6.
- vGPU est pris en charge sur RHEL 7 Workstation x64 avec des cartes graphiques NVIDIA M6.

Redirection du Presse-papiers

La fonction de redirection du Presse-papiers vous permet de copier et coller du texte enrichi ou du texte brut entre un hôte client et un poste de travail Linux distant. Vous pouvez définir la direction du copier-coller et la taille maximale du texte à l'aide des options d'Horizon Agent. Cette fonction est activée par défaut. Vous pouvez la désactiver lors de l'installation.

Authentification unique

L'authentification unique est prise en charge sur les versions suivantes de Linux :

- RHEL 6/7 Workstation x64
- CentOS 6/7 x64
- SLED 11 SP3/SP4 x64
- Ubuntu 14.04/16.04 x64

Redirection de carte à puce avec authentification unique (SSO)

La redirection de carte à puce est prise en charge sur RHEL 6 Workstation x64. Les cartes PIV (Personal Identity Verification) et CAC (Common Access Card) sont prises en charge. Le client Mac n'est pas pris en charge.

Entrée audio

La redirection d'entrée audio entre un hôte client et un poste de travail Linux distant est prise en charge. Cette fonctionnalité n'est pas basée sur la fonction de redirection USB. Si vous voulez activer cette fonctionnalité, vous devez la sélectionner lors de l'installation. Vous devez sélectionner le périphérique d'entrée audio par défaut du système « Serveur PulseAudio (local) » dans votre application pour l'entrée audio. La fonctionnalité est prise en charge sous :

- Ubuntu 14.04/16.04 x64
- CentOS 7 x64
- RHEL 7 Workstation x64

Sortie audio

La redirection de la sortie audio est prise en charge. Cette fonction est activée par défaut. Pour la désactiver, vous devez définir l'option `RemoteDisplay.allowAudio` sur **false**. À partir de la version de la version 7.2 d'Horizon 7, VMWare Horizon HTML Access ouvert dans les navigateurs Chrome et Firefox fournit un support de sortie audio pour les postes de travail Linux.

Redirection de lecteur client

La fonctionnalité de redirection de lecteur client (CDR) est disponible à partir d'Horizon 7 version 7.2. L'activation de la fonction CDR vous ouvre l'accès aux dossiers et lecteurs partagés de votre système local. Vous utilisez le dossier `tsc\client` qui se trouve dans votre répertoire de base sur le poste de travail Linux distant. Pour utiliser cette fonctionnalité, vous devez installer les composants CDR.

Redirection USB

La fonctionnalité de redirection USB est disponible à partir d'Horizon 7 version 7.2. Cette fonctionnalité vous permet d'accéder à des périphériques USB connectés localement à partir de postes de travail Linux distants. Vous devez installer les composants de la redirection USB et le module de noyau du pilote VHCI USB pour utiliser la fonctionnalité USB. Vérifiez que vous disposez de privilèges suffisants pour utiliser le périphérique USB que vous voulez rediriger.

Note Le protocole USB 3.0 est pris en charge dans Horizon 7 version 7.2.

Synchronisation de la disposition et des paramètres régionaux du clavier

Cette fonctionnalité spécifie s'il faut synchroniser ou non les paramètres régionaux système et la disposition de clavier actuelle d'un client avec les postes de travail Horizon Linux Agent. Lorsque ce paramètre est activé ou qu'il n'est pas configuré, la synchronisation est autorisée. Lorsque ce paramètre est désactivé, la synchronisation n'est pas autorisée.

Cette fonctionnalité est prise en charge uniquement pour Horizon Client pour Windows et dans les langues suivantes : anglais, français, allemand, japonais, coréen, espagnol, chinois simplifié et chinois traditionnel.

K Desktop Environment

Dans Horizon 7 version 7.2, K Desktop Environment (KDE) est pris en charge sur les distributions Linux suivantes.

- CentOS 6 x64
- RHEL 6 x64

Mode FIPS 140-2

La prise en charge du mode FIPS (Federal Information Processing Standard) 140-2, même si elle n'est pas encore validée avec le Programme de validation des modules cryptographiques (CMVP) NIST, est disponible à partir d'Horizon 7 version 7.2.

L'agent Horizon 7 for Linux implémente les modules cryptographiques qui sont conçus pour garantir la conformité FIPS 140-2. Ces modules ont été validés dans les environnements d'exploitation répertoriés dans le certificat CMVP #2839 et #2866 et ont été portés dans cette plate-forme. Toutefois, l'exigence de test CAVP et CMVP d'inclure les nouveaux environnements d'exploitation dans les certificats CAVP et CMVP NIST de VMware doit toujours être exécutée sur le plan d'évolution du produit.

Note La version 1.2 du protocole TLS (Transport Layer Security) est nécessaire pour la prise en charge du mode FIPS 140-2.

Les postes de travail et les pools de postes de travail Linux ont les limites suivantes :

- L'impression virtuelle, l'impression basée sur l'emplacement et la Vidéo en temps réel ne sont pas prises en charge.

Note Lorsqu'un serveur de sécurité est utilisé, le port 22443 doit être ouvert dans le pare-feu interne pour autoriser le trafic entre le serveur de sécurité et le poste de travail Linux.

Présentation des étapes de configuration des postes de travail Horizon 7 for Linux

Lorsque vous installez et configurez des postes de travail Horizon 7 for Linux, vous devez effectuer des étapes différentes selon que vous installez des graphiques 2D ou 3D sur les machines virtuelles.

Graphiques 2D - Présentation des étapes de configuration

Pour les graphiques 2D, effectuez les étapes suivantes :

- 1 Consultez la configuration système requise pour le déploiement d'Horizon 7 for Linux. Reportez-vous à la section [Configuration système requise pour Horizon 7 for Linux](#).
- 2 Créez une machine virtuelle dans vSphere et installez le système d'exploitation Linux. Reportez-vous à la section [Créer une machine virtuelle et installer Linux](#).
- 3 Préparez le système d'exploitation invité pour le déploiement en tant que poste de travail dans un environnement Horizon 7. Reportez-vous à la section [Préparer une machine Linux pour un déploiement de postes de travail distants](#).
- 4 Configurez le système d'exploitation invité Linux pour qu'il s'authentifie avec Active Directory. Cette étape est implémentée avec un logiciel tiers, en fonction des exigences de votre environnement, et elle n'est pas décrite dans ce guide.
- 5 Installez Horizon Agent sur la machine virtuelle Linux. Reportez-vous à la section [Installer Horizon Agent sur une machine virtuelle Linux](#).
- 6 Créez un pool de postes de travail contenant les machines virtuelles Linux configurées. Reportez-vous à la section [Créer un pool de postes de travail manuel pour Linux](#).

Graphiques 3D - Présentation des étapes de configuration

Vous devez réaliser la configuration NVIDIA GRID vGPU, vDGA ou vSGA sur les machines virtuelles Linux avant d'installer Horizon Agent sur les machines et de déployer un pool de postes de travail dans View Administrator.

- 1 Consultez la configuration système requise pour le déploiement d'Horizon 7 for Linux. Reportez-vous à la section [Configuration système requise pour Horizon 7 for Linux](#).
- 2 Créez une machine virtuelle dans vSphere et installez le système d'exploitation Linux. Reportez-vous à la section [Créer une machine virtuelle et installer Linux](#).
- 3 Préparez le système d'exploitation invité pour le déploiement en tant que poste de travail dans un environnement Horizon 7. Reportez-vous à la section [Préparer une machine Linux pour un déploiement de postes de travail distants](#).
- 4 Configurez le système d'exploitation invité Linux pour qu'il s'authentifie avec Active Directory. Cette étape est implémentée avec un logiciel tiers, en fonction des exigences de votre environnement, et elle n'est pas décrite dans ce guide.
- 5 Configurez des capacités 3D sur vos hôtes ESXi et sur la machine virtuelle Linux. Suivez les procédures pour la fonction 3D que vous voulez installer.
 - Reportez-vous à la section [Configurer des distributions RHEL prises en charge pour vGPU](#).
 - Reportez-vous à la section [Configurer RHEL 6 pour vDGA](#).
 - Reportez-vous à la section [Configurer RHEL 7 pour vSGA](#).
- 6 Installez Horizon Agent sur la machine virtuelle Linux. Reportez-vous à la section [Installer Horizon Agent sur une machine virtuelle Linux](#).
- 7 Créez un pool de postes de travail contenant les machines virtuelles Linux configurées. Reportez-vous à la section [Créer un pool de postes de travail manuel pour Linux](#).

Déploiement en bloc

Avec View Administrator, vous ne pouvez déployer que des machines virtuelles Linux dans un pool de postes de travail manuel. Avec vSphere PowerCLI, vous pouvez développer des scripts qui automatisent le déploiement d'un pool de machines de poste de travail Linux. Reportez-vous à la section [Chapitre 8 Déploiement en bloc de pools de postes de travail manuels Horizon 7](#).

Configuration système requise pour Horizon 7 for Linux

Pour installer Horizon 7 for Linux, votre système Linux doit répondre à certaines exigences pour le système d'exploitation, Horizon 7 et la plate-forme vSphere.

Versions de Linux prises en charge pour Horizon Agent

Le tableau suivant répertorie les systèmes d'exploitation Linux qui sont pris en charge sur les machines virtuelles dans un pool de postes de travail.

Tableau 1-1. Systèmes d'exploitation Linux pris en charge pour View Agent

| Distribution Linux | Architecture |
|--|--------------|
| Ubuntu 14.04 et 16.04 | x64 |
| Note Désactivez Compiz pour éviter les faibles performances. Pour plus d'informations, reportez-vous à http://kb.vmware.com/kb/2114809 . | |
| Ubuntu 12.04 | x64 |
| RHEL 6.6, 6.7, 6.8, 6.9, 7.2 et 7.3 | x64 |
| CentOS 6.6, 6.7, 6.8, 6.9, 7.2 et 7.3 | x64 |
| NeoKylin 6 Update 1 | x64 |
| SLED 11 SP3/SP4, SLED 12 SP1/SP2 | x64 |
| SLES 12 SP1/SP2 | x64 |

Note L'agent Linux dispose de modules de dépendance sur certaines distributions Linux. Pour plus d'informations, reportez-vous à [Installer des modules de dépendance pour Horizon Agent](#).

Plate-forme et versions du logiciel Horizon 7 requises

Pour installer et utiliser Horizon 7 for Linux, votre déploiement doit répondre à certaines exigences pour la plate-forme vSphere, Horizon 7 et le logiciel Horizon Client.

Tableau 1-2. Versions de la plate-forme et du logiciel Horizon 7 requises

| Plate-forme et logiciel | Versions prises en charge |
|-----------------------------------|--|
| Version de la plate-forme vSphere | <ul style="list-style-type: none"> ■ vSphere 6.0 U2 ou version ultérieure ■ vSphere 6.5 ou version ultérieure |
| Environnement Horizon | <ul style="list-style-type: none"> ■ Serveur de connexion Horizon 7.2 |
| Logiciel Horizon Client | <ul style="list-style-type: none"> ■ Horizon Client 4.5.0 pour Android ■ Horizon Client 4.5.0 pour Windows ■ Horizon Client 4.5.0 pour Linux ■ Horizon Client 4.5.0 pour Mac OS X ■ Horizon Client 4.5.0 pour iOS (iPad Pro) ■ HTML Access 4.5.0 sur Chrome, Firefox et Internet Explorer ■ Les clients ultra légers ne sont pas pris en charge |

Ports TCP utilisés par des machines virtuelles Linux

View Agent et Horizon Client utilisent des ports TCP pour l'accès réseau entre eux et divers composants de View Server.

Tableau 1-3. Ports TCP utilisés par des machines virtuelles Linux

| Source | Port | Cible | Port | Protocole | Description |
|---|------|---------------------------|------------|-----------|---|
| Horizon Client | * | Agent Linux | 22443 | TCP | Blast si Blast Security Gateway n'est pas utilisé |
| Serveur de sécurité, Serveur de connexion View ou dispositif Access Point | * | Agent Linux | 22443 | TCP | Blast si Blast Security Gateway est utilisé |
| View Agent | * | Serveur de connexion View | 4001, 4002 | TCP | Trafic JMS SSL. |

Note Pour plus d'informations sur les ports TCP et UDP utilisés par les clients, consultez le point Ports TCP et UDP utilisés par les clients et View Agent dans la section *Sécurité d'Horizon Client et de View Agent* du document View.

Vérifier le compte Linux utilisé par les machines virtuelles Linux

Le tableau suivant répertorie le nom et le type de compte utilisé par les machines virtuelles Linux.

Tableau 1-4. Nom et type de compte

| Nom de compte | Type de compte | Utilisé par |
|-------------------------------|--|--|
| racine | Système d'exploitation Linux intégré | Agent Java autonome, mksvchanserver, scripts shell |
| vmwblast | créé par le programme d'installation de l'agent Linux | VMwareBlastServer |
| <utilisateur connecté actuel> | Système d'exploitation Linux intégré ou utilisateur AD ou utilisateur LDAP | script python |

Environnement de poste de travail

Horizon 7 pour postes de travail Linux prend en charge plusieurs environnements de postes de travail sur les différentes distributions Linux. Le tableau suivant répertorie les environnements de postes de travail par défaut pour chaque distribution Linux prise en charge par Horizon 7 pour postes de travail Linux.

Tableau 1-5. Environnements de postes de travail pris en charge

| Distribution Linux | Poste de travail par défaut Environnement | Environnement de postes de travail pris en charge par Horizon 7 pour postes de travail Linux |
|--------------------|--|--|
| Ubuntu 14.04/16.04 | Unity | Gnome Fallback/Flashback (Metacity) |
| Ubuntu 12.04 | Unity | Unity |
| RHEL/CentOS 6 | Gnome | Gnome, K Desktop Environment (KDE) |
| RHEL/CentOS 7 | Gnome | Gnome |

| Distribution Linux | Poste de travail par défaut Environnement | Environnement de postes de travail pris en charge par Horizon 7 pour postes de travail Linux |
|---------------------|--|--|
| SLED 11 SP4 | Gnome | Gnome |
| SLED 12 SP1/SP2 | Gnome | Gnome |
| SLES 12 SP1/SP2 | Gnome | Gnome |
| NeoKylin 6 Update 1 | Mate | Mate |

Pour installer l'environnement de poste de travail Gnome Fallback/Flashback (Metacity) sur Ubuntu 14.04/16.04, consultez l'article <http://kb.vmware.com/kb/2114809> de la base de connaissances de VMware pour plus d'informations.

Utilisez les informations suivantes pour installer KDE en tant qu'environnement de poste de travail par défaut sur les distributions RHEL/CentOS 6.

Note L'authentification unique (SSO) pour KDE fonctionne uniquement si vous l'installez à l'aide de la procédure décrite ci-dessous.

- 1 Installez le système d'exploitation RHEL/CentOS 6 avec le paramètre d'environnement de poste de travail par défaut, ce qui installera Gnome.
- 2 Installez KDE à l'aide de la commande suivante.

```
sudo yum groupinstall "X Window System" "KDE Desktop"
```

Si vous avez activé l'authentification unique sur une distribution Linux où plusieurs environnements de postes de travail sont installés, utilisez les informations suivantes pour sélectionner l'environnement de poste de travail.

- Pour Ubuntu 14.04/16.04, activez l'option UseGnomeFlashback dans le fichier `/etc/vmware/viewagent-custom.conf` pour forcer l'utilisateur à utiliser Gnome Fallback/Flashback (Metacity).
- Pour RHEL/CentOS 6, les utilisateurs finaux doivent spécifier le nom de l'environnement de poste de travail `kde` ou `gnome` dans le fichier `~/.dmrc` pour déterminer l'environnement utilisé dans leur prochaine session de connexion SSO. Par exemple, pour utiliser KDE comme environnement de poste de travail par défaut, l'utilisateur final doit inclure le paramètre suivant dans son fichier `~/.dmrc`.

```
[Desktop]
Session=kde
```

Après la configuration initiale, l'utilisateur final doit se déconnecter ou redémarrer le système Linux pour faire de KDE, pour l'exemple ci-dessus, le poste de travail par défaut lors de sa prochaine session de connexion.

Si vous avez désactivé l'authentification unique sur la distribution Linux où plusieurs environnements de postes de travail sont installés, l'utilisateur final doit sélectionner l'environnement de poste de travail souhaité lorsqu'il se connecte à la distribution Linux en question.

Pilote VHCI pour la redirection USB

La fonctionnalité de redirection USB est prise en charge à partir d'Horizon 7 version 7.1 pour postes de travail Linux. La fonction a une dépendance sur le pilote de noyau VHCI (Virtual Host Controller Interface) USB. Vous devez appliquer un correctif au pilote VHCI pour qu'il prenne en charge le protocole USB 3.0.

Le programme d'installation de Linux Horizon inclut le binaire de pilote VHCI pour le noyau par défaut des distributions Linux prises en charge. Il installe le pilote VHCI lorsque la fonctionnalité de redirection USB est sélectionnée. Le tableau suivant répertorie les versions de noyau par défaut que le programme d'installation d'Horizon pour postes de travail Linux va installer.

Tableau 1-6. Versions du noyau par défaut

| Distribution Linux | Version de noyau par défaut |
|--------------------|-----------------------------|
| RHEL/CentOS 6.9 | 2.6.32-696.el6.x86_64 |
| SUSE 12 SP2 | 4.4.21-69-default |
| RHEL/CentOS 7.3 | 3.10.0-514.el7.x86_64 |
| Ubuntu 14.04 | 3.13.0-24-generic |
| Ubuntu 16.04 | 4.4.0-21-generic |

Si votre système Linux utilise une version de noyau différente des versions par défaut incluses dans le programme d'installation d'Horizon for Linux, vous devez télécharger le code source du pilote VHCI USB à partir de <https://sourceforge.net/projects/usb-vhci/files/linux%20kernel%20module/>. Vous devez ensuite compiler le code source du pilote VHCI et installer le binaire ainsi obtenu sur votre système Linux.

Note L'installation du pilote VHCI doit être effectuée avant l'installation d'Horizon for Linux.

Après avoir téléchargé la dernière version du code source du pilote VHCI USB, utilisez les commandes suivantes pour le compiler et l'installer sur votre système Linux. Par exemple, si vous décompressez le fichier d'installation, VMware-horizonagent-linux-x86_64-*<version>*-*<build-number>*.tar.gz, sous le répertoire /install_tmp/, le chemin *full-path-to-patch-file* est /install_tmp/VMware-horizonagent-linux-x86_64-*<version>*-*<buildnumber>*/resources/vhci/patch/vhci.patch et la commande patch à utiliser est

```
# patch -p1 < /install_tmp/VMware-horizonagent-linux-x86_64-<version>-<build-number>/resources/vhci/patch/vhci.patch
```

Tableau 1-7. Compilez et installez le pilote VHCI USB

| Distribution Linux | Procédure de compilation et d'installation du pilote VHCI USB |
|--|---|
| Ubuntu 14.04 Ubuntu 16.04 | <p>Compilez et installez les pilotes VHCI.</p> <pre># tar -xzvf vhci-hcd-1.15.tar.gz # cd vhci-hcd-1.15 # patch -p1 < full-path_to_patch-file # make clean && make && make install</pre> |
| RHEL/ CentOS 6.9 RHEL/ CentOS 7.3 | <ol style="list-style-type: none"> 1 Installez les modules de dépendance. <pre># yum install gcc-c++ # yum install kernel-devel-\$(uname -r) # yum install kernel-headers-\$(uname -r) # yum install patch</pre> 2 Compilez et installez les pilotes VHCI. <pre># tar -xzvf vhci-hcd-1.15.tar.gz # cd vhci-hcd-1.15 # patch -p1 < full-path_to_patch-file # make clean && make && make install</pre> |
| SUSE 11 SP4 SUSE 12 SP2 | <ol style="list-style-type: none"> 1 Déterminez la version du module de noyau actuel <pre># rpm -qa grep kernel-default-\$(echo \$(uname -r) cut -d '-' -f 1,2)</pre> <p>Le résultat est le nom du module de noyau actuellement installé. Si, par exemple, le nom du module est kernel-default-3.0.101-63.1, la version actuelle du module de noyau est 3.0.101-63.1.</p> 2 Installez les modules de dépendance. <ol style="list-style-type: none"> a Pour SUSE 11, installez les modules de kernel-source et kernel-default-devel qui correspondent au noyau actuel, ainsi que les modules gcc et patch. <pre>#zypper install --oldpackage kernel-source-<kernel-package-version> \ kernel-default-devel-<kernel-package-version> gcc patch</pre> <p>Par exemple :</p> <pre>#zypper install --oldpackage kernel-source-3.0.101-63.1 kernel-default-devel-3.0.101-63.1 gcc patch</pre> b Pour SUSE 12, installez les modules kernel-devel, kernel-default-devel, kernel-macros et patch. <pre>#zypper install --oldpackage kernel-devel-<kernel-package-version> \ kernel-default-devel-<kernel-package-version> kernel-macros-<kernel-package-version> patch</pre> <p>Par exemple :</p> <pre>#zypper install --oldpackage kernel-devel-4.4.21-90.1 kernel-default-devel-4.4.21-90.1 kernel-macros-4.4.21-90.1 patch</pre> 3 Compilez et installez les pilotes VHCI. <pre># tar -xzvf vhci-hcd-1.15.tar.gz # cd vhci-hcd-1.15 # patch -p1 < full-path_to_patch-file # mkdir -p linux/\$(echo \$(uname -r) cut -d '-' -f 1)/drivers/usb/core # cp /lib/modules/\$(uname -r)/source/include/linux/usb/hcd.h linux/\$(echo \$(uname -</pre> |

Si la version du noyau Linux est modifiée, vous devez recompiler et réinstaller le pilote VHCI, mais vous n'avez pas à réinstaller Horizon for Linux.

Paramètres de machine virtuelle pour les graphiques 2D et vSGA

Lorsque vous créez certaines machines virtuelles Horizon 7 for Linux, vous devez modifier les paramètres de mémoire et de configuration sur les valeurs minimales recommandées.

Les machines virtuelles configurées pour utiliser NVIDIA vDGA utilisent la carte graphique physique NVIDIA. Les machines virtuelles configurées pour utiliser NVIDIA GRID vGPU utilisent la carte graphique virtuelle NVIDIA, qui est basée sur l'accélérateur graphique physique NVIDIA. Vous n'avez pas besoin de modifier les paramètres de mémoire vidéo (vRAM) et de configuration pour ces machines virtuelles.

Les machines virtuelles configurées pour utiliser des graphiques 2D ou vSGA utilisent la carte graphique virtuelle VMware et vous devez modifier les paramètres suivants pour ces types de machines virtuelles :

- Paramètres de mémoire vidéo (vRAM)
- Paramètres de configuration
- Paramètres de mémoire 3D
- Paramètres de mémoire vCPU et virtuelle pour répondre aux performances

Paramètres de mémoire vidéo (vRAM)

Lorsque vous créez une machine virtuelle Linux dans vSphere Client, configurez la taille vRAM comme indiqué dans la section [Tableau 1-8. Paramètres vRAM recommandés pour les graphiques 2D ou vSGA](#). Définissez la taille vRAM qui est recommandée pour le nombre et la résolution des écrans que vous configurez pour la machine virtuelle.

Tableau 1-8. Paramètres vRAM recommandés pour les graphiques 2D ou vSGA

| Taille vRAM | Nombre d'écrans | Résolution maximale |
|-------------|-----------------|----------------------------|
| 10 Mo | 1 | 1 600x1 200 ou 1 680x1 050 |
| 12 Mo | 1 | 1920x1440 |
| 32 Mo | 1 | 2 560x1 600 |
| 48 Mo | 2 | 2048x1536 |
| 80 Mo | 2 | 2 560x1 600 |
| 128 Mo | 3 | 2 560x1 600 |
| 128 Mo | 4 | 2048x1536 |

Ces tailles vRAM sont les recommandations minimales. Si davantage de ressources sont disponibles sur la machine virtuelle, définissez la vRAM sur des valeurs supérieures pour de meilleures performances vidéo.

La taille vRAM minimale recommandée est 10 Mo pour une machine configurée avec un seul écran à la résolution la plus faible.

Vous devez mettre la machine virtuelle hors tension pour définir le nombre d'écrans et la quantité de mémoire vidéo à utiliser, comme décrit dans [Créer une machine virtuelle et installer Linux](#).

Le Serveur de connexion Horizon 7 ne configure pas automatiquement les paramètres de vRAM sur les machines virtuelles Linux comme il le fait sur les machines virtuelles Windows. Vous devez configurer manuellement les paramètres de vRAM dans vSphere Client.

Si une machine virtuelle Linux est configurée avec une taille vRAM inférieure à la taille recommandée, les problèmes suivants peuvent se produire :

- Des sessions de poste de travail peuvent être déconnectées juste après l'établissement de la connexion initiale.
- L'ajustement automatique peut ne pas fonctionner. Le poste de travail est alors affiché dans une petite partie de l'écran.

Si la valeur **Nombre d'écrans** d'une machine virtuelle Linux est inférieure au nombre requis réel, un ou plusieurs moniteurs n'affichent rien pour le poste de travail.

Si vous rencontrez un problème d'ajustement automatique avec les paramètres recommandés, vous pouvez spécifier une taille vRAM plus grande. vSphere Client autorise une taille vRAM maximale de 128 Mo. Si votre taille spécifiée dépasse 128 Mo, vous devez modifier le fichier de configuration vmx manuellement. L'exemple suivant spécifie une taille vRAM de 256 Mo :

```
svga.vramSize = "268435456"
```

Paramètres de configuration

Pour afficher le poste de travail distant Linux sur plusieurs moniteurs, vous devez définir certains paramètres de configuration pour la machine virtuelle. Les étapes générales pour définir un paramètre de configuration pour une machine virtuelle sont les suivantes :

- 1 Mettez la machine virtuelle hors tension
- 2 Dans vSphere Web Client, cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
- 3 Cliquez sur l'onglet **Options VM**, puis sur **Avancé**.
- 4 Cliquez sur **Modifier la configuration**, puis sur **Ajouter une ligne**.
- 5 Entrez le nom et la valeur du paramètre de configuration.
- 6 Cliquez sur **OK** pour enregistrer les modifications.

Vous devez définir les paramètres de configuration suivants :

- Définissez `svga.autodetect` sur faux.

```
svga.autodetect="false"
```

- Calculez les valeurs `svga.maxWidth` et `svga.maxHeight` en fonction du nombre et de l'orientation (horizontale ou verticale) des moniteurs. La règle générale est que les valeurs `svga.maxWidth` et `svga.maxHeight` doivent être suffisamment grandes pour prendre en charge tous les écrans. Par exemple, pour prendre en charge quatre écrans avec une résolution maximale de 2 560 x 1 600, vous devez définir les valeurs suivantes :

```
svga.maxHeight="3200"
svga.maxWidth="10240"
```

Si vous disposez de plusieurs moniteurs, vous devez définir ces paramètres de configuration. Sinon, vous pouvez rencontrer un ou plusieurs des problèmes suivants :

- Le poste de travail est affiché sur certains des moniteurs et les autres moniteurs n'affichent rien.
- Une séquence de touches s'affiche plusieurs fois.
- Le poste de travail devient lent.
- Le poste de travail est affiché dans une petite partie de l'écran.

Limite de la taille d'écran des moniteurs 4 096 x 4 096

Pour RHEL 6.8/6.9/7.3, CentOS 6.8/6.9/7.3, Ubuntu 16.04, SLED 12 SP2 et SLES 12 SP2, la taille d'écran maximale pour 2D et vSGA est de 4 096 x 4 096. Lorsque vous exécutez la commande `xrandr`, la première ligne de la sortie indique `maximum 4 096 x 4 096`.

Pour Ubuntu 14.04, la limite est également introduite si vous installez les derniers correctifs à partir des référentiels Ubuntu officiels.

La connexion de plusieurs moniteurs peut nécessiter une taille d'écran supérieure à 4 096 x 4 096. Pour contourner cette limite, utilisez l'une des solutions suivantes :

- Si vous devez utiliser la version de matériel 11 (HWv11) de VMware ou une version ultérieure pour votre machine virtuelle, ajoutez la ligne suivante dans le fichier de configuration VMX de la machine virtuelle :

```
mks.enable3d = TRUE
```

Avec cette solution, le système d'exploitation Linux peut signaler les capacités 3D à des applications logicielles, telles que Chrome. Toutefois, cela peut affecter les performances du système Linux.

- Si votre machine virtuelle peut utiliser la version de matériel 10 de VMware, utilisez la ligne suivante dans le fichier VMX de votre machine virtuelle :

```
virtualHW.version = "10"
```

Cette solution ne s'applique pas à RHEL 6.8 et CentOS 6.8.

Pour que cette solution fonctionne sur les systèmes Ubuntu 16.04, vous devez installer les derniers correctifs à partir des référentiels Ubuntu officiels.

Paramètres de vCPU et de mémoire

Pour améliorer les performances d'un poste de travail 2D ou vSGA, définissez davantage de vCPU et de mémoire virtuelle pour la machine virtuelle Linux. Par exemple, définissez 2 vCPU et 2 Go de mémoire virtuelle.

Pour le grand écran de plusieurs moniteurs, comme quatre moniteurs, définissez 4 vCPU et 4 Go de mémoire virtuelle pour la machine virtuelle.

Pour la lecture de vidéos dans un poste de travail 2D ou vSGA, définissez 4 vCPU et 4 Go de mémoire virtuelle pour la machine virtuelle.

Paramètres de mémoire 3D

Pour améliorer les performances dans un environnement à plusieurs moniteurs vSGA, définissez le paramètre **Mémoire 3D** pour la machine virtuelle sur 1 Go ou plus.

Préparation d'une machine virtuelle Linux pour un déploiement de postes de travail

2

La configuration d'un poste de travail Linux implique de créer une machine virtuelle Linux et de préparer le système d'exploitation pour le déploiement de postes de travail distants.

Ce chapitre contient les rubriques suivantes :

- [Créer une machine virtuelle et installer Linux](#)
- [Préparer une machine Linux pour un déploiement de postes de travail distants](#)
- [Installer des modules de dépendance pour Horizon Agent](#)

Créer une machine virtuelle et installer Linux

Vous créez une machine virtuelle dans vCenter Server pour chaque poste de travail distant déployé dans Horizon 7. Vous devez installer votre distribution Linux sur la machine virtuelle.

Conditions préalables

- Vérifiez que votre déploiement répond aux exigences pour prendre en charge les postes de travail Linux. Reportez-vous à la section [Configuration système requise pour Horizon 7 for Linux](#).
- Familiarisez-vous avec les étapes de création de machines virtuelles dans vCenter Server et d'installation de systèmes d'exploitation invités. Reportez-vous à la section « Création et préparation de machines virtuelles » dans le document *Configuration des postes de travail virtuels dans Horizon 7*.
- Familiarisez-vous avec les valeurs de mémoire vidéo recommandée (vRAM) pour les écrans que vous utiliserez avec la machine virtuelle. Reportez-vous à la section [Configuration système requise pour Horizon 7 for Linux](#).

Procédure

- 1 Dans vSphere Web Client ou vSphere Client, créez une machine virtuelle.

2 Configurez des options de configuration personnalisées.

- a Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur **Modifier les paramètres**.
- b Spécifiez le nombre de vCPU et la taille de la mémoire virtuelle.

Pour les valeurs recommandées, suivez les instructions dans le guide d'installation de votre distribution Linux.

Par exemple, Ubuntu 12.04 recommande de configurer 2 048 Mo de mémoire virtuelle et 2 vCPU.

- c Sélectionnez **Carte vidéo** et spécifiez le nombre d'écrans et la mémoire vidéo (vRAM) totale.

Réglez la taille vRAM dans vSphere Web Client pour les machines virtuelles utilisant 2D ou vSGA, qui utilisent le pilote VMware. La taille vRAM n'a aucun effet sur les machines vDGA ou NVIDIA GRID vGPU, qui utilisent des pilotes NVIDIA.

Pour les valeurs recommandées, suivez les instructions dans *Configuration système requise pour Horizon 7 for Linux*. N'utilisez pas le Calculateur de mémoire vidéo.

3 Mettez la machine virtuelle sous tension et installez la distribution Linux.

4 Configurez l'environnement de poste de travail à utiliser pour la distribution Linux spécifique.

Reportez-vous à la section Environnement de poste de travail de la rubrique [Configuration système requise pour Horizon 7 for Linux](#) pour plus d'informations.

5 Vérifiez que le nom d'hôte du système est résoluble sur 127.0.0.1.

Préparer une machine Linux pour un déploiement de postes de travail distants

Vous devez exécuter certaines tâches pour préparer une machine Linux afin de l'utiliser en tant que poste de travail dans un déploiement d'Horizon 7.

Avant qu'une machine Linux puisse être gérée par Horizon 7, elle doit pouvoir communiquer avec le Serveur de connexion. Vous devez configurer la mise en réseau sur la machine Linux pour qu'elle puisse effectuer un test ping sur l'instance du Serveur de connexion avec son nom de domaine complet.

Open VMware Tools (OVT) est préinstallé sur les machines RHEL 7, CentOS 7, SLED 12 et SLES 12. Si vous préparez une de ces machines pour l'utiliser en tant que poste de travail distant, vous pouvez ignorer les étapes 1 à 5 dans la procédure suivante, qui décrivent comment installer VMware Tools en exécutant manuellement le programme d'installation.

Si vous utilisez une machine Ubuntu 16.04, installez-y OVT. Si vous préparez cette machine pour l'utiliser comme un poste de travail distant, vous pouvez ignorer les étapes 1 à 5 dans la procédure suivante et installer manuellement OVT sur votre machine Ubuntu 16.04 à l'aide de la commande suivante :

```
apt-get install open-vm-tools-desktop
```

Conditions préalables

- Vérifiez qu'une nouvelle machine virtuelle (VM) a été créée dans vCenter Server et que votre distribution Linux a été installée sur la machine.
- Familiarisez-vous avec les étapes de montage et d'installation de VMware Tools sur une VM Linux. Reportez-vous à la section « Installer ou mettre à niveau manuellement VMware Tools dans une machine virtuelle Linux » dans le document *Administration d'une machine virtuelle vSphere*.
- Familiarisez-vous avec les étapes de configuration de votre machine Linux pour qu'elle soit résoluble via DNS. Ces étapes varient pour les différentes distributions et versions de Linux. Pour plus d'instructions, consultez la documentation de votre distribution et de votre version de Linux.

Procédure

- 1 Dans vSphere Web Client ou vSphere Client, montez le disque virtuel de VMware Tools sur la VM.
- 2 Cliquez avec le bouton droit sur le fichier du programme d'installation de VMware Tools, `VMwareTools.x.x.x-xxxx.tar.gz`, cliquez sur **Extraire vers** et sélectionnez le poste de travail pour votre distribution Linux.

Le dossier `vmware-tools-distrib` est extrait vers le poste de travail.

- 3 Sur la VM, connectez-vous en tant qu'utilisateur racine et ouvrez une fenêtre de terminal.
- 4 Décompressez le fichier du programme d'installation tar de VMware Tools.

Par exemple :

```
tar xzpf /mnt/cdrom/VMwareTools-x.x.x-yyyy.tar.gz
```

- 5 Exécutez le programme d'installation et configurez VMware Tools.

La commande peut varier légèrement dans les différentes distributions Linux. Par exemple :

```
cd vmware-tools-distrib
sudo ./vmware-install.pl -d
```

Généralement, le fichier de configuration `vmware-config-tools.pl` s'exécute à la fin de l'exécution du fichier du programme d'installation.

- 6 Mappez le nom d'hôte de la machine Linux sur 127.0.0.1 dans le fichier `/etc/hosts`.

Pour RHEL, CentOS, SLES et SLED, vous devez mapper manuellement le nom d'hôte sur 127.0.0.1, car il n'est pas mappé automatiquement. Pour Ubuntu, cette étape n'est pas nécessaire, car le mappage existe par défaut. Cette étape n'est pas nécessaire non plus lorsque vous déployez en bloc des postes de travail, car le processus de clonage ajoute ce mappage.

Note Si vous modifiez le nom d'hôte de la machine Linux après l'installation d'Horizon Agent, vous devez mapper le nouveau nom d'hôte sur 127.0.0.1 dans le fichier `/etc/hosts`. Sinon, l'ancien nom d'hôte sera toujours utilisé.

- 7 Pour RHEL 7 et CentOS 7, vérifiez que `virbr0` est désactivé.

```
virsh net-destroy default
virsh net-undefine default
service libvirtd restart
```

- 8 Assurez-vous que les instances du Serveur de connexion View dans le groupe peuvent être résolues via DNS.

- 9 Configurez la machine Linux pour que le niveau d'exécution par défaut soit 5.

Le niveau d'exécution doit être 5 pour que le poste de travail Linux fonctionne.

- 10 Sur une machine Ubuntu qui a été configurée pour s'authentifier avec un serveur OpenLDAP, définissez le nom de domaine complet sur la machine.

Cette étape vérifie que les informations peuvent s'afficher correctement dans le champ Utilisateur sur la page Sessions dans View Administrator. Modifiez le fichier `/etc/hosts` comme suit :

- a # nano `/etc/hosts`
- b Ajoutez le nom de domaine complet. Par exemple : `127.0.0.1 hostname.domainname hostname`
- c Quittez et enregistrez le fichier.

- 11 Pour SUSE, désactivez Modifier le nom d'hôte via DHCP. Définissez le nom d'hôte ou le nom de domaine.

- a Dans Yast, cliquez sur **Paramètres réseau**.
- b Cliquez sur l'onglet **Nom d'hôte/DNS**.
- c Décochez **Modifier le nom d'hôte via DHCP**.
- d Entrez le nom d'hôte et le nom de domaine.
- e Cliquez sur **OK**.

Après l'installation de VMware Tools, si vous mettez à niveau le noyau Linux, VMware Tools peut s'arrêter. Pour résoudre le problème, reportez-vous à <http://kb.vmware.com/kb/2050592>.

Installer des modules de dépendance pour Horizon Agent

Horizon Agent for Linux dispose de modules de dépendance uniques pour une distribution Linux. Vous devez installer ces modules avant d'installer Horizon Agent for Linux.

Conditions préalables

Vérifiez qu'une nouvelle machine virtuelle est créée dans vCenter Server et que votre distribution Linux est installée sur la machine.

Procédure

- 1 Installez les modules obligatoires qui ne sont pas installés ou mis à niveau par défaut. Le programme d'installation interrompt l'installation si un module ne répond pas à la configuration requise.

Tableau 2-1. Modules de dépendance obligatoires

| Distribution Linux | Modules |
|--|---|
| SLED 11 SP3/SP4 Mettez à niveau xorg-x11-server vers une version ultérieure à 7.4.27.111.1 | <pre>zypper install xorg-x11-server</pre> |
| SLES 12 SP1/SLED 12 SP1 Mettez à niveau xf86-video-vmware vers une version ultérieure à 13.0.2-3.2 à partir du référentiel SUSE | <ol style="list-style-type: none"> 1 Enregistrez SUSE 12 pour activer les référentiels SUSE. <pre>SUSEConnect -r Code d'enregistrement -e E-mail</pre> 2 Mettez à jour la version xf86-video-vmware. <pre>zypper install xf86-video-vmware</pre> |
| SLES 12 | <p>L'installation de python-gobject2 est requise pour les postes de travail Linux SLES 12 lorsque vous installez Horizon Agent.</p> <ol style="list-style-type: none"> 1 Enregistrez SUSE 12 pour activer les référentiels SUSE. <pre>SUSEConnect -r Code d'enregistrement -e E-mail</pre> 2 Installez python-gobject2. <pre>zypper install python-gobject2</pre> |
| Ubuntu 14.04 Mettez à niveau indicator-session vers 12.10.5+15.04.20150327, disponible dans https://launchpad.net/ubuntu/wily/amd64/indicator-session/12.10.5+15.04.20150327-0ubuntu1 | <pre>wget http://launchpadlibrarian.net/201393830/indicator-session_12.10.5+15.04.20150327-0ubuntu1_amd64.deb</pre> <pre>sudo dpkg -i ./indicator-session_12.10.5+15.04.20150327-0ubuntu1_amd64.deb</pre> |
| Ubuntu 16.04 | <pre>apt-get install python-dbus python-gobject</pre> |

- 2 Installez le module facultatif pour Horizon Agent.

- Par défaut, glibc-2.12-1.166.el6.x86_64 est installé sur RHEL ou CentOS 6.7, ce qui peut entraîner un problème de blocage. Par conséquent, la connexion du poste de travail est bloquée. Pour résoudre ce problème, vous devez mettre à niveau glibc vers la dernière version depuis un référentiel en ligne.

```
sudo yum install glibc
```

- Sur les postes de travail Ubuntu 14.04 avec plusieurs moniteurs, gnome-session-fallback est nécessaire pour désactiver Compiz pour de meilleures performances.

```
sudo apt-get install gnome-session-fallback
```

- Sur les postes de travail Ubuntu 16.04 avec plusieurs moniteurs, gnome-session-flashback est nécessaire pour désactiver Compiz pour de meilleures performances.

```
sudo apt-get install gnome-session-flashback
```

Configuration de l'intégration Active Directory pour les postes de travail Linux

3

View utilise l'infrastructure Microsoft Active Directory (AD) existante pour l'authentification et la gestion des utilisateurs. Vous pouvez intégrer les postes de travail Linux avec Active Directory pour que les utilisateurs puissent se connecter à un poste de travail Linux avec leur compte d'utilisateur Active Directory.

Ce chapitre contient les rubriques suivantes :

- [Intégration de Linux à Active Directory](#)
- [Configuration de l'authentification unique et de la redirection de carte à puce](#)

Intégration de Linux à Active Directory

Il existe plusieurs solutions pour intégrer Linux à Active Directory (AD) et Horizon 7 pour postes de travail Linux n'a pas de dépendance vis-à-vis d'une solution particulière.

Les solutions suivantes fonctionnent dans un environnement Horizon 7 pour postes de travail Linux :

- Authentification directe via le serveur OpenLDAP
- Authentification LDAP SSSD (System Security Services Daemon) via Microsoft Active Directory
- Jonction de domaine Winbind

Globalement, la solution d'authentification directe OpenLDAP implique les étapes suivantes :

- 1 Installer les services de certificats sur Active Directory pour activer le protocole LDAPS (Lightweight Directory Access Protocol over SSL).
- 2 Configurer un serveur OpenLDAP.
- 3 Synchroniser les informations utilisateur (sauf le mot de passe) à partir d'Active Directory vers le serveur OpenLDAP.
- 4 Configurer le serveur OpenLDAP pour déléguer la vérification des mots de passe à un processus distinct, tel que `saslauthd`, qui peut effectuer la vérification des mots de passe avec Active Directory.
- 5 Configurer les postes de travail Linux de manière à utiliser un client LDAP pour authentifier les utilisateurs avec le serveur OpenLDAP.

L'authentification LDAP SSSD reposant sur la solution Microsoft Active Directory implique les étapes suivantes :

- 1 Installer les services de certificats sur Active Directory pour activer le protocole LDAPS.
- 2 Configurer le protocole SSSD sur le poste de travail Linux pour utiliser directement l'authentification LDAP via Microsoft Active Directory.

La solution de jonction de domaine Winbind implique les étapes suivantes :

- 1 Installer les modules Winbind, Samba et Kerberos sur le poste de travail Linux.
- 2 Joindre le poste de travail Linux à Microsoft Active Directory.

Si vous utilisez les solutions basées sur LDAP, vous devez effectuer la configuration sur une machine virtuelle modèle et aucune action supplémentaire n'est requise sur les machines virtuelles clonées.

Si vous utilisez la solution de jonction de domaine Winbind ou une autre solution basée sur l'authentification Kerberos, vous devez joindre la machine virtuelle modèle à Active Directory, puis joindre la machine virtuelle clonée à Active Directory. Par exemple, utilisez la commande suivante :

```
sudo /usr/bin/net ads join -U <domain user>%<domain password>
```

Utilisez les options suivantes pour exécuter la commande de jonction de domaine sur la machine virtuelle clonée pour la solution Winbind :

- Connectez chaque machine virtuelle à distance à l'aide de SSH ou vSphere PowerCLI et exécutez la commande. Pour plus d'informations sur les scripts, reportez-vous à la section [Chapitre 8 Déploiement en bloc de pools de postes de travail manuels Horizon 7](#).
- Incluez la commande à un script shell et spécifiez le chemin du script vers l'option RunOnceScript d'Horizon Agent dans le fichier `/etc/vmware/viewagent-custom.conf`. Pour plus d'informations, reportez-vous à la section [Définir des options dans des fichiers de configuration sur un poste de travail Linux](#).

Note Pour faciliter le déploiement, utilisez l'authentification LDAP SSSD via la solution Microsoft Active Directory.

Configuration de l'authentification unique et de la redirection de carte à puce

Pour configurer l'authentification unique (SSO) et la redirection de carte à puce, vous devez effectuer des étapes de configuration.

Authentification unique

Le mode d'authentification unique Horizon View parle à PAM (Pluggable Authentication Modules) dans Linux et ne dépend pas de la méthode que vous utilisez pour intégrer Linux à Active Directory (AD). Horizon View SSO est connu pour fonctionner avec les solutions OpenLDAP et Winbind qui intègrent Linux à AD.

Par défaut, SSO suppose que l'attribut `sAMAccountName` d'AD est l'ID de connexion. Pour vérifier que le bon ID de connexion est utilisé pour SSO, vous devez effectuer les étapes de configuration suivantes si vous utilisez la solution OpenLDAP ou Winbind :

- Pour OpenLDAP, définissez `sAMAccountName` sur `uid`.
- Pour Winbind, ajoutez l'instruction suivante au fichier de configuration `/etc/samba/smb.conf`.

```
winbind use default domain = true
```

Si des utilisateurs doivent spécifier le nom de domaine pour se connecter, vous devez définir l'option `SSOUserFormat` sur le poste de travail Linux. Pour plus d'informations, reportez-vous à la section [Définir des options dans des fichiers de configuration sur un poste de travail Linux](#). Sachez que SSO utilise toujours le nom de domaine court en majuscules. Par exemple, si le domaine est `mydomain.com`, SSO utilise `MYDOMAIN` comme nom de domaine. Par conséquent, vous devez spécifier `MYDOMAIN` lorsque vous définissez l'option `SSOUserFormat`. Concernant les noms de domaine courts et longs, les règles suivantes s'appliquent :

- Pour OpenLDAP, vous devez utiliser les noms de domaine courts en majuscules.
- Winbind prend en charge les noms de domaine longs et courts.

AD prend en charge les caractères spéciaux dans les noms de connexion, mais ce n'est pas le cas de Linux. Par conséquent, n'utilisez pas de caractères spéciaux dans les noms de connexion lorsque vous configurez SSO.

Dans AD, si l'attribut `UserPrincipalName` (UPN) d'un utilisateur et l'attribut `sAMAccount` ne correspondent pas et que l'utilisateur se connecte avec l'UPN, SSO échoue. La solution pour l'utilisateur consiste à se connecter avec le nom stocké dans `sAMAccount`.

View n'exige pas que le nom d'utilisateur soit sensible à la casse. Vous devez vérifier que le système d'exploitation Linux peut gérer les noms d'utilisateur non sensibles à la casse.

- Pour Winbind, le nom d'utilisateur n'est pas sensible à la casse par défaut.
- Pour OpenLDAP, Ubuntu utilise NSCD pour authentifier les utilisateurs et n'est pas sensible à la casse par défaut. RHEL et CentOS utilisent SSSD pour authentifier des utilisateurs et ne sont pas sensibles à la casse par défaut. Pour modifier le paramètre, modifiez le fichier `/etc/sss/sss.conf` et ajoutez la ligne suivante dans la section `[domain/default]` :

```
case_sensitive = false
```

Pour Ubuntu 16.04 ou 14.04, configurez `UseGnomeFlashback=TRUE` dans le fichier `/etc/vmware/viewagent-custom.conf` afin d'utiliser l'environnement de poste de travail GNOME Flashback (Metacity).

Redirection de carte à puce

Pour configurer la redirection de carte à puce, suivez tout d'abord les instructions du distributeur Linux et celles du fournisseur de la carte à puce. Ensuite, mettez à jour le package pcsc-lite à la version 1.7.4. Par exemple, exécutez les commandes suivantes :

```
#yum groupinstall "Development tools"
#yum install libudev-devel
#service pcscd stop
#wget https://alioth.debian.org/frs/download.php/file/3598/pcsc-lite-1.7.4.tar.bz2
#tar -xjvf pcsc-lite-1.7.4.tar.bz2
#cd ./pcsc-lite-1.7.4
#./configure --prefix=/usr/ --libdir=/usr/lib64/ --enable-usbdropdir=/usr/lib64/pcsc/drivers
--enable-confdir=/etc --enable-ipcdire=/var/run --disable-libusb --disable-serial --disable-usb
--disable-libudev
#make
#make install
#service pcscd start
```

Pour Winbind, ajoutez l'instruction suivante au fichier de configuration `/etc/samba/smb.conf`.

```
winbind use default domain = true
```

Lorsque vous installez Horizon Agent, vous devez d'abord désactiver SELinux ou activer le mode permissif pour SELinux. De plus, vous devez spécifiquement sélectionner le composant de redirection de carte à puce, car le composant n'est pas sélectionné par défaut. Pour plus d'informations, reportez-vous à la section [Options de ligne de commande install_viewagent.sh](#).

L'authentification unique de la carte à puce est activée dans Horizon View 7.0.1 ou version ultérieure. De plus, si la fonctionnalité de redirection de carte à puce est installée sur une machine virtuelle, la redirection USB de vSphere Client ne fonctionne pas avec la carte à puce.

La redirection de carte à puce ne prend en charge qu'un seul lecteur de carte à puce. Cette fonctionnalité ne fonctionne pas si deux lecteurs ou plus sont connectés au périphérique client.

La redirection de carte à puce ne prend en charge qu'un seul certificat sur la carte. Si plusieurs certificats se trouvent sur la carte, celui dans le premier emplacement est utilisé et les autres sont ignorés. Il s'agit d'une limitation de Linux.

Note

- La carte à puce prend en charge la valeur Winbind suivante. Autrement, l'authentification unique de la carte à puce et la connexion manuelle échouent.

```
winbind use default domain=true
```

- Lorsque vous utilisez le client Linux pour authentifier le Broker avec la carte PIV, qui est prise en charge par la redirection de carte à puce de postes de travail Linux, vous devez ajouter la configuration `view.sslProtocolString = "TLSv1.1"` pour le client Linux à `~/ .vmware/view-preferences` pour éviter une erreur SSL.

Configuration des graphiques pour les postes de travail Linux

4

Vous pouvez configurer les distributions RHEL prises en charge actuellement pour profiter des capacités de NVIDIA sur l'hôte ESXi ou sur un système d'exploitation invité.

Exigences de clone de VM pour configurer des graphiques 3D

Vous devez prendre en compte les exigences suivantes pour le clone de VM avant de configurer des graphiques 3D.

- Pour vGPU et vSGA, effectuez la configuration des graphiques dans la VM de base. Clonez les VM. Les paramètres graphiques fonctionnent pour les VM clonées et aucun autre paramètre n'est requis.
- Pour vDGA, effectuez la configuration des graphiques dans la VM de base. Clonez les VM. Toutefois, avant de mettre sous tension les VM clonées, vous devez supprimer le périphérique PCI de relais NVIDIA existant de la VM clonée et ajouter le nouveau périphérique PCI de relais NVIDIA à la VM clonée. Le périphérique PCI de relais NVIDIA ne peut pas être partagé entre les VM. Chaque VM utilise un périphérique PCI de relais NVIDIA dédié.

Ce chapitre contient les rubriques suivantes :

- [Configurer des distributions RHEL prises en charge pour vGPU](#)
- [Configurer RHEL 6 pour vDGA](#)
- [Configurer RHEL 7 pour vSGA](#)

Configurer des distributions RHEL prises en charge pour vGPU

Vous pouvez configurer une distribution RHEL pour profiter des capacités de NVIDIA vGPU (accélération matérielle GPU partagée) sur l'hôte ESXi.

Vous devez utiliser le pilote d'affichage de VM Linux NVIDIA qui correspond au pilote de processeur graphique de l'hôte ESXi (.vib). Consultez le site Web NVIDIA pour obtenir plus d'informations sur les packages de pilote.

Important NVIDIA vGPU est pris en charge sur les cartes graphiques NVIDIA Maxwell M60 et NVIDIA M6. Cette fonctionnalité ne fonctionne pas sur d'autres cartes graphiques NVIDIA, telles que GRID K1 ou K2.

Attention Avant de commencer, vérifiez qu'Horizon Agent n'est pas installé sur la machine virtuelle Linux. Si vous installez Horizon Agent avant de configurer la machine afin qu'elle utilise NVIDIA vGPU, les paramètres de configuration requis dans le fichier `xorg.conf` sont remplacés et NVIDIA vGPU ne fonctionne pas. Vous devez installer Horizon Agent lorsque la configuration NVIDIA vGPU est terminée.

Installer le VIB pour la carte graphique NVIDIA GRID vGPU sur l'hôte ESXi

Vous devez télécharger et installer le VIB pour votre carte graphique NVIDIA GRID sur l'hôte ESXi 6.0 U1 ou version ultérieure.

NVIDIA fournit un package logiciel vGPU qui inclut vGPU Manager, que vous installez sur l'hôte ESXi au cours de cette procédure, et un pilote d'affichage Linux, que vous installerez sur la machine virtuelle Linux dans une procédure ultérieure.

Conditions préalables

- Vérifiez que vSphere 6.0 U1 ou une version ultérieure est installé dans votre environnement.
- Vérifiez que les GPU NVIDIA Maxwell M60 ou M6 sont installés sur l'hôte ESXi.

Procédure

- 1 Téléchargez le VIB pour votre carte graphique NVIDIA GRID vGPU sur le site [Téléchargements de pilotes NVIDIA](#).

Sélectionnez la version de VIB appropriée dans les menus déroulants.

| Option | Description |
|------------------------|--|
| Type de produit | GRID |
| Série de produits | Sélectionnez NVIDIA GRID vGPU . |
| Produit | Sélectionnez la version (telle que GRID K2) installée sur l'hôte ESXi. |
| Système d'exploitation | Sélectionnez la version de VMware vSphere ESXi. |

- 2 Décompressez le fichier .zip du package logiciel vGPU.
- 3 Chargez le dossier vGPU Manager sur l'hôte ESXi 6.0 U1.

Note Vous installerez le pilote d'affichage Linux sur la machine virtuelle Linux dans une procédure ultérieure.

- 4 Mettez hors tension ou interrompez toutes les machines virtuelles sur l'hôte ESXi.
- 5 Connectez-vous à l'hôte ESXi à l'aide de SSH.
- 6 Arrêtez le service xorg.

```
# /etc/init.d/xorg stop
```

- 7 Installez le VIB NVIDIA.

Par exemple :

```
# esxcli system maintenanceMode set --enable true
# esxcli software vib install -v /path-to-vib/NVIDIA-VIB-name.vib
# esxcli system maintenanceMode set --enable false
```

- 8 Redémarrez ou mettez à jour l'hôte ESXi.

- ◆ Pour un hôte ESXi installé, redémarrez l'hôte.
- ◆ Pour un hôte ESXi sans état, effectuez les étapes suivantes pour mettre l'hôte à jour. (Ces étapes fonctionnent également sur un hôte installé.)

```
Update vmkdevmgr:
# kill -HUP $(cat /var/run/vmware/vmkdevmgr.pid)

Wait for the update to complete:
# localcli --plugin-dir /usr/lib/vmware/esxcli/int deviceInternal bind

This is a new requirement with the NVIDIA 352.* host driver:
# /etc/init.d/nvidia-vgpu start

Restart xorg, which is used for GPU assignment:
# /etc/init.d/xorg start
```

- 9 Vérifiez que le service xorg est en cours d'exécution après le redémarrage de l'hôte.

Configurer un périphérique PCI partagé pour vGPU sur la machine virtuelle Linux

Pour utiliser NVIDIA vGPU, vous devez configurer un périphérique PCI partagé pour la machine virtuelle Linux.

Conditions préalables

- Vérifiez que la machine virtuelle Linux est préparée pour être utilisée en tant que poste de travail. Reportez-vous aux sections [Créer une machine virtuelle et installer Linux](#) et [Préparer une machine Linux pour un déploiement de postes de travail distants](#).
- Vérifiez qu'Horizon Agent n'est pas installé sur la machine virtuelle Linux.
- Vérifiez que le VIB NVIDIA est installé sur l'hôte ESXi. Reportez-vous à la section [Installer le VIB pour la carte graphique NVIDIA GRID vGPU sur l'hôte ESXi](#).

- Familiarisez-vous avec les types de GPU virtuel disponibles avec NVIDIA vGPU, que vous sélectionnez avec le paramètre **Profil de GPU**. Les types de GPU virtuel fournissent diverses capacités sur les GPU physiques installés sur l'hôte ESXi. Reportez-vous à la section [Types de GPU virtuel NVIDIA](#).

Procédure

- 1 Mettez la machine virtuelle hors tension
- 2 Dans vSphere Web Client, sélectionnez la machine virtuelle et, sous l'onglet **Matériel VM**, cliquez sur **Modifier les paramètres**.
- 3 Dans le menu **Nouveau périphérique**, sélectionnez **Périphérique PCI partagé**.
- 4 Cliquez sur **Ajouter** et sélectionnez **NVIDIA GRID vGPU** dans le menu déroulant.
- 5 Pour le paramètre **Profil de GPU**, sélectionnez un type de GPU virtuel dans le menu déroulant.
- 6 Cliquez sur **Réserver toute la mémoire**, puis sur **OK**.

Vous devez réserver toute la mémoire de machine virtuelle pour que le GPU puisse prendre en charge NVIDIA GRID vGPU.

- 7 Activez la machine virtuelle.

Types de GPU virtuel NVIDIA

Avec le paramètre **Profils de GPU** sur la page Matériel virtuel dans vSphere Web Client, vous pouvez sélectionner un type de GPU virtuel fournissant des capacités spécifiques sur le GPU NVIDIA physique sur l'hôte ESXi.

Sur des machines virtuelles Linux, NVIDIA GRID vGPU est pris en charge sur des GPU NVIDIA Maxwell M60 ou NVIDIA M6.

Tableau 4-1. Types de GPU virtuels disponibles pour NVIDIA GRID M60 vGPU sur des machines virtuelles Linux

| Type de GPU virtuel | Carte physique | GPU physiques | Tampon de trame par GPU virtuel | Têtes d'affichage | Résolution maximale | Nombre maximal de GPU virtuels par GPU physique | Nombre maximal de GPU virtuels par carte physique |
|---------------------|----------------|---------------|---------------------------------|-------------------|---------------------|---|---|
| GRID M60-0q | GRID M60 | deux | 512M | 2 | 2 560x1 600 | 16 | 32 |
| GRID M60-1q | GRID M60 | deux | 1G | 2 | 2 560x1 600 | 8 | 16 |
| GRID M60-2q | GRID M60 | deux | 2G | 4 | 2 560x1 600 | 4 | 8 |
| GRID M60-4q | GRID M60 | deux | 4G | 4 | 3 840x2 160 | 2 | 4 |
| GRID M60-8q | GRID M60 | deux | 8G | 4 | 3 840x2 160 | 1 | 2 |

Tableau 4-2. Types de GPU virtuels disponibles pour NVIDIA GRID M6 vGPU sur des machines virtuelles Linux

| Type de GPU virtuel | Carte physique | GPU physiques | Tampon de trame par GPU virtuel | Têtes d'affichage | Résolution maximale | Nombre maximal de GPU virtuels par GPU physique | Nombre maximal de GPU virtuels par carte physique |
|---------------------|----------------|---------------|---------------------------------|-------------------|---------------------|---|---|
| GRID M6-0q | GRID M6 | un | 512M | 2 | 2 560x1 600 | 16 | 16 |
| GRID M6-1q | GRID M6 | un | 1G | 2 | 2 560x1 600 | 8 | 8 |
| GRID M6-2q | GRID M6 | un | 2G | 4 | 2 560x1 600 | 4 | 4 |
| GRID M6-4q | GRID M6 | un | 4G | 4 | 3 840x2 160 | 2 | 2 |
| GRID M6-8q | GRID M6 | un | 8G | 4 | 3 840x2 160 | 1 | 1 |

Installer le pilote d'affichage NVIDIA GRID vGPU

Pour installer le pilote d'affichage NVIDIA GRID vGPU, vous devez désactiver le pilote NVIDIA par défaut, télécharger les pilotes d'affichage NVIDIA et configurer le périphérique PCI sur la machine virtuelle.

Conditions préalables

- Vérifiez que vous avez téléchargé le package logiciel vGPU sur le site de téléchargement NVIDIA, que vous avez décompressé le package et que le pilote d'affichage Linux (un composant de package) est prêt. Reportez-vous à la section [Installer le VIB pour la carte graphique NVIDIA GRID vGPU sur l'hôte ESXi](#).

Vérifiez également qu'un périphérique PCI partagé a été ajouté à la machine virtuelle. Reportez-vous à la section [Configurer un périphérique PCI partagé pour vGPU sur la machine virtuelle Linux](#).

Procédure

- 1 Désactivez et mettez sur liste noire le pilote NVIDIA Nouveau par défaut.

- a Modifiez le fichier `grub.conf` ou `grub`.

Pour RHEL 6, le fichier est `/boot/grub/grub.conf`. Pour RHEL 7, le fichier est `/etc/default/grub`.

| Version de RHEL | vdmadmin |
|-----------------|---|
| 6 | <code>sudo vi /boot/grub/grub.conf</code> |
| 7 | <code>sudo vi /etc/default/grub</code> |

- b Ajoutez la ligne `rdblacklist=nouveau` à la fin des options du noyau.

- c Modifiez le fichier `blacklist.conf`.

```
sudo vi /etc/modprobe.d/blacklist.conf
```

- d Ajoutez la ligne suivante n'importe où dans le fichier `blacklist.conf`.

```
blacklist nouveau
```

- 2 Redémarrez la machine virtuelle.

L'affichage n'a plus la même apparence.

- 3 (Facultatif) Vérifiez que le pilote Nouveau est désactivé.

```
/sbin/lsmmod | grep nouveau
```

Si la recherche `grep` ne renvoie aucun résultat, le pilote Nouveau est désactivé.

- 4 Copiez le pilote d'affichage NVIDIA Linux sur la machine virtuelle.

- 5 Ouvrez un terminal distant sur la machine virtuelle, ou basculez vers une console texte en saisissant `Ctrl-Alt-F2`, ouvrez une session en tant qu'utilisateur racine et exécutez la commande `init 3` afin de désactiver X Windows.

- 6 Installez les composants supplémentaires qui sont requis pour le pilote NVIDIA.

```
sudo yum install gcc-c++
sudo yum install kernel-devel-$(uname -r)
sudo yum install kernel-headers-$(uname -r)
```

- 7 Ajoutez un indicateur exécutable au package du pilote NVIDIA GRID vGPU.

```
chmod +x NVIDIA-Linux-x86_64-version-grid.run
```

- 8 Démarrez le programme d'installation de NVIDIA GRID vGPU.

```
sudo ./NVIDIA-Linux-x86_64-version-grid.run
```

- 9 Acceptez le contrat de licence du logiciel NVIDIA et sélectionnez **Oui** pour mettre à jour automatiquement les paramètres de configuration de X.

Étape suivante

Installez Horizon Agent sur la machine virtuelle Linux. Reportez-vous à la section [Installer Horizon Agent sur une machine virtuelle Linux](#).

Créez un pool de postes de travail contenant les machines virtuelles Linux configurées. Reportez-vous à la section [Créer un pool de postes de travail manuel pour Linux](#).

Vérifier que le pilote d'affichage NVIDIA est installé

Vous pouvez vérifier que le pilote d'affichage NVIDIA est installé sur une machine virtuelle RHEL 6 en affichant la sortie du pilote NVIDIA dans une session de poste de travail View.

Conditions préalables

- Vérifiez que vous avez installé le pilote d'affichage NVIDIA.
- Vérifiez qu'Horizon Agent est installé sur la machine virtuelle Linux. Reportez-vous à la section [Installer Horizon Agent sur une machine virtuelle Linux](#).
- Vérifiez que la machine virtuelle Linux est déployée dans un pool de postes de travail. Reportez-vous à la section [Créer un pool de postes de travail manuel pour Linux](#).

Procédure

- 1 Redémarrez la machine virtuelle Linux.

Le script de démarrage d'Horizon Agent initialise le serveur X et la topologie d'affichage.

Vous ne pouvez plus voir l'affichage de la machine virtuelle dans la console vSphere.

- 2 Depuis Horizon Client, connectez-vous au poste de travail Linux.
- 3 Dans la session de poste de travail Linux, vérifiez que le pilote d'affichage NVIDIA est installé.

Ouvrez une fenêtre de terminal et exécutez la commande `glxinfo | grep NVIDIA`.

La sortie du pilote NVIDIA s'affiche. Par exemple :

```
[root]# glxinfo | grep NVIDIA
server glx vendor string: NVIDIA Corporation
client glx vendor string: NVIDIA Corporation
OpenGL vendor string: NVIDIA Corporation
OpenGL version string: 4.5.0 NVIDIA 346.47
OpenGL shading language version string: 4.50 NVIDIA
```

L'utilisateur peut accéder aux capacités graphiques NVIDIA sur le poste de travail distant.

Après avoir vérifié l'installation du pilote d'affichage NVIDIA, exécutez les tâches suivantes pour que l'installation fonctionne correctement.

- Si vous mettez à niveau le noyau Linux, Horizon Agent peut ne pas pouvoir communiquer avec le Serveur de connexion View. Pour résoudre le problème, réinstallez le pilote NVIDIA.
- Définissez la licence NVIDIA GRID dans la machine virtuelle Linux. Consultez la documentation de NVIDIA pour plus d'informations. Le poste de travail Linux ne fonctionnera pas correctement si la licence n'est pas définie. Par exemple, l'ajustement automatique ne fonctionnera pas.

Configurer RHEL 6 pour vDGA

Vous pouvez configurer un système d'exploitation invité RHEL 6 de sorte qu'un poste de travail Horizon 7 for Linux puisse bénéficier des capacités vDGA sur l'hôte ESXi.

Attention Avant de commencer, vérifiez qu'Horizon Agent n'est pas installé sur la machine virtuelle Linux. Si vous installez Horizon Agent avant de configurer la machine afin qu'elle utilise vDGA, les paramètres de configuration requis dans le fichier `xorg.conf` sont remplacés et vDGA ne fonctionne pas. Vous devez installer Horizon Agent lorsque la configuration vDGA est terminée.

Activer DirectPath I/O pour NVIDIA GRID sur un hôte

Avant de configurer une machine virtuelle Linux afin qu'elle utilise vDGA, vous devez rendre les périphériques PCI de GPU NVIDIA GRID disponibles pour le relais DirectPath I/O sur l'hôte ESXi.

Conditions préalables

- Vérifiez que vSphere 6.0 ou une version ultérieure est installé dans votre environnement.
- Vérifiez que les cartes graphiques NVIDIA GRID K1 ou K2 sont installées sur l'hôte ESXi.

Procédure

- 1 Dans vSphere Web Client, accédez à l'hôte ESXi.
- 2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.
- 3 Dans la section Matériel, cliquez sur **Périphériques PCI**.
- 4 Pour activer le relais DirectPath I/O pour les GPU NVIDIA GRID, cliquez sur **Modifier**.

| Icône | Description |
|---------------------|--|
| Icône verte | Le périphérique PCI est actif et peut être activé. |
| Icône orange | L'état du périphérique a changé. L'hôte doit être redémarré avant que le périphérique puisse être utilisé. |

- 5 Sélectionnez les GPU NVIDIA GRID et cliquez sur **OK**.

Les périphériques PCI sont ajoutés au tableau Périphériques PCI DirectPath I/O disponibles pour les VM.

- 6 Redémarrez l'hôte pour que les périphériques PCI puissent être utilisés par les machines virtuelles Linux.

Ajouter un périphérique de relais vDGA à une machine virtuelle RHEL 6

Pour configurer une machine virtuelle RHEL 6 de manière qu'elle utilise vDGA, vous devez ajouter le périphérique PCI à la machine virtuelle. Avec cette étape, le périphérique physique sur l'hôte ESXi peut être transmis pour une utilisation sur la machine virtuelle.

Conditions préalables

- Vérifiez que la machine virtuelle Linux est préparée pour être utilisée en tant que poste de travail. Reportez-vous aux sections [Créer une machine virtuelle et installer Linux](#) et [Préparer une machine Linux pour un déploiement de postes de travail distants](#).
- Vérifiez qu'Horizon Agent n'est pas installé sur la machine virtuelle Linux.
- Vérifiez que le périphérique PCI de GPU NVIDIA GRID est disponible pour le relais DirectPath I/O sur l'hôte. Reportez-vous à la section [Activer DirectPath I/O pour NVIDIA GRID sur un hôte](#).

Procédure

- 1 Ouvrez une session sur le système d'exploitation invité RHEL 6 en tant qu'utilisateur local configuré avec des droits sudo.
- 2 Dans vSphere Web Client, sélectionnez la machine virtuelle et, sous l'onglet **Matériel VM**, cliquez sur **Modifier les paramètres**.
- 3 Dans le menu **Nouveau périphérique**, sélectionnez **Périphérique PCI**.
- 4 Cliquez sur **Ajouter** et sélectionnez le périphérique PCI dans le menu déroulant.
- 5 Cliquez sur **Réserver toute la mémoire**, puis sur **OK**.

Vous devez réserver toute la mémoire de machine virtuelle pour que le GPU puisse prendre en charge vDGA.

- 6 Mettez la machine virtuelle sous tension et ouvrez la console vSphere pour la connecter à la machine.
- 7 Vérifiez que le périphérique NVIDIA GRID est transmis à la machine virtuelle.

Ouvrez une fenêtre de terminal et exécutez la commande suivante :

```
lspci | grep NVIDIA
```

Le contrôleur XX:00.0 compatible VGA s'affiche. Par exemple :

```
NVIDIA Corporation GK104GL [GRID K2]
```

Installer le pilote d'affichage NVIDIA pour vDGA

Pour installer le pilote d'affichage NVIDIA pour vDGA, vous devez désactiver le pilote NVIDIA par défaut, télécharger les pilotes d'affichage NVIDIA et configurer le périphérique PCI sur la machine virtuelle.

Conditions préalables

- Vérifiez que le périphérique PCI a été ajouté à la machine virtuelle RHEL 6. Reportez-vous à la section [Ajouter un périphérique de relais vDGA à une machine virtuelle RHEL 6](#).

Procédure

- 1 Désactivez et mettez sur liste noire le pilote NVIDIA Nouveau par défaut.

- a Modifiez le fichier `grub.conf`.

Pour RHEL 6, le fichier est `/boot/grub/grub.conf`.

| Version de RHEL | vdmadmin |
|-----------------|---|
| 6 | <code>sudo vi /boot/grub/grub.conf</code> |

- b Ajoutez la ligne `rdblacklist=nouveau` à la fin des options du noyau.

- c Modifiez le fichier `blacklist.conf`.

```
sudo vi /etc/modprobe.d/blacklist.conf
```

- d Ajoutez la ligne suivante n'importe où dans le fichier `blacklist.conf`.

```
blacklist nouveau
```

- 2 Redémarrez la machine virtuelle.

L'affichage n'a plus la même apparence.

- 3 (Facultatif) Vérifiez que le pilote Nouveau est désactivé.

```
/sbin/lsmmod | grep nouveau
```

Si la recherche `grep` ne renvoie aucun résultat, le pilote Nouveau est désactivé.

- 4 Téléchargez le pilote NVIDIA sur le site [Téléchargements de pilotes NVIDIA](#).

Sélectionnez la version de pilote appropriée dans les menus déroulants NVIDIA :

| Option | Description |
|------------------------|--|
| Type de produit | GRID |
| Série de produits | GRID Series |
| Produit | Sélectionnez la version (telle que GRID K2) installée sur l'hôte ESXi. |
| Système d'exploitation | Linux 64-bit ou Linux 32-bit |

- 5 Ouvrez un terminal distant sur la machine virtuelle, ou basculez vers une console texte en saisissant `Ctrl-Alt-F2`, ouvrez une session en tant qu'utilisateur racine et exécutez la commande `init 3` afin de désactiver X Windows.

- 6 Installez les composants supplémentaires qui sont requis pour le pilote NVIDIA.

```
sudo yum install gcc-c++
sudo yum install kernel-devel-$(uname -r)
sudo yum install kernel-headers-$(uname -r)
```

- 7 Ajoutez un indicateur exécutable au package du pilote NVIDIA pour vDGA.

```
chmod +x NVIDIA-Linux-x86_64-version.run
```

- 8 Démarrez le programme d'installation NVIDIA.

```
sudo ./NVIDIA-Linux-x86_64-version.run
```

- 9 Acceptez le contrat de licence du logiciel NVIDIA et sélectionnez **Oui** pour mettre à jour automatiquement les paramètres de configuration de X.

Étape suivante

Installez Horizon Agent sur la machine virtuelle Linux. Reportez-vous à la section [Installer Horizon Agent sur une machine virtuelle Linux](#).

Créez un pool de postes de travail contenant les machines virtuelles Linux configurées. Reportez-vous à la section [Créer un pool de postes de travail manuel pour Linux](#).

Vérifier que le pilote d'affichage NVIDIA est installé

Vous pouvez vérifier que le pilote d'affichage NVIDIA est installé sur une machine virtuelle RHEL 6 en affichant la sortie du pilote NVIDIA dans une session de poste de travail View.

Conditions préalables

- Vérifiez que vous avez installé le pilote d'affichage NVIDIA.
- Vérifiez qu'Horizon Agent est installé sur la machine virtuelle Linux. Reportez-vous à la section [Installer Horizon Agent sur une machine virtuelle Linux](#).
- Vérifiez que la machine virtuelle Linux est déployée dans un pool de postes de travail. Reportez-vous à la section [Créer un pool de postes de travail manuel pour Linux](#).

Procédure

- 1 Redémarrez la machine virtuelle Linux.

Le script de démarrage d'Horizon Agent initialise le serveur X et la topologie d'affichage.

Vous ne pouvez plus voir l'affichage de la machine virtuelle dans la console vSphere.

- 2 Depuis Horizon Client, connectez-vous au poste de travail Linux.
- 3 Dans la session de poste de travail Linux, vérifiez que le pilote d'affichage NVIDIA est installé.

Ouvrez une fenêtre de terminal et exécutez la commande `glxinfo | grep NVIDIA`.

La sortie du pilote NVIDIA s'affiche. Par exemple :

```
[root]# glxinfo | grep NVIDIA
server glx vendor string: NVIDIA Corporation
client glx vendor string: NVIDIA Corporation
OpenGL vendor string: NVIDIA Corporation
OpenGL version string: 4.5.0 NVIDIA 346.47
OpenGL shading language version string: 4.50 NVIDIA
```

L'utilisateur peut accéder aux capacités graphiques NVIDIA sur le poste de travail distant.

Après avoir vérifié l'installation du pilote d'affichage NVIDIA, exécutez les tâches suivantes pour que l'installation fonctionne correctement.

- Si vous mettez à niveau le noyau Linux, Horizon Agent peut ne pas pouvoir communiquer avec le Serveur de connexion View. Pour résoudre le problème, réinstallez le pilote NVIDIA.

- Définissez la licence NVIDIA GRID dans la machine virtuelle Linux. Consultez la documentation de NVIDIA pour plus d'informations. Le poste de travail Linux ne fonctionnera pas correctement si la licence n'est pas définie. Par exemple, l'ajustement automatique ne fonctionnera pas.

Configurer RHEL 7 pour vSGA

Vous pouvez configurer un système d'exploitation invité RHEL 7 de sorte qu'un poste de travail Horizon 7 for Linux puisse bénéficier des capacités vSGA.

Installer le VIB pour la carte graphique NVIDIA pour vSGA sur l'hôte ESXi

Vous devez télécharger et installer le VIB pour votre carte graphique NVIDIA GRID sur l'hôte ESXi 6.0 U1 ou version ultérieure.

NVIDIA fournit un pilote VMware vSphere ESXi pour vSGA. Pour vSGA, un pilote d'affichage NVIDIA n'est pas installé sur la machine virtuelle Linux.

Conditions préalables

- Vérifiez que vSphere 6.0 U1 ou une version ultérieure est installé dans votre environnement.
- Vérifiez que le pilote NVIDIA est installé dans votre environnement.
- Vérifiez que les GPU NVIDIA GRID K1 ou K2 sont installés sur l'hôte ESXi.

Procédure

- 1 Téléchargez le VIB pour votre carte graphique NVIDIA GRID vGPU sur le site [Téléchargements de pilotes NVIDIA](#).

Sélectionnez la version de VIB appropriée dans les menus déroulants.

| Option | Description |
|------------------------|--|
| Type de produit | GRID |
| Série de produits | Sélectionnez Série GRID . |
| Produit | Sélectionnez la version (telle que GRID K2) installée sur l'hôte ESXi. |
| Système d'exploitation | Sélectionnez la version de VMware vSphere ESXi. |

- 2 Téléchargez le pilote VMware vSphere ESXi pour vSGA sur l'hôte ESXi 6.0 U1.
- 3 Mettez hors tension ou interrompez toutes les machines virtuelles sur l'hôte ESXi.
- 4 Connectez-vous à l'hôte ESXi à l'aide de SSH.
- 5 Arrêtez le service xorg.

```
# /etc/init.d/xorg stop
```

6 Installez le VIB NVIDIA.

Par exemple :

```
# esxcli system maintenanceMode set --enable true
# esxcli software vib install -v /path-to-vib/NVIDIA-VIB-name.vib
# esxcli system maintenanceMode set --enable false
```

7 Redémarrez xorg, qui est utilisé pour l'attribution de GPU :

```
# /etc/init.d/xorg start
```

8 Redémarrez l'hôte ESXi.

9 Vérifiez que le service xorg est en cours d'exécution après le redémarrage de l'hôte.

Configurer des capacités 3D pour vSGA sur la machine virtuelle Linux

Pour configurer une machine virtuelle RHEL 7 de manière qu'elle utilise vSGA, vous devez configurer les paramètres 3D de la carte vidéo de la machine virtuelle dans vSphere Web Client.

Conditions préalables

- Vérifiez que la machine virtuelle Linux est préparée pour être utilisée en tant que poste de travail, qu'Horizon Agent est installé et que la machine est déployée dans un pool de postes de travail.
- Vérifiez que le VIB NVIDIA est installé sur l'hôte ESXi. Reportez-vous à la section [Installer le VIB pour la carte graphique NVIDIA pour vSGA sur l'hôte ESXi](#).

Procédure

- 1 Mettez la machine virtuelle hors tension
- 2 Dans vSphere Web Client, sélectionnez la machine virtuelle et, sous l'onglet **Matériel VM**, cliquez sur **Modifier les paramètres**.
- 3 Dans l'onglet Matériel virtuel, cliquez sur **Carte vidéo** pour développer les paramètres du menu.
- 4 Réglez la **Mémoire vidéo totale** sur 128 Mo.
- 5 Pour **Graphiques 3D**, sélectionnez **Activer support 3D**.
- 6 Pour **Convertisseur 3D**, sélectionnez **Matériel** dans le menu déroulant.
- 7 Pour **Mémoire 3D**, sélectionnez une valeur adaptée aux exigences de votre application.
Si vos utilisateurs se connectent à plus de 3 moniteurs, réglez cette valeur sur au moins 1 024 Mo.
- 8 Cliquez sur **OK**.
- 9 Activez la machine virtuelle.

Étape suivante

Vérifiez que vSGA est en cours d'exécution sur la machine virtuelle Linux.

Ensuite, installez Horizon Agent sur la machine virtuelle Linux. Reportez-vous à la section [Installer Horizon Agent sur une machine virtuelle Linux](#).

Vérifier que vSGA est en cours d'exécution sur une machine virtuelle Linux

Vous pouvez vérifier que vSGA est exécuté sur une machine virtuelle RHEL 7 en consultant le fichier journal de la machine virtuelle et en vérifiant le système d'exploitation invité.

Procédure

- 1 Ouvrez le fichier `vmware.log` de la machine virtuelle.

Si un GPU et un VIB NVIDIA pris en charge sont installés correctement, le fichier journal affiche des lignes telles que celles dans l'exemple suivant :

```
2015-06-24T22:19:25.259Z| mks| I120: OpenGL Version: "4.0.0 NVIDIA 346.69" (4.0.0)
2015-06-24T22:19:25.259Z| mks| I120: GLSL Version: "4.00 NVIDIA" (4.00.0)
2015-06-24T22:19:25.259Z| mks| I120: OpenGL Vendor: "NVIDIA Corporation"
2015-06-24T22:19:25.259Z| mks| I120: OpenGL Renderer: "Quadro 4000/PCIe/SSE2"
```

Si un GPU et un VIB NVIDIA pris en charge ne sont pas installés correctement, la machine virtuelle utilise le convertisseur logiciel. Le fichier `vmware.log` affiche des lignes telles que celles dans l'exemple suivant :

```
2015-07-06T17:09:26.423Z| vmx| I120: [msg.mks.noGPUResourceFallback] Hardware GPU resources are
not available. The virtual machine uses software rendering.
2015-07-06T17:09:26.423Z| vmx| I120: -----
2015-07-06T17:09:26.425Z| svga| I120: MKS-SWP: plugin started - llvmpipe (LLVM 3.3, 256 bits)
2015-07-06T17:09:26.426Z| svga| I120: Started Shim3D
2015-07-06T17:09:26.426Z| svga| I120: MKS-RenderMain: Starting SWRenderer
```

- 2 Dans le système d'exploitation invité sur la machine virtuelle, saisissez la commande suivante.

```
glxinfo|grep Gallium
```

Si vSGA fonctionne, la commande renvoie le texte suivant :

```
OpenGL renderer string: Gallium 0.4 on SVGA3D; build : RELEASE;
```

Si vSGA ne fonctionne pas correctement, la commande renvoie le texte suivant :

```
OpenGL renderer string: Gallium 0.4 on llvmpipe (LLVM 3.3, 256 bits)
```

Étape suivante

Installez Horizon Agent sur la machine virtuelle Linux. Reportez-vous à la section [Installer Horizon Agent sur une machine virtuelle Linux](#).

Installation d'Horizon Agent

Vous devez installer Horizon Agent sur les postes de travail Linux pour que le Serveur de connexion View puisse communiquer avec les postes de travail et les gérer.

Ce chapitre contient les rubriques suivantes :

- [Installer Horizon Agent sur une machine virtuelle Linux](#)
- [Configurer le certificat de Linux Agent](#)
- [Mise à niveau d'Horizon Agent sur une machine virtuelle Linux](#)
- [Désinstaller Horizon 7 pour les machines Linux](#)

Installer Horizon Agent sur une machine virtuelle Linux

Vous devez installer Horizon Agent sur une machine virtuelle Linux avant de pouvoir déployer la machine en tant que poste de travail distant.

À partir d'Horizon 7.0.1, Horizon Agent for Linux utilise les machines virtuelles gérées par vCenter. Les machines virtuelles gérées offrent les améliorations suivantes.

- vCenter est obligatoire pour le déploiement de postes de travail Linux.
- L'installation d'Horizon Agent sur Linux ne requiert pas d'enregistrement.
- Pour un grand nombre de déploiements de postes de travail Linux, vous pouvez installer Horizon Agent sur la machine virtuelle de base.

Attention Si vous prévoyez d'utiliser NVIDIA GRID vGPU, vDGA ou vSGA, vous devez configurer ces fonctionnalités 3D sur la machine virtuelle Linux avant d'installer Horizon Agent. Si vous installez Horizon Agent en premier, les paramètres requis dans le fichier `xorg.conf` sont remplacés et les fonctionnalités de graphique 3D ne sont pas opérationnelles.

Reportez-vous à [Configurer des distributions RHEL prises en charge pour vGPU](#), [Configurer RHEL 6 pour vDGA](#) ou à [Configurer RHEL 7 pour vSGA](#). Installez Horizon Agent une fois la configuration graphique 3D terminée.

Pour la configuration graphique 2D, vous pouvez installer Horizon Agent après avoir réalisé les étapes de la section [Préparer une machine Linux pour un déploiement de postes de travail distants](#).

Conditions préalables

- Vérifiez que le système d'exploitation invité Linux est préparé à une utilisation comme poste de travail. Reportez-vous à la section [Préparer une machine Linux pour un déploiement de postes de travail distants](#).
- Familiarisez-vous avec le script du programme d'installation d'Horizon Agent pour Linux. Reportez-vous à la section [Options de ligne de commande install_viewagent.sh](#).

Procédure

- 1 Téléchargez le fichier du programme d'installation d'Horizon Agent pour Linux sur le site de téléchargement VMware, à l'adresse <https://my.vmware.com/web/vmware/downloads>.

Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut le programme d'installation d'Horizon Agent pour Linux.

Le nom de fichier du programme d'installation est VMware-horizonagent-linux-x86_64-y.y.y-xxxxxxx.tar.gz pour Linux 64 bits où y.y.y est le numéro de version et xxxxxxx le numéro de build.

- 2 Décompressez l'archive de votre distribution Linux sur le système d'exploitation invité.

Par exemple :

```
tar -xzf <archive View Agent>
```

- 3 Accédez au dossier de l'archive.
- 4 Exécutez le script `install_viewagent.sh` en tant que super utilisateur.

Reportez-vous à la section [Options de ligne de commande install_viewagent.sh](#) pour voir une liste des options de ligne de commande.

Par exemple :

```
sudo ./install_viewagent.sh
```

- 5 Saisissez **Oui** pour accepter le CLUF si vous exécutez `install_viewagent.sh` sans spécifier l'option `-A`.

Le programme d'installation ne s'exécute pas tant que vous n'avez pas accepté le CLUF.

- 6 Redémarrez Linux pour appliquer vos modifications.

Après l'installation, le service `viewagent` est lancé. Vérifiez que le service est lancé à l'aide de `sudo service viewagent status`.

Étape suivante

Déployez la machine virtuelle dans un pool de postes de travail. Reportez-vous à la section [Créer un pool de postes de travail manuel pour Linux](#).

Options de ligne de commande install_viewagent.sh

Le script `install_viewagent.sh` installe Horizon Agent sur un système d'exploitation invité Linux.

Utilisez la forme suivante du script `install_viewagent.sh` dans une fenêtre de commande dans l'environnement de poste de travail gnome.

```
install_viewagent.sh command_option argument [command_option argument] . . .
```

Le script `install_viewagent.sh` inclut des paramètres obligatoires et facultatifs.

Tableau 5-1. `install_viewagent.sh` Paramètre facultatif, mais requis

| Paramètre facultatif (informations requises) | Description |
|--|--|
| -A yes | Acceptation des déclarations CLUF et FIPS. Vous devez spécifier yes pour que l'installation soit exécutée. Si ce paramètre n'est pas spécifié, le script d'installation vous invite à saisir la valeur. |

Tableau 5-2. Paramètres facultatifs `install_viewagent.sh`

| Paramètres facultatifs | Description |
|------------------------|--|
| -a yes no | Installer ou contourner la prise en charge de la redirection d'entrée audio. La valeur par défaut est yes . |
| -f yes no | Installez ou contournez la prise en charge des modules cryptographiques conçus pour garantir les normes FIPS (Federal Information Processing Standards) 140-2. La valeur par défaut est no . Pour plus d'informations, reportez-vous à la description du mode FIPS 140-2 dans Fonctionnalités des postes de travail Horizon Linux . |
| -j | Mot de passe du magasin de clés JMS SSL. Par défaut, le programme d'installation génère une chaîne aléatoire. |
| -m yes no | Installer ou contourner la prise en charge de la redirection de carte à puce. La valeur par défaut est no . |
| -r yes no | Redémarrer automatiquement le système après l'installation. La valeur par défaut est no . |
| -s | DN du sujet du certificat auto-signé. Par défaut, le programme d'installation utilise Blast. |
| -C yes no | Installer ou contourner la prise en charge de la redirection du Presse-papiers. La valeur par défaut est yes . |
| -F yes no | Installer ou contourner la prise en charge de la CDR. La valeur par défaut est yes . |
| -M yes no | Mettre à niveau l'agent Linux vers un agent géré ou non géré. La valeur par défaut est yes . |
| -S yes no | Installer ou contourner la prise en charge de l'authentification unique (SSO). La valeur par défaut est yes . |
| -U yes no | Installer ou contourner la prise en charge USB. La valeur par défaut est no . |

Tableau 5-3. Exemples de paramètres install_viewagent.sh

| Condition | Exemples |
|---|---|
| Nouvelle installation | <pre>sudo ./install_viewagent.sh -A yes</pre> <p>Une nouvelle installation requiert toujours la création d'un nouveau pool de postes de travail.</p> |
| Mettre à niveau depuis une machine virtuelle non gérée et conserver le style de la machine virtuelle non gérée | <pre>sudo ./install_viewagent.sh -A yes-M no</pre> <p>Ce type de mise à niveau ne requiert pas la création d'un nouveau pool de postes de travail. Vous pouvez réutiliser le pool de postes de travail existant.</p> <p>Note Pour garantir les meilleures performances possibles, n'utilisez pas de machine virtuelle non gérée.</p> |
| Mettre à niveau un déploiement de machines virtuelles non gérées vers un déploiement de machines virtuelles gérées. La mise à niveau requiert la création d'un nouveau pool de postes de travail sur Broker | <pre>sudo ./install_viewagent.sh -A yes</pre> <p>Ce type de mise à niveau requiert la création d'un nouveau pool de postes de travail. Vous pouvez supprimer le pool de postes de travail existant.</p> |

Configurer le certificat de Linux Agent

Lorsque vous installez Linux Agent, le programme d'installation génère un certificat auto-signé pour VMwareBlastServer.

- Lorsque Blast Security Gateway est désactivé sur le broker, VMwareBlastServer présente ce certificat au navigateur qui utilise HTML Access pour se connecter au poste de travail Linux.
- Lorsque Blast Security Gateway est activé sur le broker, son certificat présente le certificat au navigateur.

Pour respecter les réglementations du secteur et de sécurité, vous pouvez remplacer le certificat auto-signé par un certificat signé par une autorité de certification.

Procédure

- 1 Installez la clé privée et le certificat sur VMwareBlastServer.
 - a Renommez la clé privée rui.key et le certificat rui.crt.
 - b Exécutez `sudo chmod 550 /etc/vmware/ssl`.

- c Copiez rui.crt et rui.key sur /etc/vmware/ssl.
 - d Exécutez `chmod 440 /etc/vmware/ssl`.
- 2 Installez l'autorité de certification racine et intermédiaire sur le magasin d'autorité de certification Linux OS.

Note Consultez votre documentation de distribution Linux pour voir les changements apportés aux paramètres du système Linux.

Mise à niveau d'Horizon Agent sur une machine virtuelle Linux

Vous pouvez mettre à niveau Horizon Agent sur une machine virtuelle Linux en installant la dernière version d'Horizon Agent.

Machine virtuelle non gérée : le programme d'installation de l'agent enregistre la machine virtuelle sur le Broker, ce qui nécessite les informations d'administration du Broker. L'assistant de **création de pool de postes de travail** utilise **Autres sources** sur la page Source de machines pour sélectionner la machine virtuelle enregistrée.

Machine virtuelle gérée : le programme d'installation ne communique pas avec le Broker. L'assistant de **création de pool de postes de travail** utilise **Machines virtuelles vCenter** sur la page Source de machines pour sélectionner les machines virtuelles via vCenter. Le déploiement de machines virtuelles gérées prend en charge les fonctions suivantes.

- Stratégie d'alimentation de machine distante
- Autoriser les utilisateurs à réinitialiser leurs machines

Note Horizon Agent for Linux 7.0.0 et versions antérieures fonctionnaient en tant que machines virtuelles non gérées. Horizon Agent for Linux 7.0.1 fonctionne en tant que machine virtuelle gérée.

Vous pouvez utiliser les méthodes suivantes pour mettre à niveau un déploiement de machines virtuelles non gérées vers un déploiement de machines virtuelles gérées.

- Conserver le déploiement de machines virtuelles non gérées et mettre à niveau vers la version requise. Ce type de mise à niveau ne nécessite aucune modification de configuration du Serveur de connexion View.
- Mettre à niveau un déploiement de machines virtuelles non gérées vers un déploiement de machines virtuelles gérées de n'importe quelle version. Ce type de mise à niveau nécessite la création d'un nouveau pool de postes de travail sur le Serveur de connexion View.

Note Pour la mise à niveau depuis un déploiement de machines virtuelles gérées, vous pouvez conserver le déploiement de machines virtuelles gérées et mettre à niveau vers la version requise. Cependant, la conversion d'un déploiement de machines virtuelles gérées en déploiement de machines virtuelles non gérées au cours d'une mise à niveau n'est pas prise en charge.

Les paramètres suivants sont disponibles pour la mise à niveau.

Tableau 5-4. Paramètres facultatifs pour la mise à niveau d'Horizon Agent

| Paramètre | Description |
|-----------|--|
| -A yes | Acceptation des déclarations CLUF et FIPS. Vous devez spécifier yes pour que l'installation soit exécutée. Si ce paramètre n'est pas spécifié, le script d'installation vous invite à saisir la valeur. |
| -a yes no | Installer ou contourner la prise en charge de la redirection d'entrée audio. La valeur par défaut est yes . |
| -f yes no | Installez ou contournez la prise en charge des modules cryptographiques conçus pour garantir les normes FIPS (Federal Information Processing Standards) 140-2. La valeur par défaut est no . Pour plus d'informations, reportez-vous à la description du mode FIPS 140-2 dans Fonctionnalités des postes de travail Horizon Linux . |
| -m yes no | Installer ou contourner la prise en charge de la redirection de carte à puce. La valeur par défaut est no . |
| -r yes no | Redémarrez le système d'exploitation après l'installation. La valeur par défaut est no . |
| -C yes no | Installer ou contourner la prise en charge de la redirection du Presse-papiers. La valeur par défaut est yes . |
| -F yes no | Installer ou contourner la prise en charge de la CDR. La valeur par défaut est yes . |
| -M yes no | Met à niveau l'agent Linux vers un agent géré/non géré. La valeur par défaut est yes . |
| -S yes no | Installer ou contourner la prise en charge de l'authentification unique (SSO). La valeur par défaut est yes . |
| -U yes no | Installer ou contourner la prise en charge USB. La valeur par défaut est no . |

Mettre à niveau Horizon Agent sur une machine virtuelle Linux

Vous pouvez mettre à niveau Horizon Agent sur une machine Linux en installant la dernière version d'Horizon Agent.

Conditions préalables

- Vérifiez que le processus VMwareBlastServer n'est pas en cours d'exécution.

Pour arrêter ce processus, vérifiez que l'utilisateur ferme sa session sur la machine et qu'aucune session de poste de travail n'est active, ou redémarrez la machine.

Procédure

- 1 Téléchargez le dernier fichier du programme d'installation d'Horizon Agent pour Linux sur le site de téléchargement VMware, à l'adresse <https://my.vmware.com/web/vmware/downloads>.

Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut le programme d'installation d'Horizon Agent pour Linux.

Le nom de fichier du programme d'installation est VMware-viewagent-linux-x86_64-y.y.y-xxxxxxx.tar.gz pour Linux 64 bits où y.y.y est le numéro de version et xxxxxx le numéro de build.

- 2 Décompressez l'archive de votre distribution Linux sur le système d'exploitation invité.

Par exemple :

```
tar -xzf <archive View Agent>
```

- 3 Accédez au dossier de l'archive.

- 4 Exécutez le script `install_viewagent.sh` pour mettre à niveau les machines virtuelles non gérées à l'aide de l'un des scénarios de déploiement suivants :

| Option | Description |
|--|---|
| Mettre à niveau un déploiement de machines virtuelles non gérées et conserver le déploiement de machines virtuelles non gérées | <pre>sudo ./install_viewagent.sh -A yes -M no</pre> <p>Note Pour garantir les meilleures performances possibles, n'utilisez pas de machine virtuelle non gérée.</p> |
| Mettre à niveau un déploiement de machines virtuelles non gérées et le changer en déploiement de machines virtuelles gérées | <pre>sudo ./install_viewagent.sh -A yes -M yes</pre> <p>Note Dans View Administrator, supprimez le pool de postes de travail existant pour le déploiement de machine virtuelle non gérée, puis créez un nouveau pool de postes de travail pour un déploiement de machine virtuelle gérée. Pour plus d'informations, reportez-vous à la section Créer un pool de postes de travail manuel pour Linux.</p> |
| Mettre à niveau un déploiement de machine virtuelle gérée | <pre>sudo ./install_viewagent.sh -A yes -M yes</pre> <p>Note Après la mise à niveau, votre pool de postes de travail existant peut être réutilisé.</p> |

Désinstaller Horizon 7 pour les machines Linux

Pour désinstaller Horizon 7 pour Linux sur une machine virtuelle, vous devez désinstaller Horizon Agent et supprimer les fichiers de configuration.

Conditions préalables

Vérifiez que le processus VMwareBlastServer n'est pas en cours d'exécution. Pour arrêter ce processus, assurez-vous de fermer votre session sur la machine et qu'aucune session de poste de travail n'est active, ou redémarrez la machine.

Procédure

- Ouvrez une fenêtre de terminal sur la machine virtuelle et exécutez le script de désinstallation d'Horizon Agent.

```
sudo /usr/lib/vmware/viewagent/bin/uninstall_viewagent.sh
```

Le script met fin aux processus d'Horizon Agent et supprime le logiciel et le service d'Horizon Agent du répertoire d'installation `/usr/lib/vmware/viewagent`.

- Supprimez manuellement les fichiers de configuration d'Horizon 7 for Linux dans le répertoire `/etc/vmware`.

Options de configuration pour les postes de travail Linux

6

Vous pouvez configurer diverses options pour personnaliser l'expérience utilisateur à l'aide de fichiers de configuration.

Ce chapitre contient les rubriques suivantes :

- Définir des options dans des fichiers de configuration sur un poste de travail Linux
- Exemples de paramètres Blast pour des postes de travail Linux
- Exemples d'options de la redirection du lecteur client pour des postes de travail Linux
- Supprimer l'affichage de la console vSphere d'un poste de travail Linux

Définir des options dans des fichiers de configuration sur un poste de travail Linux

Vous pouvez configurer certaines options en ajoutant des entrées aux fichiers `/etc/vmware/config` ou `/etc/vmware/viewagent-custom.conf`.

Au cours de l'installation de View Agent ou d'Horizon Agent, le programme d'installation copie deux fichiers de modèle de configuration, `config.template` et `viewagent-custom.conf.template`, dans `/etc/vmware`. De plus, si les fichiers `/etc/vmware/config` et `/etc/vmware/viewagent-custom.conf` n'existent pas, le programme d'installation copie `config.template` dans `config` et `viewagent-custom.conf.template` dans `viewagent-custom.conf`. Dans les fichiers de modèle, toutes les options de configuration sont répertoriées et documentées. Pour définir une option, supprimez simplement le commentaire et modifiez la valeur si nécessaire.

Par exemple, la ligne suivante dans `/etc/vmware/config` active le mode PNG sans perte.

```
RemoteDisplay.alwaysLossless=TRUE
```

Après avoir modifié la configuration, redémarrez Linux pour que les modifications prennent effet.

Options de configuration dans /etc/vmware/config

VMwareBlastServer et ses plug-ins liés utilisent le fichier de configuration /etc/vmware/config.

Note Le tableau suivant décrit chaque paramètre de stratégie appliqué par agent pour USB dans le fichier de configuration d'Horizon Agent. Horizon Agent utilise les paramètres pour décider si un périphérique USB peut être transmis à la machine hôte. Horizon Agent transmet également les paramètres à Horizon Client pour qu'il les interprète et les applique, selon que vous spécifiez le modificateur de fusion (**m**) pour appliquer les paramètres de stratégie de filtre Horizon Agent et Horizon Client ou le modificateur de remplacement (**o**) pour utiliser le paramètre de stratégie de filtre Horizon Agent au lieu du paramètre de stratégie de filtre Horizon Client.

Tableau 6-1. Options de configuration dans /etc/vmware/config

| Option | Valeur/Format | Valeur par défaut | Description |
|----------------------------------|---|-------------------|---|
| RemoteDisplay.alwaysLossless | true ou false | false | Les applications graphiques, en particulier les applications de conception graphique, requièrent un rendu exact des pixels d'images dans l'affichage client d'un poste de travail Linux. Vous pouvez configurer un mode PNG sans perte pour la lecture des images et des vidéos qui sont générées sur un poste de travail et rendues sur le périphérique client. Cette fonctionnalité utilise de la bande passante supplémentaire entre le client et l'hôte ESXi. |
| mksVNCServer.useUIButton Mapping | true ou false | false | Définissez cette option pour activer la prise en charge d'une souris pour gauchers sous Ubuntu ou RHEL 7. CentOS et RHEL 6 prennent en charge les souris pour gauchers et vous n'avez pas besoin de définir cette option. |
| RemoteDisplay.allowAudio | true ou false | true | Définissez cette option pour activer/désactiver la sortie audio. |
| VVC.ScRedir.Enable | true ou false | true | Définissez cette option pour activer/désactiver la redirection de carte à puce. |
| VVC.logLevel | fatal error, warn, info, debug ou trace | info | Utilisez cette option pour définir le niveau de journalisation du nœud de proxy VVC. |
| VVC.RTAV.Enable | true ou false | true | Définissez cette option pour activer/désactiver l'entrée audio. |

| Option | Valeur/Format | Valeur par défaut | Description |
|-------------------------|---|-------------------|---|
| Clipboard.Direction | 0, 1, 2, ou 3 | 2 | <p>Cette option détermine la stratégie de redirection de Presse-papiers.</p> <ul style="list-style-type: none"> ■ 0 - Désactivez la redirection de Presse-papiers. ■ 1 - Activez la redirection de Presse-papiers dans les deux sens. ■ 2 - Activez la redirection de Presse-papiers uniquement depuis le client vers le poste de travail distant. ■ 3 - Activez la redirection de Presse-papiers uniquement depuis le poste de travail vers le client. |
| cdrserver.logLevel | error, warn, info, debug, trace ou verbose | info | Utilisez cette option pour définir le niveau de journalisation pour <code>vmware-CDRserver.log</code> |
| cdrserver.forcedByAdmin | true ou false | false | Définissez cette option pour empêcher ou autoriser le client à partager des dossiers supplémentaires qui ne sont pas spécifiés avec l'option <code>cdrserver.shareFolders</code> . |
| cdrserver.sharedFolders | <i>file_path1,R; file_path2,; file_path3,R; .</i> .. | non défini | <p>Spécifiez un ou plusieurs chemins de fichier vers les dossiers que le client peut partager avec le poste de travail Linux. Par exemple :</p> <ul style="list-style-type: none"> ■ pour un client Windows : C:\spreadsheets,;D:\ebooks,R ■ pour un client non-Windows : /tmp/spreadsheets;/tmp/ebooks,;/home/finance,R |
| cdrserver.permissions | R | RW | <p>Utilisez cette option pour appliquer des autorisations en lecture/écriture supplémentaires dont dispose Horizon Agent sur les dossiers partagés par Horizon Client. Par exemple :</p> <ul style="list-style-type: none"> ■ Si le dossier partagé par Horizon Client dispose des autorisations <code>read</code> et <code>write</code> et que vous définissez cdrserver.permissions=R, Horizon Agent ne dispose que des autorisations d'accès <code>read</code>. ■ Si le dossier partagé par Horizon Client ne dispose que des autorisations <code>read</code> et que vous définissez cdrserver.permissions=RW, Horizon Agent disposera toujours que des droits d'accès <code>read</code>. Horizon Agent ne peut pas modifier l'attribut <code>read</code> seule qui a été défini par Horizon Client. La seule action possible pour Horizon Agent consiste à supprimer les droits d'accès en écriture. <p>Utilisations classiques :</p> <ul style="list-style-type: none"> ■ cdrserver.permissions=R ■ #cdrserver.permissions=R (c.-à-d. commenter ou supprimer l'entrée) |

| Option | Valeur/Format | Valeur par défaut | Description |
|----------------------------------|--|-------------------------------------|--|
| cdserver.cacheEnable | true ou false | true | Définissez cette option pour activer ou désactiver la fonctionnalité de cache en écriture de l'agent vers le client. |
| UsbRedirPlugin.log.logLevel | error, warn, info, debug, trace ou verbose | info | Utilisez cette option pour définir le niveau de journalisation du plug-in de redirection USB. |
| UsbRedirServer.log.logLevel | error, warn, info, debug, trace ou verbose | info | Utilisez cette option pour définir le niveau de journalisation du serveur de redirection USB. |
| viewusb.AllowAutoDeviceSplitting | {m o}: {true false} | non défini, ce qui équivaut à false | Définissez cette option pour autoriser ou interdire le fractionnement automatique de périphériques USB composites. Exemple : m:true |
| viewusb.SplitExcludeVidPid | {m o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...] | non défini | Utilisez cette option pour exclure ou inclure un périphérique USB composite spécifié du fractionnement par ID de fournisseur et par ID de produit. Le format du paramètre est vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...] . Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (*) à la place de chiffres dans un ID. Exemple : m:vid-0f0f_pid-55** |
| viewusb.SplitVidPid | {m o}: vid-xxxx_pid-yyyy([exintf:zz[;exintf:ww]])[;...] | non défini | Définissez cette option pour traiter les composants d'un périphérique USB composite spécifiés par des ID de fournisseur et de produit en tant que périphériques séparés. Le format du paramètre est vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww]) . Vous pouvez utiliser le mot-clé exintf pour exclure des composants de la redirection en spécifiant leur numéro d'interface. Vous devez spécifier les numéros d'ID au format hexadécimal et les numéros d'interface au format décimal en incluant les zéros à gauche. Vous pouvez utiliser le caractère générique (*) à la place de chiffres dans un ID. Exemple : o:vid-0f0f_pid-***([exintf-01];vid-0781_pid-554c(exintf:01;exintf:02)) Note Horizon n'inclut pas automatiquement les composants que vous n'avez pas explicitement exclus. Vous devez spécifier une stratégie de filtre telle que Inclure un périphérique VidPid pour inclure ces composants. |
| viewusb.AllowAudioIn | {m o}: {true false} | non défini, ce qui équivaut à true | Utilisez cette option pour autoriser ou interdire les périphériques d'entrée audio à rediriger. Exemple : o:false |

| Option | Valeur/Format | Valeur par défaut | Description |
|------------------------------|--------------------------------------|-------------------------------------|--|
| viewusb.AllowAudioOut | {m o}: {true false} | non défini, ce qui équivaut à false | Définissez cette option pour autoriser ou interdire la redirection de périphériques de sortie audio. |
| viewusb.AllowHIDBootable | {m o}: {true false} | non défini, ce qui équivaut à true | Utilisez cette option pour autoriser ou interdire la redirection de périphériques d'entrée, autres que des claviers et des souris, qui sont disponibles lors du démarrage, également connus sous le nom de périphériques de démarrage HID. |
| viewusb.AllowDevDescFailsafe | {m o}: {true false} | non défini, ce qui équivaut à false | Définissez cette option pour autoriser ou interdire les périphériques à rediriger même si Horizon Client ne parvient pas à obtenir les descripteurs de configuration ou de périphérique. Pour autoriser un périphérique même s'il ne parvient pas à obtenir les descripteurs de configuration ou de périphérique, incluez-le dans les filtres Include, tels que IncludeVidPid ou IncludePath . |
| viewusb.AllowKeyboardMouse | {m o}: {true false} | non défini, ce qui équivaut à false | Utilisez cette option pour autoriser ou interdire la redirection de claviers avec des périphériques de pointage intégrés (souris, trackball ou pavé tactile). |
| viewusb.AllowSmartcard | {m o}: {true false} | non défini, ce qui équivaut à false | Définissez cette option pour autoriser ou interdire les périphériques de carte à puce à rediriger. |
| viewusb.AllowVideo | {m o}: {true false} | non défini, ce qui équivaut à true | Utilisez cette option pour autoriser ou interdire les périphériques vidéo à rediriger. |
| viewusb.DisableRemoteConfig | {m o}: {true false} | non défini, ce qui équivaut à false | Définissez cette option pour désactiver ou activer l'utilisation des paramètres d'Horizon Agent lors du filtrage des périphériques USB. |
| viewusb.ExcludeAllDevices | {true false} | non défini, ce qui équivaut à false | Utilisez cette option pour exclure ou inclure tous les périphériques USB de la redirection. Si ce paramètre est défini sur true , vous pouvez utiliser d'autres paramètres de règle pour autoriser la redirection de périphériques spécifiques ou de familles de périphériques. Si ce paramètre est défini sur false , vous pouvez utiliser d'autres paramètres de règle pour empêcher la redirection de périphériques spécifiques ou de familles de périphériques. Si vous définissez la valeur de ExcludeAllDevices sur true sur Horizon Agent, et si ce paramètre est transmis à Horizon Client, le paramètre d'Horizon Agent remplace le paramètre d'Horizon Client. |

| Option | Valeur/Format | Valeur par défaut | Description |
|-----------------------|---|-------------------|---|
| viewusb.ExcludeFamily | <code>{m o}: family_name_1[; family_name_2;. ..]</code> | non défini | <p>Utilisez cette option pour exclure des familles de périphériques de la redirection. Par exemple : m:bluetooth;smart-card</p> <p>Si vous avez activé le fractionnement automatique de périphérique, Horizon examine la famille de périphériques de chaque interface d'un périphérique USB composite pour décider quelles interfaces doivent être exclues. Si vous avez désactivé le fractionnement automatique de périphérique, Horizon examine la famille de périphérique de l'ensemble du périphérique USB composite.</p> <p>Note Toutefois, les souris et les claviers sont exclus de la redirection par défaut et il n'est pas nécessaire de les exclure avec ce paramètre.</p> |
| viewusb.ExcludeVidPid | <code>{m o}:vid-xxx1_ pid-yyy1[;vid- xxx2_pid- yyy2;..]</code> | non défini | <p>Définissez cette option pour exclure des périphériques avec des ID de fournisseur et de produit spécifiés de la redirection. Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (*) à la place de chiffres dans un ID.</p> <p>Par exemple : o:vid-0781_pid- ****;vid-0561_pid-554c</p> |
| viewusb.ExcludePath | <code>{m o}:bus-x1[/ y1].../ port- z1[;bus-x2[/ y2].../port- z2;...]</code> | non défini | <p>Utilisez cette option pour exclure des périphériques dans des chemins de concentrateur ou de port spécifiés de la redirection. Vous devez spécifier des numéros de bus et de port au format hexadécimal. Vous ne pouvez pas utiliser le caractère générique dans les chemins.</p> <p>Par exemple : m:bus-1/2/3_port- 02;bus-1/1/1/4_port-ff</p> |
| viewusb.IncludeFamily | <code>{m o}:family_name_ 1[;family_name_ 2]...</code> | non défini | <p>Définissez cette option pour inclure des familles de périphériques pouvant être redirigées.</p> <p>Par exemple : o:storage; smart-card</p> |
| viewusb.IncludePath | <code>{m o}:bus-x1[/ y1].../ port- z1[;bus-x2[/ y2].../ portz2;...]</code> | non défini | <p>Utilisez cette option pour inclure des périphériques dans des chemins de concentrateur ou de port spécifiés pour être redirigés. Vous devez spécifier des numéros de bus et de port au format hexadécimal. Vous ne pouvez pas utiliser le caractère générique dans les chemins.</p> <p>Par exemple : m:bus-1/2_port- 02;bus-1/7/1/4_port-0f</p> |

| Option | Valeur/Format | Valeur par défaut | Description |
|-----------------------------------|--|-------------------|---|
| viewusb.IncludeVidPid | <code>{m o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]</code> | non défini | Définissez cette option pour inclure des périphériques avec des ID de fournisseur et de produit spécifiés pouvant être redirigés. Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (*) à la place de chiffres dans un ID. Par exemple : o:vid-***_pid-0001;vid-0561_pid-554c |
| mksVNCServer.useXExtButtonMapping | true ou false | false | Définissez cette option pour activer ou désactiver la prise en charge d'une souris pour gauchers sous SLED 11 SP3. |
| mksvhan.clipboardSize | Un entier | 1024 | Utilisez cette option pour spécifier la taille maximale du Presse-papiers pour copier et coller. |
| RemoteDisplay.maxBandwidthKbps | Un entier | 4096000 | Spécifie la bande passante maximale, en kilobits par seconde (Kbit/s), pour une session VMware Blast. La bande passante inclut la création d'images, le son, le canal virtuel et le trafic de contrôle VMware Blast. La valeur maximale est de 4 Gbit/s (4096000). |
| RemoteDisplay.maxFPS | Un entier | 60 | Spécifie le nombre maximal d'actualisations d'écran. Utilisez ce paramètre pour gérer la bande passante moyenne que les utilisateurs consomment. La valeur valide doit être entre 3 et 60. La valeur par défaut est de 60 actualisations par seconde. |
| RemoteDisplay.enableStats | true ou false | false | Active ou désactive les statistiques du protocole Blast dans le journal mks, telles que la bande passante, FPS, RTT, etc. |
| RemoteDisplay.allowH264 | true ou false | true | Définissez cette option pour activer ou désactiver le codage H.264. |
| vdpservice.log.logLevel | fatal error, warn, info, debug ou trace | info | Utilisez cette option pour définir le niveau de journalisation de vdp-service. |
| RemoteDisplay.qpmaxH264 | plage de valeurs disponible : 0 à 51 | 36 | Utilisez cette option pour définir le paramètre de quantification H264minQP, qui spécifie la meilleure qualité d'image pour l'écran distant configuré pour utiliser le codage H.264. Définissez une valeur supérieure à celle définie pour RemoteDisplay.qpminH264. |
| RemoteDisplay.qpminH264 | plage de valeurs disponible : 0 à 51 | 10 | Utilisez cette option pour définir le paramètre de quantification H264maxQP, qui spécifie la plus faible qualité d'image pour l'écran distant configuré pour utiliser le codage H.264. Définissez une valeur inférieure à celle définie pour RemoteDisplay.qpmaxH264. |
| RemoteDisplay.minQualityJPEG | plage de valeurs disponible : 1 à 100 | 25 | Spécifie la qualité d'image de l'écran de poste de travail pour le codage JPEG/PNG. Les paramètres de qualité faible sont destinés aux zones de l'écran qui changent souvent, par exemple, lors du défilement. |

| Option | Valeur/Format | Valeur par défaut | Description |
|------------------------------|---------------------------------------|-------------------|---|
| RemoteDisplay.midQualityJPEG | plage de valeurs disponible : 1 à 100 | 35 | Spécifie la qualité d'image de l'écran de poste de travail pour le codage JPEG/PNG. Utilisez cette option pour définir les paramètres de qualité moyenne de l'écran de poste de travail. |
| RemoteDisplay.maxQualityJPEG | plage de valeurs disponible : 1 à 100 | 90 | Spécifie la qualité d'image de l'écran de poste de travail pour le codage JPEG/PNG. Les paramètres de qualité élevée sont destinés aux zones de l'écran qui sont plus statiques, ce qui se traduit par une meilleure qualité d'image. |

Options de configuration dans /etc/vmware/viewagent-custom.conf

Java Standalone Agent utilise le fichier de configuration /etc/vmware/viewagent-custom.conf.

Tableau 6-2. Options de configuration dans /etc/vmware/viewagent-custom.conf

| Option | Valeur | Valeur par défaut | Description |
|---------------|---|-------------------|--|
| Sous-réseau | NULL ou adresse et masque de réseau au format d'adresse IP/CIDR | NULL | <p>S'il existe plusieurs adresses IP locales avec différents sous-réseaux, utilisez cette option pour définir le sous-réseau que l'agent Linux fournit au Serveur de connexion View.</p> <p>Lorsque plusieurs configurations de sous-réseau sont détectées sur une machine d'agent Linux, cette option est requise pour spécifier le sous-réseau correct qui doit être utilisé par l'agent Linux. Par exemple, si vous avez installé Docker sur la machine Linux, il sera introduit en tant qu'adaptateur réseau virtuel. Pour empêcher l'agent Linux d'utiliser Docker comme un adaptateur réseau virtuel, vous devez définir cette option pour utiliser l'adaptateur réseau physique réel.</p> <p>Vous devez spécifier la valeur au format d'adresse IP/CIDR. Par exemple, Sous-réseau=192.168.1.0/24.</p> <p>NULL implique que l'agent Linux sélectionne l'adresse IP de façon aléatoire.</p> |
| SSOEnable | true ou false | true | Définissez cette option pour activer/désactiver l'authentification unique (SSO). |
| SSOUserFormat | Une chaîne de texte | [username] | <p>Utilisez cette option pour spécifier le format du nom de connexion pour l'authentification unique. La valeur par défaut est le nom d'utilisateur uniquement. Définissez cette option si le nom de domaine est également requis. En général, le nom de connexion est le nom de domaine plus un caractère spécial suivi du nom d'utilisateur. Si le caractère spécial est une barre oblique inverse, vous devez l'échapper avec une autre barre oblique inverse. Exemples de formats de nom de connexion :</p> <ul style="list-style-type: none"> ■ SSOUserFormat=[domain]\\[username] ■ SSOUserFormat=[domain]+[username] ■ SSOUserFormat=[username]@[domain] |

| Option | Valeur | Valeur par défaut | Description |
|---------------------------|---------------------|---|--|
| CDREnable | true ou false | true | Définissez cette option pour activer ou désactiver la fonctionnalité de redirection du lecteur client (CDR). |
| USBEnable | true ou false | true | Définissez cette option pour activer ou désactiver la fonctionnalité de redirection USB. |
| KeyboardLayoutSync | true ou false | true | <p>Utilisez cette option pour spécifier s'il faut synchroniser ou non la liste de paramètres régionaux système et la disposition de clavier actuelle d'un client avec les postes de travail Horizon Agent for Linux.</p> <p>Lorsque ce paramètre est activé ou qu'il n'est pas configuré, la synchronisation est autorisée. Lorsque ce paramètre est désactivé, la synchronisation n'est pas autorisée.</p> <p>Cette fonctionnalité est prise en charge uniquement pour Horizon Client pour Windows et dans les langues suivantes : anglais, français, allemand, japonais, coréen, espagnol, chinois simplifié et chinois traditionnel.</p> |
| StartBlastServerTime out | Un entier | 20 | Cette option détermine la durée, en secondes, allouée au processus VMwareBlastServer pour l'initialisation. Si le processus n'est pas prêt avant la fin de cette durée, la connexion de l'utilisateur échouera. |
| SSLCiphers | Une chaîne de texte | !aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES | Utilisez cette option pour spécifier la liste de chiffrements. Vous devez utiliser le format défini dans https://www.openssl.org/docs/manmaster/man1/ciphers.html . |
| SSLProtocols | Une chaîne de texte | TLSv1_1:TLSv1_2 | Utilisez cette option pour spécifier les protocoles de sécurité. Les protocoles pris en charge sont TLSv1.0, TLSv1.1 et TLSv1.2. |
| SSLCipherServerPreference | true ou false | true | Utilisez cette option pour activer ou désactiver l'option SSL_OP_CIPHER_SERVER_PREFERENCE. Pour plus d'informations, reportez-vous à la section https://www.openssl.org/docs/manmaster/ssl/SSL_CTX_set_options.html . |
| UseGnomeFlashback | true ou false | false | <p>Cette option détermine s'il faut utiliser ou non l'environnement de poste de travail GNOME Flashback (Metacity) s'il est installé dans un système Ubuntu 14.04 ou Ubuntu 16.04. L'option prend effet que la fonctionnalité SSO soit activée ou non.</p> <p>Une fois cette option définie sur TRUE, l'environnement de poste de travail GNOME Flashback (Metacity) est toujours utilisé à la place de l'environnement de poste de travail par défaut.</p> <p>Info-bulle Pour améliorer les performances de votre système, configurez UseGnomeFlashback=TRUE après avoir installé le poste de travail GNOME Flashback (Metacity) sur votre système Ubuntu 14.04 ou Ubuntu 16.04.</p> |

| Option | Valeur | Valeur par défaut | Description |
|----------------------|-----------|-------------------|--|
| LogCnt | Un entier | -1 | Utilisez cette option pour définir le nombre de fichiers journaux réservés dans /tmp/vmware-root. <ul style="list-style-type: none"> ■ -1 : tout conserver ■ 0 : tout supprimer ■ > 0 : nombre de journaux réservés. |
| RunOnceScript | | | Utilisez cette option pour joindre la machine virtuelle clonée à AD. Après le changement du nom d'hôte, définissez le script à exécuter une fois. Le script spécifié est exécuté une seule fois après le changement du premier nom d'hôte. Le script est exécuté en tant qu'autorisation racine lorsque le service de l'agent démarre et que le nom d'hôte a été modifié après l'installation de l'agent. Par exemple, pour la solution Winbind, vous devez joindre la machine virtuelle de base à AD avec Winbind, puis définir cette option sur un chemin de script. Cela doit contenir la commande de jonction de domaine /usr/bin/net ads join -U <ADUserName>%<ADUserPassword>. Après le clone de machine virtuelle, la personnalisation du système d'exploitation modifie le nom d'hôte. Lorsque le service de l'agent démarre, le script est exécuté pour joindre la machine virtuelle clonée à AD. |
| RunOnceScriptTimeout | | 120 | Utilisez cette option pour définir le délai d'expiration en secondes de l'option RunOnceScript. Par exemple, définissez RunOnceScriptTimeout=120 |

Note Les trois options de sécurité, SSLCiphers, SSLProtocols et SSLCipherServerPreference, sont conçues pour le processus VMwareBlastServer. Lorsque le processus VMwareBlastServer démarre, Java Standalone Agent transmet ces options sous forme de paramètres. Lorsque Blast Secure Gateway (BSG) est activé, ces options affectent la connexion entre BSG et le poste de travail Linux. Lorsque BSG est désactivé, ces options affectent la connexion entre le client et le poste de travail Linux.

Exemples de paramètres Blast pour des postes de travail Linux

Vous pouvez régler la qualité d'image de l'écran de votre poste de travail distant afin d'améliorer l'expérience utilisateur. Il est utile d'améliorer la qualité d'image pour garantir une expérience utilisateur constante en cas de mauvaise connexion réseau.

Exemples de paramètres du protocole VMware Blast Extreme

VMwareBlastServer et ses plug-ins liés utilisent le fichier de configuration /etc/vmware/config.

Tableau 6-3. Exemples d'options de configuration de Blast dans /etc/vmware/config

| Nom de l'option | Paramètre | Réseau LAN haute vitesse | Réseau LAN | Réseau WAN dédié | Réseau WAN à large bande | Réseau WAN basse vitesse | Connexion très basse vitesse |
|--------------------------------|--------------------------------|--------------------------|----------------------|----------------------|--------------------------|--------------------------|------------------------------|
| Paramètres de bande passante | RemoteDisplay.maxBandwidthKbps | 1 000 000 (1 Gbit/s) | 1 000 000 (1 Gbit/s) | 1 000 000 (1 Gbit/s) | 5 000 (5 Mbit/s) | 2 000 (2 Mbit/s) | 1 000 (1 Mbit/s) |
| Image/s max. | RemoteDisplay.maxFPS | 60 | 30 | 30 | 20 | 15 | 5 |
| Lecture audio | RemoteDisplay.allowAudio | VRAI | VRAI | VRAI | VRAI | VRAI | FAUX |
| Qualité d'affichage (JPEG/PNG) | RemoteDisplay.maxQualityJPEG | 90 | 90 | 90 | 70 | 60 | 50 |
| Qualité d'affichage (JPEG/PNG) | RemoteDisplay.midQualityJPEG | 35 | 35 | 35 | 35 | 35 | 35 |
| Qualité d'affichage (JPEG/PNG) | RemoteDisplay.minQualityJPEG | 25 | 25 | 25 | 20 | 20 | 20 |
| Qualité d'affichage (H.264) | RemoteDisplay.qpmaxH264 | 28 | 36 | 36 | 36 | 36 | 42 |
| Qualité d'affichage (H.264) | RemoteDisplay.qpminH264 | 10 | 10 | 10 | 10 | 10 | 10 |

Exemples d'options de la redirection du lecteur client pour des postes de travail Linux

Configurez des options de redirection du lecteur client (CDR) pour déterminer les dossiers partagés et les lecteurs d'un système local qui sont accessibles depuis les postes de travail Linux distants.

Configurez des paramètres CDR en ajoutant des entrées au fichier /etc/vmware/config.

L'exemple de configuration suivant partage les dossiers C:\ebooks et C:\spreadsheets, met les deux dossiers en lecture seule et empêche le client de partager des dossiers supplémentaires.

```
cdserver.forcedByAdmin=true
cdserver.sharedFolders=d:\ebooks,;c:\spreadsheets,
cdserver.permissions=R
```

Dans l'exemple précédent, la virgule « , » placée après **ebooks** et **spreadsheets** est obligatoire pour une analyse correcte de l'option.

Le fait d'ajouter un **R** dans l'option `cdserver.sharedFolders` a une incidence sur tous les dossiers répertoriés dans ce paramètre. Dans l'exemple suivant, les dossiers **ebooks** et **spreadsheets** sont en lecture seule même si la valeur **R** est seulement placée après le chemin d'accès du dossier `/home/jsmith`.

```
cdserver.sharedFolders=d:\ebooks,;c:\spreadsheets,;/home/jsmith,R
```

Supprimer l'affichage de la console vSphere d'un poste de travail Linux

Lorsqu'un utilisateur se connecte à un poste de travail Linux, le poste de travail peut également être affiché dans la console vSphere pour la machine virtuelle Linux. Vous pouvez configurer des machines virtuelles Linux pour vous assurer que la console vSphere est vide lorsque des utilisateurs se connectent à leurs postes de travail.

Procédure

- ◆ Sur l'hôte ESXi, ajoutez la ligne suivante au fichier `vmx` de la machine virtuelle Linux.

```
RemoteDisplay.maxConnections = "0"
```

L'affichage de la console vSphere reste vide même lorsque vous vous connectez à la machine virtuelle lorsque la session de l'utilisateur est fermée sur le poste de travail.

Créer et gérer des pools de postes de travail Linux

7

Pour configurer des machines virtuelles Linux afin de les utiliser en tant que postes de travail distants, vous devez créer un pool de postes de travail avec des machines virtuelles Linux.

Horizon for Linux prend en charge les types de pool de postes de travail suivants :

- Pool de postes de travail manuel avec machine virtuelle vCenter
- Pool de postes de travail de clone complet automatisé

Pour créer un pool de postes de travail manuel avec une machine virtuelle vCenter, vous devez installer Horizon Agent sur toutes les machines virtuelles. Ensuite, utilisez l'assistant de création de pool de postes de travail du Serveur de connexion pour ajouter les machines virtuelles au pool de postes de travail. Pour cloner un grand nombre de machines virtuelles, consultez [Présentation du déploiement en bloc de postes de travail Linux](#).

Pour créer un pool de postes de travail de clone complet automatisé, vous devez installer Horizon Agent sur un modèle de machine virtuelle Linux. Ensuite, utilisez l'assistant de création de pool de postes de travail du Serveur de connexion pour cloner des machines virtuelles complètes.

Ce chapitre contient les rubriques suivantes :

- [Créer un pool de postes de travail manuel pour Linux](#)
- [Gérer un pool de postes de travail pour Linux](#)
- [Créer un pool de postes de travail de clone complet automatisé pour Linux](#)
- [Commandes PowerCLI Broker](#)

Créer un pool de postes de travail manuel pour Linux

Vous pouvez créer un pool de postes de travail manuel pour des machines virtuelles Linux.

Conditions préalables

- Vérifiez qu'Horizon Agent est installé sur les systèmes d'exploitation invités Linux. Reportez-vous à la section [Installer Horizon Agent sur une machine virtuelle Linux](#).
- Vérifiez que vCenter Server est ajouté au Serveur de connexion Horizon.

Procédure

- 1 Dans View Administrator, ajoutez un pool de postes de travail manuel.
Sélectionnez **Catalogue > Pools de postes de travail > Ajouter**.
- 2 Sélectionnez **Pool de postes de travail manuel**.
- 3 Sur la page Attribution d'utilisateur, sélectionnez des attributions flottantes ou dédiées pour les machines du pool de postes de travail, puis cliquez sur **Suivant**.
- 4 Sur la page Source de machines, sélectionnez **Machines virtuelles vCenter**, puis cliquez sur **Suivant**.
- 5 Sur la page vCenter Server, sélectionnez le serveur vCenter approprié, puis cliquez sur **Suivant**.
- 6 Entrez l'**ID de pool de postes de travail**.
- 7 Sur la page Paramètres de pool de postes de travail, définissez les options suivantes.

| Option | Description |
|---|--|
| Protocole d'affichage par défaut | VMware Blast |
| Autoriser les utilisateurs à choisir un protocole | Non |
| Convertisseur 3D | Gérer à l'aide de vSphere Client pour les postes de travail 2D, vSGA ou vDGA, et de NVIDIA GRID vGPU pour les postes de travail vGPU |

Note Les paramètres du pool sont obligatoires. Sinon, vous risquez de ne pas pouvoir vous connecter au poste de travail et d'obtenir une erreur de protocole ou un écran noir.

- 8 Sur la page Ajouter des machines virtuelles vCenter, sélectionnez la machine virtuelle Linux. Cliquez sur **Ajouter**, puis sur **Suivant**.

Note Ne créez pas des machines virtuelles Windows et Linux dans le même pool de postes de travail.

- 9 Suivez les invites pour finaliser la procédure.

Autorisez des utilisateurs sur les machines dans le pool de postes de travail. Dans View Administrator, sélectionnez le pool de postes de travail, puis **Droits > Ajouter un droit** et ajoutez des utilisateurs ou des groupes.

Les machines virtuelles Linux sont prêtes à être utilisées en tant que postes de travail distants dans un déploiement d'Horizon 7.

Gérer un pool de postes de travail pour Linux

Lorsque vous créez un pool de postes de travail manuel et que vous ajoutez des machines Linux au pool, vous pouvez gérer les pools de postes de travail manuels en configurant les paramètres. Vous devez ajouter uniquement des systèmes d'exploitation invités Linux au pool de postes de travail manuel. Si le

pool contient des systèmes d'exploitation invités Windows et Linux, le pool est traité comme un pool Windows et vous ne pourrez pas vous connecter aux postes de travail Linux.

Prise en charge des opérations de gestion

- Désactiver ou activer un pool de postes de travail
- Cloner un pool de postes de travail automatisé
- Supprimer le pool de postes de travail

Vous pouvez soit supprimer les machines virtuelles de View Manager, soit supprimer les machines virtuelles du disque

Prise en charge des paramètres distants

Tableau 7-1. Paramètres distants

| Paramètre distant | Options |
|---|---|
| Stratégie d'alimentation de machine distante | <ul style="list-style-type: none"> ■ Ne prendre aucune action d'alimentation ■ S'assurer que les machines sont toujours sous tension ■ Interrompre ■ Désactiver |
| Fermeture de session automatique après la déconnexion | <ul style="list-style-type: none"> ■ Immédiatement ■ Jamais ■ Après n minutes |
| Autoriser les utilisateurs à réinitialiser/redémarrer leurs machines | <ul style="list-style-type: none"> ■ Oui ■ Non |
| Autoriser l'utilisateur à ouvrir des sessions séparées depuis différents périphériques clients | <ul style="list-style-type: none"> ■ Oui ■ Non |
| « Supprimer la machine après la fermeture de session » pour un pool de postes de travail automatisé avec un clone complet et flottant | <ul style="list-style-type: none"> ■ Oui ■ Non |

Prise en charge des opérations de View Administrator

- Déconnecter la session
- Fermer la session
- Réinitialiser/redémarrer un poste de travail
- Envoyer un message

Pour les pools de postes de travail dédiés, vous pouvez ajouter ou supprimer des attributions d'utilisateur pour chaque machine virtuelle. Pour un nombre important d'opérations, vous devez utiliser les cmdlets View PowerCLI.

- Update-UserOwnership

■ Remove-UserOwnership

Note Ne modifiez pas les paramètres **Protocole d'affichage distant**. Ce paramètre doit toujours être le même que la création du pool de postes de travail.

| Paramètre | Option |
|--|--|
| Protocole d'affichage par défaut | VMware Blast |
| Autoriser l'utilisateur à choisir un protocole | Non |
| Convertisseur 3D | <ul style="list-style-type: none"> ■ Gérer à l'aide de vSphere Client pour 2D, vSGA ou vDGA ■ NVIDIA GRID vGPU |

Pour plus d'informations, consultez le guide *Administration de View*.

Créer un pool de postes de travail de clone complet automatisé pour Linux

Vous pouvez créer un pool de postes de travail de clone complet automatisé pour des machines virtuelles Linux. Une fois que vous avez créé le pool de postes de travail de clone complet automatisé, vous pouvez utiliser les machines virtuelles Linux en tant que postes de travail distants dans un déploiement d'Horizon 7.

Conditions préalables

- Vérifiez qu'Horizon Agent est installé sur les systèmes d'exploitation invités Linux. Reportez-vous à la section [Installer Horizon Agent sur une machine virtuelle Linux](#).
- Si vous utilisez la solution Winbind pour joindre la machine virtuelle Linux à Active Directory, vous devez terminer la configuration de la solution Winbind dans le modèle de machine virtuelle.
- Si vous utilisez la solution Winbind, vous devez exécuter la commande de jonction de domaine sur la machine virtuelle. Incluez la commande dans un script shell et spécifiez le chemin du script à l'option RunOnceScript d'Horizon Agent dans `/etc/vmware/viewagent-custom.conf`. Pour plus d'informations, reportez-vous à la section [Définir des options dans des fichiers de configuration sur un poste de travail Linux](#).
- Vérifiez que vCenter Server est ajouté au Serveur de connexion Horizon.

Procédure

- 1 Créer une spécification de personnalisation de l'invité.

Reportez-vous à la section « Créer une spécification de personnalisation pour Linux dans vSphere Web Client » dans le document *Administration d'une machine virtuelle vSphere*. Lorsque vous créez la spécification, assurez-vous de spécifier les paramètres suivants correctement.

| Paramètre | Valeur |
|-------------------------------|--|
| SE de machine virtuelle cible | Linux |
| Nom de l'ordinateur | Utilisez le nom de la machine virtuelle. |

| Paramètre | Valeur |
|-------------------|---|
| Domaine | Spécifiez le domaine de l'environnement View. |
| Paramètres réseau | Utilisez les paramètres réseau standard. |
| DNS principal | Spécifiez une adresse valide. |

Note Pour plus d'informations sur la matrice de prise en charge de la personnalisation du système d'exploitation invité, consultez <http://partnerweb.vmware.com/programs/guestOS/guest-os-customization-matrix.pdf>.

- 2 Dans Horizon Administrator, sélectionnez **Catalogue > Pools de postes de travail > Ajouter**.
- 3 Sélectionnez **Pool de postes de travail automatisé** et cliquez sur **Suivant**.
- 4 Sélectionnez des affectations d'utilisateur dédiées ou flottantes pour les machines dans le pool de postes de travail et cliquez sur **Suivant**.
- 5 Sur la page vCenter Server, sélectionnez **Machines virtuelles complètes**, puis le serveur vCenter approprié et cliquez sur **Suivant**.
- 6 Sur la page Identification du pool de postes de travail, entrez l'ID de pool de postes de travail et cliquez sur **Suivant**.
- 7 Sur la page Paramètres du pool de postes de travail, définissez les options suivantes et cliquez sur **Suivant**.

| Option | Description |
|---|--|
| Protocole d'affichage par défaut | VMware Blast |
| Autoriser les utilisateurs à choisir un protocole | Non |
| Convertisseur 3D | Gérer à l'aide de vSphere Client pour les postes de travail 2D, vSGA ou vDGA, et de NVIDIA GRID vGPU pour les postes de travail vGPU |

Note Les paramètres du pool sont obligatoires. Sinon, vous risquez de ne pas pouvoir vous connecter au poste de travail et d'obtenir une erreur de protocole ou un écran noir.

- 8 Sur la page Paramètres d'approvisionnement, définissez les options **Attribution de nom aux machines virtuelles** et cliquez sur **Suivant**.

| Option | Description |
|---------------------------------------|--|
| Spécifier des noms manuellement | Entrez des noms manuellement. |
| Utiliser un mode d'attribution de nom | <p>Par exemple, spécifiez LinuxVM-{n}.</p> <p>Vous devez également spécifier les options de dimensionnement du pool de postes de travail suivantes :</p> <ul style="list-style-type: none"> ■ Nombre maximal de machines ■ Nombre de machines de rechange sous tension |

- 9 Sur la page Optimisation du stockage, sélectionnez une stratégie de gestion du stockage et cliquez sur **Suivant**.
- 10 Sur la page Paramètres de vCenter, vous devez cliquer sur Parcourir, sélectionner les paramètres de vCenter Server en séquence et cliquer sur **Suivant**.
Vous ne pouvez pas ignorer un paramètre de vCenter Server :
 - a Modèle
 - b Emplacement du dossier de machine virtuelle
 - c Host or cluster (Hôte ou cluster)
 - d Resource pool (Pool de ressources)
 - e Magasins de données
- 11 Sur la page Options de stockage avancées, sélectionnez les options de stockage appropriées et cliquez sur **Suivant**.
- 12 Sur la page Personnalisation invité, sélectionnez votre personnalisation d'invité pour Linux et cliquez sur **Suivant**.
- 13 Sur la page Prêt à terminer, examinez les détails et sélectionnez **Autoriser les utilisateurs quand cet assistant a terminé**.
- 14 Cliquez sur **Terminer**.
- 15 Pour autoriser les utilisateurs sur les machines dans le pool de postes de travail, sélectionnez le pool de postes de travail, cliquez sur **Droits > Ajouter des droits** et ajoutez les utilisateurs et les groupes.
- 16 Attendez que toutes les machines virtuelles Linux du pool de postes de travail soient disponibles.

Commandes PowerCLI Broker

Les cmdlets View PowerCLI, qui permettent d'effectuer de nombreuses tâches administratives sur le Serveur de connexion et les postes de travail Windows, peuvent également fonctionner pour les postes de travail Linux.

Créer un pool de postes de travail manuel

```
Add-ManualPool -DefaultProtocol Blast -AllowProtocolOverride $false -threadRender usevc|vgpu -
Pool_id <pool id> [more parameters]
```

Pour les postes de travail Linux, les options et valeurs suivantes sont obligatoires.

- DefaultProtocol Blast
- AllowProtocolOverride \$false
- threadRender usevc|vgpu. Pour les postes de travail vGPU, utilisez -threadRender vgpu. Pour les postes de travail 2D/vSGA/vDGA, utilisez -threadRender usevc.

Exemples

- Création d'un pool de postes de travail Linux flottant nommé LinuxDesktop avec une machine virtuelle, LinuxVM-01.

```
Add-ManualPool -DefaultProtocol Blast -AllowProtocolOverride $false -threadRender usevc -Pool_id
LinuxDesktop -Id (Get-DesktopVM -Name LinuxVM-01).id -Persistence NonPersistent -Vc_name
myvc.myorg.org
```

- Création d'un pool de postes de travail vGPU Linux dédié nommé LinuxDesktop avec toutes les machines virtuelles dont le nom commence par LinuxVM-.

```
Get-DesktopVM | Where-Object {$_.Name.StartsWith("LinuxVM-")} | Add-ManualPool -DefaultProtocol
Blast -AllowProtocolOverride $false -Persistence Persistent -threadRender vgpu -Pool_id
LinuxDesktop
```

- Création d'un pool de postes de travail Linux flottant LinuxDesktop avec la première machine virtuelle RHEL 6 x64.

```
Get-DesktopVM | Where-Object {$_.GuestID -eq "rhel6_64Guest"} | Select-Object -Index 0 | Add-
ManualPool -DefaultProtocol Blast -AllowProtocolOverride $false -Persistence NonPersistent -
threadRender usevc -Pool_id LinuxDesktop
```

Créer un pool de postes de travail automatisé de clone complet

```
Add-AutomaticPool -DefaultProtocol Blast -AllowProtocolOverride $false -threadRender usevc|vgpu `
-Pool_id <pool id> -Vc_id <vCenter id> `
-NamePrefix <VM Name Prefix> `
-templatePath <Virtual Machine Template Path> `
-VmFolderPath <Virtual Machine Folder Path> `
-ResourcePoolPath <Resource Pool Path> `
-dataStorePaths <Datastore Path> `
-customizationSpecName <Customization Specification Name> `
[more parameters]
```

Pour les postes de travail Linux, les options et valeurs suivantes sont obligatoires.

- DefaultProtocol Blast
- AllowProtocolOverride \$false
- threadRender usevc|vgpu. Pour les postes de travail vGPU, utilisez -threadRender vgpu. Pour les postes de travail 2D/vSGA, utilisez -threadRender usevc.

Exemple

```
Add-AutomaticPool -DefaultProtocol Blast -AllowProtocolOverride $false -threadrender usevc `
-pool_id FullClone-Linux `
-Vc_id (Get-ViewVC -serverName myvc.myorg.org).vc_id `
-NamePrefix "FullClone-{n:fixed=3}" `
-Persistence NonPersistent -deletePolicy DeleteOnUse `
-VmFolderPath "/LinuxVDI/vm/FullClone" `
-ResourcePoolPath "/LinuxVDI/host/LinuxVDICluster/Resources" `
```

```
-templatePath "/LinuxVDI/vm/LinuxTemplate" `
-dataStorePaths "/LinuxVDI/host/LinuxVDICluster/datastore" `
-customizationSpecName "linux-spec" `
-maximumCount 100
```

Ajouter ou supprimer un droit de pool de postes de travail

- Autoriser le groupe d'utilisateurs du domaine mydomain.org à accéder à LinuxDesktop.

```
Add-PoolEntitlement -Pool_id LinuxDesktop -Sid (Get-User -Name "domain user" -Domain
"mydomain.org").sid
```

- Supprimer le droit d'accès du groupe d'utilisateurs du domaine mydomain.org à LinuxDesktop.

```
Remove-PoolEntitlement -Pool_id LinuxDesktop -Sid (Get-User -Name "domain user" -Domain
"mydomain.org").sid
```

Attribuer ou supprimer un utilisateur de la machine virtuelle dans le pool de postes de travail dédié

- Attribuer un utilisateur myuser à une machine virtuelle LinuxVM-01 qui se trouve dans un pool de postes de travail dédié.

```
Update-UserOwnership -Machine_id (Get-DesktopVM -Name "LinuxVM-01").machine_id -Sid (Get-User -
Name "myuser" | Where-Object {$_.cn -eq "myuser"}).sid
```

- Supprimer un utilisateur myuser d'une machine virtuelle LinuxVM-01 qui se trouve dans un pool de postes de travail dédié.

```
Remove-UserOwnership -Machine_id (Get-DesktopVM -Name "LinuxVM-01").machine_id
```

Fermer la session de connexion du poste de travail

- Fermer la session du poste de travail de myuser.

```
Get-RemoteSession -Username "mydomain.org\myuser" | Send-SessionLogoff
```

Pour plus d'informations sur les cmdlets View PowerCLI Broker, reportez-vous à la section Utilisation de View PowerCLI dans *Intégration de View*.

Déploiement en bloc de pools de postes de travail manuels

Horizon 7



Avec View Administrator, vous pouvez créer un pool de machines de poste de travail Windows, mais pas Linux, automatiquement. Toutefois, vous pouvez développer des scripts qui automatisent le déploiement d'un pool de machines de poste de travail Linux.

Les exemples de scripts sont fournis uniquement à titre d'illustration. VMware n'assume aucune responsabilité quant aux problèmes découlant de l'utilisation des exemples de scripts.

Ce chapitre contient les rubriques suivantes :

- [Présentation du déploiement en bloc de postes de travail Linux](#)
- [Présentation de la mise à niveau en bloc de postes de travail Linux](#)
- [Créer un modèle de machine virtuelle pour cloner des machines de poste de travail Linux](#)
- [Fichier d'entrée des exemples de scripts PowerCLI pour déployer des postes de travail Linux](#)
- [Exemple de script pour cloner des machines virtuelles Linux](#)
- [Exemple de script pour joindre des machines virtuelles clonées à un domaine AD](#)
- [Exemple de script pour joindre des machines virtuelles clonées à un domaine AD avec SSH](#)
- [Exemple de script pour télécharger des fichiers de configuration sur des machines virtuelles Linux](#)
- [Exemple de script pour télécharger des fichiers de configuration sur des machines virtuelles Linux avec SSH](#)
- [Exemple de script pour mettre à niveau Horizon Agent sur des machines de poste de travail Linux](#)
- [Exemple de script pour mettre à niveau Horizon Agent sur des machines virtuelles Linux avec SSH](#)
- [Exemple de script pour effectuer des opérations sur des machines virtuelles Linux](#)

Présentation du déploiement en bloc de postes de travail Linux

Le déploiement de postes de travail Linux manuels implique plusieurs étapes. Si vous prévoyez de déployer un grand nombre de postes de travail, vous pouvez automatiser certaines étapes à l'aide de scripts PowerCLI.

Pour certaines opérations, vous pouvez choisir de demander à PowerCLI ou SSH d'exécuter les commandes sur la machine Linux. Le tableau suivant décrit les différences entre les deux approches.

| PowerCLI | SSH |
|--|---|
| Pas besoin d'installer d'outils supplémentaires. | <ul style="list-style-type: none"> Pour Ubuntu, vous devez installer le serveur SSH avec la commande <code>sudo apt-get install openssh-server</code>. Pour RHEL et CentOS, openssh-server est installé par défaut, mais vous devez vous assurer que les paramètres du pare-feu autorisent ssh. Nécessité de télécharger les applications clients SSH <code>pscp.exe</code> et <code>plink.exe</code> et de les placer dans le même dossier que les scripts PowerCLI. |
| Le téléchargement des fichiers et l'exécution des commandes sont plus lents. | Le téléchargement des fichiers et l'exécution des commandes sont plus rapides. |
| Nécessité de fournir les informations d'identification d'administrateur de l'hôte ESXi. | Pas besoin de fournir les informations d'identification d'administrateur de l'hôte ESXi. |
| Impossible de gérer les caractères spéciaux dans le mot de passe de l'administrateur lors de l'exécution du script pour installer Horizon Agent ou dans le mot de passe de l'utilisateur AD lors de l'exécution du script pour joindre le domaine. | Possible de gérer les caractères spéciaux dans le mot de passe de l'administrateur lors de l'exécution du script pour installer Horizon Agent ou dans le mot de passe de l'utilisateur AD lors de l'exécution du script pour joindre le domaine. |

Note Les scripts PowerCLI et SSH peuvent gérer les caractères spéciaux dans les mots de passe pour l'administrateur de vCenter Server et pour l'administrateur Linux. Les scripts PowerCLI peuvent également gérer les caractères spéciaux dans le mot de passe de l'administrateur de l'hôte ESXi. Dans tous ces cas, aucun caractère d'échappement n'est nécessaire.

Pour plus d'informations sur vSphere PowerCLI, reportez-vous à la section <https://www.vmware.com/support/developer/PowerCLI>.

Le processus de déploiement en bloc d'un pool de postes de travail Linux implique les étapes suivantes :

- 1 Créez un modèle de machine virtuelle et installez Horizon Agent sur la machine virtuelle.
Reportez-vous à la section [Créer un modèle de machine virtuelle pour cloner des machines de poste de travail Linux](#).
- 2 Créer une spécification de personnalisation de l'invité.
Reportez-vous à la section « Créer une spécification de personnalisation pour Linux dans vSphere Web Client » dans le document *Administration d'une machine virtuelle vSphere*. Lorsque vous créez la spécification, assurez-vous de spécifier les paramètres suivants correctement.

| Paramètre | Valeur |
|-------------------------------|---|
| SE de machine virtuelle cible | Linux |
| Nom de l'ordinateur | Utilisez le nom de la machine virtuelle. |
| Domaine | Spécifiez le domaine de l'environnement View. |

| Paramètre | Valeur |
|-------------------|--|
| Paramètres réseau | Utilisez les paramètres réseau standard. |
| DNS principal | Spécifiez une adresse valide. |

Note Pour plus d'informations sur la matrice de prise en charge de la personnalisation du système d'exploitation invité, consultez <http://partnerweb.vmware.com/programs/guestOS/guest-os-customization-matrix.pdf>.

3 Clonez des machines virtuelles.

Reportez-vous à la section [Exemple de script pour cloner des machines virtuelles Linux](#).

4 Joignez les machines virtuelles clonées au domaine Active Directory (AD) si vous utilisez la solution Winbind. Vous pouvez exécuter la commande de jonction de domaine avec les scripts d'exemple ci-dessous ou utiliser l'option RunOnceScript dans /etc/vmware/viewagent-custom.conf, configurée dans la machine virtuelle modèle.

Reportez-vous à la section [Exemple de script pour joindre des machines virtuelles clonées à un domaine AD](#) ou [Exemple de script pour joindre des machines virtuelles clonées à un domaine AD avec SSH](#).

5 Mettez à jour les options de configuration dans les machines virtuelles.

Reportez-vous à la section [Exemple de script pour télécharger des fichiers de configuration sur des machines virtuelles Linux](#) ou [Exemple de script pour télécharger des fichiers de configuration sur des machines virtuelles Linux avec SSH](#).

6 Créez un pool de postes de travail.

Reportez-vous à la section [Créer un pool de postes de travail manuel pour Linux](#).

Pour voir un exemple de script qui effectue des opérations telles que la mise sous tension, l'arrêt, le redémarrage ou la suppression de machines virtuelles, reportez-vous à la section [Exemple de script pour effectuer des opérations sur des machines virtuelles Linux](#). Ce script peut supprimer des machines virtuelles de vCenter Server.

Présentation de la mise à niveau en bloc de postes de travail Linux

La mise à niveau en bloc de postes de travail Linux manuels implique plusieurs étapes. Vous pouvez automatiser certaines étapes à l'aide de scripts PowerCLI.

Mise à niveau en bloc d'un poste de travail non géré

Pour réaliser une mise à niveau en bloc de la machine virtuelle non gérée vers une machine virtuelle gérée ou non gérée, vous devez utiliser l'exemple de script de mise à niveau pour charger le nouvel Horizon Agent sur les machines virtuelles existantes, puis exécuter la commande de mise à niveau.

- Si vous conservez la machine virtuelle non gérée, il se peut que votre pool de postes de travail existant soit réutilisé.

- Si vous effectuez une mise à niveau depuis une machine virtuelle non gérée vers une machine virtuelle gérée, vous devez supprimer le pool de postes de travail existant et créer un nouveau pool de postes de travail. Pour plus d'informations, reportez-vous à la section [Mettre à niveau Horizon Agent sur une machine virtuelle Linux](#).

Mise à niveau en bloc d'un poste de travail géré

Pour réaliser une mise à niveau en bloc de la machine virtuelle gérée, sélectionnez une des méthodes suivantes.

| Méthode | Description |
|--|--|
| Dans la machine virtuelle modèle, installez ou mettez à niveau le nouvel Horizon Agent et créez un snapshot. | <ul style="list-style-type: none"> ■ Le profil et les données utilisateur sont perdus puisque les machines virtuelles existantes sont supprimées, sauf si le profil et les données utilisateur se trouvent sur le serveur de partage tel que le serveur NFS. ■ Après le remplacement de la machine virtuelle, il se peut que l'état de la machine virtuelle sur View Administrator soit manquant. Vous devez redémarrer le service Broker pour corriger ce problème. ■ Si vous utilisez un clone lié, cette méthode permet d'éviter la duplication de données sur chaque machine virtuelle. |
| Utilisez l'exemple de script de mise à niveau pour charger le nouvel Horizon Agent sur les machines virtuelles existantes, puis exécutez la commande de mise à niveau. | <ul style="list-style-type: none"> ■ Le profil et les données utilisateur sont conservés. ■ Si vous utilisez un clone lié, cette méthode introduit la duplication de données sur chaque machine virtuelle. |

Créer un modèle de machine virtuelle pour cloner des machines de poste de travail Linux

Avant d'effectuer le clonage d'une machine virtuelle, vous devez créer un modèle de machine virtuelle sur lequel les clones sont basés.

Conditions préalables

- Vérifiez que votre déploiement répond aux exigences pour prendre en charge les postes de travail Linux. Reportez-vous à la section [Configuration système requise pour Horizon 7 for Linux](#).
- Familiarisez-vous avec les étapes de création de machines virtuelles dans vCenter Server et d'installation de systèmes d'exploitation invités. Reportez-vous à la section « Création et préparation de machines virtuelles » dans le document *Configuration des postes de travail virtuels dans Horizon 7*.
- Familiarisez-vous avec les valeurs de mémoire vidéo recommandée (vRAM) pour les écrans que vous utiliserez avec la machine virtuelle. Reportez-vous à la section [Configuration système requise pour Horizon 7 for Linux](#).
- Familiarisez-vous avec les étapes de l'intégration AD. Reportez-vous à la section [Chapitre 3 Configuration de l'intégration Active Directory pour les postes de travail Linux](#).

- Familiarisez-vous avec les étapes d'installation d'Horizon Agent sur Linux. Consultez le chapitre « Installation d'Horizon Agent et gestion des postes de travail Linux ».
- Si nécessaire, familiarisez-vous avec les étapes de configuration des options à l'aide des fichiers de configuration de View. Reportez-vous à la section [Chapitre 6 Options de configuration pour les postes de travail Linux](#).
- Si vous prévoyez de configurer des graphiques, familiarisez-vous avec les étapes. Reportez-vous à la section [Chapitre 4 Configuration des graphiques pour les postes de travail Linux](#).

Procédure

- 1 Dans vSphere Web Client ou vSphere Client, créez une machine virtuelle.
- 2 Configurez des options de configuration personnalisées.
 - a Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur **Modifier les paramètres**.
 - b Spécifiez le nombre de vCPU et la taille de la mémoire virtuelle.

 Pour les valeurs recommandées, suivez les instructions dans le guide d'installation de votre distribution Linux.

 Par exemple, Ubuntu 12.04 recommande de configurer 2 048 Mo de mémoire virtuelle et 2 vCPU.
 - c Sélectionnez **Carte vidéo** et spécifiez le nombre d'écrans et la mémoire vidéo (vRAM) totale.

 Réglez la taille vRAM dans vSphere Web Client pour les machines virtuelles utilisant 2D ou vSGA, qui utilisent le pilote VMware. La taille vRAM n'a aucun effet sur les machines vDGA ou NVIDIA GRID vGPU, qui utilisent des pilotes NVIDIA.

 Pour les valeurs recommandées, suivez les instructions dans *Configuration système requise pour Horizon 7 for Linux*. N'utilisez pas le Calculateur de mémoire vidéo.
- 3 Mettez la machine virtuelle sous tension et installez la distribution Linux.
- 4 Créez un utilisateur avec des privilèges root, par exemple, ViewUser. Cet utilisateur est utilisé pour installer et désinstaller Horizon Agent uniquement.
- 5 Modifiez `/etc/sudoers` et ajoutez la ligne `ViewUser ALL=(ALL) NOPASSWD:ALL`.

 Avec cette ligne dans `/etc/sudoers`, aucun mot de passe n'est requis pour exécuter `sudo` en tant que ViewUser. Lorsque vous exécutez l'exemple de script pour installer Horizon Agent qui est fourni dans ce chapitre, vous spécifiez ViewUser comme entrée.
- 6 Si la distribution Linux est RHEL, CentOS ou NeoKylin, modifiez `/etc/sudoers` et commentez les lignes suivantes :


```
Defaults requiretty
Defaults !visiblepw
```
- 7 Si la distribution Linux n'est pas RHEL 7, CentOS 7, SLED 12 ou SLES 12, installez VMware Tools. Open VM Tools est installé par défaut sur RHEL 7, CentOS 7, SLED 12 et SLES 12.

- 8 Si la distribution Linux est RHEL 7, CentOS 7 ou SLED 12, installez le plug-in deployPkg.
Les instructions sont disponibles à l'adresse <http://kb.vmware.com/kb/2075048>.
- 9 Pour RHEL et CentOS, activez le paramètre de connexion réseau **Se connecter automatiquement**.
- 10 Exécutez les tâches d'intégration AD.
- 11 Exécutez les étapes pour configurer des graphiques.
- 12 Installer Horizon Agent

```
sudo ./install_viewagent.sh -A yes
```

- 13 Exécutez des configurations supplémentaires à l'aide des fichiers de configuration de View.
- 14 Arrêtez la machine virtuelle et créez un snapshot.

Fichier d'entrée des exemples de scripts PowerCLI pour déployer des postes de travail Linux

Les exemples de scripts PowerCLI pour déployer des postes de travail Linux lisent un fichier d'entrée unique qui contient des informations sur les machines de poste de travail.

Le type du fichier d'entrée est csv et il contient les informations suivantes :

- Nom de la machine virtuelle de poste de travail
- Nom de la machine virtuelle parente
- Spécification de personnalisation de l'invité
- Magasin de données où réside la machine de poste de travail clonée
- Serveur ESXi qui héberge la machine de poste de travail
- Snapshot de la machine virtuelle parente utilisé pour le clonage
- Indicateur précisant s'il faut supprimer la machine virtuelle de poste de travail si elle existe

L'exemple suivant montre ce que le fichier d'entrée peut contenir.

```
VMName,Parentvm,CustomSpec,Datastore,Host,FromSnapshot,DeleteIfPresent  
linux-001,Ubuntu1204x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE  
linux-002,Ubuntu1204x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE  
linux-003,Ubuntu1204x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE  
linux-004,Ubuntu1204x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE  
linux-005,Ubuntu1204x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
```

Les exemples de scripts supposent que le nom de ce fichier d'entrée est CloneVMs.csv et que le fichier se trouve dans le même dossier que les scripts.

Exemple de script pour cloner des machines virtuelles Linux

Vous pouvez personnaliser et utiliser l'exemple de script suivant pour cloner plusieurs machines virtuelles (VM).

Pour copier et coller le contenu du script sans saut de page, utilisez la version HTML de cette rubrique, disponible sur la page de documentation d'Horizon 7 à l'adresse https://www.vmware.com/support/pubs/view_pubs.html.

Entrée du script

Ce script lit un fichier d'entrée, qui est décrit dans la section [Fichier d'entrée des exemples de scripts PowerCLI pour déployer des postes de travail Linux](#). Ce script demande également de façon interactive les informations suivantes :

- Adresse IP de vCenter Server
- Nom de connexion de l'administrateur pour vCenter Server
- Mot de passe de l'administrateur pour vCenter Server
- Type de clone, pouvant être lié ou complet
- S'il faut désactiver la console VM vSphere

Contenu du script

```
<#
Create Clones from a Master VM

The Tool supports creation of Full clone and linked clone from Master VM.
The parent VM is required for the linked-clone to work and the parent VMs file cannot be renamed or
moved.
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }
}
```

```

    [Console]::ResetColor()
    return $input
}

function IsVMExists ()
{
    Param($VMExists)
    Write-Host "Checking if the VM $VMExists already Exists"
    [bool]$Exists = $false

    #Get all VMS and check if the VMs is already present in VC
    $listvm = Get-vm
    foreach ($lvm in $listvm)
    {
        if($VMExists -eq $lvm.Name )
        {
            $Exists = $true
        }
    }
    return $Exists
}

function Disable_VM_Console()
{
    Param($VMToDisableConsole)
    $vmConfigSpec = New-Object VMware.Vim.VirtualMachineConfigSpec
    $extra = New-Object VMware.Vim.optionvalue
    $extra.Key="RemoteDisplay.maxConnections"
    $extra.Value="0"
    $vmConfigSpec.extraconfig += $extra
    $vm = Get-VM $VMToDisableConsole | Get-View
    $vm.ReconfigVM($vmConfigSpec)
}

function Delete_VM()
{
    Param($VMToDelete)
    Write-Host "Deleting VM $VMToDelete"
    Get-VM $VMToDelete | where { $_.PowerState -eq "PoweredOn" } | Stop-VM -confirm:$false
    Get-VM $VMToDelete | Remove-VM -DeleteFromDisk -confirm:$false
}

#----- Main Script -----

SvcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
SvcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
SvcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
$cloneType = GetInput -prompt 'Clone Type ("linked" or "full")' -IsPassword $false
$disableVMConsole = GetInput -prompt 'Disable vSphere VM Console ("yes" or "no", recommend "yes")' -
IsPassword $false
"-----"
$csvFile = '.\CloneVMs.csv'

# Check that user passed only linked or full clone

```

```

if (($CloneType.length >0) -and ($CloneType -ne "linked" -or $CloneType -ne "full"))
{
    write-host -ForegroundColor Red "Clone type supports only 'linked' or 'full' (case sensitive)"
    exit
}
if (($disableVMConsole.length >0) -and ($disableVMConsole -ne "yes" -or $disableVMConsole -ne "no"))
{
    write-host -ForegroundColor Red "Disable vSphere VM Console supports only 'yes' or 'no' (case sensitive)"
    exit
}

#check if file exists
if (!(Test-Path $csvFile))
{
    write-host -ForegroundColor Red "CSV File $CSVFile not found"
    exit
}

# Connect to the VC (Parameterize VC)
#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile
#$csvData = Import-CSV $csvFile -
header("VMName","Parentvm","CustomSpec","Datastore","Host","FromSnapshot","DeleteIfPresent")
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $destVMName=$line.VMName
    $srcVM = $line.Parentvm
    $cSpec = $line.CustomSpec
    $targetDSName = $line.Datastore
    $destHost = $line.Host
    $srcSnapshot = $line.FromSnapshot
    $deleteExisting = $line.DeleteIfPresent
    if (IsVMExists ($destVMName))
    {
        Write-Host "VM $destVMName Already Exists in VC $vcAddress"
        if($deleteExisting -eq "TRUE")
        {
            Delete_VM ($destVMName)
        }
    }
}

```



```

    }
    else
    {
        Write-Host "Skip clone for $destVMName"
        continue
    }
}
$vm = get-vm $srcvm -ErrorAction Stop | get-view -ErrorAction Stop
$cloneSpec = new-object VMware.VIM.VirtualMachineCloneSpec
$cloneSpec.Location = new-object VMware.VIM.VirtualMachineRelocateSpec
if ($CloneType -eq "linked")
{
    $cloneSpec.Location.DiskMoveType =
[VMware.VIM.VirtualMachineRelocateDiskMoveOptions]::createNewChildDiskBacking
}
Write-Host "Using Datastore $targetDSName"
$newDS = Get-Datastore $targetDSName | Get-View
$cloneSpec.Location.Datastore = $newDS.summary.Datastore
Set-VM -vm $srcVM -snapshot (Get-Snapshot -vm $srcVM -Name $srcSnapshot) -confirm:$false
$cloneSpec.Snapshot = $vm.Snapshot.CurrentSnapshot
$cloneSpec.Location.Host = (get-vmhost -Name $destHost).Extensiondata.MoRef
$cloneSpec.Location.Pool = (Get-ResourcePool -Name Resources -Location (Get-VMHost -Name
$destHost)).Extensiondata.MoRef
# Start the Clone task using the above parameters
$task = $vm.CloneVM_Task($vm.parent, $destVMName, $cloneSpec)
# Get the task object
$task = Get-Task | where { $_.id -eq $task }
#Wait for the taks to Complete
Wait-Task -Task $task

$newvm = Get-vm $destVMName
$customSpec = Get-OSCustomizationSpec $cSpec
Set-vm -OSCustomizationSpec $cSpec -vm $newvm -confirm:$false
if ($disableVMConsole -eq "yes")
{
    Disable_VM_Console($destVMName)
}
# Start the VM
Start-VM $newvm
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

Exécution du script

Les messages suivants proviennent d'une exécution du script :

```

PowerCLI C:\scripts> .\CloneVMs.ps1
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
Clone Type<"linked" or "Full"> : linked
Disable vSphere VM Console ("yes" or "no", recommend "yes") : yes

```

La durée du clonage dépend du nombre de machines de poste de travail et peut aller de plusieurs minutes à plusieurs heures. Pour vérifier que le processus est terminé, dans vSphere Client, assurez-vous que la dernière machine virtuelle de poste de travail est mise sous tension, qu'elle dispose de son propre nom d'hôte unique et que VMware Tools est exécuté.

Exemple de script pour joindre des machines virtuelles clonées à un domaine AD

Vous pouvez personnaliser et utiliser l'exemple de script suivant pour joindre des machines virtuelles (VM) clonées à un domaine Active Directory (AD).

Vous devez exécuter ce script si vous utilisez la solution Winbind pour l'intégration AD, car l'étape de jonction du domaine échouera pour les VM clonées. Ce script exécute une commande pour joindre le domaine sur chaque VM. Vous n'avez pas besoin d'exécuter ce script si vous utilisez la solution OpenLDAP.

Pour copier et coller le contenu du script sans saut de page, utilisez la version HTML de cette rubrique, disponible sur la page de documentation d'Horizon 7 à l'adresse https://www.vmware.com/support/pubs/view_pubs.html.

Entrée du script

Ce script lit un fichier d'entrée, qui est décrit dans la section [Fichier d'entrée des exemples de scripts PowerCLI pour déployer des postes de travail Linux](#). Ce script demande également de façon interactive les informations suivantes :

- Adresse IP de vCenter Server
- Nom de connexion de l'administrateur pour vCenter Server
- Mot de passe de l'administrateur pour vCenter Server
- Nom de connexion de l'administrateur pour l'hôte ESXi
- Mot de passe de l'administrateur pour l'hôte ESXi
- Nom de connexion d'utilisateur pour la VM Linux
- Mot de passe d'utilisateur pour la VM Linux
- Nom de connexion d'un utilisateur AD autorisé à joindre des machines au domaine
- Mot de passe de l'utilisateur AD autorisé

Contenu du script

```
<#
.SYNOPSIS
run command "sudo /usr/bin/net ads join"

.DESRIPTION
The tool is to run the command "sudo /usr/bin/net ads join" to join Linux to AD
```

```
.NOTES
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}
#----- Handle input -----
"-----"
$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$hostAdmin = GetInput -prompt 'Your ESXi host admin user name, such as root' -IsPassword $false
$hostPassword = GetInput -prompt "Your ESXi admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"
$adUser = GetInput -prompt 'Type the AD user name to join the AD' -IsPassword $false
""
"
Please type the AD user password."
"Plase note that special character in password may not work with the script"
$adUserPassword = GetInput -prompt 'Your AD user password' -IsPassword $true
"-----"

#$csvFile = Read-Host 'Csv File '
$csvFile = '.\CloneVMs.csv'

#----- Main Script -----

#Connect to vCenter
#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
```

```

    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $cmd = "sudo /usr/bin/net ads join -U $adUser%$adUserPassword"
    Write-Host "Run cmd 'sudo /usr/bin/net ads join' in VM '$VMName' with user '$guestUser'"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
}

Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

Exécution du script

Les messages suivants proviennent d'une exécution du script :

```

PowerCLI C:\scripts> .\ClonedVMs_JoinDomain.ps1
-----
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your ESXi host admin user name, such as root: root
Your ESXi host admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****
-----
Type the AD user name to join the AD: viewadmin
Please type the AD user password.
Please note that special character in password may not work with the script.
Your AD user password: *****

```

Exemple de script pour joindre des machines virtuelles clonées à un domaine AD avec SSH

Vous pouvez personnaliser et utiliser l'exemple de script suivant pour joindre des machines virtuelles (VM) clonées à un domaine Active Directory (AD). Ce script utilise SSH pour exécuter des commandes sur les VM Linux.

Vous devez exécuter ce script si vous utilisez la solution Winbind pour l'intégration AD, car l'étape de jonction du domaine échouera pour les VM clonées. Ce script exécute une commande pour joindre le domaine sur chaque VM. Vous n'avez pas besoin d'exécuter ce script si vous utilisez la solution OpenLDAP.

Pour copier et coller le contenu du script sans saut de page, utilisez la version HTML de cette rubrique, disponible sur la page de documentation d'Horizon 7 à l'adresse https://www.vmware.com/support/pubs/view_pubs.html.

Entrée du script

Ce script lit un fichier d'entrée, qui est décrit dans la section [Fichier d'entrée des exemples de scripts PowerCLI pour déployer des postes de travail Linux](#). Ce script demande également de façon interactive les informations suivantes :

- Adresse IP de vCenter Server
- Nom de connexion de l'administrateur pour vCenter Server
- Mot de passe de l'administrateur pour vCenter Server
- Nom de connexion d'utilisateur pour la VM Linux
- Mot de passe d'utilisateur pour la VM Linux
- Nom de connexion d'un utilisateur AD autorisé à joindre des machines au domaine
- Mot de passe de l'utilisateur AD autorisé

Contenu du script

```
<#
.SYNOPSIS
run command "sudo /usr/bin/net ads join" via SSH

.DESCRPTION
The tool is to run the command "sudo /usr/bin/net ads join" to join Linux machine to AD via SSH

.NOTES
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
```

```

[Console]::ForegroundColor = "Blue"
if ($IsPassword)
{
    $input = Read-Host -AsSecureString
    $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
}
else
{
    $input = Read-Host
}

[Console]::ResetColor()
return $input
}

function Check_SSH_Client
{
    Param($IsPlink, $IsPSCP)
    if ($IsPlink)
    {
        if (Test-Path ".\plink.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "plink.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "plink.exe" not found, please download from
its official web site'
            exit
        }
    }
    if ($IsPSCP)
    {
        if (Test-Path ".\pscp.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "pscp.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "pscp.exe" not found, please download from its
official web site'
            exit
        }
    }
}

function RunCmdViaSSH
{
    Param($VM_Name, $User, $Password, $Cmd, $returnOutput = $false)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    write-host "Run cmd on $VM_Name ($IP)"

```

```

    if($returnOutput)
    {
        $command = "echo yes | .\plink.exe -ssh -l $user -pw $password $IP " + "'" + $cmd + "'"
        $output = Invoke-Expression $command
        return $output
    }
    else
    {
        echo yes | .\plink.exe -ssh -l $user -pw $password $IP "$cmd"
    }
}

function UploadFileViaSSH
{
    Param($VM_Name, $User, $Password, $LocalPath, $DestPath)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    $command = "echo yes | .\pscp.exe -l $User -pw $Password $LocalPath $IP" + ":" + "$DestPath"
    write-host "Upload file: $command"
    Invoke-Expression $command
}

#----- Handle input -----
"-----"
Check_SSH_Client -IsPlink $true -IsPSCP $false
"-----"
$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"
$adUser = GetInput -prompt 'Type the AD user name to join the AD' -IsPassword $false
""
"
Please type the AD user password."
[Console]::ForegroundColor = "Yellow"
"Plase note that special character should be escaped. For example, $ should be \$"
[Console]::ResetColor()
$adUserPassword = GetInput -prompt 'Your AD user password' -IsPassword $true
"-----"

#$csvFile = Read-Host 'Csv File '
$csvFile = '.\CloneVMs.csv'

#----- Main Script -----

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}

```

```

}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $cmd = "sudo /usr/bin/net ads join -U $adUser%$adUserPassword"
    Write-Host "Run cmd 'sudo /usr/bin/net ads join' in VM '$VMName' with user '$guestUser'"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
}

Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

Exécution du script

Les messages suivants proviennent d'une exécution du script :

```

PowerCLI C:\scripts> .\ClonedVMs_JoinDomain_SSH.ps1

-----
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****

-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****

-----
Type the AD user name to join the AD: viewadmin
Please type the AD user password.
Please note that special character should be escaped. For example, $ should be \$
Your AD user password: *****

```

Exemple de script pour télécharger des fichiers de configuration sur des machines virtuelles Linux

Vous pouvez personnaliser et utiliser l'exemple de script suivant pour télécharger les fichiers de configuration config et viewagent-custom.conf sur plusieurs machines virtuelles (VM) Linux.

Pour copier et coller le contenu du script sans saut de page, utilisez la version HTML de cette rubrique, disponible sur la page de documentation d'Horizon 7 à l'adresse https://www.vmware.com/support/pubs/view_pubs.html.

Entrée du script

Ce script lit un fichier d'entrée, qui est décrit dans la section [Fichier d'entrée des exemples de scripts PowerCLI pour déployer des postes de travail Linux](#). Ce script demande également de façon interactive les informations suivantes :

- Adresse IP de vCenter Server
- Nom de connexion de l'administrateur pour vCenter Server
- Mot de passe de l'administrateur pour vCenter Server
- Nom de connexion de l'administrateur pour l'hôte ESXi
- Mot de passe de l'administrateur pour l'hôte ESXi
- Nom de connexion d'utilisateur pour la VM Linux
- Mot de passe d'utilisateur pour la VM Linux

Contenu du script

```
<#
Upload the configuration files config and viewagent-custom.conf to Linux VMs
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}

#----- Handle Input -----
"-----"
write-host -ForegroundColor Blue 'Please ensure your config file and viewagent-custom.conf file are
```

```

in current working directory'
SvcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
SvcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
SvcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$hostAdmin = GetInput -prompt 'Your ESXi host admin user name, such as root' -IsPassword $false
$hostPassword = GetInput -prompt "Your ESXi admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"

$csvFile = '.\CloneVMs.csv'
$setConfig = $false
$setCustomConf = $false
$config_File = "config"
$customConf_File = "viewagent-custom.conf"

#check if config file exists
if(Test-Path $config_File)
{
    $setConfig = $true
    write-host -ForegroundColor Yellow '"config" file found'
}
else
{
    write-host -ForegroundColor Yellow '"config" file not found, skip it'
}

if(Test-Path $customConf_File)
{
    $setCustomConf = $true
    write-host -ForegroundColor Yellow '"viewagent-custom.conf" file found'
}
else
{
    write-host -ForegroundColor Yellow '"viewagent-custom.conf" file not found, skip it'
}

if (($setConfig -eq $false)-AND ($setCustomConf -eq $false))
{
    write-host -ForegroundColor Red 'Both file not found, exit'
    exit
}

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{

```

```

Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    #Try to delete the configuration file from home folder on destination VM
    $cmd = "rm -rf config viewagent-custom.conf"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    if ($setConfig)
    {
        Write-Host "Upload File '$config_File' to '$destFolder' of VM '$VMName' with user '$guestUser'"
        Copy-VMGuestFile -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -LocalToGuest -Destination $destFolder -
Source $config_File

        $cmd = "sudo mv ./ $config_File /etc/vmware/";
        Write-Host "Move configuraton file: $cmd"
        Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
    }

    if ($setCustomConf)
    {
        Write-Host "Upload File '$customConf_File' to '$destFolder' of VM '$VMName' with user
'$guestUser'"
        Copy-VMGuestFile -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -LocalToGuest -Destination $destFolder -
Source $customConf_File

        $cmd = "sudo mv ./ $customConf_File /etc/vmware/";
        Write-Host "Move configuraton file: $cmd"
        Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
    }
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

Exécution du script

Les messages suivants proviennent d'une exécution du script :

```
PowerCLI C:\scripts> .\UpdateOptionFile.ps1

-----
Please ensure your config file and view-agent.conf file are in current working directory.
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your ESXi host admin user name, such as root: root
Your ESXi host admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****
```

Exemple de script pour télécharger des fichiers de configuration sur des machines virtuelles Linux avec SSH

Vous pouvez personnaliser et utiliser l'exemple de script suivant pour télécharger les fichiers de configuration config et viewagent-custom.conf sur plusieurs machines virtuelles (VM) Linux. Ce script utilise SSH pour exécuter des commandes sur les VM Linux.

Pour copier et coller le contenu du script sans saut de page, utilisez la version HTML de cette rubrique, disponible sur la page de documentation d'Horizon 7 à l'adresse https://www.vmware.com/support/pubs/view_pubs.html.

Entrée du script

Ce script lit un fichier d'entrée, qui est décrit dans la section [Fichier d'entrée des exemples de scripts PowerCLI pour déployer des postes de travail Linux](#). Ce script demande également de façon interactive les informations suivantes :

- Adresse IP de vCenter Server
- Nom de connexion de l'administrateur pour vCenter Server
- Mot de passe de l'administrateur pour vCenter Server
- Nom de connexion d'utilisateur pour la VM Linux
- Mot de passe d'utilisateur pour la VM Linux

Contenu du script

```
<#
Upload the configuration files config and viewagent-custom.conf to Linux VMs using SSH
#>
#----- Functions -----
function GetInput
{
```

```

    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}
function Check_SSH_Client
{
    Param($IsPlink, $IsPSCP)
    if ($IsPlink)
    {
        if (Test-Path ".\plink.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "plink.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "plink.exe" not found, please download from
its official web site'
            exit
        }
    }
    if ($IsPSCP)
    {
        if (Test-Path ".\pscp.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "pscp.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "pscp.exe" not found, please download from its
official web site'
            exit
        }
    }
}

function RunCmdViaSSH
{
    Param($VM_Name, $User, $Password, $Cmd, $returnOutput = $false)

    $VM= Get-VM $VM_Name

```

```

    $IP = $VM.guest.IPAddress[0]
    write-host "Run cmd on $VM_Name ($IP)"
    if($returnOutput)
    {
        $command = "echo yes | .\plink.exe -ssh -l $user -pw $password $IP " + '"' + $cmd + '"'
        $output = Invoke-Expression $command
        return $output
    }
    else
    {
        echo yes | .\plink.exe -ssh -l $user -pw $password $IP "$cmd"
    }
}

function UploadFileViaSSH
{
    Param($VM_Name, $User, $Password, $LocalPath, $DestPath)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    $command = "echo yes | .\pscp.exe -l $User -pw $Password $LocalPath $IP" + ":" + "$DestPath"
    write-host "Upload file: $command"
    Invoke-Expression $command
}

#----- Handle Input -----
"-----"
Check_SSH_Client -IsPlink $true -IsPSCP $true
"-----"
write-host -ForegroundColor Blue 'Please ensure your config file and viewagent-custom.conf file are
in current working directory'
$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"

$csvFile = '.\CloneVMs.csv'
$setConfig = $false
$setCustomConf = $false
$config_File = "config"
$customConf_File = "viewagent-custom.conf"

#check if config file exists
if(Test-Path $config_File)
{
    $setConfig = $true
    write-host -ForegroundColor Yellow '"config" file found'
}
else
{
    write-host -ForegroundColor Yellow '"config" file not found, skip it'
}

```

```

}

if(Test-Path $customConf_File)
{
    $setCustomConf = $true
    write-host -ForegroundColor Yellow '"viewagent-custom.conf" file found'
}
else
{
    write-host -ForegroundColor Yellow '"viewagent-custom.conf" file not found, skip it'
}

if (($setConfig -eq $false)-AND ($setCustomConf -eq $false))
{
    write-host -ForegroundColor Red 'Both file not found, exit'
    exit
}

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    #Try to delete the configuration file from home folder on destination VM
    $cmd = "rm -rf config viewagent-custom.conf"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

    if ($setConfig)
    {
        Write-Host "Upload File '$config_File' to '$destFolder' of VM '$VMName' with user '$guestUser'"
        UploadFileViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -LocalPath
        $config_File -DestPath $destFolder

        $cmd = "sudo mv ./ $config_File /etc/vmware/";
        Write-Host "Move configuraton file: $cmd"
    }
}

```

```

RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
}

if ($setCustomConf)
{
    Write-Host "Upload File '$customConf_File' to '$destFolder' of VM '$VMName' with user '$guestUser'"
    UploadFileViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -LocalPath $customConf_File -DestPath $destFolder

    $cmd = "sudo mv ./$customConf_File /etc/vmware/";
    Write-Host "Move configuraton file: $cmd"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
}
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

Exécution du script

Les messages suivants proviennent d'une exécution du script :

```

PowerCLI C:\scripts> .\UpdateOptionFile.ps1
-----
Please ensure your config file and view-agent.conf file are in current working directory.
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****

```

Exemple de script pour mettre à niveau Horizon Agent sur des machines de poste de travail Linux

Vous pouvez personnaliser et utiliser l'exemple de script suivant pour mettre à niveau Horizon Agent sur plusieurs machines virtuelles (VM) Linux.

Ce script télécharge l'archive du programme d'installation sur chaque VM avant l'installation d'Horizon Agent. La tâche de téléchargement peut prendre du temps, en particulier lorsqu'un grand nombre de VM est impliqué et que la vitesse du réseau est lente. Pour gagner du temps, vous pouvez exécuter le script qui utilise SSH, ou placer l'archive du programme d'installation dans un emplacement partagé disponible pour chaque VM, de sorte que le téléchargement du fichier n'est pas nécessaire.

Pour copier et coller le contenu du script sans saut de page, utilisez la version HTML de cette rubrique, disponible sur la page de documentation d'Horizon 7 à l'adresse https://www.vmware.com/support/pubs/view_pubs.html.

Entrée du script

Ce script lit un fichier d'entrée, qui est décrit dans la section [Fichier d'entrée des exemples de scripts PowerCLI pour déployer des postes de travail Linux](#). Ce script demande également de façon interactive les informations suivantes :

- Acceptation du CLUF (contrat de licence utilisateur final) d'Horizon Agent
- Adresse IP de vCenter Server
- Nom de connexion de l'administrateur pour vCenter Server
- Mot de passe de l'administrateur pour vCenter Server
- Nom de connexion de l'administrateur pour l'hôte ESXi
- Mot de passe de l'administrateur pour l'hôte ESXi
- Nom de connexion de l'utilisateur pour le système d'exploitation invité Linux
- Mot de passe de l'utilisateur pour le système d'exploitation invité Linux
- Chemin de l'archive Horizon Agent
- Mise à niveau vers une machine virtuelle gérée
- Installation de la fonctionnalité de redirection de carte à puce

Contenu du script

```
<#
Upload the Linux Agent installer tar ball and re-install
#>

#-----
Functions-----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}
```

```

}
#-----Handle
input-----
"-----"
$acceptEULA = GetInput -prompt 'Accept Linux View Agent EULA in tar bundle ("yes" or "no")' -
IsPassword $false
if ($acceptEULA -ne "yes")
{
    write-host -ForegroundColor Red "You need accept the EULA with 'yes'(case sensitive)"
    exit
}
$svcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$svcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$svcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$hostAdmin = GetInput -prompt 'Your ESXi host admin user name, such as root' -IsPassword $false
$hostPassword = GetInput -prompt "Your ESXi admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"
$agentInstaller = GetInput -prompt 'Type the View Agent tar ball path' -IsPassword $false
"-----"
$UpgradeToManagedVM = GetInput -prompt 'Upgrade to managed VM ("yes" or "no")' -IsPassword $false
if (($UpgradeToManagedVM -ne "yes") -AND $UpgradeToManagedVM -ne "no")
{
    write-host -ForegroundColor Red "You need select 'yes' or 'no'(case sensitive)"
    exit
}
$installSmartcard = GetInput -prompt 'Install the Smartcard redirection feature ("yes" or "no")' -
IsPassword $false
if (($installSmartcard -ne "yes") -AND $installSmartcard -ne "no")
{
    write-host -ForegroundColor Red "You need select 'yes' or 'no'(case sensitive)"
    exit
}
}
"-----"

#$csvFile = Read-Host 'Csv File '
$csvFile = '.\CloneVMs.csv'

#check if file exists
if (!(Test-Path $agentInstaller))
{
    write-host -ForegroundColor Red "installer File not found"
    exit
}

#check if file exists
if (!(Test-Path $csvFile))
{
    write-host -ForegroundColor Red "CSV File not found"
    exit
}
}
#-----

```

```

Functions-----
function GetSourceInstallerMD5()
{
    $agentInstallerPath = Convert-Path $agentInstaller;
    $md5 = New-Object -TypeName System.Security.Cryptography.MD5CryptoServiceProvider;
    $md5HashWithFormat =
[System.BitConverter]::ToString($md5.ComputeHash([System.IO.File]::ReadAllBytes($agentInstallerPath)))
;
    $md5Hash = ($md5HashWithFormat.replace("-", "").ToLower());
    return $md5Hash;
}

#-----
Main-----
#Get installer MD5Sum
$installerMD5Hash = GetSourceInstallerMD5;

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $cmd = "rm -rf VMware-*linux-*"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    #Upload installer tar ball to Linux VM
    Write-Host "Upload File '$agentInstaller' to '$destFolder' of VM '$VMName' with user '$guestUser'"
    Copy-VMGuestFile -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -LocalToGuest -Destination $destFolder -
Source $agentInstaller

    #Check the uploaded installer md5sum
    $cmd = "md5sum VMware-*linux-*"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"

```

```

$output = Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -
GuestUser $guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

if($output.Contains($installerMD5Hash))
{
    Write-Host $VMName": Uploaded installer's MD5Sum matches the local installer's MD5Sum";
    Write-Host $VMName": Extract the installer and do installation";
    $cmd = "tar -xzf VMware-*linux-*.tar.gz"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    $cmd = "sudo setenforce 0";
    Write-Host "Set the selinux to permissive mode: $cmd"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    $cmd = "sudo killall /usr/lib/vmware/viewagent/VMwareBlastServer/VMwareBlastServer"
    Write-Host "Stop VMwareBlastServer before upgrading: $cmd"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    #Run the upgrade command.
    $cmd = "cd VMware-*linux-* && sudo ./install_viewagent.sh -A yes -m $installSmartcard -M
$UpgradeToManagedVM"
    Write-Host "Run upgrade cmd in VM '$VMName' with user '$guestUser': $cmd"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    $cmd = "sudo shutdown -r +1&"
    Write-Host "Reboot to apply the View Agent installation"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
}
else
{
    Write-Host $VMName": Uploaded installer's MD5Sum does NOT match the local installer's MD5Sum";
    Write-Host $VMName": Skip the installation. Please check your network and VMware Tools
status";
    exit;
}
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

Exécution du script

Les messages suivants proviennent d'une exécution du script :

```

PowerCLI C:\scripts> .\InstallAgent.ps1
-----
Accept Linux Horizon Agent EULA in tar bundle ("yes" or "no"): yes
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator

```

```

Your vCenter admin user password: *****
-----
Your ESXi host admin user name, such as root: root
Your ESXi host admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****
-----
Type the Horizon Agent tar ball path. Please take care of the installer arch: .\VMware-viewagent-
linux-x86_64-x.y.z-1234567.tar.gz
-----
Upgrade to managed VM ("yes" or "no"): yes
Install the Smartcard redirection feature ("yes" or "no"): no

```

Exemple de script pour mettre à niveau Horizon Agent sur des machines virtuelles Linux avec SSH

Vous pouvez personnaliser et utiliser l'exemple de script suivant pour mettre à niveau Horizon Agent sur plusieurs machines virtuelles (VM) Linux. Ce script utilise SSH pour exécuter des commandes sur les VM Linux.

Pour copier et coller le contenu du script sans saut de page, utilisez la version HTML de cette rubrique, disponible sur la page de documentation d'Horizon 7 à l'adresse https://www.vmware.com/support/pubs/view_pubs.html.

Entrée du script

Ce script lit un fichier d'entrée, qui est décrit dans la section [Fichier d'entrée des exemples de scripts PowerCLI pour déployer des postes de travail Linux](#). Ce script demande également de façon interactive les informations suivantes :

- Acceptation du CLUF (contrat de licence utilisateur final) d'Horizon Agent
- Adresse IP de vCenter Server
- Nom de connexion de l'administrateur pour vCenter Server
- Mot de passe de l'administrateur pour vCenter Server
- Nom de connexion de l'administrateur pour l'hôte ESXi
- Mot de passe de l'administrateur pour l'hôte ESXi
- Nom de connexion de l'utilisateur pour le système d'exploitation invité Linux
- Mot de passe de l'utilisateur pour le système d'exploitation invité Linux
- Chemin de l'archive Horizon Agent
- Mise à niveau vers une machine virtuelle gérée
- Installation de la fonctionnalité de redirection de carte à puce

Contenu du script

```
<#
Upload the Linux Agent installer tar ball and re-install
#>

#-----
Functions-----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}
function Check_SSH_Client
{
    Param($IsPlink, $IsPSCP)
    if ($IsPlink)
    {
        if (Test-Path ".\plink.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "plink.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "plink.exe" not found, please download from
its official web site'
            exit
        }
    }
    if ($IsPSCP)
    {
        if (Test-Path ".\pscp.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "pscp.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "pscp.exe" not found, please download from its
```

```

official web site'
    exit
}
}

function RunCmdViaSSH
{
    Param($VM_Name, $User, $Password, $Cmd, $returnOutput = $false)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    write-host "Run cmd on $VM_Name ($IP)"
    if($returnOutput)
    {
        $command = "echo yes | .\plink.exe -ssh -l $user -pw $password $IP " + "'" + $cmd + "'"
        $output = Invoke-Expression $command
        return $output
    }
    else
    {
        echo yes | .\plink.exe -ssh -l $user -pw $password $IP "$cmd"
    }
}

function UploadFileViaSSH
{
    Param($VM_Name, $User, $Password, $LocalPath, $DestPath)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    $command = "echo yes | .\pscp.exe -l $User -pw $Password $LocalPath $IP" + ":" + "$DestPath"
    write-host "Upload file $LocalPath to VM $VM_Name with user $User"
    Invoke-Expression $command
}

#-----Handle
input-----
"-----"
Check_SSH_Client -IsPlink $true -IsPSCP $true
"-----"
$acceptEULA = GetInput -prompt 'Accept Linux View Agent EULA in tar bundle ("yes" or "no")' -
IsPassword $false
if ($acceptEULA -ne "yes")
{
    write-host -ForegroundColor Red "You need accept the EULA with 'yes'(case sensitive)"
    exit
}
$svcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$svcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$svcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true

```

```

"-----"
$agentInstaller = GetInput -prompt 'Type the View Agent tar ball path' -IsPassword $false
"-----"
$UpgradeToManagedVM = GetInput -prompt 'Upgrade to managed VM ("yes" or "no")' -IsPassword $false
if (($UpgradeToManagedVM -ne "yes") -AND $UpgradeToManagedVM -ne "no")
{
    write-host -ForegroundColor Red "You need select 'yes' or 'no'(case sensitive)"
    exit
}
$installSmartcard = GetInput -prompt 'Install the Smartcard redirection feature ("yes" or "no")' -
IsPassword $false
if (($installSmartcard -ne "yes") -AND $installSmartcard -ne "no")
{
    write-host -ForegroundColor Red "You need select 'yes' or 'no'(case sensitive)"
    exit
}
"-----"

#$csvFile = Read-Host 'Csv File '
$csvFile = '.\CloneVMs.csv'

#check if file exists
if (!(Test-Path $agentInstaller))
{
    write-host -ForegroundColor Red "installer File not found"
    exit
}

#check if file exists
if (!(Test-Path $csvFile))
{
    write-host -ForegroundColor Red "CSV File not found"
    exit
}
#-----
Functions-----
function GetSourceInstallerMD5()
{
    $agentInstallerPath = Convert-Path $agentInstaller;
    $md5 = New-Object -TypeName System.Security.Cryptography.MD5CryptoServiceProvider;
    $md5HashWithFormat =
[System.BitConverter]::ToString($md5.ComputeHash([System.IO.File]::ReadAllBytes($agentInstallerPath)))
;
    $md5Hash = ($md5HashWithFormat.replace("-", "")).ToLower();
    return $md5Hash;
}

#-----
Main-----
#Get installer MD5Sum
$installerMD5Hash = GetSourceInstallerMD5;

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))

```



```

{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $cmd = "rm -rf VMware-*linux-*"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

    #Upload installer tar ball to Linux VM
    Write-Host "Upload File '$agentInstaller' to '$destFolder' of VM '$VMName' with user '$guestUser'"
    UploadFileViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -LocalPath
$agentInstaller -DestPath $destFolder

    #Check the uploaded installer md5sum
    $cmd = "md5sum VMware-*linux-*"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    $output = RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd -
$returnOutput $true

    if($output.Contains($installerMD5Hash))
    {
        Write-Host $VMName": Uploaded installer's MD5Sum matches the local installer's MD5Sum";
        Write-Host $VMName": Extract the installer and do installation";

        $cmd = "tar -xzf VMware-*linux-*.tar.gz"
        Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
        RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

        $cmd = "sudo setenforce 0";
        Write-Host "Set the selinux to permissive mode: $cmd"
        RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

        $cmd = "sudo killall /usr/lib/vmware/viewagent/VMwareBlastServer/VMwareBlastServer"
        Write-Host "Stop VMwareBlastServer before upgrading: $cmd"
        RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

        #Run the upgrade command.
    }
}

```

```

    $cmd = "cd VMware-*linux-* && sudo ./install_viewagent.sh -r yes -A yes -m $installSmartcard
-M $UpgradeToManagedVM"
    Write-Host "Run upgrade cmd in VM '$VMName' with user '$guestUser': $cmd"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
    Write-Host -ForegroundColor Yellow "Linux Agent installer will reboot the Linux VM after
upgrade, and you may hit the ssh connection closed error message, which is expectation"
}
else
{
    Write-Host $VMName": Uploaded installer's MD5Sum does NOT match the local installer's MD5Sum";
    Write-Host $VMName": Skip the installation. Please check your network and VMware Tools
status";
    exit;
}
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

Exécution du script

Les messages suivants proviennent d'une exécution du script :

```

PowerCLI C:\scripts> .\InstallAgent.ps1
-----
Accept Linux Horizon Agent EULA in tar bundle ("yes" or "no"): yes
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****
-----
Type the Horizon Agent tar ball path. Please take care of the installer arch: .\VMware-viewagent-
linux-x86_64-x.y.z-1234567.tar.gz
-----
-----
Upgrade to managed VM ("yes" or "no"): yes
Install the Smartcard redirection feature ("yes" or "no"): no

```

Exemple de script pour effectuer des opérations sur des machines virtuelles Linux

Vous pouvez personnaliser et utiliser l'exemple de script suivant pour exécuter des opérations sur plusieurs machines virtuelles (VM) Linux. Les opérations incluent la mise sous tension, la mise hors tension, l'arrêt, le redémarrage et la suppression des VM.

Ce script peut supprimer des machines virtuelles de vCenter Server, mais pas de View.

Pour copier et coller le contenu du script sans saut de page, utilisez la version HTML de cette rubrique, disponible sur la page de documentation d'Horizon 7 à l'adresse https://www.vmware.com/support/pubs/view_pubs.html.

Entrée du script

Ce script lit un fichier d'entrée, qui est décrit dans la section [Fichier d'entrée des exemples de scripts PowerCLI pour déployer des postes de travail Linux](#). Ce script demande également de façon interactive les informations suivantes :

- Adresse IP de vCenter Server
- Nom de connexion de l'administrateur pour vCenter Server
- Mot de passe de l'administrateur pour vCenter Server
- Action à exécuter : il peut s'agir de la mise sous tension, la mise hors tension, l'arrêt de l'invité, le redémarrage d'une VM, le redémarrage d'un invité de VM ou la suppression d'une VM.
- Temps d'attente, en secondes, entre les opérations sur les VM.

Contenu du script

```
<#
.DESCRIPTION
The Tool supports:
1. Power off VMs
2. Power on VMs
3. Shutdown VMs
4. Restart VMs
5. Restart VM guest
6. Delete VMs from Disk
.NOTES
#>

#----- Functions -----

function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}
```

```

function IsVMExists ($VMExists)
{
    Write-Host "Checking if the VM $VMExists Exists"
    [bool]$Exists = $false

    #Get all VMS and check if the VMs is already present in VC
    $listvm = Get-vm
    foreach ($lvm in $listvm)
    {
        if($VMExists -eq $lvm.Name )
        {
            $Exists = $true
            Write-Host "$VMExists is Exist"
        }
    }
    return $Exists
}

function Delete_VM($VMToDelete)
{
    Write-Host "Deleting VM $VMToDelete"
    Get-VM $VMToDelete | where { $_.PowerState -eq "PoweredOn" } | Stop-VM -confirm:$false
    Get-VM $VMToDelete | Remove-VM -DeleteFromDisk -confirm:$false
}

#----- Handle input -----
"-----"
$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"

$action = GetInput -prompt 'Select action: 1). Power On 2). Power Off 3) Shutdown VM Guest 4).
Restart VM 5). Restart VM Guest 6). Delete VM' -IsPassword $false
$sleepTime = GetInput -prompt 'Wait time (seconds) between each VM' -IsPassword $false
"-----"

[Console]::ForegroundColor = "Yellow"
switch ($action)
{
    1
    {
        "Your selection is 1). Power On"
    }
    2
    {
        "Your selection is 2). Power Off"
    }
    3
    {
        "Your selection is 3) Shutdown"
    }
    4
    {
        "Your selection is 4). Restart VM"
    }
    5
}

```

```

{
    "Your selection is 5). Restart VM Guest"
}
6
{
    "Your selection is 6). Delete VM"
}
default
{
    "Invalid selection for action: $action"
    exit
}
}
[Console]::ResetColor()
$csvFile = '.\CloneVMs.csv'

#check if file exists
if (!(Test-Path $csvFile))
{
    write-host -ForegroundColor Red "CSV File not found"
    exit
}
"-----"

#----- Main -----
#Read input CSV file
Disconnect-VIServer $vcAddress -Confirm:$false
#Connect-VIServer $vcAddress -ErrorAction Stop -user $vcAdmin -password $vcPassword
Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
$csvData = Import-CSV $csvFile

foreach ($line in $csvData)
{
    $VMName = $line.VMName
    switch ($action)
    {
        1
        {
            Get-VM $VMName | Start-VM -Confirm:$false
        }
        2
        {
            Get-VM $VMName | Stop-VM -Confirm:$false
        }
        3
        {
            Get-VM $VMName | Shutdown-VMGuest -Confirm:$false
        }
        4
        {
            Get-VM $VMName | Restart-VM -Confirm:$false
        }
        5
        {
            Get-VM $VMName | Restart-VMGuest -Confirm:$false
        }
    }
}

```

```

    }
    6
    {
        if (IsVMExists ($VMName))
        {
            Delete_VM ($VMName)
        }
    }
    default{}
}
Start-Sleep -s $sleepTime
}

Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

Exécution du script

Les messages suivants proviennent d'une exécution du script :

```

PowerCLI C:\scripts> .\VMOperations.ps1
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****

-----
Select action: 1). Power On 2). Power Off 3) Shutdown VM Guest 4). Restart VM 5). Restart VM Guest
6). Delete VM: 1
Wait time (seconds) between each VM: 20
-----

Your selection is 6). Delete VM

```

Pour les opérations de mise sous tension, redémarrage d'une VM et redémarrage d'un invité de VM, spécifiez un temps d'attente entre les machines virtuelles d'au moins 20 secondes pour éviter les tempêtes de démarrage, qui pourraient entraîner l'échec de certaines opérations.

Dépannage des postes de travail Linux

9

Certains problèmes peuvent se produire lorsque vous gérez des postes de travail Linux. Vous pouvez suivre diverses procédures pour diagnostiquer et résoudre les problèmes.

Ce chapitre contient les rubriques suivantes :

- [Collecter des informations de diagnostic pour une machine Horizon 7 for Linux](#)
- [Dépannage du copier/coller entre un poste de travail distant et un hôte client](#)
- [Configuration du pare-feu Linux pour autoriser les connexions TCP entrantes](#)
- [View Agent ne se déconnecte pas d'Horizon Client sur iPad Pro](#)
- [Le poste de travail SLES 12 SP1 ne s'actualise pas automatiquement après un glisser-déplacer](#)
- [L'authentification unique \(SSO\) ne peut pas se connecter à un agent de mise hors tension](#)
- [Machine virtuelle inaccessible après la création d'un pool de postes de travail manuel pour Linux](#)

Collecter des informations de diagnostic pour une machine Horizon 7 for Linux

Vous pouvez collecter des informations de diagnostic pour aider le support technique de VMware à diagnostiquer et résoudre les problèmes avec une machine Horizon 7 for Linux. Vous créez un groupe DCT (Data Collection Tool) qui rassemble les informations de configuration de la machine et se connecte à une archive compressée.

Procédure

- 1 Ouvrez une session sur la machine virtuelle Linux en tant qu'utilisateur avec les privilèges requis.
- 2 Ouvrez une invite de commande et exécutez le script `dct-debug.sh`.

```
sudo /usr/lib/vmware/viewagent/bin/dct-debug.sh
```

Le script génère une archive qui contient le groupe DCT. Par exemple :

```
ubuntu-12-vdm-sdct-20150201-0606-agent.tgz
```

L'archive est générée dans le répertoire depuis lequel le script était exécuté (le répertoire de travail actuel).

Dépannage du copier/coller entre un poste de travail distant et un hôte client

L'opération copier/coller entre le poste de travail distant et l'hôte client prend plus de trois secondes pour les données prises en charge maximales de 1 Mo. Ce problème ne se produit pas si vous copiez et collez des données de petite taille.

Problème

Lorsque vous configurez 1 vCPU et 1 Go de mémoire pour un poste de travail SLED 11 SP3/SP4, l'opération copier/coller entre le poste de travail distant et l'hôte client local peut prendre plus de trois secondes.

Cause

Le délai de l'opération copier/coller peut être dû aux anciennes API de système d'exploitation de SLED 11 SP3/SP4.

Solution

- ◆ Configurez deux vCPU et 2 Go de mémoire pour SLED 11 SP3/SP4.

Configuration du pare-feu Linux pour autoriser les connexions TCP entrantes

Pour autoriser les utilisateurs à se connecter à leurs postes de travail Linux, les postes de travail doivent pouvoir accepter les connexions TCP entrantes depuis les périphériques Horizon Client, le serveur de sécurité et le Serveur de connexion View.

Sur les distributions Ubuntu et Kylin, le pare-feu `iptables` est configuré par défaut avec la stratégie entrante `ACCEPT`.

Sur les distributions RHEL et CentOS, si possible, le script du programme d'installation d'Horizon Agent configure le pare-feu `iptables` avec la stratégie entrante `ACCEPT`.

Assurez-vous que `iptables` sur un système d'exploitation invité RHEL ou CentOS a une stratégie entrante `ACCEPT` pour les nouvelles connexions depuis le port Blast, 22443.

Lorsque BSG est activé, les connexions client sont dirigées depuis un périphérique Horizon Client via BSG sur un serveur de sécurité ou le Serveur de connexion View vers le poste de travail Linux. Lorsque BSG n'est pas activé, les connexions sont établies directement depuis le périphérique Horizon Client vers le poste de travail Linux.

View Agent ne se déconnecte pas d'Horizon Client sur iPad Pro

La connexion View Agent SUSE ne se déconnecte pas d'Horizon Client sur un iPad Pro après un redémarrage ou un arrêt.

Problème

Lorsque vous redémarrez ou arrêtez une machine virtuelle SUSE sur Horizon Client pour iPad Pro, le poste de travail ne répond pas. View Agent ne se déconnecte pas.

Cause

Il est possible que la machine SUSE n'envoie pas correctement les messages à Horizon Client après une opération de redémarrage ou d'arrêt.

Solution

- ◆ Déconnectez manuellement la connexion du poste de travail depuis Horizon Client sur iPad Pro.

Le poste de travail SLES 12 SP1 ne s'actualise pas automatiquement après un glisser-déplacer

SLES 12 SP1 ne s'actualise pas automatiquement en mode multimoniteur lorsque vous faites glisser un terminal gnome.

Problème

Lorsque vous lancez SLES 12 SP1 en mode multimoniteur et que vous revenez au mode fenêtre, le poste de travail ne s'actualise pas automatiquement quand vous faites glisser un terminal gnome.

Cause

Le terminal gnome ne répond pas à l'opération de glisser-déplacer.

Solution

- 1 Mettez fin au gnome-shell.



```
kill -9 `pidof gnome-shell`
```

- 2 Redémarrez à nouveau le gnome-shell.

L'authentification unique (SSO) ne peut pas se connecter à un agent de mise hors tension

L'authentification unique (SSO) ne se connecte pas à un agent de mise hors tension.

Problème

Lorsque vous ouvrez une session en tant que Broker et que vous vous connectez à un agent, l'authentification unique ne se connecte pas à un agent de mise hors tension.

Solution

- ◆ Connectez-vous manuellement au poste de travail ou déconnectez-vous et reconnectez-vous à l'agent.

Machine virtuelle inaccessible après la création d'un pool de postes de travail manuel pour Linux

L'état de la machine virtuelle ne répond pas.

Problème

Il est possible que l'état de la machine virtuelle soit « En attente de l'agent » ou « Inaccessible » après avoir créé un pool de postes de travail manuel.

Cause

Ces deux états peuvent être causés par des erreurs d'installation et de configuration dues à l'utilisateur.

- Vérifiez que l'option `machine.id` existe dans le fichier de configuration `vmx` des machines virtuelles.

Si elle n'existe pas, vérifiez alors que la machine virtuelle a correctement été ajoutée au pool de postes de travail. Si ce n'est pas le cas, recréez le pool de postes de travail pour laisser le Broker réécrire l'option dans le fichier de configuration `vmx`.

- Vérifiez que VMware Tool ou Open VM Tool est correctement installé.

Si les étapes d'installation de VMware Tool ou d'Open VM Tool n'ont pas été effectuées correctement, il se peut que la commande `vmware-rpctool` n'existe pas sous `PATH` dans la machine virtuelle Linux. Vous devez suivre le guide pour installer VMware Tool ou Open VM Tool.

Exécutez la commande après la fin de l'installation.

```
#vmware-rpctool "machine.id.get"
```

Les valeurs `machine.id` sont répertoriées dans le fichier de configuration `vmx` des machines virtuelles.

- Vérifiez que le FQDN du Broker peut être résolu à l'adresse IP dans la machine virtuelle de l'agent Linux.