Configuration des postes de travail Horizon 7 for Linux

Décembre 2019
VMware Horizon 7 7.11

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

Table des matières

Configuration des postes de travail Horizon 7 for Linux

Le document *Configuration des postes de travail Horizon 7 for Linux* fournit des informations sur la configuration d'une machine virtuelle Linux à utiliser en tant que poste de travail VMware Horizon® 7 for Linux. Les informations incluent la préparation du système d'exploitation invité Linux, l'installation d'Horizon Agent sur la machine virtuelle et la configuration de la machine dans Horizon Console pour une utilisation dans un déploiement 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 destinées aux administrateurs système Linux expérimentés qui connaissent bien le fonctionnement des centres de données et de la technologie des machines virtuelles.

Fonctionnalités et configuration système requise

1

Avec Horizon 6.2.x 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

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

Fonctionnalités prises en charge sur les postes de travail Linux

Intégration d'Active Directory

Les postes de travail Instant Clone exécutant les distributions Linux suivantes peuvent effectuer une jonction de domaine hors ligne avec Active Directory à l'aide de PowerBroker Identity Services Open (PBISO).

- Ubuntu 16.04 et 18.04
- SLED/SLES 12.x

Pour plus d'informations, reportez-vous à la section Authentification PBISO (PowerBroker Identity Services Open) dans Intégration de Linux à Active Directory.

Les postes de travail Instant Clone exécutant les distributions Linux suivantes peuvent effectuer une jonction de domaine hors ligne avec Active Directory à l'aide de Samba.

- Ubuntu 16.04 et 18.04

	■ RHEL 7.3 et 8.0
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. Cette fonctionnalité est prise en charge sur les distributions Linux suivantes. ■ Ubuntu 16.04 x64 avec un environnement de poste de travail MATE ou Gnome Flashback (Metacity) ■ Ubuntu 18.04 x64 avec un environnement de poste de travail MATE ou Gnome Ubuntu ■ RHEL 7.x Workstation x64 avec un environnement de poste de travail KDE ou Gnome ■ RHEL 8.0 Workstation x64 avec un environnement de poste de travail Gnome ■ SLED/SLES 12.x SP3 x64
Sortie audio	La redirection de la sortie audio est prise en charge. Cette fonctionnalité est activée par défaut. Pour la désactiver, vous devez définir l'option `RemoteDisplay.allowAudio` sur **`false`**. Lors d'un accès avec les navigateurs Chrome et Firefox, VMware Horizon HTML Access prend en charge la sortie audio pour les postes de travail Linux.
Pool de postes de travail de clone complet automatisé	Vous pouvez créer des pools de postes de travail de clone complet automatisés pour les postes de travail Linux.
Redirection du lecteur client	L'activation de la fonctionnalité de redirection du lecteur client (CDR) vous ouvre l'accès aux dossiers et lecteurs partagés de votre système local. Vous utilisez le dossier `tsclient` 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 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 fonctionnalité est activée par défaut. Vous pouvez la désactiver lors de l'installation.
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 pour les postes de travail Linux.

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 les certificats CMVP n° 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.

Outil Service d'assistance

Horizon Help Desk Tool est une application Web que vous pouvez utiliser pour résoudre les problèmes de sessions de poste de travail Linux. Vous pouvez utiliser Horizon Help Desk Tool pour obtenir l'état des sessions utilisateur Horizon 7 et effectuer des opérations de dépannage et de maintenance. Reportez-vous à la section Utilisation d'Horizon Help Desk Tool dans la Horizon Console.

Stratégies de carte à puce d'Horizon

Vous pouvez utiliser VMware Dynamic Environment Manager™ 9.4 ou version ultérieure pour créer des Stratégies de carte à puce Horizon qui contrôlent le comportement des fonctionnalités de redirection USB, de redirection du Presse-papiers et de redirection du lecteur client sur des postes de travail Linux distants spécifiques. Reportez-vous à la section Utilisation de Stratégies de carte à puce.

Codeur 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 H.264 est désactivé sur le système client, Blast Extreme revient automatiquement à un codage JPEG/PNG.

Le codeur H.264 inclut la prise en charge du matériel H.264 et la prise en charge du codeur logiciel. La configuration suivante est requise pour la prise en charge du codeur matériel H.264.

- Le vGPU doit être configuré avec une carte graphique NVIDIA.
- Le pilote NVIDIA 384 ou version ultérieure doit être installé pour la carte graphique NVIDIA.

Si le système remplit les conditions précédentes, Horizon 7 for Linux peut utiliser le codeur matériel H.264. Dans le cas contraire, le codeur logiciel H.264 est utilisé.

Pool de postes de travail flottants d'Instant Clone	Vous pouvez créer des pools de postes de travail flottants Instant Clone pour les postes de travail Linux. Cette fonctionnalité est prise en charge uniquement sur les systèmes avec les distributions Linux suivantes installées. ■ Ubuntu 16.04 et 18.04 ■ RHEL 7.1 ou version ultérieure ■ RHEL 8.0 ■ SLED/SLES 12.x Pour plus d'informations, reportez-vous à la section Créer un pool de postes de travail flottant Instant Clone pour Linux.
K Desktop Environment	K Desktop Environment (KDE) est pris en charge sur les distributions Linux suivantes. ■ CentOS 6.x et 7.x ■ RHEL 6.x et 7.x ■ Ubuntu 16.04 et 18.04
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 VMware Horizon pour Windows et dans les langues suivantes : anglais, français, allemand, japonais, coréen, espagnol, chinois simplifié et chinois traditionnel.
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.
Pool de postes de travail manuel.	Source de machines. ■ 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.

Environnement de poste de travail MATE

L'environnement de poste de travail MATE est pris en charge sur les distributions Linux suivantes.

- Ubuntu 16.04
- Ubuntu 18.04

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 sur VMware 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 16.04 et 18.04, vous devez utiliser l'environnement de poste de travail Gnome, KDE ou MATE pour utiliser la fonctionnalité de moniteurs multiples. Pour plus d'informations, reportez-vous à la section http://kb.vmware.com/kb/2151294.

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.

À partir de VMware Horizon HTML Access™ version 5.0, la fonctionnalité plusieurs moniteurs est prise en charge dans Horizon 7 pour les postes de travail Linux.

Prise en charge de Network Intelligence pour VMware Blast

Le transport Network Intelligence est pris en charge pour VMware Blast. Cette fonctionnalité est activée par défaut.

Lorsque le protocole UDP (User Datagram Protocol) est activé, Blast établit des connexions TCP (Transmission Control Protocol) et UDP. En fonction des conditions actuelles du réseau, Blast sélectionne de façon dynamique l'un des transports pour transmettre des données afin de garantir une expérience utilisateur optimale. Par exemple, dans un réseau local, TCP s'exécute mieux qu'UDP, donc Blast sélectionne TCP pour le transport des données. De même, dans un réseau étendu (WAN), les performances UDP sont meilleures que celles de TCP, donc Blast sélectionne le transport UDP dans cet environnement.

Si l'un des composants en ligne utilisés ne prend pas en charge UDP, Blast établit une connexion TCP uniquement. Par exemple, si votre connexion utilise le composant Blast Security Gateway du Serveur de connexion Horizon ou du serveur de sécurité, seule une connexion TCP est établie. Même si le client et l'agent ont activé UDP, la connexion utilise le protocole TCP, car Blast Security Gateway ne prend pas en charge UDP. Si des

	utilisateurs se connectent en dehors du réseau de leur entreprise, le composant UDP requiert l'utilisation de VMware Unified Access Gateway (anciennement appelé Access Point), qui prend en charge le protocole UDP. Utilisez les informations suivantes pour établir une connexion Blast basée sur le protocole UDP. ■ Si le client se connecte directement à un poste de travail Linux, activez le protocole UDP côté client et agent. Par défaut, le protocole UDP est activé côté client et agent. ■ Si le client se connecte à un poste de travail Linux à l'aide d'Unified Access Gateway, activez le protocole UDP côté client et agent, ainsi que sur Unified Access Gateway.
Collaboration de session	Avec la fonctionnalité Collaboration de session, les utilisateurs peuvent inviter d'autres utilisateurs à rejoindre une session de poste de travail Linux distante existante, ou vous pouvez rejoindre une session de collaboration lorsque vous recevez une invitation d'un autre utilisateur. Cette fonctionnalité est prise en charge uniquement sur les postes de travail Linux distants avec les distributions Linux suivantes installées. ■ Ubuntu 18.04 avec un environnement de poste de travail Gnome ■ RHEL 7.5 ou version ultérieure avec un environnement de poste de travail Gnome Classic ■ RHEL 8.0 avec un environnement de poste de travail Gnome classique
Authentification unique	L'authentification unique (SSO) est prise en charge sur les distributions Linux suivantes. ■ RHEL 8.0/7.x/6.x Workstation x64 ■ CentOS 8.0/7.x/6.x x64 ■ SLED/SLES 12.x SP3/SP2/SP1 ■ Ubuntu 18.04/16.04 x64
Redirection de carte à puce	La redirection de carte à puce est prise en charge sur les distributions Linux suivantes. ■ RHEL 8.0 ■ RHEL 7.1 et versions ultérieures ■ RHEL 6.6 et versions ultérieures ■ Ubuntu 18.04/16.04 ■ SLED/SLES 12.x SP3

	Cette fonctionnalité prend en charge les cartes PIV (Personal Identity Verification) et les cartes CAC (Common Access). Pour plus d'informations, reportez-vous à la section Configuration de la redirection de carte à puce.
Prise en charge de l'authentification unique réelle	L'authentification unique réelle est prise en charge sur les distributions Linux suivantes. ■ RHEL 7.x/8.0 ■ CentOS 7.x/8.0 ■ SLED/SLES 12.x SP3 ■ Ubuntu 18.04/16.04 Pour plus d'informations, reportez-vous à la section Configuration de l'authentification unique réelle pour les postes de travail Linux.
Redirection USB	La fonctionnalité de redirection USB 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.
Souris 3Dconnexion	Pour commencer à utiliser la souris 3Dconnexion, vous devez installer le pilote de périphérique approprié et associer la souris à l'aide du menu Connecter le périphérique USB sur votre poste de travail Linux.
Graphiques 3D	La fonctionnalité de graphique 3D prend en charge les combinaisons suivantes de versions de Linux et de cartes graphiques : ■ vDGA est pris en charge sur RHEL 6.x Workstation x64 avec les cartes graphiques NVIDIA GRID K1 ou K2. ■ Le vGPU est pris en charge sur les distributions Linux et NVIDIA répertoriées sur https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html.

Limites des postes de travail et des pools de postes de travail Linux

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.
- La fonctionnalité de transfert de fichiers VMware HTML Access n'est pas prise 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. Pour plus d'informations, reportez-vous à la section Intégration de Linux à Active Directory.

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 ou vDGA sur les machines virtuelles Linux avant d'installer Horizon Agent sur les machines et de déployer un pool de postes de travail dans Horizon Console.

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. Pour plus d'informations, reportez-vous à la section Intégration de Linux à Active Directory.

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 Linux prises en charge pour vGPU.
   - Reportez-vous à la section Configurer RHEL 6.x pour vDGA.
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 Horizon Console, 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 d'Horizon 7 pour des pools de postes de travail manuels.

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 pris en charge pour Horizon Agent.

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

Distribution Linux	Architecture
Ubuntu 16.04 et 18.04 **Note** Vous devez appliquer l'une des solutions décrites dans l'article de la base de connaissances de VMware http://kb.vmware.com/kb/2151294.	x64
RHEL 6.6, 6.7, 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, et 8.0	x64
CentOS 6.6, 6.7, 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7 et 8.0	x64
NeoKylin 6 Update 1	x64
SLED 12.x SP1/SP2/SP3	x64
SLES 12.x SP1/SP2/SP3	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.

Note Sur les systèmes RHEL/CentOS 8.0, Horizon Agent ne prend en charge que le protocole de serveur d'affichage X11. Le protocole Wayland n'est pas pris en charge.

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. Plate-forme et versions du logiciel Horizon 7 requises

Plate-forme et logiciel	Versions prises en charge
Version de la plate-forme vSphere	■ vSphere 6.0 U2 ou version ultérieure ■ vSphere 6.5 U1 ou version ultérieure ■ vSphere 6.7 ou version ultérieure
Environnement Horizon	■ Serveur de connexion Horizon 7.11
Logiciel Horizon Client	■ Horizon Client 5.3.0 pour Android ■ Horizon Client 5.3.0 pour Windows ■ Horizon Client 5.3.0 pour Linux ■ Horizon Client 5.3.0 pour Mac OS X ■ Horizon Client 5.3.0 pour iOS (iPad Pro) ■ HTML Access 5.3.0 dans Chrome, Firefox et Internet Explorer ■ Les clients ultra légers ne sont pas pris en charge.

Ports TCP/UDP utilisés par des machines virtuelles Linux

Horizon Agent et Horizon Client utilisent des ports TCP ou UDP pour l'accès réseau entre eux et divers composants d'Horizon Server.

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

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

Note Pour plus d'informations sur les ports TCP et UDP utilisés par les clients, reportez-vous au document *Sécurité d'Horizon Client et d'Horizon Agent* et au Guide des ports réseau dans VMware Horizon 7.

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 Horizon Connection Server.

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 Horizon Connection Server 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.

Vérifier le compte Linux utilisé par des machines virtuelles Linux

Tableau 1-4. Nom et type de compte répertorie le nom et le type de compte utilisés 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 for Linux prend en charge plusieurs environnements de poste de travail sur les différentes distributions Linux. Tableau 1-5. Environnements de postes de travail pris en charge répertorie les environnements de poste de travail par défaut pour chaque distribution Linux, ainsi que les environnements de poste de travail supplémentaires pris en charge par Horizon 7 for Linux.

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

Distribution Linux	Environnement de poste de travail par défaut	Environnements de poste de travail pris en charge par Horizon 7 for Linux
Ubuntu 18.04	Gnome	Gnome Ubuntu, K Desktop Environment (KDE), MATE
Ubuntu 16.04	Unity	Gnome Flashback (Metacity), KDE, MATE
RHEL/CentOS 6.x	Gnome	Gnome, KDE
RHEL/CentOS 7.x	Gnome	Gnome, KDE
RHEL/CentOS 8.0	Gnome	Gnome
SLED 12 SP1/SP2/SP3	Gnome	Gnome

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

Distribution Linux	Environnement de poste de travail par défaut	Environnements de poste de travail pris en charge par Horizon 7 for Linux
SLES 12 SP1/SP2/SP3	Gnome	Gnome
NeoKylin 6 Update 1	Mate	Mate

Pour modifier l'environnement de poste de travail par défaut utilisé sur l'une des distributions Linux prises en charge, vous devez respecter les étapes suivantes et utiliser les commandes adaptées à votre poste de travail Linux.

Note L'authentification unique (SSO) pour les environnements de poste de travail KDE et MATE fonctionne uniquement lorsque votre poste de travail Linux utilise l'écran d'accueil par défaut (l'écran de connexion). Vous devez installer KDE et MATE à l'aide des commandes répertoriées dans Tableau 1-6. Commandes pour l'installation des environnements de poste de travail.

Lorsque vous utilisez les distributions RHEL/CentOS 7.x et Ubuntu 18.04/16.04, l'authentification automatique ne parvient pas à déverrouiller une session KDE verrouillée. Vous devez alors entrer manuellement votre mot de passe pour déverrouiller la session verrouillée.

1 Installez le système d'exploitation de la distribution Linux pris en charge avec le paramètre d'environnement de poste de travail par défaut.

2 Exécutez les commandes appropriées dans Tableau 1-6. Commandes pour l'installation des environnements de poste de travail de votre distribution Linux spécifique.

Tableau 1-6. Commandes pour l'installation des environnements de poste de travail

Distribution Linux	Nouvel environnement de poste de travail par défaut	Commandes pour modifier l'environnement de poste de travail par défaut
RHEL/CentOS 6.x	KDE	`# yum groupinstall "X Window System" "KDE Desktop"`
RHEL/CentOS 7.x	KDE	`# yum groupinstall "KDE Plasma Workspaces"`
Ubuntu 18.04/16.04	KDE	`# apt install plasma-desktop`
Ubuntu 18.04	MATE 1.225	`# apt install ubuntu-mate-desktop`

Ubuntu 16.04	MATE 1.16	`# apt-add-repository ppa:ubuntu-mate-dev/xenial-mate`
		`# apt update`
		`# apt upgrade`
		`# apt install mate`
		`# apt install ubuntu-mate-themes`

Ubuntu 16.04	Gnome Flashback (Metacity)	`# apt install gnome-session-flashback`

3 Pour commencer à utiliser le nouvel environnement de poste de travail par défaut, redémarrez le poste de travail.

Si vous avez activé l'authentification unique (SSO) sur un poste de travail Linux où plusieurs environnements de poste de travail sont installés, utilisez les informations suivantes pour sélectionner l'environnement de poste de travail à utiliser dans une session SSO.

- Pour Ubuntu 18.04/16.04 et RHEL/CentOS 7.x, utilisez les informations dans Tableau 1-7. Option SSODesktopType pour définir l'option `SSODesktopType` du fichier `/etc/vmware/viewagent-custom.conf` afin de spécifier l'environnement de poste de travail à utiliser avec l'authentification unique.

Tableau 1-7. Option SSODesktopType

Type de poste de travail	Paramètre de l'option SSODesktopType
MATE	SSODesktopType=UseMATE
GnomeUbuntu	SSODesktopType=UseGnomeUbuntu
GnomeFlashback	SSODesktopType=UseGnomeFlashback
KDE	SSODesktopType=UseKdePlasma
GnomeClassic	SSODEsktopType=UseGnomeClassic

- Pour RHEL/CentOS 6.x, pour que la session d'authentification unique (SSO) utilise KDE, supprimez du répertoire `/usr/share/xsession` tous les fichiers de démarrage de poste de travail, à l'exception du fichier de démarrage de KDE. Utilisez l'ensemble de commandes suivant comme exemple.

```
# cd /usr/share/xsessions
# mkdir backup
# mv *.desktop backup
# mv backup/kde*.desktop ./
```

  Après la configuration initiale, l'utilisateur final doit se déconnecter ou redémarrer son poste de travail Linux pour utiliser KDE comme poste de travail par défaut lors de sa prochaine session d'authentification unique (SSO).

- Pour RHEL/CentOS 8.0, afin que la session d'authentification unique (SSO) utilise Gnome Classic, supprimez du répertoire `/usr/share/xsession` tous les fichiers de démarrage de poste de travail, à l'exception du fichier de démarrage de Gnome Classic. Utilisez l'ensemble de commandes suivant comme exemple.

```
# cd /usr/share/xsessions
# mkdir backup
# mv *.desktop backup
# mv backup/gnome-classic.desktop ./
```

  Après la configuration initiale, l'utilisateur final doit se déconnecter ou redémarrer son poste de travail Linux pour utiliser Gnome Classic comme poste de travail par défaut lors de sa prochaine session d'authentification unique (SSO).

Si vous avez désactivé l'authentification unique (SSO) sur un poste de travail Linux sur lequel plusieurs environnements de poste de travail sont installés, vous n'avez pas besoin d'effectuer la procédure décrite précédemment. Les utilisateurs finaux doivent sélectionner l'environnement de poste de travail de leur choix lorsqu'ils se connectent à ce poste de travail Linux.

Conditions requises pour le réseau

VMware Blast Extreme prend en charge les protocoles UDP (User Datagram Protocol) et TCP (Transmission Control Protocol). Les conditions du réseau affectent les performances des protocoles UDP et TCP. Pour bénéficier d'une expérience utilisateur optimale, sélectionnez UDP ou TCP en fonction de la condition de réseau.

- Sélectionnez TCP si la condition du réseau est correcte, par exemple, s'il s'agit d'un environnement de réseau local (LAN).
- Sélectionnez UDP si la condition du réseau est faible, par exemple, s'il s'agit d'un environnement de réseau étendu (WAN) avec une perte de paquets et un délai de transmission.

Utilisez un analyseur de réseau, tel que Wireshark, pour déterminer si VMware Blast Extreme utilise TCP ou UDP. Utilisez les étapes suivantes, qui utilisent Wireshark, comme exemple de référence.

1 Téléchargez et installez Wireshark sur votre machine virtuelle Linux.

   Pour RHEL/CentOS 6 :

   ```
   sudo yum install wireshark
   ```

   Pour Ubuntu 18.04/16.04 :

   ```
   sudo apt install tshark
   ```

   Pour SLED/SLES 12 :

   ```
   sudo zypper install wireshark
   ```

2 Connectez-vous au poste de travail Linux à l'aide de VMware Horizon Client.

3 Ouvrez une fenêtre de terminal et exécutez la commande suivante, qui affiche le module TCP ou UDP utilisé par VMware Blast Extreme.

   ```
   sudo tshark –i any | grep 22443
   ```

Les fonctionnalités de redirection USB et de redirection du lecteur client sont sensibles aux conditions du réseau. Si la condition de réseau n'est pas correcte, par exemple, s'il s'agit d'une bande passante limitée avec des pertes de paquets et un délai de transmission, l'expérience client est fortement dégradée. Dans ces conditions, l'utilisateur final peut rencontrer l'un des problèmes suivants.

- La copie de fichiers distants peut être lente. Dans ce cas, optez plutôt pour une réduction de la taille des fichiers transmis.
- Le périphérique USB ne s'affiche pas dans le poste de travail Linux distant.

- Les données USB ne sont pas complètement transférées. Par exemple, si vous copiez un fichier volumineux, vous pouvez obtenir un fichier de taille inférieure à celle du fichier d'origine.

Pilote VHCI pour la redirection USB

La fonctionnalité de redirection USB a une dépendance sur le pilote de noyau VHCI (Virtual Host Controller Interface) USB. Pour prendre en charge la norme USB 3.0 et la fonctionnalité de redirection USB, vous devez effectuer les étapes suivantes :

1 Télécharger le code source VHCI USB depuis https://sourceforge.net/projects/usb-vhci/files/linux%20kernel%20module/.

2 Pour compiler le code source du pilote VHCI et installer le code binaire résultant sur votre système Linux, utilisez les commandes de Tableau 1-8. Compilez et installez le pilote VHCI USB.

   Par exemple, si vous décompressez le fichier d'installation, `VMware-horizonagent-linux-x86_64-<version>-<build-number>.tar.gz`, dans le répertoire `/install_tmp/`, le *`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
```

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

Tableau 1-8. Compilez et installez le pilote VHCI USB

Distribution Linux	Procédure de compilation et d'installation du pilote VHCI USB

Ubuntu 18.04	1 Installez les modules de dépendance.
	`# apt-get install make`
	`# apt-get install gcc`
	`# apt-get install libelf-dev`
	2 Compilez et installez les pilotes VHCI.
	`# 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`

Ubuntu 16.04	Compilez et installez les pilotes VHCI.
	`# 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`

Tableau 1-8. Compilez et installez le pilote VHCI USB (suite)

Distribution Linux	Procédure de compilation et d'installation du pilote VHCI USB

RHEL/ CentOS 6.9/6.10
RHEL/ CentOS 7.x
RHEL/ CentOS 8.0
	1 Installez les modules de dépendance.
	`# yum install gcc-c++`
	`# yum install kernel-devel-$(uname -r)`
	`# yum install kernel-headers-$(uname -r)`
	`# yum install patch`
	`# yum install elfutils-libelf-devel`
	2 Compilez et installez les pilotes VHCI.
	`# 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`
	3 (RHEL/CentOS 8.0) Pour vous assurer que les pilotes VHCI fonctionnent correctement avec la redirection USB, configurez des paramètres de signature pour le pilote USB.
	a Créez une paire de clés SSL pour le pilote USB.
	`openssl req -new -x509 -newkey rsa:2048 -keyout MOK.priv -outform DER -out MOK.der -nodes -days 36500 -subj "/CN=Descriptive name/"`
	b Signez le pilote USB.
	`sudo /usr/src/kernels/$(uname -r)/scripts/sign-file sha256 ./MOK.priv ./ MOK.der /lib/modules/$(uname -r)/kernel/drivers/usb/host/usb-vhci-iocifc.ko`
	`sudo /usr/src/kernels/$(uname -r)/scripts/sign-file sha256 ./MOK.priv ./ MOK.der /lib/modules/$(uname -r)/kernel/drivers/usb/host/usb-vhci-hcd.ko`
	c Enregistrez la clé pour le démarrage sécurisé UEFI.
	`sudo mokutil --import MOK.der`
	Note Cette commande émet une demande de définition d'un mot de passe de clé propriétaire de machine (MOK) pour le démarrage sécurisé UEFI.
	d Pour configurer le démarrage sécurisé UEFI dans la console vSphere, redémarrez le système. Pour plus d'informations, reportez-vous à la section https://sourceware.org/systemtap/wiki/SecureBoot.

SLED/SLES 12 SP2	1 Déterminez la version du module de noyau actuel.
	`# rpm -qa | grep kernel-default-$(echo $(uname -r) | cut -d '-' -f 1,2)`
	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.
	2 Installez les modules `kernel-devel`, `kernel-default-devel`, `kernel-macros` et `patch`.
	`# zypper install --oldpackage kernel-devel-<kernel-package-version> \ kernel-default-devel-<kernel-package-version> kernel-macros-<kernel-package-version> patch`
	Par exemple :
	`# 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`

Tableau 1-8. Compilez et installez le pilote VHCI USB (suite)

Distribution Linux	Procédure de compilation et d'installation du pilote VHCI USB

	3 Compilez et installez les pilotes VHCI.
	`# 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 –r) | cut –d '–' –f 1)/drivers/usb/core`
	`# make clean && make && make install`

En outre, observez les directives suivantes :

- 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.
- Vous pouvez aussi ajouter une prise en charge de module de noyau dynamique (DKMS) au pilote VHCI en suivant les mêmes étapes que celles de l'exemple suivant, consacré à un système Ubuntu 18.04/16.04.

  a Installez les en-têtes du noyau.

  ```
  # apt install linux–headers–`uname –r`
  ```

  b Installez la `dkms` à l'aide de la commande suivante.

  ```
  # apt install dkms
  ```

  c Procédez à l'extraction et à la correction du fichier TAR VHCI.

  ```
  # tar xzvf vhci–hcd–1.15.tar.gz
  # cd vhci–hcd–1.15
  # patch –p1 <full–path_to_patch–file>
  # cd ..
  ```

  d Copiez les fichiers source VHCI extraits vers le répertoire `/usr/src`.

  ```
  # cp –r vhci–hcd–1.15 /usr/src/usb–vhci–hcd–1.15
  ```

  e Créez un fichier nommé `dkms.conf`, puis placez-le dans le répertoire `/usr/src/usb–vhci–hcd–1.15`.

  ```
  # touch /usr/src/usb–vhci–hcd–1.15/dkms.conf
  ```

  f Ajoutez les contenus suivants au fichier `dkms.conf`.

  ```
  PACKAGE_NAME="usb–vhci–hcd"
  PACKAGE_VERSION=1.15
  MAKE_CMD_TMPL="make KVERSION=$kernelver"
  ```

```
CLEAN="$MAKE_CMD_TMPL clean"

BUILT_MODULE_NAME[0]="usb-vhci-iocifc"
DEST_MODULE_LOCATION[0]="/kernel/drivers/usb/host"
MAKE[0]="$MAKE_CMD_TMPL"

BUILT_MODULE_NAME[1]="usb-vhci-hcd"
DEST_MODULE_LOCATION[1]="/kernel/drivers/usb/host"
MAKE[1]="$MAKE_CMD_TMPL"

AUTOINSTALL="YES"
```

g Ajoutez ce pilote VHCI dans `dkms`.

```
# dkms add usb-vhci-hcd/1.15
```

h Générez le pilote VHCI.

```
# dkms build usb-vhci-hcd/1.15
```

i Installez le pilote VHCI.

```
# dkms install usb-vhci-hcd/1.15
```

Paramètres de machine virtuelle pour les graphiques 2D

Lorsque vous créez certains systèmes Horizon 7 pour des machines virtuelles Linux, vous devez modifier les paramètres de vCPU et de la mémoire virtuelle pour connaître les performances requises.

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. Il n'est pas nécessaire de modifier les paramètres de vCPU et de mémoire virtuelle pour ces machines virtuelles.

Les machines virtuelles configurées pour utiliser des graphiques 2D utilisent la carte graphique virtuelle VMware et vous devez modifier les paramètres de vCPU et de mémoire virtuelle pour améliorer les performances des postes de travail. Utilisez les instructions suivantes :

- Pour améliorer les performances d'un poste de travail 2D, définissez une plus grande quantité de vCPU et de mémoire virtuelle pour la machine virtuelle Linux. Par exemple, définissez 2 vCPU et 2 Go de mémoire virtuelle.
- Pour l'affichage de plusieurs moniteurs sur grand écran, comme quatre moniteurs, définissez 4 vCPU et 4 Go de mémoire virtuelle pour la machine virtuelle.
- Pour une lecture améliorée de vidéos dans un poste de travail 2D, définissez 4 vCPU et 4 Go de mémoire virtuelle pour la machine virtuelle.

Configuration de la collaboration de session sur des postes de travail Linux

Avec la fonctionnalité de collaboration de session, les utilisateurs peuvent inviter d'autres utilisateurs à rejoindre une session de poste de travail distant Linux existante.

Configuration système requise pour la collaboration de session

Pour prendre en charge la fonctionnalité de collaboration de session, votre déploiement d'Horizon doit satisfaire certaines exigences.

Tableau 1-9. Configuration système requise pour la collaboration de session

Composant	Configuration requise
Système client	Les propriétaires de session et les collaborateurs doivent disposer d'Horizon Client 4.10 ou version ultérieure pour Windows, Mac ou Linux installé sur le système client, ou ils doivent utiliser HTML Access 4.10 ou version ultérieure.
Postes de travail à distance Linux	Horizon Agent 7.7 ou version ultérieure doit être installé dans le poste de travail virtuel Linux. La fonctionnalité de collaboration de session doit être activée au niveau du pool de postes de travail et de VDI.
Serveur de connexion	L'instance du Serveur de connexion utilise une licence d'entreprise.
Protocole d'affichage	VMware Blast

Note Les postes de travail RHEL 8.0 requièrent une configuration système supplémentaire pour prendre en charge la collaboration de session. Reportez-vous à la section Configurer un poste de travail RHEL 8.0 pour la collaboration de session.

Pour plus d'informations sur l'utilisation de la fonctionnalité de collaboration de session, consultez la documentation de Horizon Client.

Définition des options de collaboration de session dans les fichiers de configuration

Définissez l'option suivante dans le fichier `/etc/vmware/viewagent-custom.conf` pour activer ou désactiver la fonctionnalité Collaboration de session.

- `CollaborationEnable`

Définissez les options suivantes dans le fichier `/etc/vmware/config` pour configurer les paramètres utilisés lors d'une session de collaboration.

- `collaboration.logLevel`
- `collaboration.maxCollabors`
- `collaboration.enableEmail`
- `collaboration.serverUrl`
- `collaboration.enableControlPassing`

Pour plus d'informations, reportez-vous à la section Définir des options dans des fichiers de configuration sur un poste de travail Linux.

Limites de la fonctionnalités de collaboration de session

Les utilisateurs ne peuvent pas utiliser les fonctionnalités suivantes de poste de travail distant dans une session de collaboration.

- Redirection USB
- Redirection d'entrée audio
- Redirection du lecteur client
- Redirection de carte à puce
- Redirection du Presse-papiers

Les utilisateurs ne peuvent pas modifier la résolution du poste de travail distant dans une session de collaboration.

Les utilisateurs ne peuvent pas disposer de plusieurs sessions de collaboration sur la même machine cliente.

Note Si l'icône de collaboration de session dans la barre d'état système ne répond pas lorsqu'un utilisateur se connecte pour la première fois au poste de travail distant, demandez à l'utilisateur de redimensionner la fenêtre du poste de travail distant. L'icône de collaboration de session répond une fois la fenêtre du poste de travail redimensionnée.

Configurer un poste de travail RHEL 8.0 pour la collaboration de session

Pour utiliser la fonctionnalité Collaboration de session sur un poste de travail RHEL 8.0, vous devez d'abord télécharger et installer l'extension de shell GNOME 3.28.26.

Procédure

1. Téléchargez l'extension de shell GNOME requise sur le système RHEL 8.0 depuis https://extensions.gnome.org/extension/615/appindicator-support/. Pour la version du shell, sélectionnez **3.28**. Pour la version de l'extension, sélectionnez **26**.
2. Décompactez le module téléchargé et renommez le répertoire `appindicatorsupport@rgcjonas.gmail.com` (valeur « UUID » dans le fichier `metadata.json` dans le module).
3. Utilisez la commande `mv` pour déplacer le répertoire `appindicatorsupport@rgcjonas.gmail.com` vers cet emplacement : `/usr/share/gnome-shell/extensions`.

   Par défaut, le fichier `metadata.json` dans le répertoire `appindicatorsupport@rgcjonas.gmail.com` est accessible uniquement à l'utilisateur racine. Pour prendre en charge la collaboration de session, vous devez également rendre ce fichier accessible aux autres utilisateurs.

4 Exécutez la commande pour rendre `metadata.json` lisible par d'autres utilisateurs, comme indiqué dans l'exemple suivant.

```
chmod a+r metadata.json
```

5 Installez `gnome-tweaks`.

6 Dans l'environnement de poste de travail, redémarrez le shell GNOME en appuyant sur la séquence de touches suivante sur le clavier.

```
Alt+F2
r
Enter
```

7 Dans l'environnement de poste de travail, exécutez `gnome-tweaks`, puis activez la **prise en charge de KStatusNotifierItem/AppIndicator**.

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

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 paramètres de mémoire vidéo (vRAM) des écrans que vous prévoyez d'utiliser 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 paramètres requis, suivez les instructions dans le guide d'installation de votre distribution Linux.

   Par exemple, Ubuntu 18.04 indique 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, 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 paramètres requis, suivez les instructions dans le document Paramètres de machine virtuelle pour les graphiques 2D. 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.

Pour préparer une machine Linux à des fins de gestion par Horizon 7, vous devez activer la communication entre la machine et 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 8.0/7x, CentOS 8.0/7x et SLED/SLES 12.x. Si vous préparez l'une de ces machines pour l'utiliser en tant que poste de travail distant, vous pouvez ignorer les étapes 1 à 5 de la procédure suivante, qui expliquent comment installer VMware Tools en exécutant manuellement le programme d'installation.

Si vous utilisez une machine Ubuntu 16.04/18.04, installez OVT. Si vous préparez cette machine pour l'utiliser comme poste de travail distant, vous pouvez ignorer les étapes 1 à 5 dans la procédure suivante et installer manuellement OVT sur votre machine Ubuntu 16.04/18.04 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 zxpf /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 et CentOS, vérifiez que `virbr0` est désactivé.

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

8 Assurez-vous que les instances du Horizon Connection Server 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 Horizon Console. 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. Si aucun module ne respecte les exigences, le programme d'installation interrompt l'installation.

Tableau 2-1. Modules de dépendance obligatoires

Distribution Linux	Modules
RHEL 7.5	`yum install libappindicator-gtk3`

SLES 12.x SP1/SLED 12.x SP1
Mettez à niveau `xf86-video-vmware` vers une version ultérieure à 13.0.2-3.2 à partir du référentiel SUSE.
	1 Enregistrez SUSE 12.x pour activer les référentiels SUSE.
	`SUSEConnect -r Code d'enregistrement -e E-mail`
	2 Mettez à jour la version `xf86-video-vmware`.
	`zypper update xf86-video-vmware`

SLES 12.x	L'installation de python-gobject2 est nécessaire pour les postes de travail Linux SLES 12.x lorsque vous installez Horizon Agent.
	1 Enregistrez SUSE 12.x pour activer les référentiels SUSE.
	`SUSEConnect -r Code d'enregistrement -e E-mail`
	2 Installez `python-gobject2`.
	`zypper install python-gobject2`

Ubuntu 16.04	`apt-get install python-dbus python-gobject`
Ubuntu 18.04	`apt-get install python python-dbus python-gobject`

2 Installez le module facultatif pour Horizon Agent.

- Par défaut, RHEL ou CentOS 6.7 dispose de `glibc-2.12-1.166.el6.x86_64` installé, 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
```

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

3

Horizon 7 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.

Note Horizon Agent s'attend à ce que le poste de travail Linux et l'utilisateur client résident dans le même domaine Active Directory. Si le poste de travail et l'utilisateur résident dans des domaines différents, Horizon Agent peut mal identifier le domaine de poste de travail comme étant le domaine d'utilisateur.

Ce chapitre contient les rubriques suivantes :

Intégration de Linux à Active Directory

Il existe plusieurs solutions pour intégrer Linux à Microsoft 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
- Authentification PBISO (PowerBroker Identity Services Open)
- Jonction de domaine hors ligne Samba

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

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

Utiliser l'authentification directe via le serveur OpenLDAP

Vous pouvez configurer un serveur OpenLDAP et utiliser le mécanisme d'authentification relais (PTA) pour vérifier les informations d'identification d'utilisateur via Active Directory.

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

Procédure

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.

Configurer l'authentification LDAP SSSD via Microsoft Active Directory

Vous pouvez utiliser l'authentification LDAP via Windows Active Directory en configurant SSSD (System Security Services Daemon) dans le poste de travail Linux.

Utilisez les étapes générales suivantes pour l'authentification LDAP SSSD.

Procédure

1. Pour activer le protocole LDAPS (Lightweight Directory Access Protocol over Secure Socket Layer), installez les services de certificats sur le serveur Active Directory.
2. Pour utiliser l'authentification LDAP directement par rapport à Microsoft Active Directory, configurez le protocole SSSD sur le poste de travail Linux.

Utiliser la solution de jonction de domaine Windbind

La solution de jonction de domaine Windbind, une solution d'authentification basée sur Kerberos, est une autre méthode d'authentification avec Active Directory.

Utilisez les étapes de haut niveau suivantes pour configurer la solution de jonction de domaine Windbind.

Procédure

1. Installez les modules `winbind`, `samba` et Kerberos sur le poste de travail Linux.
2. Joindre le poste de travail Linux à Microsoft Active Directory.

Étape suivante

Si vous utilisez la solution de jonction de domaine Winbind ou une autre solution basée sur l'authentification Kerberos, joignez la machine virtuelle modèle à Active Directory, puis joignez de nouveau 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 d'Horizon 7 pour des pools de postes de travail manuels.
- Incluez la commande à un script shell et définissez le chemin du script sur 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.

Configurer l'authentification PBISO (PowerBroker Identity Services Open)

La méthode d'authentification PBISO (PowerBroker Identity Services Open) est une des solutions prises en charge pour l'exécution d'une jonction de domaine hors ligne.

Suivez les étapes ci-dessous pour joindre un poste de travail Linux à Active Directory à l'aide de PBISO.

Procédure

1. Télécharger PBISO 8.5.6 ou version ultérieure à partir de `https://www.beyondtrust.com/products/powerbroker–identity–services–open/`.
2. Installer PBISO sur votre machine virtuelle Linux.

   ```
   sudo ./pbis–open–8.5.6.2029.linux.x86_64.deb.sh
   ```
3. Installer Horizon 7 Agent pour Linux.
4. Utiliser PBISO pour joindre le poste de travail Linux au domaine AD.

   Dans l'exemple suivant, **`lxdc.vdi`** est le nom de domaine et **`administrator`** est le nom d'utilisateur de domaine.

   ```
   sudo domainjoin–cli join lxdc.vdi administrator
   ```

5 Définissez la configuration par défaut pour les utilisateurs du domaine.

```
sudo /opt/pbis/bin/config UserDomainPrefix lxdc
sudo /opt/pbis/bin/config AssumeDefaultDomain true
sudo /opt/pbis/bin/config LoginShellTemplate /bin/bash
sudo /opt/pbis/bin/config HomeDirTemplate %H/%U
```

6 Modifiez le fichier `/etc/pamd.d/common-session`.

a Localisez la ligne indiquant **`session sufficient pam_lsass.so`**.

b Remplacez cette ligne par **`session [success=ok default=ignore] pam_lsass.so`**.

Note Cette étape doit être répétée après la réinstallation ou la mise à jour d'Horizon Agent for Linux.

7 Pour Ubuntu 16.04, ajoutez les lignes suivantes au fichier de configuration `/usr/share/lightdm/lightdm.conf.d/50-unity-greeter.conf`.

```
allow-guest=false
greeter-show-manual-login=true
```

Note Si vous utilisez Ubuntu 18.04, il n'est pas nécessaire de modifier le fichier de configuration `lightdm`.

8 Redémarrez votre système et connectez-vous.

Étape suivante

Note

- Si l'option `/opt/pbis/bin/config AssumeDefaultDomain` est définie sur **`false`**, vous devez mettre à jour le paramètre `SSOUserFormat=<username>@<domain>` dans le fichier `/etc/vmware/viewagent-custom.conf`.
- Lorsque vous utilisez la fonctionnalité de pool de postes de travail flottant Instant Clone Horizon, pour éviter de perdre le paramètre de serveur DNS lorsque le nouvel adaptateur réseau est ajouté à la machine virtuelle clonée, modifiez le fichier `resolv.conf` pour votre système Linux. Pour un système Ubuntu 16.04, utilisez l'exemple suivant comme un guide pour ajouter les lignes nécessaires au fichier `/etc/resolvconf/resolv.conf.d/head`.

```
nameserver 10.10.10.10
search mydomain.org
```

Configurer la jonction de domaine hors ligne Samba

Pour prendre en charge l'authentification unique sur une machine virtuelle Instant Clone dans un environnement de poste de travail Linux Horizon 7, configurez Samba sur la machine virtuelle Linux maître.

Utilisez la procédure suivante comme exemple d'utilisation de Samba pour effectuer une jonction de domaine hors ligne sur un poste de travail Linux Instant Clone à Active Directory. Cette procédure décrit les étapes pour un système Ubuntu.

Procédure

1. Sur votre machine virtuelle Linux maître, installez les modules `winbind` et `samba`, y compris les autres bibliothèques dépendantes, comme `smbfs` et `smbclient`.
2. Installez le module `tdb-tools` Samba à l'aide de la commande suivante.

```
sudo apt-get install tdb-tools
```

3. Installer Horizon 7 Agent pour Linux.
4. Modifiez le fichier de configuration `/etc/samba/smb.conf` afin que son contenu soit semblable à l'exemple suivant.

```
[global]
security = ads
realm = LAB.EXAMPLE.COM
workgroup = LAB
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum group = yes
template homedir = /home/%D/%U
template shell = /bin/bash
client use spnego = yes
client ntlmv2 auth = yes
encrypt passwords = yes
winbind use default domain = yes
restrict anonymous = 2
```

5. Modifiez le fichier de configuration `/etc/krb5.conf` afin que son contenu soit semblable à l'exemple suivant.

```
[libdefaults]
default_realm = EXAMPLE.COM

krb4_config = /etc/krb.conf
krb4_realms = /etc/krb.realms

kdc_timesync = 1
ccache_type = 4
forwardable = true
proxiable = true

[realms]
YOUR-DOMAIN = {
kdc = 10.111.222.33
}
```

```
[domain_realm]
your-domain = EXAMPLE.COM
.your-domain = EXAMPLE.COM
```

6 Modifiez le fichier de configuration `/etc/nsswitch.conf`, comme indiqué dans l'exemple suivant.

```
passwd: files winbind
group: files winbind
shadow: files winbind
gshadow: files
```

7 Vérifiez que le nom d'hôte est correct et que la date et l'heure du système sont synchronisées avec votre système DNS.

8 Pour informer Horizon Agent que la machine virtuelle Linux est jointe au domaine à l'aide de la méthode Samba, définissez l'option suivante dans le fichier `/etc/vmware/viewagent-custom.conf`.

```
OfflineJoinDomain=samba
```

9 Redémarrez votre système et reconnectez-vous.

Utiliser la solution de jonction de domaine pour RHEL/CentOS 8.0

Pour garantir le fonctionnement de fonctionnalités telles que l'authentification unique pour un poste de travail RHEL/CentOS 8.0, utilisez la solution de domaine pour joindre le poste de travail à votre domaine Active Directory (AD).

Procédure

1 Configurez un nom d'hôte complet pour le système RHEL/CentOS 8.0.

Par exemple, si **rhel8** correspond au nom d'hôte non complet du système et **LXD.VDI** correspond au domaine AD, exécutez la commande suivante.

```
# hostnamectl set-hostname rhel8.lxd.vdi
```

2 Vérifiez la connexion réseau avec le domaine AD, comme illustré dans l'exemple suivant.

```
# realm discover -vvv LXD.VDI
```

3 Installez les modules de dépendance souhaités, comme illustré dans l'exemple suivant.

```
 # dnf install -y sssd adcli samba-common-tools oddjob oddjob-mkhomedir
```

4 Joignez le domaine AD, comme indiqué dans l'exemple suivant.

```
# realm join -U Administrator LXD.VDI
```

5 Modifiez le fichier `/etc/sssd/sssd.conf` de sorte qu'il se présente comme dans l'exemple suivant. Ajoutez `ad_gpo_map_interactive = +gdm-vmwcred` sous la section *[domaine/nom de domaine]*.

```
[sssd]
domains = LXD.VDI
config_file_version = 2
services = nss, pam

[domain/LXD.VDI]
ad_domain = LXD.VDI
krb5_realm = LXD.VDI
realmd_tags = manages-system joined-with-adcli
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = False
fallback_homedir = /home/%u
access_provider = ad
ad_gpo_map_interactive = +gdm-vmwcred
```

6 Pour vous assurer que la jonction de domaine prend effet, redémarrez votre système et reconnectez-vous.

7 Vérifiez que les utilisateurs du domaine sont correctement configurés. L'exemple suivant illustre comment utiliser la commande `id` pour renvoyer la sortie de configuration de l'utilisateur du domaine **zyc1**.

```
# id zyc1

uid=1084401403(zyc1) gid=1084400513(domain users) groups=1084400513(domain users)
```

8 À l'aide des informations d'identification d'un utilisateur de domaine, vérifiez que vous parvenez à vous connecter au poste de travail.

Note Horizon Agent ne prend en charge que le protocole de serveur d'affichage X11 pour les postes de travail RHEL/CentOS 8.0. Pour configurer X11 en tant que protocole de serveur d'affichage par défaut pour votre système, cliquez sur l'icône Paramètres sur l'écran de connexion et sélectionnez **Classique (serveur d'affichage X11)** dans le menu déroulant.

Configuration de l'authentification unique

Pour configurer l'authentification unique (SSO), vous devez effectuer des étapes de configuration.

Le mode d'authentification unique Horizon communique avec PAM (Pluggable Authentication Modules) dans Linux et ne dépend pas de la méthode que vous utilisez pour intégrer Linux à Active Directory (AD). Horizon 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. L'authentification unique 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. Par exemple, si vous disposez d'un utilisateur, `juser` dans AD `mycompany.com`, mais que l'UPN de l'utilisateur est défini sur `juser123@mycompany.com` plutôt que sur `juser@mycompany.com`, SSO échoue. La solution pour l'utilisateur consiste à se connecter avec le nom stocké dans `sAMAccount`. Par exemple, `juser`.

Horizon 7 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/sssd/sssd.conf` et ajoutez la ligne suivante dans la section `[domain/default]` :

```
case_sensitive = false
```

Si plusieurs environnements de poste de travail sont installés sur votre poste de travail Linux, reportez-vous au document Environnement de poste de travail pour sélectionner l'environnement de poste de travail à utiliser avec l'authentification unique.

Configuration de la redirection de carte à puce

Pour configurer la redirection de carte à puce, vous devez effectuer des étapes de configuration.

Présentation de la redirection de carte à puce

La redirection de carte à puce est prise en charge sur les postes de travail exécutant les distributions Linux suivantes avec les versions spécifiées d'Horizon Agent installées.

Tableau 3-1. Configuration système requise pour la redirection de carte à puce

Distribution Linux	Horizon Agent
RHEL 8.0	Horizon Agent 7.10 ou version ultérieure
RHEL 7.1 ou version ultérieure	Horizon Agent 7.8 ou version ultérieure
RHEL 6.6 ou version ultérieure	Horizon Agent 6.2.1 ou version ultérieure
Ubuntu 18.04/16.04	Horizon Agent 7.9 ou version ultérieure
SLED/SLES 12.x SP3	Horizon Agent 7.9 ou version ultérieure

Lorsque vous installez Horizon Agent, vous devez d'abord désactiver 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.

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 à la fois. Cette fonctionnalité ne fonctionne pas si deux lecteurs ou plus sont connectés au système 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. Ce comportement est une limite de Linux.

Note La redirection de carte à puce prend en charge les cartes PIV sur les postes de travail Linux. Lorsque vous utilisez Horizon Client pour Linux pour authentifier le broker avec une carte PIV, vous devez configurer la carte à puce PIV avec prise en charge de TLSv1.2 pour éviter de recevoir une erreur SSL. Utilisez la solution décrite dans l'article de la base de connaissances de VMware http://kb.vmware.com/kb/2150470.

Note L'authentification unique de carte à puce est activée dans Horizon 7 version 7.0.1 ou version ultérieure. Les postes de travail RHEL 6.x prennent en charge l'authentification unique de carte à puce, contrairement aux postes de travail RHEL 7.x et RHEL 8.0.

Configuration de la redirection de carte à puce

Pour configurer la redirection de carte à puce, effectuez les tâches suivantes.

1 Configurez la carte à puce pour votre poste de travail en suivant les instructions du distributeur Linux et du fournisseur de la carte à puce.

2 Intégrez votre poste de travail à un domaine Active Directory, en suivant la procédure de votre distribution Linux.

3 Configurez la redirection de carte à puce sur votre poste de travail, en suivant la procédure de votre distribution Linux.

Configuration de la redirection de carte à puce pour les postes de travail RHEL 8.0

Pour configurer la direction de carte à puce pour un poste de travail RHEL 8.0, intégrez d'abord le poste de travail à un domaine Active Directory. Installez ensuite les bibliothèques et le certificat d'autorité de certification racine nécessaires avant Horizon Agent.

Intégrer un poste de travail RHEL 8.0 à Active Directory pour la redirection de carte à puce

Utilisez la procédure suivante pour intégrer un poste de travail RHEL 8.0 à un domaine Active Directory (AD) pour la redirection de carte à puce.

Certains exemples de la procédure utilisent des valeurs d'espace réservé pour représenter des entités dans votre configuration réseau, telles que le nom DNS de votre domaine AD. Remplacez les valeurs d'espace réservé par des informations spécifiques à votre configuration, comme décrit dans le tableau suivant.

Valeur d'espace réservé	Description
dns_IP_ADDRESS	Adresse IP de votre serveur de nom DNS
rhel8sc.rzview2.com	Nom d'hôte complet de votre système RHEL 8.0
rhel8sc	Nom d'hôte non qualifié de votre système RHEL 8.0
rzview2.com	Nom DNS de votre domaine AD
RZVIEW2.COM	Nom DNS de votre domaine AD en majuscules
RZVIEW2	Nom DNS du groupe de travail ou domaine NT qui inclut votre serveur Samba, en majuscules
rzviewdns.rzview2.com	Nom d'hôte de votre serveur AD

Procédure

1 Sur votre système RHEL 8.0, procédez comme suit.

a Configurez les paramètres réseau et DNS selon les besoins de votre organisation.

b Désactivez **IPv6**.

c Désactivez **DNS automatique**.

2 Configurez le fichier de configuration `/etc/hosts` de sorte qu'il se présente comme dans l'exemple suivant.

```
127.0.0.1        rhel8sc.rzview2.com rhel8sc localhost localhost.localdomain localhost4
localhost4.localdomain4
::1              localhost localhost.localdomain localhost6 localhost6.localdomain6

dns_IP_ADDRESS   rzviewdns.rzview2.com
```

3 Configurez le fichier de configuration `/etc/resolv.conf` afin qu'il se présente comme dans l'exemple suivant.

```
# Generated by NetworkManager
search rzview2.com
nameserver dns_IP_ADDRESS
```

4 Installez les modules souhaités pour l'intégration AD.

```
# yum install –y samba–common–tools oddjob–mkhomedir
```

5 Activez le service `oddjobd`.

```
# systemctl enable oddjobd.service
# systemctl start oddjobd.service
```

6 Spécifiez l'identité système et les sources d'authentification.

```
# authselect select sssd with–smartcard with–mkhomedir
```

7 Démarrez le service `oddjobd`.

```
# systemctl enable oddjobd.service
# systemctl start oddjobd.service
```

8 Pour prendre en charge l'authentification par carte à puce, créez le fichier `/etc/sssd/sssd.conf`.

```
# touch /etc/sssd/sssd.conf
# chmod 600 touch /etc/sssd/sssd.conf
# chown root:root /etc/sssd/sssd.conf
```

9 Ajoutez le contenu souhaité à `/etc/sssd/sssd.conf`, comme illustré dans l'exemple suivant. Dans la section **`[pam]`**, spécifiez **`pam_cert_auth = True`**.

```
[sssd]
config_file_version = 2
domains = rzview2.com
services = nss, pam, pac

[domain/RZVIEW2.COM]
id_provider = ad
auth_provider = ad
```

```
chpass_provider = ad
access_provider = ad
cache_credentials = true

[pam]
pam_cert_auth = True
```

10 Activez le service `sssd`.

```
# systemctl enable sssd.service
# systemctl start sssd.service
```

11 Modifiez le fichier de configuration `/etc/krb5.conf` de sorte qu'il se présente comme dans l'exemple suivant.

```
# To opt out of the system crypto-policies configuration of krb5, remove the
# symlink at /etc/krb5.conf.d/crypto-policies which will not be recreated.
includedir /etc/krb5.conf.d/

[logging]
    default = FILE:/var/log/krb5libs.log
    kdc = FILE:/var/log/krb5kdc.log
    admin_server = FILE:/var/log/kadmind.log

[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    pkinit_anchors = /etc/pki/tls/certs/ca-bundle.crt
    spake_preauth_groups = edwards25519
    default_realm = RZVIEW2.COM
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
 RZVIEW2.COM = {
     kdc = rzviewdns.rzview2.com
     admin_server = rzviewdns.rzview2.com
     default_domain = rzviewdns.rzview2.com
     pkinit_anchors = FILE:/etc/pki/nssdb/certificate.pem
     pkinit_cert_match = <KU>digitalSignature
     pkinit_kdc_hostname = rzviewdns.rzview2.com
 }

[domain_realm]
 .rzview2.com = RZVIEW2.COM
 rzview2.com = RZVIEW2.COM
```

12 Modifiez le fichier de configuration `/etc/samba/smb.conf` de sorte qu'il se présente comme dans l'exemple suivant.

```
[global]
        workgroup = RZVIEW2
```

```
        security = ads
        passdb backend = tdbsam
        printing = cups
        printcap name = cups
        load printers = yes
        cups options = raw
        password server = rzviewdns.rzview2.com
        realm = RZVIEW2.COM
        idmap config * : range = 16777216-33554431
        template homedir =/home/RZVIEW2/%U
        template shell = /bin/bash
        kerberos method = secrets and keytab

[homes]
        comment = Home Directories
        valid users = %S, %D%w%S
        browseable = No
        read only = No
        inherit acls = Yes

[printers]
        comment = All Printers
        path = /var/tmp
        printable = Yes
        create mask = 0600
        browseable = No

[print$]
        comment = Printer Drivers
        path = /var/lib/samba/drivers
        write list = @printadmin root
        force group = @printadmin
        create mask = 0664
        directory mask = 0775
```

13 Joignez le domaine AD, comme indiqué dans l'exemple suivant.

```
# net ads join -U AdminUser
```

L'exécution de la commande `join` renvoie un résultat similaire à l'exemple suivant.

```
Enter AdminUser's password:
Using short domain name -- RZVIEW2
Joined 'RHEL8SC' to dns domain 'rzview2.com'
```

14 Vérifiez que le poste de travail RHEL 8.0 est correctement joint au domaine AD.

```
# net ads testjoin

Join is OK
```

Étape suivante

Configurer la redirection de carte à puce pour un poste de travail RHEL 8.0

Configurer la redirection de carte à puce pour un poste de travail RHEL 8.0

Pour configurer la redirection de carte à puce sur un poste de travail RHEL 8.0, installez les bibliothèques dont dépend la fonctionnalité, le certificat d'autorité de certification racine pour prendre en charge l'authentification approuvée des cartes à puce et la bibliothèque PC/SC Lite requise.

Conditions préalables

Intégrer un poste de travail RHEL 8.0 à Active Directory pour la redirection de carte à puce

Procédure

1 Installez les bibliothèques requises.

```
# yum install -y opensc pcsc-lite pcsc-lite-libs pcsc-lite-ccid nss-tools
```

2 Activez le service `pcscd`.

```
# systemctl enable pcscd
# systemctl start pcscd
```

3 Assurez-vous que le fichier de configuration `/etc/sssd/sssd.conf` contient les lignes suivantes, qui activent l'authentification de la carte à puce.

```
[pam]
pam_cert_auth = True
```

4 Copiez le certificat d'autorité de certification requis sur `/etc/sssd/pki/sssd_auth_ca_db.pem`.

```
# openssl x509 -inform der -in certificate.cer -out certificate.pem
# cp certificate.pem /etc/sssd/pki/sssd_auth_ca_db.pem
```

5 Pour vérifier l'état de la carte à puce, exécutez les commandes `pkcs11-tool` suivantes et assurez-vous qu'elles renvoient la sortie correcte.

```
# pkcs11-tool -L

# pkcs11-tool --login -O

# pkcs11-tool --test --login
```

6 Configurez le module PKCS11.

```
cp libcmP11.so /usr/lib64/
```

7 Créez le fichier `/usr/share/p11-kit/modules/libcmP11.module`. Ajoutez le contenu suivant au fichier.

```
# This file describes how to load the opensc module
# See: http://p11-glue.freedesktop.org/doc/p11-kit/config.html

# This is a relative path, which means it will be loaded from
# the p11-kit default path which is usually $(libdir)/pkcs11.
```

```
# Doing it this way allows for packagers to package opensc for
# 32-bit and 64-bit and make them parallel installable
module: /usr/lib64/libcmP11.so
priority: 99
```

8 Mettez PC/SC Lite à jour vers la version 1.8.8.

```
# yum install -y git flex autoconf automake libtool libudev-devel flex
# git clone https://salsa.debian.org/rousseau/PCSC.git
# cd PCSC
# git checkout -b 1.8.8 pcsc-1.8.8
# ./bootstrap
# ./configure --build=x86_64-redhat-linux-gnu --host=x86_64-redhat-linux-gnu
     --program-prefix= --disable-dependency-tracking --prefix=/usr --exec-prefix=/usr
     --bindir=/usr/bin --sbindir=/usr/sbin --sysconfdir=/etc --datadir=/usr/share
     --includedir=/usr/include --libdir=/usr/lib64 --libexecdir=/usr/libexec
     --localstatedir=/var --sharedstatedir=/var/lib --mandir=/usr/share/man
     --infodir=/usr/share/info --disable-static --enable-usbdropdir=/usr/lib64/pcsc/drivers
# make
# make install
```

9 Installez Horizon Agent 7.10 ou version ultérieure, avec la redirection de carte à puce activée.

10 Redémarrez votre système et reconnectez-vous.

Configuration de la redirection de carte à puce pour les postes de travail RHEL 7.x/6.x

Pour configurer la direction de la carte à puce pour un poste de travail RHEL 7.x/6.x, intégrez d'abord le poste de travail à un domaine Active Directory. Installez ensuite les bibliothèques et le certificat d'autorité de certification racine nécessaires avant Horizon Agent.

Intégrer un poste de travail RHEL 7.x/6.x à Active Directory pour la redirection de carte à puce

Pour prendre en charge la redirection de carte à puce sur un poste de travail RHEL 7.x/6.x, intégrez le poste de travail à un domaine Active Directory (AD) à l'aide des solutions Samba et Winbind.

Utilisez la procédure suivante pour intégrer un poste de travail RHEL 7.x/6.x à un domaine AD pour la redirection de carte à puce.

Certains exemples de la procédure utilisent des valeurs d'espace réservé pour représenter des entités dans votre configuration réseau, telles que le nom DNS de votre domaine AD. Remplacez les valeurs d'espace réservé par des informations spécifiques à votre configuration, comme décrit dans le tableau suivant.

Valeur d'espace réservé	Description
dns_IP_ADDRESS	Adresse IP de votre serveur de nom DNS
mydomain.com	Nom DNS de votre domaine AD
MYDOMAIN.COM	Nom DNS de votre domaine AD en majuscules

Valeur d'espace réservé	Description
MYDOMAIN	Nom DNS du groupe de travail ou domaine NT qui inclut votre serveur Samba, en majuscules
ads-hostname	Nom d'hôte de votre serveur AD

Note La redirection de carte à puce est prise en charge sur les postes de travail exécutant RHEL 6.0 ou version ultérieure ou RHEL 7.1 ou version ultérieure.

Procédure

1 Sur votre poste de travail RHEL 7.x/6.x, installez les modules souhaités.

```
# yum install nscd samba-winbind krb5-workstation pam_krb5 samba-winbind-clients authconfig-gtk
```

2 Modifiez les paramètres réseau pour la connexion à votre système. Ouvrez le panneau de configuration NetworkManager et accédez à **Paramètres IPv4** pour la connexion à votre système. Pour la méthode IPv4, sélectionnez **Automatique (DHCP)**. Dans la zone de texte **Serveur DNS**, entrez l'adresse IP de votre serveur de nom DNS. Puis cliquez sur **Appliquer**.

3 Exécutez la commande suivante et vérifiez que le système renvoie le nom de domaine complet de votre poste de travail RHEL.

```
# hostname –f
```

4 Modifiez le fichier de configuration `/etc/resolve.conf`, comme indiqué dans l'exemple suivant.

```
search mydomain.com
nameserver dns_IP_ADDRESS
```

5 Désactivez Security-Enhanced Linux (SELinux) sur votre poste de travail RHEL. Modifiez le fichier de configuration `/etc/selinux/config`, comme indiqué dans l'exemple suivant.

```
SELINUX=disabled
```

6 Modifiez le fichier de configuration `/etc/krb5.conf`, comme indiqué dans l'exemple suivant.

```
[libdefaults]
      dns_lookup_realm = false
      ticket_lifetime = 24h
      renew_lifetime = 7d
      forwardable = true
      rdns = false
      default_realm = MYDOMAIN.COM
      default_ccache_name = KEYRING:persistent:%{uid}

[realms]
      MYDOMAIN.COM = {
            kdc = ads-hostname
            admin_server = ads-hostname
            default_domain = ads-hostname
```

```
      }

[domain_realm]
      .mydomain.com = MYDOMAIN.COM
      mydomain.com = MYDOMAIN.COM
```

7 Modifiez le fichier de configuration `/etc/samba/smb.conf`, comme indiqué dans l'exemple suivant.

```
[global]
      workgroup = MYDOMAIN
      password server = ads-hostname
      realm = MYDOMAIN.COM
      security = ads
      idmap config * : range = 16777216-33554431
      template homedir =/home/MYDOMAIN/%U
      template shell = /bin/bash
      kerberos method = secrets and keytab
      winbind use default domain = true
      winbind offline logon = false
      winbind refresh tickets = true

      passdb backend = tdbsam
```

8 Ouvrez l'outil `authconfig-gtk` et configurez les paramètres comme suit.

a Sélectionnez l'onglet **Identity & Authentication (Identité et authentification)**. Pour User Account Database (Base de données du compte d'utilisateur), sélectionnez **Winbind**.

b Sélectionnez l'onglet **Advanced Options (Options avancées)** et cochez la case **Create home directories on the first login (Créer des répertoires de base lors de la première connexion)**.

c Sélectionnez l'onglet **Identity & Authentication (Identité et authentification)**, puis cliquez sur **Join Domain (Joindre le domaine)**. À l'alerte vous invitant à enregistrer les modifications, cliquez sur **Save (Enregistrer)**.

d Lorsque vous y êtes invité, entrez le nom d'utilisateur et le mot de passe de l'administrateur de domaine, puis cliquez sur **OK**.

Votre poste de travail RHEL est joint au domaine AD.

9 Configurez la mise en cache de ticket sur PAM Winbind. Modifiez le fichier de configuration `/etc/security/pam_winbind.conf` afin qu'il inclue les lignes indiquées dans l'exemple suivant.

```
[global]

# authenticate using kerberos
;krb5_auth = yes

# create homedirectory on the fly
;mkhomedir = yes
```

10 Redémarrez le service Winbind.

```
# sudo service winbind restart
```

11 Pour vérifier la jonction AD, exécutez les commandes suivantes et assurez-vous qu'elles renvoient le résultat correct.

- `net ads testjoin`
- `net ads info`

12 Redémarrez votre système et reconnectez-vous.

Étape suivante

Configurer la redirection de carte à puce pour un poste de travail RHEL 7.x/6.x

Configurer la redirection de carte à puce pour un poste de travail RHEL 7.x/6.x

Pour configurer la redirection de carte à puce sur un poste de travail RHEL 7.x/6.x, installez les bibliothèques dont dépend la fonctionnalité, le certificat d'autorité de certification racine pour l'authentification et la bibliothèque PC/SC Lite souhaitée. En outre, vous devez modifier certains fichiers de configuration pour terminer la configuration de l'authentification.

Utilisez la procédure suivante pour configurer la redirection de carte à puce pour un poste de travail RHEL 7.x/6.x.

Certains exemples de la procédure utilisent des valeurs d'espace réservé pour représenter des entités dans votre configuration réseau, telles que le nom DNS de votre domaine AD. Remplacez les valeurs d'espace réservé par des informations spécifiques à votre configuration, comme décrit dans le tableau suivant.

Valeur d'espace réservé	Description
dns_IP_ADDRESS	Adresse IP de votre serveur de nom DNS
mydomain.com	Nom DNS de votre domaine AD
MYDOMAIN.COM	Nom DNS de votre domaine AD en majuscules
MYDOMAIN	Nom DNS du groupe de travail ou domaine NT qui inclut votre serveur Samba, en majuscules
ads-hostname	Nom d'hôte de votre serveur AD

La redirection de carte à puce est prise en charge sur les postes de travail exécutant RHEL 6.0 ou version ultérieure ou RHEL 7.1 ou version ultérieure.

Note Si vous utilisez la console vSphere pour vous connecter à un système RHEL 7.x sur lequel Horizon Agent est installé et que la redirection de carte à puce est activée, vous pouvez observer une durée de déconnexion différée d'au moins deux minutes. Cette déconnexion différée se produit uniquement à partir de la console vSphere. L'expérience de déconnexion de RHEL 7.x de Horizon Client n'est pas affectée.

Conditions préalables

Intégrer un poste de travail RHEL 7.x/6.x à Active Directory pour la redirection de carte à puce

Procédure

1 Installez les bibliothèques requises.

```
yum install nss-tools nss-pam-ldapd esc pam_pkcs11 pam_krb5 opensc pcsc-lite-ccid authconfig
      authconfig-gtk krb5-libs krb5-workstation krb5-pkinit pcsc-lite pcsc-lite-libs
```

2 Installez un certificat d'autorité de certification racine (CA).

a Téléchargez un certificat d'autorité de certification racine et enregistrez-le dans `/tmp/certificate.cer` sur votre poste de travail. Reportez-vous à Exportation du certificat d'autorité de certification de racine.

b Localisez le certificat d'autorité de certification racine que vous avez téléchargé et transférez-le vers un fichier `.pem`.

```
openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

c Utilisez la commande `certutil` pour installer le certificat d'autorité de certification racine dans la base de données système `/etc/pki/nssdb`.

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

d Copiez le certificat d'autorité de certification racine dans le répertoire `/etc/pam_pkcs11/cacerts`.

```
mkdir -p /etc/pam_pkcs11/cacerts

cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
```

3 Accédez à **Applications > Sundry > Authentification**, cochez la case **Activer la prise en charge de l'authentification par carte à puce** et cliquez sur **Appliquer**.

4 Copiez les pilotes de carte à puce et ajoutez la bibliothèque de pilotes au système de base de données `/etc/pki/nssdb`.

```
cp libcmP11.so /usr/lib64/
modutil -add "piv card 2.0" -libfile /usr/lib64/libcmP11.so -dbdir /etc/pki/nssdb/
```

5 Modifiez le paramètre `module` dans le fichier de configuration `/etc/pam_pkcs11/pam_pkcs11.conf`, comme indiqué dans l'exemple suivant.

```
pkcs11_module coolkey {
      module = libcmP11.so;
      description = "Cool Key";
      slot_num = 0;
      ca_dir = /etc/pam_pkcs11/cacerts;
      nss_dir = /etc/pki/nssdb;
      cert_policy = ca, signature;
}
```

6 Modifiez le fichier `/etc/pam_pkcs11/cn_map` afin que son contenu soit semblable à l'exemple suivant. Pour le contenu spécifique à inclure, consultez les informations utilisateur répertoriées dans le certificat de carte à puce.

```
user sc -> user-sc
```

7 Modifiez le fichier de configuration `/etc/krb5.conf/`, comme indiqué dans l'exemple suivant.

```
[libdefaults]
      dns_lookup_realm = false
      ticket_lifetime = 24h
      renew_lifetime = 7d
      forwardable = true
      rdns = false
      default_realm = MYDOMAIN.COM
      default_ccache_name = KEYRING:persistent:%{uid}

[realms]
      MYDOMAIN.COM = {
            kdc = ads-hostname
            admin_server = ads-hostname
            default_domain = ads-hostname
            pkinit_anchors = FILE:/etc/pki/nssdb/certificate.pem
            pkinit_cert_match = <KU>digitalSignature
            pkinit_kdc_hostname = ads-hostname
      }

[domain_realm]
      .mydomain.com = MYDOMAIN.COM
      mydomain.com = MYDOMAIN.COM
```

8 Modifiez le fichier de configuration `/etc/pam.d/system-auth` afin qu'il inclue la ligne indiquée dans l'exemple suivant.

```
auth  optional  pam_krb5.so use_first_pass no_subsequent_prompt
                preauth_options=X509_user_identity=PKCS11:/usr/lib64/libcmP11.so
```

9 Redémarrez le démon PC/SC.

```
chkconfig pcscd on
service pcscd start
```

10 Installez la version PC/SC Lite requise pour votre distribution RHEL.

- Pour RHEL 7.x, installez Lite PC/SC, version 1.8.8.

```
yum install git flex autoconf automake libtool libudev-devel flex
git clone https://salsa.debian.org/rousseau/PCSC.git
cd PCSC
git checkout -b 1.8.8 pcsc-1.8.8
./bootstrap
./configure --build=x86_64-redhat-linux-gnu --host=x86_64-redhat-linux-gnu --program-prefix=
   --disable-dependency-tracking --prefix=/usr --exec-prefix=/usr --bindir=/usr/bin --
```

```
sbindir=/usr/sbin
   --sysconfdir=/etc --datadir=/usr/share --includedir=/usr/include --libdir=/usr/lib64
   --libexecdir=/usr/libexec --localstatedir=/var --sharedstatedir=/var/lib --mandir=/usr/
share/man
   --infodir=/usr/share/info --disable-static --enable-usbdropdir=/usr/lib64/pcsc/drivers
make
make install
```

- Pour RHEL 6.x, installez PC/SC Lite, version 1.7.4.

```
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-ipcdir=/var/run  --disable-libusb --disable-serial --disable-
usb
 --disable-libudev
make
make install
service pcscd start
```

11 Installez le module Horizon Agent, avec la redirection de carte à puce activée.

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

Installez le module requis pour votre distribution RHEL :

- Pour RHEL 7.x, vous devez installer Horizon Agent 7.8 ou version ultérieure.
- Pour RHEL 6.x, vous devez installer View Agent 6.2.1 ou version ultérieure.

12 Redémarrez votre système et reconnectez-vous.

Configuration de la redirection de carte à puce pour les postes de travail Ubuntu

Pour configurer la direction de carte à puce pour un poste de travail Ubuntu, intégrez d'abord le poste de travail à un domaine Active Directory. Installez ensuite les bibliothèques et le certificat d'autorité de certification racine nécessaires avant Horizon Agent.

Intégrer un poste de travail Ubuntu à Active Directory pour la redirection de carte à puce

Pour prendre en charge la redirection de carte à puce sur un poste de travail Ubuntu, intégrez le poste de travail à un domaine Active Directory (AD) à l'aide des solutions Samba et Winbind.

Utilisez la procédure suivante pour intégrer un poste de travail Ubuntu à un domaine AD pour la redirection de carte à puce.

Certains exemples de la procédure utilisent des valeurs d'espace réservé pour représenter des entités dans votre configuration réseau, telles que le nom DNS de votre domaine AD. Remplacez les valeurs d'espace réservé par des informations spécifiques à votre configuration, comme décrit dans le tableau suivant.

Valeur d'espace réservé	Description
dns_IP_ADDRESS	Adresse IP de votre serveur de nom DNS
mydomain.com	Nom DNS de votre domaine AD
MYDOMAIN.COM	Nom DNS de votre domaine AD en majuscules
MYDOMAIN	Nom DNS du groupe de travail ou domaine NT qui inclut votre serveur Samba, en majuscules
ads-hostname	Nom d'hôte de votre serveur AD
ads-hostname.mydomain.com	Nom de domaine complet (FQDN) de votre serveur AD
mytimeserver.mycompany.com	Nom DNS de votre serveur de temps NTP
AdminUser	Nom d'utilisateur de l'administrateur de poste de travail Linux

Procédure

1. Sur votre poste de travail Ubuntu, définissez le nom d'hôte du poste de travail en modifiant le fichier de configuration `/etc/hostname`.
2. Configurez DNS.
   a. Ajoutez le nom du serveur DNS et l'adresse IP au fichier de configuration `/etc/hosts`.
   b. Ajoutez l'adresse IP de votre serveur de nom DNS et le nom DNS de votre domaine AD au fichier de configuration `/etc/network/interfaces`, comme indiqué dans l'exemple suivant.

```
dns-nameservers dns_IP_ADDRESS
dns-search mydomain.com
```

3. Installez le module `resolvconfig`.
   a. Exécutez la commande d'installation.

```
# apt-get install -y resolvconf
```

   Autorisez le système à installer le module et à redémarrer.
   b. Vérifiez votre configuration DNS dans le fichier `/etc/resolve.conf`, comme indiqué dans l'exemple suivant.

```
# cat /etc/resolve.conf
…
nameserver dns_IP_ADDRESS
search mydomain.com
```

4 Configurez la synchronisation de l'heure du réseau.

a Installez le module `ntpdate`.

```
# apt-get install -y ntpdate
```

b Ajoutez les informations du serveur NTP au fichier de configuration `/etc/systemd/timesyncd.conf`, comme indiqué dans l'exemple suivant.

```
[Time]
NTP=mytimeserver.mycompany.com
```

5 Redémarrez le service NTP.

```
sudo service ntpdate restart
```

6 Installez les modules de jonction AD requis.

a Exécutez la commande d'installation.

```
# apt-get install -y samba krb5-config krb5-user winbind libpam-winbind
    libnss-winbind
```

b À l'invite d'installation demandant le domaine Kerberos par défaut, entrez le nom DNS de votre domaine AD en lettres majuscules (par exemple, `MYDOMAIN.COM`). Sélectionnez ensuite **OK**.

7 Modifiez le fichier de configuration `/etc/krb5.conf`, comme indiqué dans l'exemple suivant.

```
[libdefaults]
      dns_lookup_realm = false
      ticket_lifetime = 24h
      renew_lifetime = 7d
      forwardable = true
      rdns = false
      default_realm = MYDOMAIN.COM
      default_ccache_name = KEYRING:persistent:%{uid}

[realms]
      MYDOMAIN.COM = {
            kdc = ads-hostname.mydomain.com
            admin_server = ads-hostname.mydomain.com
            default_domain = ads-hostname.mydomain.com
            pkinit_anchors = FILE:/etc/pki/nssdb/certificate.pem
            pkinit_cert_match = <KU>digitalSignature
            pkinit_kdc_hostname = ads-hostname.mydomain.com
      }

[domain_realm]
      .mydomain.com = MYDOMAIN.COM
      mydomain.com = MYDOMAIN.COM
```

8 Pour vérifier la certification Kerberos, exécutez les commandes suivantes.

```
# kinit Administrator@MYDOMAIN.COM

# klist
```

Vérifiez que les commandes renvoient un résultat similaire à l'exemple suivant.

```
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: Administrator@MYDOMAIN.COMValid starting       Expires               Service
principal
2019-05-27T17:12:03   2019-05-28T03:12:03    krbtgt/MYDOMAIN.COM@MYDOMAIN.COM
        renew until 2019-05-28T17:12:03
```

9 Modifiez le fichier de configuration `/etc/samba/smb.conf`, comme indiqué dans l'exemple suivant.

```
[global]
      workgroup = MYDOMAIN
      realm = MYDOMAIN.COM
      password server = ads-hostname.mydomain.com
      security = ads
      kerberos method = secrets only
      winbind use default domain = true
      winbind offline logon = false
      template homedir =/home/%D/%U
      template shell = /bin/bash
      client use spnego = yes
      client ntlmv2 auth = yes
      encrypt passwords = yes
      passdb backend = tdbsam
      winbind enum users = yes
      winbind enum groups = yes
      idmap uid = 10000-20000
      idmap gid = 10000-20000
```

10 Joignez le domaine AD et vérifiez l'intégration.

a Exécutez les commandes de jonction AD.

```
# net ads join -U AdminUser@mydomain.com
# systemctl stop samba-ad-dc
# systemctl enable smbd nmbd winbind
# systemctl restart smbd nmbd winbind
```

b Modifiez le fichier de configuration `/etc/nsswitch.conf`, comme indiqué dans l'exemple suivant.

```
passwd:    compat systemd winbind
group:     compat systemd winbind
shadow:    compat
gshadow:   files
```

c Pour vérifier les résultats de la jonction AD, exécutez les commandes suivantes et vérifiez qu'elles renvoient le résultat correct.

```
# wbinfo –u

# wbinfo –g
```

d Pour vérifier Winbind Name Service Switch, exécutez les commandes suivantes et vérifiez qu'elles renvoient le résultat correct.

```
# getent group|grep 'domain admins'

# getent passwd|grep 'ads–hostname'
```

11 Activez tous les profils PAM.

```
# pam–auth–update
```

Sur l'écran Configuration PAM, sélectionnez tous les profils PAM, y compris **Créer un répertoire de base lors de la connexion**, puis sélectionnez **OK**.

12 Sur Ubuntu 16.04, activez le commutateur d'utilisateur sur l'écran de connexion. Modifiez le fichier `/usr/share/lightdm/lightdm.conf.d/50–ubuntu.conf`, comme indiqué dans l'exemple suivant.

```
user–session=ubuntu
greeter–show–manual–login=true
```

Étape suivante

Configurer la redirection de carte à puce pour un poste de travail Ubuntu

Configurer la redirection de carte à puce pour un poste de travail Ubuntu

Pour configurer la redirection de carte à puce sur un poste de travail Ubuntu, installez les bibliothèques dont dépend la fonctionnalité et le certificat d'autorité de certification racine pour prendre en charge l'authentification approuvée des cartes à puce. En outre, vous devez modifier certains fichiers de configuration pour terminer la configuration de l'authentification.

Certains exemples de la procédure utilisent des valeurs d'espace réservé pour représenter des entités dans votre configuration réseau, telles que le nom DNS de votre domaine AD. Remplacez les valeurs d'espace réservé par des informations spécifiques à votre configuration, comme décrit dans le tableau suivant.

Valeur d'espace réservé	Description
dns_IP_ADDRESS	Adresse IP de votre serveur de nom DNS
mydomain.com	Nom DNS de votre domaine AD
MYDOMAIN.COM	Nom DNS de votre domaine AD en majuscules

Valeur d'espace réservé	Description
MYDOMAIN	Nom DNS du groupe de travail ou domaine NT qui inclut votre serveur Samba, en majuscules
ads-hostname	Nom d'hôte de votre serveur AD
ads-hostname.mydomain.com	Nom de domaine complet (FQDN) de votre serveur AD
mytimeserver.mycompany.com	Nom DNS de votre serveur de temps NTP
AdminUser	Nom d'utilisateur de l'administrateur de poste de travail Linux

Conditions préalables

Intégrer un poste de travail Ubuntu à Active Directory pour la redirection de carte à puce

Procédure

1 Installez les bibliothèques requises.

```
# apt-get install -y pcscd pcsc-tools pkg-config libpam-pkcs11 opensc
      libengine-pkcs11-openssl libnss3-tools
```

2 Installez un certificat d'autorité de certification racine (CA).

a Téléchargez un certificat d'autorité de certification racine et enregistrez-le dans `/tmp/certificate.cer` sur votre poste de travail. Reportez-vous à Exportation du certificat d'autorité de certification de racine.

b Localisez le certificat d'autorité de certification racine que vous avez téléchargé et transférez-le vers un fichier `.pem`.

```
# openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

c Utilisez la commande `certutil` pour installer le certificat d'autorité de certification racine dans la base de données système `/etc/pki/nssdb`.

```
# certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

d Copiez le certificat d'autorité de certification racine dans le répertoire `/etc/pam_pkcs11/cacerts`.

```
# mkdir -p /etc/pam_pkcs11/cacerts

# cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
```

3 Créez un fichier de hachage `pkcs11`.

```
# chmod a+r certificate.pem
# pkcs11_make_hash_link
```

4 Copiez les pilotes requis et ajoutez les fichiers de bibliothèque nécessaires au répertoire `nssdb`.

a Exécutez les commandes suivantes.

```
# cp libcmP11.so /usr/lib/
# mkdir –p /etc/pki/nssdb
# certutil –N –d /etc/pki/nssdb
# certutil –A –n rootca –i certificate.pem –t "CT,CT,CT" –d /etc/pki/nssdb
# modutil –dbdir /etc/pki/nssdb/  –add "piv card 2.0" –libfile /usr/lib/libcmP11.so
```

b Vérifiez que le certificat attendu est correctement chargé.

```
# certutil –L –d /etc/pki/nssdb

Certificate Nickname

rootca
```

c Vérifiez que les bibliothèques attendues ont été ajoutées.

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

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

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

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

  2. piv card 2.0
        library name: /usr/lib/libcmP11.so
         slots: There are no slots attached to this module
        status: loaded
-----------------------------------------------------------
```

5 Configurez la bibliothèque pam_pkcs11.

a Créez un fichier pam_pkcs11.conf à l'aide de l'exemple de contenu par défaut.

```
# mkdir /etc/pam_pkcs11
# zcat /usr/share/doc/libpam-pkcs11/examples/pam_pkcs11.conf.example.gz |
       tee /etc/pam_pkcs11/pam_pkcs11.conf
```

b Modifiez le fichier /etc/pam_pkcs11/pam_pkcs11.conf, comme indiqué dans l'exemple suivant.

```
use_pkcs11_module = mysc;

pkcs11_module mysc {
              module = /usr/lib/libcmP11.so;
              description = "LIBCMP11";
              slot_num = 0;
              ca_dir = /etc/pki/cacerts;
              nss_dir = /etc/pki/nssdb;
              cert_policy = ca;
}
...
use_mappers = cn, null;
...
mapper cn {
      debug = false;
      module = internal;
      # module = /lib/pam_pkcs11/cn_mapper.so;
      ignorecase = true;
      mapfile = file:///etc/pam_pkcs11/cn_map;
      # mapfile = "none";
}
```

c Modifiez le fichier /etc/pam_pkcs11/cn_map de sorte qu'il comprenne la ligne suivante.

```
ads-hostname -> ads-hostname
```

6 Configurez l'authentification PAM.

a Modifiez le fichier de configuration `/etc/pam.d/gdm-password`. Placez la ligne d'autorisation `pam_pkcs11.so` avant la ligne `common-auth`, comme indiqué dans l'exemple suivant.

```
#%PAM-1.0
auth    requisite       pam_nologin.so
auth    required        pam_succeed_if.so user != root quiet_success
auth sufficient
pam_pkcs11.so
@include common-auth
auth    optional        pam_gnome_keyring.so
@include common-account
```

b Pour Ubuntu 16.04, modifiez le fichier de configuration `/etc/pam.d/lightdm`. Placez la ligne d'autorisation `pam_pkcs11.so` avant la ligne `common-auth`, comme indiqué dans l'exemple suivant.

```
#%PAM-1.0
auth    requisite       pam_nologin.so debug
auth    sufficient      pam_succeed_if.so user ingroup nopasswdlogin debug
auth    [success=3 default=ignore}     pam_pkcs11.so
@include common-auth
auth    optional        pam_gnome_keyring.so
auth    optional        pam_kwallet.so
```

c Pour Ubuntu 16.04, modifiez le fichier de configuration `/etc/pam.d/unity`. Placez la ligne d'autorisation `pam_pkcs11.so` avant la ligne `common-auth`, comme indiqué dans l'exemple suivant.

```
auth    [success=3 default=ignore}     pam_pkcs11.so
@include common-auth
auth optional pam_gnome_keyring.so
```

7 Pour vérifier le matériel de la carte à puce et les certificats installés sur la carte à puce, exécutez les commandes suivantes.

```
# pcsc_scan

# pkcs11_listcerts

# pkcs11_inspect
```

8 Configurez l'économiseur d'écran Gnome de sorte qu'il se verrouille lorsque la carte à puce est retirée.

a Installez le module de l'économiseur d'écran.

```
# apt-get install gnome-screensaver
```

b Pour configurer l'économiseur d'écran, modifiez le fichier `/etc/pam_pkcs11/pkcs11_eventmgr.conf`, comme indiqué dans l'exemple suivant.

```
pkcs11_eventmgr {
  # Run in background? Implies debug=false if true
  daemon = true;

  # show debug messages?
  debug = false;

  # polling time in seconds
  polling_time = 1;

  # expire time in seconds
  # default = 0 ( no expire )
  expire_time = 0;

  # pkcs11 module to use
  pkcs11_module = /usr/lib/libcmP11.so;

  #
  # list of events and actions
  # Card inserted
  event card_insert {
    # what to do if an action fail?
    # ignore : continue to next action
    # return : end action sequence
    # quit : end program
    on_error = ignore ;

    # You can enter several, comma-separated action entries
    # they will be executed in turn
    action = "gnome-screensaver-command --poke";
  }

  # Card has been removed
  event card_remove {
  on_error = ignore;
    action = "gnome-screensaver-command --lock";
  }

  # Too much time card removed
    event expire_time {
```

```
    on_error = ignore;
    action = "/bin/false";
  }
}
```

c Exécutez `pkcs11_eventmgr`.

```
# /usr/bin/pkcs11_eventmgr &
```

9 Installez le module Horizon Agent, avec la redirection de carte à puce activée.

```
# sudo ./install_viewagent.sh –m yes
```

Note Vous devez installer Horizon Agent 7.9 ou version ultérieure.

10 Redémarrez votre système et reconnectez-vous.

Configuration de la redirection de carte à puce pour les postes de travail SLED/SLES

Pour configurer la direction de carte à puce pour un poste de travail SLED/SLES, intégrez d'abord le poste de travail à un domaine Active Directory. Installez ensuite les bibliothèques et le certificat d'autorité de certification racine nécessaires avant Horizon Agent.

Intégrer un poste de travail SLED/SLES à Active Directory pour la redirection de carte à puce

Pour prendre en charge la redirection de carte à puce sur un poste de travail SLED/SLES, intégrez le poste de travail à un domaine Active Directory (AD) à l'aide des solutions Samba et Winbind.

Utilisez la procédure suivante pour intégrer un poste de travail SLED/SLES à un domaine AD pour la redirection de carte à puce.

Certains exemples de la procédure utilisent des valeurs d'espace réservé pour représenter des entités dans votre configuration réseau, telles que le nom DNS de votre domaine AD. Remplacez les valeurs d'espace réservé par des informations spécifiques à votre configuration, comme décrit dans le tableau suivant.

Valeur d'espace réservé	Description
dns_IP_ADDRESS	Adresse IP de votre serveur de nom DNS
mydomain.com	Nom DNS de votre domaine AD
MYDOMAIN.COM	Nom DNS de votre domaine AD en majuscules
MYDOMAIN	Nom DNS du groupe de travail ou domaine NT qui inclut votre serveur Samba, en majuscules
ads-hostname	Nom d'hôte de votre serveur AD
ads-hostname.mydomain.com	Nom de domaine complet (FQDN) de votre serveur AD

Valeur d'espace réservé	Description
mytimeserver.mycompany.com	Nom DNS de votre serveur de temps NTP
AdminUser	Nom d'utilisateur de l'administrateur de poste de travail Linux

Procédure

1 Configurez les paramètres réseau de votre poste de travail SLED/SLES.

   a Définissez le nom d'hôte du poste de travail en modifiant les fichiers de configuration `/etc/hostname` et `/etc/hosts`.

   b Configurez l'adresse IP du serveur DNS et désactivez **DNS automatique**. Pour SLES 12 SP3, désactivez également l'option **Modifier le nom d'hôte via DHCP**.

   c Pour configurer la synchronisation de l'heure du réseau, ajoutez vos informations de serveur NTP au fichier `/etc/ntp.conf`, comme indiqué dans l'exemple suivant.

```
server mytimeserver.mycompany.com
```

2 Installez les modules de jonction AD requis.

```
# zypper in krb5-client samba-winbind
```

3 Modifiez les fichiers de configuration requis.

a Modifiez le fichier `/etc/samba/smb.conf`, comme indiqué dans l'exemple suivant.

```
[global]
        workgroup = MYDOMAIN
        usershare allow guests = NO
        idmap gid = 10000-20000
        idmap uid = 10000-20000
        kerberos method = secrets and keytab
        realm = MYDOMAIN.COM
        security = ADS
        template homedir = /home/%D/%U
        template shell = /bin/bash
        winbind use default domain=true
        winbind offline logon = yes
        winbind refresh tickets = yes
[homes]
        ...
```

b Modifiez le fichier `/etc/krb5.conf`, comme indiqué dans l'exemple suivant.

```
[libdefaults]
        default_realm = MYDOMAIN.COM
        clockskew = 300

[realms]
        MYDOMAIN.COM = {
                kdc = ads-hostname.mydomain.com
                default_domain = mydomain.com
                admin_server = ads-hostname.mydomain.com
        }

[logging]
        kdc = FILE:/var/log/krb5/krb5kdc.log
        admin_server = FILE:/var/log/krb5/kadmind.log
        default = SYSLOG:NOTICE:DAEMON

[domain_realm]
        .mydomain.com = MYDOMAIN.COM
        mydomain.com = MYDOMAIN.COM

[appdefaults]
        pam = {
                ticket_lifetime = 1d
                renew_lifetime = 1d
                forwardable = true
                proxiable = false
                minimum_uid = 1
        }
```

c Modifiez le fichier `/etc/security/pam_winbind.conf`, comme indiqué dans l'exemple suivant.

```
cached_login = yes
krb5_auth = yes
krb5_ccache_type = FILE
```

d Modifiez le fichier `/etc/nsswitch.conf`, comme indiqué dans l'exemple suivant.

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

4 Joignez le domaine AD, comme indiqué dans l'exemple suivant.

```
# net ads join -U AdminUser
```

5 Activez le service Winbind.

a Pour activer et démarrer Winbind, exécutez la séquence de commandes suivante.

```
# pam-config --add --winbind
# pam-config -a --mkhomedir
# systemctl enable winbind
# systemctl start winbind
```

b Pour vous assurer que les utilisateurs AD peuvent se connecter au poste de travail sans avoir à redémarrer le serveur Linux, exécutez la séquence de commandes suivante.

```
# systemctl stop nscd
# nscd -i passwd
# nscd -i group
# systemctl start nscd
```

6 Pour vérifier que la jonction AD est réussie, exécutez les commandes suivantes et vérifiez qu'elles renvoient le résultat correct.

```
# wbinfo -u

# wbinfo -g
```

Étape suivante

Configurer la redirection de carte à puce pour un poste de travail SLED/SLES

Configurer la redirection de carte à puce pour un poste de travail SLED/SLES

Pour configurer la redirection de carte à puce sur un poste de travail SLED/SLES, installez les bibliothèques dont dépend la fonctionnalité et le certificat d'autorité de certification racine pour prendre en charge l'authentification approuvée des cartes à puce. En outre, vous devez modifier certains fichiers de configuration pour terminer la configuration de l'authentification.

Certains exemples de la procédure utilisent des valeurs d'espace réservé pour représenter des entités dans votre configuration réseau, telles que le nom DNS de votre domaine AD. Remplacez les valeurs d'espace réservé par des informations spécifiques à votre configuration, comme décrit dans le tableau suivant.

Valeur d'espace réservé	Description
dns_IP_ADDRESS	Adresse IP de votre serveur de nom DNS
mydomain.com	Nom DNS de votre domaine AD
MYDOMAIN.COM	Nom DNS de votre domaine AD en majuscules
MYDOMAIN	Nom DNS du groupe de travail ou domaine NT qui inclut votre serveur Samba, en majuscules
ads-hostname	Nom d'hôte de votre serveur AD
ads-hostname.mydomain.com	Nom de domaine complet (FQDN) de votre serveur AD
mytimeserver.mycompany.com	Nom DNS de votre serveur de temps NTP
AdminUser	Nom d'utilisateur de l'administrateur de poste de travail Linux

Conditions préalables

Intégrer un poste de travail SLED/SLES à Active Directory pour la redirection de carte à puce

Procédure

1 Installez les modules de bibliothèque requis.

a Installez la bibliothèque PAM et d'autres modules.

```
# zypper install pam_pkcs11 mozilla-nss mozilla-nss-tools
    pcsc-lite pcsc-ccid opensc coolkey pcsc-tools
```

b Pour installer les outils PC/SC, exécutez la série de commandes suivante.

```
# SUSEConnect --list-extensions
# SUSEConnect -p PackageHub/12.3/x86_64
# zypper in pcsc-tools
```

2 Installez un certificat d'autorité de certification racine (CA).

a Téléchargez un certificat d'autorité de certification racine et enregistrez-le dans `/tmp/certificate.cer` sur votre poste de travail. Reportez-vous à Exportation du certificat d'autorité de certification de racine.

b Localisez le certificat d'autorité de certification racine que vous avez téléchargé, transférez-le vers un fichier `.pem` et créez un fichier de hachage.

```
# openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
# cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
# chmod a+r /etc/pam_pkcs11/cacerts/certificate.pem
# cd /etc/pam_pkcs11/cacerts
# pkcs11_make_hash_link
```

c Installez les ancres d'approbation dans la base de données NSS.

```
# mkdir /etc/pam_pkcs11/nssdb
# certutil –N –d /etc/pam_pkcs11/nssdb
# certutil –L –d /etc/pam_pkcs11/nssdb
# certutil –A –n rootca –i certificate.pem –t "CT,CT,CT" –d /etc/pam_pkcs11/nssdb
```

d Installez les pilotes requis.

```
# cp libcmP11.so /usr/lib64/
# modutil –add "piv card 2.0" –libfile /usr/lib64/libcmP11.so –dbdir /etc/pam_pkcs11/nssdb/
```

3 Modifiez le fichier `/etc/pam_pkcs11/pam_pkcs11.conf`.

a Supprimez la ligne `use_pkcs11_module = nss`. À sa place, ajoutez la ligne `use_pkcs11_module = mysc`.

b Ajoutez le module `mysc`, comme indiqué dans l'exemple suivant.

```
pkcs11_module mysc {
  module = /usr/lib64/libcmP11.so;
  description = "MY Smartcard";
  slot_num = 0;
  nss_dir = /etc/pam_pkcs11/nssdb;
  cert_policy = ca, ocsp_on, signature, crl_auto;
}
```

c Mettez à jour la configuration du mappeur de nom commun, comme indiqué dans l'exemple suivant.

```
# Assume common name (CN) to be the login
mapper cn {
      debug = false;
      module = internal;
      # module = /usr/lib64/pam_pkcs11/cn_mapper.so;
      ignorecase = true;
      mapfile = file:///etc/pam_pkcs11/cn_map;}
```

d Supprimez la ligne `use_mappers = ms`. À sa place, ajoutez la ligne `use_mappers = cn, null`.

4 Modifiez le fichier de configuration `/etc/pam_pkcs11/cn_map` de sorte qu'il comprenne la ligne suivante.

```
ads-hostname -> ads-hostname
```

5 Modifiez la configuration PAM.

a Pour qu'il soit possible de configurer l'authentification par carte à puce, désactivez d'abord l'outil `pam_config`.

```
# find /etc/pam.d/ -type l -iname "common-*" -delete
# for X in /etc/pam.d/common-*-pc; do cp -ivp $X ${X:0:-3}; done
```

b Créez un fichier nommé `common-auth-smartcard` dans le répertoire `/etc/pam.d/`. Ajoutez le contenu suivant au fichier.

```
auth    required        pam_env.so
auth    sufficient      pam_pkcs11.so
auth    optional        pam_gnome_keyring.so
auth    [success=1 default=ignore]      pam_unix.so nullok_secure try_first_pass
auth    required        pam_winbind.so  use_first_pass
```

c Pour SLED/SLES 12 SP3, remplacez la ligne `auth include common-auth` par la ligne `auth include common-auth-smartcard` dans les deux fichiers `/etc/pam.d/gdm` et `/etc/pam.d/xscreensaver`.

6 Désactivez le pare-feu.

```
# rcSuSEfirewall2 stop
# chkconfig SuSEfirewall2_setup off
# chkconfig SuSEfirewall2_init off
```

Note La redirection de carte à puce échoue parfois lorsque le pare-feu est activé.

7 Installez les modules de bibliothèque requis pour la redirection de carte à puce.

a Pour SLED/SLES 12 SP3, exécutez les commandes d'installation suivantes.

```
# SUSEConnect -p sle-sdk/12.3/x86_64
# zypper in git autoconf automake libtool flex libudev-devel gcc
```

b Pour SLES 12 SP3, installez `systemd-devel`.

```
# zypper in systemd-devel
```

8 Installez le module Horizon Agent, avec la redirection de carte à puce activée.

```
# sudo ./install_viewagent.sh -m yes
```

Note Vous devez installer Horizon Agent 7.9 ou version ultérieure.

9 Redémarrez votre système et reconnectez-vous.

Configuration de l'authentification unique réelle pour les postes de travail Linux

La fonctionnalité d'authentification unique réelle (True SSO) accorde aux utilisateurs un accès à un poste de travail virtuel Linux ou à une application ou un poste de travail publié après leur première connexion à VMware Identity Manager. Les utilisateurs peuvent se connecter à VMware Identity Manager à l'aide d'une carte à puce ou d'une authentification RSA SecurID ou RADIUS, puis accéder aux ressources Linux distantes sans entrer leurs informations d'identification Active Directory.

Si un utilisateur s'authentifie à l'aide des informations d'identification Active Directory (AD), la fonctionnalité d'authentification unique réelle n'est pas nécessaire. Cependant, vous pouvez configurer l'authentification unique réelle afin qu'elle soit utilisée même dans ce cas, ce qui permet au poste de travail de prendre en charge les informations d'identification AD et d'authentification unique réelle.

Lorsqu'ils se connectent à un poste de travail virtuel Linux ou à une application ou un poste de travail publié(e), les utilisateurs peuvent choisir d'utiliser Horizon Client ou HTML Access natif.

L'authentification unique réelle présente les limites suivantes :

- La fonctionnalité est prise en charge uniquement sur les postes de travail avec les distributions suivantes : RHEL/CentOS 8.0, RHEL/CentOS 7.x, Ubuntu 16.04 et 18.04, et SLED/SLES 12.x SP3.
- Pour les postes de travail RHEL/CentOS 7.x, la fonctionnalité est prise en charge uniquement avec les méthodes de jonction suivantes : outils de jonction de domaine par défaut, Samba, System Security Services Daemon (SSSD) et le protocole d'authentification réseau Kerberos.

Pour configurer l'authentification unique réelle dans votre environnement Linux, effectuez les tâches suivantes.

1. Installez et configurez l'authentification unique réelle dans votre environnement Horizon 7. Reportez-vous à la section « Configuration de l'authentification unique réelle » du document *Administration d'Horizon 7*.
2. Intégrez votre poste de travail à un domaine AD, en suivant la procédure de votre distribution Linux.
3. Configurez l'authentification unique réelle sur votre poste de travail, en suivant la procédure de votre distribution Linux.

Configurer l'authentification unique réelle sur des postes de travail RHEL/CentOS 8.0

Pour prendre en charge l'authentification unique réelle sur un poste de travail RHEL/CentOS 8.0, vous devez d'abord intégrer le système à votre domaine Active Directory (AD). Vous devez ensuite modifier certaines configurations sur le système pour prendre en charge la fonctionnalité d'authentification unique réelle.

Note L'authentification unique réelle n'est pas prise en charge sur les postes de travail RHEL 8.0 Instant Clone.

Certains exemples de la procédure utilisent des valeurs d'espace réservé pour représenter des entités dans votre configuration réseau, telles que le nom DNS de votre domaine AD. Remplacez les valeurs d'espace réservé par des informations spécifiques à votre configuration, comme décrit dans le tableau suivant.

Valeur d'espace réservé	Description
mydomain.com	Nom DNS de votre domaine AD
MYDOMAIN.COM	Nom DNS de votre domaine AD en majuscules
MYDOMAIN	Nom de votre domaine NetBIOS

Conditions préalables

- Vérifiez que le serveur Active Directory (AD) peut être résolu par DNS sur le système RHEL/CentOS 8.0.
- Configurez le nom d'hôte du système.
- Configurez le protocole NTP (Network Time Protocol) sur le système.

Procédure

1 Sur le système RHEL/CentOS 8.0, vérifiez la connexion réseau à Active Directory.

```
# realm discover mydomain.com
```

2 Installez les modules de dépendance requis.

```
# yum install oddjob oddjob-mkhomedir sssd adcli samba-common-tools
```

3 Joignez le domaine AD.

```
# realm join --verbose mydomain.com -U administrator
```

4 Téléchargez le certificat de l'autorité de certification racine et copiez-le dans le répertoire requis en tant que fichier .pem.

```
# openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem

# cp /tmp/certificate.pem /etc/sssd/pki/sssd_auth_ca_db.pem
```

5 Modifiez le fichier de configuration `/etc/sssd/sssd.conf`, comme indiqué dans l'exemple suivant.

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

[domain/mydomain.com]
ad_domain = mydomain.com
krb5_realm = IMYDOMAIN.COM
realmd_tags = manages-system joined-with-adcli
```

```
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = False        <----------------- Use short name for user
fallback_homedir = /home/%u@%d
access_provider = ad
ad_gpo_map_interactive = +gdm-vmwcred    <----------------- Add this line for SSO

[pam]                                    <----------------- Add pam section for certificate logon
pam_cert_auth = True                     <----------------- Add this line to enable certificate
logon for system
pam_p11_allowed_services = +gdm-vmwcred  <----------------- Add this line to enable certificate
logon for VMware Horizon Agent

[certmap/mydomain.com/truesso]          <----------------- Add this section and following lines to
set match and map rule for certificate user
matchrule = <EKU>msScLogin
maprule = (|(userPrincipal={subject_principal})(samAccountName={subject_principal.short_name}))
domains = mydomain.com
priority = 10
```

6 Installez le module Horizon Agent, avec l'authentification unique réelle activée.

Note Vous devez installer Horizon Agent 7.11 ou version ultérieure.

```
# sudo ./install_viewagent.sh -T yes
```

7 Modifiez le fichier de configuration de `/etc/vmware/viewagent-custom.conf` afin qu'il inclue la ligne suivante.

```
NetbiosDomain = MYDOMAIN
```

8 Redémarrez le système et reconnectez-vous.

Configuration de l'authentification unique réelle sur des postes de travail RHEL/CentOS 7.x

Pour configurer l'authentification unique réelle pour un poste de travail RHEL/CentOS 7.x, intégrez d'abord le poste de travail à un domaine Active Directory. Installez ensuite les bibliothèques et le certificat d'autorité de certification racine requis avant d'installer Horizon Agent.

Intégrer un poste de travail RHEL/CentOS 7.x à Active Directory pour l'authentification unique réelle

Pour prendre en charge l'authentification unique réelle sur une machine virtuelle Instant Clone dans un environnement de poste de travail Linux Horizon 7sur un système RHEL/CentOS 7.x, vous devez configurer Samba sur la machine virtuelle Linux maître.

La fonctionnalité `realmd` de RHEL/CentOS 7.x représente un moyen simple d'identifier et de joindre des domaines d'identité. Au lieu de connecter le système au domaine lui-même, `realmd` configure les services système Linux sous-jacents, tels que SSSD ou Winbind, pour se connecter au domaine. Les étapes suivantes décrivent comment utiliser `realmd` et Samba pour effectuer une jonction de domaine hors ligne d'un poste de travail RHEL/CentOS 7.x à Active Directory.

Conditions préalables

- Le système RHEL (RedHat Enterprise Linux) est inscrit sur RHN (Red Hat Network) ou l'outil `yum` est installé dessus localement.
- Le serveur Active Directory (AD) peut être résolu par DNS sur le système Linux.
- Le protocole NTP (Network Time Protocol) est configuré sur le système Linux.

Procédure

1. Vérifiez que le système RHEL/CentOS peut découvrir le serveur AD. Utilisez l'exemple suivant, où *ADdomain.example.com* doit être remplacé par vos informations de serveur AD.

   ```
   sudo realm discover ADdomain.example.com
   ```

2. Installez le module `tdb-tools` de Samba.

   Le module `tdb-tools` de Samba ne peut pas être téléchargé depuis le référentiel officiel de Red Hat. Vous devez le télécharger manuellement. Par exemple, utilisez la commande suivante pour le télécharger à partir d'un système CentOS 7.5 et installer le module téléchargé dans votre système RHEL.

   ```
   yumdownloader tdb-tools
   ```

   Si vous ne disposez pas d'un système CentOS, accédez à `https://rpmfind.net/linux/rpm2html/search.php?query=tdb-tools&submit=Search+…&system=&arch`, téléchargez le module `tdb-tools-1.3.15-1.el7.x86_64.rpm` et installez-le sur votre système RHEL.

3. Installez Samba et les modules de dépendance.

   ```
   sudo yum install sssd-tools sssd adcli samba-common pam_ldap pam_krb5 samba samba-client krb5-workstation
   ```

4. Exécutez la commande `join`, à l'aide de l'exemple suivant, où *DNSdomain.example.com* doit être remplacé par le chemin du domaine DNS spécifique à votre environnement.

   ```
   sudo realm join DNSdomain.example.com -U administrator
   ```

   Lorsque la commande join réussit, le message d'erreur suivant s'affiche.

   ```
   Machine inscrite avec succès dans le domaine
   ```

5. Redémarrez votre système et reconnectez-vous.

Étape suivante

Configurer l'authentification unique réelle sur des postes de travail RHEL/CentOS 7.x

Configurer l'authentification unique réelle sur des postes de travail RHEL/CentOS 7.x

Pour activer la fonctionnalité d'authentification unique réelle sur un poste de travail RHEL/CentOS 7.x, installez les bibliothèques dont dépend la fonctionnalité d'authentification unique réelle, le certificat d'autorité de certification racine pour prendre en charge l'authentification approuvée et Horizon Agent. En outre, vous devez modifier certains fichiers de configuration pour terminer la configuration de l'authentification.

Utilisez la procédure suivante pour activer l'authentification unique réelle sur des postes de travail RHEL 7.x et CentOS 7.x. Pour prendre en charge l'authentification unique réelle sur ces postes de travail, vous devez installer Horizon Agent 7.6 ou version ultérieure.

Certains exemples de la procédure utilisent des valeurs d'espace réservé pour représenter des entités dans votre configuration réseau, telles que le nom DNS de votre domaine AD. Remplacez les valeurs d'espace réservé par des informations spécifiques à votre configuration, comme décrit dans le tableau suivant.

Valeur d'espace réservé	Description
dns_server	Chemin d'accès à votre serveur de nom DNS
mydomain.com	Nom DNS de votre domaine AD
MYDOMAIN.COM	Nom DNS de votre domaine AD en majuscules

Conditions préalables

- Configurez l'authentification unique réelle pour VMware Identity Manager et Horizon Connection Server.
- Intégrer un poste de travail RHEL/CentOS 7.x à Active Directory pour l'authentification unique réelle
- Procurez-vous un certificat d'autorité de certification racine et enregistrez-le dans `/tmp/certificate.cer` sur votre poste de travail RHEL/CentOS 7.x. Reportez-vous à Exportation du certificat d'autorité de certification de racine.

Procédure

1 Installez le groupe de module de prise en charge PKCS11.

```
yum install –y nss–tools nss–pam–ldapd pam_krb5 krb5–libs krb5–workstation krb5–pkinit
```

2 Installez un certificat d'autorité de certification racine (CA).

a Localisez le certificat d'autorité de certification racine que vous avez téléchargé et transférez-le vers un fichier `.pem`.

```
openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

b Utilisez la commande `certutil` pour installer le certificat d'autorité de certification racine dans la base de données système `/etc/pki/nssdb`.

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

c Ajoutez le certificat d'autorité de certification racine à la liste des certificats d'autorité de certification approuvés sur votre système RHEL/CentOS 7.x et mettez à jour la configuration du magasin de confiance à l'échelle du système à l'aide de la commande `update-ca-trust`.

```
cp /tmp/certificate.pem /etc/pki/ca-trust/source/anchors/ca_cert.pem
update-ca-trust
```

3 Modifiez la section appropriée dans le fichier de configuration SSSD de votre système pour votre domaine, comme indiqué dans l'exemple suivant.

```
[domain/mydomain.com]
ad_domain = mydomain.com
krb5_realm = MYDOMAIN.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
#set the next line to false, so you can use the short name instead of the full domain name.
use_fully_qualified_names = False
fallback_homedir = /home/%u@%d
access_provider = ad
```

4 Modifiez le fichier de configuration Kerberos `/etc/krb5.conf`, comme indiqué dans l'exemple suivant.

```
[libdefaults]
 dns_lookup_realm = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_ccache_name = KEYRING:persistent:%{uid}
 # Add following line, if the system doesn't add it automatically
 default_realm = MYDOMAIN.COM

[realms]
MYDOMAIN.COM = {
  kdc = dns_server
```

```
  admin_server = dns_server
  # Add the following three lines for pkinit_*
  pkinit_anchors = DIR:/etc/pki/ca-trust/source/anchors
  pkinit_kdc_hostname = your_org_DNS_server
  pkinit_eku_checking = kpServerAuth
 }
[domain_realm]
 mydomain.com = MYDOMAIN.COM
 .mydomain.com = MYDOMAIN.COM
```

5 Installez le module Horizon Agent, avec l'authentification unique réelle activée.

```
sudo ./install_viewagent.sh –T yes
```

Note Vous devez installer Horizon Agent 7.6 ou version ultérieure.

6 Ajoutez le paramètre suivant au fichier de configuration personnalisé Horizon Agent `/etc/vmware/viewagent-custom.conf`. Utilisez l'exemple suivant, où *NETBIOS_NAME_OF_DOMAINE* est le nom NetBIOS du domaine de votre organisation.

```
NetbiosDomain=NETBIOS_NAME_OF_DOMAIN
```

7 Redémarrez votre système et reconnectez-vous.

Configuration de l'authentification unique réelle pour les postes de travail Ubuntu

Pour configurer l'authentification unique réelle pour un poste de travail Ubuntu, intégrez d'abord le poste de travail à un domaine Active Directory. Installez ensuite les bibliothèques et le certificat d'autorité de certification racine requis avant d'installer Horizon Agent.

Intégrer un poste de travail Ubuntu à Active Directory pour l'authentification unique réelle

Pour prendre en charge l'authentification unique réelle sur un poste de travail Ubuntu 16.04 ou 18.04, intégrez le poste de travail à un domaine Active Directory à l'aide des solutions Samba et Winbind.

Utilisez la procédure suivante pour intégrer un poste de travail Ubuntu 16.04 ou 18.04 à un domaine AD.

Certains exemples de la procédure utilisent des valeurs d'espace réservé pour représenter des entités dans votre configuration réseau, telles que le nom d'hôte de votre poste de travail Ubuntu. Remplacez les valeurs d'espace réservé par des informations spécifiques à votre configuration, comme décrit dans le tableau suivant.

Valeur d'espace réservé	Description
dns_IP_ADDRESS	Adresse IP de votre serveur de nom DNS
mydomain.com	Nom DNS de votre domaine AD
MYDOMAIN.COM	Nom DNS de votre domaine AD en majuscules
myhost	Nom d'hôte de votre poste de travail Ubuntu

Valeur d'espace réservé	Description
MYDOMAIN	Nom DNS du groupe de travail ou domaine NT qui inclut votre serveur Samba, en majuscules
ads-hostname	Nom d'hôte de votre serveur AD
admin-user	Nom d'utilisateur de l'administrateur de domaine AD

Conditions préalables

- Le serveur Active Directory (AD) peut être résolu par DNS sur le système Linux.
- Le protocole NTP (Network Time Protocol) est configuré sur le système Linux.

Procédure

1 Sur votre poste de travail Ubuntu 16.04 ou 18.04, installez les modules `samba` et `winbind`.

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

2 Lorsque vous y êtes invité, configurez les paramètres d'authentification Kerberos en procédant comme suit.

   a Pour **Default Kerberos version 5 realm**, entrez le nom DNS de votre domaine AD en majuscules.

   Par exemple, si votre nom de domaine AD est **`mydomain.com`**, entrez **`MYDOMAIN.COM`**.

   b Pour **Kerberos servers for your realm**, entrez le nom d'hôte de votre serveur AD (représenté par **`ads_hostname`** dans les exemples de cette procédure).

   c Pour **Administrative server for your Kerberos realm**, entrez à nouveau le nom d'hôte de votre serveur AD.

3 Mettez à jour la configuration PAM.

   a Ouvrez la page de configuration PAM.

```
pam-auth-update
```

   b Sélectionnez **Create home directory on login**, puis **OK**.

4 Modifiez le fichier de configuration `/etc/nsswitch.conf`, comme indiqué dans l'exemple suivant.

```
passwd: compat winbind
group: compat winbind
shadow: compat
gshadow: files
```

5 Pour vous assurer que le fichier généré automatiquement `resolv.conf` fait référence à votre domaine AD en tant que domaine de recherche, modifiez les paramètres de NetworkManager pour la connexion à votre système.

   a Ouvrez le panneau de configuration NetworkManager et accédez à **Paramètres IPv4** pour la connexion à votre système. Pour Méthode, sélectionnez **Adresses automatiques (DHCP) uniquement**. Dans la zone de texte **Serveurs DNS**, entrez l'adresse IP de votre serveur de nom DNS (représenté par **`dns_IP_ADDRESS`** dans les exemples de cette procédure). Cliquez ensuite sur **Enregistrer**.

   b Modifiez le fichier de configuration pour la connexion à votre système situé dans `/etc/NetworkManager/system-connections`. Utilisez l'exemple suivant.

```
[ipv4]
dns=dns_IP_ADDRESS
dns-search=mydomain.com
ignore-auto-dns=true
method=auto
```

   Note Un nouvel adaptateur réseau virtuel est ajouté lors de la création d'un poste de travail virtuel Instant Clone. Tout paramètre dans l'adaptateur réseau, par exemple le serveur DNS, dans le modèle de poste de travail virtuel est perdu lorsque le nouvel adaptateur réseau est ajouté au poste de travail virtuel Instant Clone. Pour éviter de perdre le paramètre de serveur DNS lorsque le nouvel adaptateur réseau est ajouté à un poste de travail virtuel cloné, vous devez spécifier un serveur DNS pour votre système Linux.

   c Spécifiez le serveur DNS en modifiant le fichier de configuration `/etc/resolv.conf`, comme indiqué dans l'exemple suivant.

```
nameserver dns_IP_ADDRESS

search mydomain.com
```

   d Redémarrez votre système et reconnectez-vous.

6 Modifiez le fichier de configuration `/etc/hosts`, comme indiqué dans l'exemple suivant.

```
127.0.0.1     localhost
127.0.1.1     myhost.mydomain.com myhost
```

7 Modifiez le fichier de configuration `/etc/samba/smb.conf`, comme indiqué dans l'exemple suivant.

```
[global]
security = ads
realm = MYDOMAIN.COM
workgroup = MYDOMAIN
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum group = yes
template homedir = /home/%D/%U
```

```
template shell = /bin/bash
client use spnego = yes
client ntlmv2 auth = yes
encrypt passwords = yes
winbind use default domain = yes
restrict anonymous = 2
kerberos method = secrets and keytab
winbind refresh tickets = true
```

8 Redémarrez le service `smbd`.

```
sudo systemctl restart smbd.service
```

9 Modifiez le fichier de configuration `/etc/krb5.conf` afin que son contenu soit semblable à l'exemple suivant.

```
[libdefaults]
      default_realm = MYDOMAIN.COM
      dns_lookup_realm = true
      dns_lookup_kdc = true

[realms]
      MYDOMAIN.COM = {
            kdc = ads-hostname
            admin_server = ads-hostname
      }

[domain_realm]
      .mydomain.com = MYDOMAIN.COMmydomain.com = MYDOMAIN.COM
```

10 Joignez votre poste de travail Ubuntu au domaine AD.

a Initiez un ticket Kerberos.

```
 sudo kinit admin-user
```

Lorsque vous y êtes invité, entrez votre mot de passe administrateur.

b Vérifiez que le ticket a bien été créé.

```
sudo klist
```

Cette commande renvoie des informations sur le ticket, y compris son heure de début et son délai d'expiration valides.

c Créez un fichier keytab Kerberos.

```
sudo net ads keytab create -U admin-user
```

d Joignez le domaine AD.

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

11 Redémarrez et vérifiez le service Winbind.

a Redémarrez le service Winbind.

```
sudo systemctl restart winbind.service
```

b Pour vérifier le service Winbind, exécutez les commandes suivantes et vérifiez qu'elles renvoient le résultat correct.

- `wbinfo –u`
- `wbinfo –g`
- `getend passwd`
- `getend group`

12 Redémarrez votre système et reconnectez-vous.

Étape suivante

Configurer l'authentification unique réelle sur les postes de travail Ubuntu

Configurer l'authentification unique réelle sur les postes de travail Ubuntu

Pour activer la fonctionnalité d'authentification unique réelle sur un poste de travail Ubuntu 16.04 ou 18.04, installez les bibliothèques dont dépend la fonctionnalité d'authentification unique réelle, le certificat d'autorité de certification racine pour prendre en charge l'authentification approuvée et Horizon Agent. En outre, vous devez modifier certains fichiers de configuration pour terminer la configuration de l'authentification.

Utilisez la procédure suivante pour activer l'authentification unique réelle sur des postes de travail Ubuntu 16.04 et 18.04. Pour prendre en charge l'authentification unique réelle sur ces postes de travail, vous devez installer Horizon Agent 7.8 ou version ultérieure.

Conditions préalables

- Configurez l'authentification unique réelle pour VMware Identity Manager et Horizon Connection Server.
- Intégrer un poste de travail Ubuntu à Active Directory pour l'authentification unique réelle
- Procurez-vous un certificat d'autorité de certification racine et enregistrez-le dans `/tmp/certificate.cer` sur votre poste de travail. Reportez-vous à Exportation du certificat d'autorité de certification de racine.

Procédure

1 Sur votre poste de travail Ubuntu 16.04 ou 18.04, installez le module de prise en charge `pkcs11`.

```
sudo apt install libpam–pkcs11
```

2 Installez le module `libnss3-tools`.

```
sudo apt install libnss3-tools
```

3 Installez un certificat d'autorité de certification racine (CA).

a Localisez le certificat d'autorité de certification racine que vous avez téléchargé et transférez-le vers un fichier `.pem`.

```
openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

b Utilisez la commande `certutil` pour installer le certificat d'autorité de certification racine dans la base de données système `/etc/pki/nssdb`.

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

c Copiez le certificat d'autorité de certification racine dans le répertoire `/etc/pam_pkcs11/cacerts`.

```
mkdir -p /etc/pam_pkcs11/cacerts

cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
```

d Créez un lien de hachage pour le certificat d'autorité de certification racine. Dans le répertoire `/etc/pam_pkcs11/cacerts`, exécutez la commande suivante.

```
pkcs11_make_hash_link
```

4 Installez le module Horizon Agent, avec l'authentification unique réelle activée.

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

Note Pour utiliser la fonctionnalité d'authentification unique réelle, vous devez installer Horizon Agent 7.8 ou version ultérieure.

5 Ajoutez le paramètre suivant au fichier de configuration personnalisé Horizon Agent`/etc/vmware/viewagent-custom.conf`. Utilisez l'exemple suivant, où *NETBIOS_NAME_OF_DOMAINE* est le nom NetBIOS du domaine de votre organisation.

```
NetbiosDomain=NETBIOS_NAME_OF_DOMAIN
```

6 Modifiez le fichier de configuration `/etc/pam_pkcs11/pam_pkcs11.conf`.

   a Si nécessaire, créez le fichier de configuration `/etc/pam_pkcs11/pam_pkcs11.conf`. Localisez le fichier d'exemple dans `/usr/share/doc/libpam-pkcs11/examples`, copiez-le dans le répertoire `/etc/pam_pkcs11` et renommez le fichier `pam_pkcs11.conf`. Ajoutez les informations de votre système dans le fichier en fonction des besoins.

   b Modifiez le fichier de configuration `/etc/pam_pkcs11/pam_pkcs11.conf` afin que son contenu soit semblable à l'exemple suivant.

```
use_pkcs11_module = coolkey;
pkcs11_module coolkey {
  module = /usr/lib/vmware/viewagent/sso/libvmwpkcs11.so;
  slot_num = 0;
  ca_dir = /etc/pam_pkcs11/cacerts;
  nss_dir = /etc/pki/nssdb;
}
```

7 Modifier les paramètres `auth` dans le fichier de configuration PAM.

   a Ouvrez le fichier de configuration PAM.

      - Pour Ubuntu 16.04, ouvrez `/etc/pam.d/lightdm`.
      - Pour Ubuntu 18.04, ouvrez `/etc/pam.d/gdm-vmwcred`.

   b Modifiez le fichier de configuration PAM, comme indiqué dans l'exemple suivant.

```
auth requisite pam_vmw_cred.so
auth sufficient pam_pkcs11.so try_first_pass
```

8 Redémarrez votre système et reconnectez-vous.

Configuration de l'authentification unique réelle pour les postes de travail SLED/SLES

Pour configurer l'authentification unique réelle pour un poste de travail SLED/SLES, intégrez d'abord le poste de travail à un domaine Active Directory. Installez ensuite les bibliothèques et le certificat d'autorité de certification racine requis avant d'installer Horizon Agent.

Intégrer un poste de travail SLED/SLES à Active Directory pour l'authentification unique réelle

Pour prendre en charge l'authentification unique réelle sur un poste de travail SLED 12.x SP3 ou SLES 12.x SP3, intégrez le poste de travail à un domaine Active Directory à l'aide des solutions Samba et Winbind.

Utilisez la procédure suivante pour intégrer un poste de travail SLED/SLES à un domaine AD.

Conditions préalables

- Le serveur Active Directory (AD) peut être résolu par DNS sur le système Linux.
- Le protocole NTP (Network Time Protocol) est configuré sur le système Linux.

Procédure

1 Sur votre poste de travail SLED/SLES, installez les modules `samba` et `winbind`.

```
zypper install samba-winbind krb5-client samba-winbind-32bit
```

2 Ouvrez l'outil de configuration YaST et accédez à **Services réseau > Appartenance au domaine Windows**.

3 Sur l'écran Appartenance au domaine Windows, configurez les paramètres comme suit.

a Pour **Domaine ou Groupe de travail**, entrez le nom DNS du groupe de travail ou domaine NT qui inclut votre serveur Samba, en majuscules. Par exemple, si votre nom de groupe de travail est **`mydomain`**, entrez **`MYDOMAIN`**.

b Sélectionnez **Utiliser aussi les informations SMB pour l'authentification Linux**.

c Sélectionnez **Créer un répertoire de base à la connexion**.

d Sélectionnez **Authentification hors ligne**.

e Sélectionnez **Authentification unique pour SSH**.

4 À l'invite vous demandant si vous voulez joindre le domaine, sélectionnez **Oui**.

5 Entrez le nom et le mot de passe d'administrateur du groupe de travail spécifié et sélectionnez **OK**.

Un message s'affiche pour confirmer que votre poste de travail SLED/SLES a rejoint le domaine. Sélectionnez **OK**.

6 Modifiez le fichier de configuration `/etc/samba/smb.conf` pour qu'il inclue le paramètre suivant.

```
[global]
...
winbind use default domain = yes
```

7 Redémarrez votre système et reconnectez-vous.

8 Testez et vérifiez votre intégration de poste de travail SLED/SLES.

Exécutez les commandes de test suivantes et vérifiez qu'elles renvoient le bon résultat. Remplacez `mydomain` par le nom de votre groupe de travail de serveur Samba ou domaine NT.

- `net ads testjoin`
- `net ads info`
- `wbinfo --krb5auth=mydomain\\open%open`
- `ssh localhost -l mydomain\\open`

Étape suivante

Configurer l'authentification unique réelle sur des postes de travail SLED/SLES

Configurer l'authentification unique réelle sur des postes de travail SLED/SLES

Pour activer la fonctionnalité d'authentification unique réelle sur un poste de travail SLED/SLES 12.x SP3, installez les bibliothèques dont dépend la fonctionnalité d'authentification unique réelle, le certificat d'autorité de certification racine pour prendre en charge l'authentification approuvée et Horizon Agent. En outre, vous devez modifier certains fichiers de configuration pour terminer la configuration de l'authentification.

Utilisez la procédure suivante pour activer l'authentification unique réelle sur des postes de travail SLED 12.x SP3 et SLES 12.x SP3. Pour prendre en charge l'authentification unique réelle sur ces postes de travail, vous devez installer Horizon Agent 7.8 ou version ultérieure.

Conditions préalables

- Configurez l'authentification unique réelle pour VMware Identity Manager et Horizon Connection Server.
- Intégrer un poste de travail SLED/SLES à Active Directory pour l'authentification unique réelle
- Procurez-vous un certificat d'autorité de certification racine et enregistrez-le dans `/tmp/certificate.cer` sur votre poste de travail SLED/SLES 12.x SP3. Reportez-vous à Exportation du certificat d'autorité de certification de racine.

Procédure

1. Pour un poste de travail SLES 12.x SP3, installez les modules nécessaires en exécutant la commande suivante.

   ```
   zypper install mozilla-nss-tools pam_krb5 krb5-client krb5-plugin-preauth-pkinit
   ```

2. Pour un poste de travail SLED 12.x SP3, installez les modules nécessaires en exécutant les étapes suivantes.

   a. Téléchargez un fichier .iso SLES sur le disque local de votre poste de travail SLED (par exemple, `/tmp/SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).

   Vous devez ajouter le fichier .iso SLES comme source de module pour votre poste de travail SLED, car le module `krb5-plugin-preauth-pkinit` nécessaire est disponible uniquement pour les systèmes SLES.

   b. Montez le fichier .iso SLES sur votre poste de travail SLED et installez les modules nécessaires.

   ```
   sudo mkdir -p /mnt/sles
   sudo mount -t iso9660 /tmp/SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso /mnt/sles
   sudo zypper ar -f /mnt/sles sles
   zypper install mozilla-nss-tools pam_krb5 krb5-client krb5-plugin-preauth-pkinit
   ```

   c. Lorsque l'installation est terminée, démontez le fichier .iso SLES.

   ```
   sudo unmount /mnt/sles
   ```

3 Installez un certificat d'autorité de certification racine (CA).

a Localisez le certificat d'autorité de certification racine que vous avez téléchargé et transférez-le vers un fichier `.pem`.

```
openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

b Utilisez la commande `certutil` pour installer le certificat d'autorité de certification racine dans la base de données système `/etc/pki/nssdb`.

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

c Ajoutez le certificat d'autorité de certification racine à `pam_pkcs11`.

```
cp /tmp/certificate.pem /etc/pki/ca-trust/source/anchors/ca_cert.pem
```

4 Modifiez le fichier de configuration `/etc/krb5.conf` afin que son contenu soit semblable à l'exemple suivant.

```
[libdefaults]
      default_realm = MYDOMAIN.COM
      dns_lookup_realm = false
      ticket_lifetime = 24h
      renew_lifetime = 7d
      forwardable = true
      rdns = false
      default_ccache_name = KEYRING:persistent:%{uid}

[realms]
      MYDOMAIN.COM = {
            kdc = ads-hostname
            admin_server = ads-hostname
            pkinit_anchors = DIR:/etc/pki/ca-trust/source/anchors
            pkinit_kdc_hostname = ads-hostname
            pkinit_eku_checking = kpServerAuth
      }

[domain_realm]
      .mydomain.com = MYDOMAIN.COMmydomain.com = MYDOMAIN.COM
```

Remplacez les valeurs d'espace réservé dans l'exemple par des informations spécifiques à votre configuration réseau, comme décrit dans le tableau suivant.

Valeur d'espace réservé	Description
mydomain.com	Nom DNS de votre domaine AD
MYDOMAIN.COM	Nom DNS de votre domaine AD (en majuscules)
ads-hostname	Nom d'hôte de votre serveur AD (sensible à la casse)

5 Installez le module Horizon Agent, avec l'authentification unique réelle activée.

```
sudo ./install_viewagent.sh –T yes
```

Note Pour utiliser la fonctionnalité d'authentification unique réelle, vous devez installer Horizon Agent 7.8 ou version ultérieure.

6 Ajoutez le paramètre suivant au fichier de configuration personnalisé Horizon Agent `/etc/vmware/viewagent–custom.conf`. Utilisez l'exemple suivant, où *NETBIOS_NAME_OF_DOMAINE* est le nom NetBIOS du domaine de votre organisation.

```
NetbiosDomain=NETBIOS_NAME_OF_DOMAIN
```

7 Redémarrez votre système et reconnectez-vous.

Configuration des graphiques pour les postes de travail Linux

4

Vous pouvez configurer les distributions Linux 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, 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 Linux prises en charge pour vGPU

Vous pouvez configurer une distribution Linux 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 de NVIDIA pour obtenir plus d'informations sur les modules de pilote.

Note Pour plus d'informations sur les cartes graphiques NVIDIA et les distributions Linux prenant en charge vGPU, reportez-vous à la section https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html.

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 la carte graphique vGPU requise est installée sur l'hôte ESXi.

Note Pour plus d'informations sur les cartes graphiques NVIDIA et les distributions Linux prenant en charge vGPU, reportez-vous à la section https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html.

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.

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.

Note Pour plus d'informations sur les cartes graphiques NVIDIA et les distributions Linux prenant en charge vGPU, reportez-vous à la section https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html.

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.

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

2 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.

3 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)
```

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

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

5 Démarrez le programme d'installation de NVIDIA GRID vGPU.

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

6 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 Linux en affichant la sortie du pilote NVIDIA dans une session de poste de travail Horizon.

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 Horizon. Pour résoudre le problème, réinstallez le pilote NVIDIA.
- Définissez la licence NVIDIA GRID dans la machine virtuelle Linux. Pour plus d'informations, consultez la documentation de NVIDIA. Si l'attribution de licence n'est pas définie, le poste de travail Linux ne fonctionne pas correctement. Par exemple, l'ajustement automatique ne fonctionne pas.

Configurer RHEL 6.x pour vDGA

Vous pouvez configurer un système d'exploitation invité RHEL 6.x afin qu'un poste de travail Horizon 7 pour 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.x

Pour configurer une machine virtuelle RHEL 6.x afin 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.x 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.x. Reportez-vous à la section Ajouter un périphérique de relais vDGA à une machine virtuelle RHEL 6.x.

Procédure

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

a Modifiez le fichier `grub.conf`.

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

Version de RHEL	Commande
6.x	`sudo vi /boot/grub/grub.conf`

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/lsmod | 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 Pour vous connecter à la machine virtuelle, ouvrez un terminal distant ou utilisez une console texte en saisissant Ctrl-Alt-F2, connectez-vous en tant qu'utilisateur racine et exécutez la commande `init 3` pour 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 Exécutez 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 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 Linux en affichant la sortie du pilote NVIDIA dans une session de poste de travail Horizon.

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 Horizon. Pour résoudre le problème, réinstallez le pilote NVIDIA.
- Définissez la licence NVIDIA GRID dans la machine virtuelle Linux. Pour plus d'informations, consultez la documentation de NVIDIA. Si l'attribution de licence n'est pas définie, le poste de travail Linux ne fonctionne pas correctement. Par exemple, l'ajustement automatique ne fonctionne pas.

Installation d'Horizon Agent 5

Vous devez installer Horizon Agent sur les postes de travail Linux afin que le Horizon Connection Server puisse communiquer avec les postes de travail et les gérer.

Ce chapitre contient les rubriques suivantes :

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 déploiement impliquant de nombreux postes de travail Linux, vous pouvez installer Horizon Agent sur la machine virtuelle de base.

Attention Si vous prévoyez d'utiliser NVIDIA GRID vGPU ou vDGA, 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 la section Configurer des distributions Linux prises en charge pour vGPU ou Configurer RHEL 6.x pour vDGA. 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.

   Dans la section Informatique de bureau et d'utilisateur final, sélectionnez Voir les composants de téléchargement pour VMware Horizon. Sous Horizon 7 for Linux, sélectionnez la page des téléchargements pour VMware Horizon 7 pour les systèmes Linux 64 bits.

   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 -xzvf VMware-horizonagent-linux-x86_64-y.y.y-xxxxxxx.tar.gz
   ```

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 afficher 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 |no	Acceptez ou refusez le contrat de licence d'utilisateur final (CLUF) et la déclaration FIPS (Federal Information Processing Standards). Vous devez spécifier **yes** pour que l'installation soit exécutée.

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**.
-T yes|no	Installer ou contourner la prise en charge de l'authentification unique réelle (SSO réelle). La valeur par défaut est **no**.
-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	`sudo ./install_viewagent.sh –A yes` Une nouvelle installation requiert toujours la création d'un nouveau pool de postes de travail.
Mettre à niveau depuis une machine virtuelle non gérée et conserver le style de la machine virtuelle non gérée	`sudo ./install_viewagent.sh –A yes–M no` 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. **Note** Pour garantir les meilleures performances possibles, n'utilisez pas de machine virtuelle non gérée.
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	`sudo ./install_viewagent.sh –A yes` 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.

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 Horizon Connection Server.
- 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 requiert la création d'un nouveau pool de postes de travail sur le Horizon Connection Server.

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 de 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.
-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 de programme d'installation pour Horizon Agent for Linux depuis le site de téléchargement VMware https://my.vmware.com/web/vmware/downloads.

   Sous Informatique de bureau et d'utilisateur final, choisissez de télécharger VMware Horizon 7, qui inclut le programme d'installation d'Horizon Agent for 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 *xxxxxxx* le numéro de build.

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

   Par exemple :

   ```
   tar –xzvf <archive Horizon Agent>
   ```

3. Accédez au dossier de l'archive.

4 Pour mettre à niveau des machines virtuelles non gérées, exécutez le script `install_viewagent.sh` 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	`sudo ./install_viewagent.sh –A yes –M no` **Note** Pour garantir les meilleures performances possibles, n'utilisez pas de machine virtuelle non gérée.
Mettre à niveau un déploiement de machines virtuelles non gérées et le changer en déploiement de machines virtuelles gérées	`sudo ./install_viewagent.sh –A yes –M yes` **Note** Dans Horizon Console, supprimez le pool de postes de travail existant pour le déploiement de machines virtuelles non gérées, puis créez un pool de postes de travail pour un déploiement de machines virtuelles gérées. Pour plus d'informations, reportez-vous à la section Créer un pool de postes de travail manuel pour Linux.
Mettre à niveau un déploiement de machine virtuelle gérée	`sudo ./install_viewagent.sh –A yes –M yes` **Note** Après la mise à niveau, votre pool de postes de travail existant peut être réutilisé.

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

1 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`.

2 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

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

Lors de l'installation 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` configure le build sur le mode PNG sans perte.

```
RemoteDisplay.buildToPNG=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. L'application est effectuée 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
Clipboard.Direction	`0`, `1`, `2`, ou `3`	`2`	Utilisez cette option pour spécifier la stratégie de redirection du Presse-papiers. Les valeurs valides sont les suivantes : ■ 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.
RemoteDisplay.allowAudio	`true` ou `false`	`true`	Définissez cette option pour activer/désactiver la sortie audio.
RemoteDisplay.allowH264	`true` ou `false`	`true`	Définissez cette option pour activer ou désactiver le codage H.264.
RemoteDisplay.buildToPNG	`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 le build sur le 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. L'activation de cette option désactive le codage H.264.
RemoteDisplay.enableNetworkContinuity	`true` ou `false`	`true`	Définissez cette option pour activer ou désactiver la fonctionnalité Network Continuity dans Horizon Agent for Linux.
RemoteDisplay.enableNetworkIntelligence	`true` ou `false`	`true`	Définissez cette option pour activer ou désactiver la fonctionnalité Network Intelligence dans Horizon Agent for Linux.

Tableau 6-1. Options de configuration dans `/etc/vmware/config` (suite)

Option	Valeur/Format	Valeur par défaut	Description
RemoteDisplay.enableStats	`true` ou `false`	`false`	Active ou désactive les statistiques du protocole d'affichage VMware Blast dans le journal mks, telles que la bande passante, FPS, RTT, etc.
RemoteDisplay.enableUDP	`true` ou `false`	`true`	Définissez cette option pour activer ou désactiver la prise en charge du protocole UDP dans Horizon Agent for Linux.
RemoteDisplay.maxBandwidthKbps	Un entier	1000000	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 valide doit être inférieure à 4 Gbit/s (4096000).
RemoteDisplay.minBandwidthKbps	Un entier	256	Spécifie la bande passante minimale, 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.
RemoteDisplay.maxFPS	Un entier	30	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 comprise entre 3 et 60. La valeur par défaut est de 30 actualisations par seconde.
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.
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.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.
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.

Tableau 6-1. Options de configuration dans `/etc/vmware/config` (suite)

Option	Valeur/Format	Valeur par défaut	Description
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.
VMWPkcs11Plugin.log.enable	`true` ou `false`	`false`	Définissez cette option afin d'activer ou de désactiver le mode de journalisation pour la fonctionnalité d'authentification unique réelle.
VMWPkcs11Plugin.log.logLevel	`error`, `warn`, `info`, `debug`, `trace` ou `verbose`	`info`	Utilisez cette option afin de définir le niveau de journalisation pour la fonctionnalité d'authentification unique réelle.
VVC.RTAV.Enable	`true` ou `false`	`true`	Définissez cette option pour activer/désactiver l'entrée 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.
cdrserver.cacheEnable	`true` ou `false`	`true`	Définissez cette option pour activer ou désactiver la fonctionnalité de cache en écriture de l'agent vers le client.
cdrserver.customizedSharedFolderPath	`folder_path`	`/home/`	Utilisez cette option pour modifier l'emplacement du dossier partagé de redirection du lecteur client (CDR) depuis le répertoire `/Home/`*`user`*`/tsclient` par défaut à un répertoire personnalisé. Par exemple, si l'utilisateur `test` souhaite placer le dossier de CDR partagé au niveau de `/mnt/test/tsclient` au lieu de `/home/test/tsclient`, l'utilisateur peut spécifier **`cdrserver. customizedSharedFolderPath =/ mnt/`**. **Note** Pour que cette option prenne effet, le dossier spécifié doit exister et être configuré avec les autorisations d'utilisateur appropriées.
cdrserver.forcedByAdmin	`true` ou `false`	`false`	Définissez cette option pour contrôler si le client peut partager des dossiers supplémentaires qui ne sont pas spécifiés avec l'option `cdrserver.shareFolders`.
cdrserver.logLevel	`error`, `warn`, `info`, `debug`, `trace` ou `verbose`	`info`	Utilisez cette option pour définir le niveau de journalisation pour le fichier `vmware-CDRserver.log`.

Tableau 6-1. Options de configuration dans `/etc/vmware/config` (suite)

Option	Valeur/Format	Valeur par défaut	Description
cdrserver.permissions	`R`	`RW`	Utilisez cette option pour appliquer des autorisations en lecture/écriture supplémentaires dont dispose Horizon Agent sur les dossiers partagés par Horizon Client. Par exemple : ■ Si le dossier partagé par Horizon Client dispose des autorisations `read` et `write` et que vous définissez **`cdrserver.permissions=R`**, Horizon Agent ne dispose que d'autorisations d'accès `read`. ■ Si le dossier partagé par Horizon Client ne dispose que d'autorisations `read` et que vous définissez **`cdrserver.permissions=RW`**, Horizon Agent ne dispose toujours que de droits d'accès `read`. Horizon Agent ne peut pas modifier l'attribut `read` seul défini par Horizon Client. Horizon Agent ne peut supprimer que les droits d'accès en écriture. Voici les utilisations classiques : ■ **`cdrserver.permissions=R`** ■ **`#cdrserver.permissions=R`** (par exemple, commenter ou supprimer l'entrée)
cdrserver.sharedFolders	***`file_path1`*`,R;`*`file_path2`*`,;`*`file_path3`*`,R; ...`	non défini	Spécifiez un ou plusieurs chemins de fichier vers les dossiers que le client peut partager avec le poste de travail Linux. Par exemple : ■ Pour un client Windows : **`C:\spreadsheets,;D:\ebooks,R`** ■ Pour un client non-Windows : **`/tmp/spreadsheets;/tmp/ebooks,;/home/finance,R`**
collaboration.logLevel	`error`, `info` ou `debug`	`info`	Utilisez cette option pour définir le niveau de journalisation utilisé pour la session de collaboration. Si le niveau de journalisation est `debug`, tous les appels effectués aux fonctions `collabui` et le contenu de la liste `collabor` sont journalisés.
collaboration.maxCollabors	Un entier inférieur à 10	5	Spécifie le nombre maximal de collaborateurs que vous pouvez inviter à rejoindre une session.
collaboration.enableEmail	`true` ou `false`	`true`	Définissez cette option pour activer ou désactiver l'envoi d'invitations de collaboration à l'aide d'une application de messagerie installée. Lorsqu'elle est désactivée, vous ne pouvez pas utiliser un e-mail pour inviter des collaborateurs, même si une application de messagerie est installée.
collaboration.serverUrl	[URL]	non défini	Spécifie les URL de serveur à inclure dans les invitations de collaboration.

Tableau 6-1. Options de configuration dans `/etc/vmware/config` (suite)

Option	Valeur/Format	Valeur par défaut	Description
collaboration.enableControlPassing	`true` ou `false`	`true`	Définissez cette option pour autoriser ou empêcher les collaborateurs d'avoir le contrôle du poste de travail Linux. Pour spécifier une session de collaboration en lecture seule, définissez cette option sur **`false`**.
mksVNCServer.useUInputButtonMapping	`true` ou `false`	`false`	Définissez cette option pour activer la prise en charge d'une souris pour gauchers sur Ubuntu ou RHEL 7.x. CentOS et RHEL 6.x prennent en charge une souris pour gauchers et il n'est pas nécessaire de définir cette option.
mksvhan.clipboardSize	Un entier	1024	Utilisez cette option pour spécifier la taille maximale du Presse-papiers pour copier et coller.
vdpservice.log.logLevel	`fatal` `error`, `warn`, `info`, `debug` ou `trace`	`info`	Utilisez cette option pour définir le niveau de journalisation de `vdpservice`.
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`**
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.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.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 Inclure, tels que **`IncludeVidPid`** ou **`IncludePath`**.
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.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.

Tableau 6-1. Options de configuration dans `/etc/vmware/config` (suite)

Option	Valeur/Format	Valeur par défaut	Description
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 celui d'Horizon Client.
viewusb.ExcludeFamily	**{m|o}:*family_name_1*[;family_name_2;...]**	non défini	Utilisez cette option pour exclure des familles de périphériques de la redirection. Par exemple : **m:bluetooth;smart-card** 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. **Note** Les souris et les claviers sont exclus de la redirection par défaut et il n'est pas nécessaire de les exclure avec ce paramètre.
viewusb.ExcludePath	**{m|o}:bus-*x1*[/*y1*].../ port-*z1*[;bus-*x2*[/*y2*].../port-*z2*;...]**	non défini	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. Par exemple : **m:bus-1/2/3_port- 02;bus-1/1/1/4_port-ff**

Tableau 6-1. Options de configuration dans `/etc/vmware/config` (suite)

Option	Valeur/Format	Valeur par défaut	Description
viewusb.ExcludeVidPid	**{m|o}:vid-*xxx1*_pid-*yyy1*[;vid-*xxx2*_pid-*yyy2*;..]**	non défini	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 individuels dans un ID. Par exemple : **o:vid-0781_pid- ****;vid-0561_pid-554c**
viewusb.IncludeFamily	**{m|o}:*family_name_1*[;*family_name_2*]...**	non défini	Définissez cette option pour inclure des familles de périphériques pouvant être redirigées. Par exemple : **o:storage; smart-card**
viewusb.IncludePath	**{m|o}:bus-*x1*[/*y1*].../ port-*z1*[;bus-*x2*[/*y2*].../ portz2;...]**	non défini	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. Par exemple : **m:bus-1/2_port- 02;bus-1/7/1/4_port-0**f
viewusb.IncludeVidPid	**{m|o}:vid-*xxx1*_pid-*yyy1*[;vid-*xxx2*_pid-*yyy2;..*]**	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 individuels dans un ID. Par exemple : **o:vid-***_pid-0001;vid-0561_pid-554c**

Tableau 6-1. Options de configuration dans `/etc/vmware/config` (suite)

Option	Valeur/Format	Valeur par défaut	Description
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 individuels 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 individuels 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.

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
CDREnable	`true` ou `false`	`true`	Utilisez cette option pour activer ou désactiver la fonctionnalité de redirection du lecteur client.
CollaborationEnable	`true` ou `false`	`true`	Utilisez cette option pour activer ou désactiver la fonctionnalité de session de collaboration sur les postes de travail Linux.

Tableau 6-2. Options de configuration dans `/etc/vmware/viewagent-custom.conf` (suite)

Option	Valeur	Valeur par défaut	Description
EndpointVPNEnable	`true` ou `false`	`false`	Définissez cette option pour spécifier si l'adresse IP de la carte de réseau physique du client ou l'adresse IP VPN doit être utilisée lors de l'évaluation de l'adresse IP du point de terminaison par rapport à la plage d'adresses IP du point de terminaison utilisée dans la Console Dynamic Environment Manager. Si l'option est définie sur `false`, l'adresse IP de carte de réseau physique du client est utilisée. Dans le cas contraire, l'adresse IP VPN est utilisée.
HelpDeskEnable	`true` ou `false`	`true`	Définissez cette option pour activer ou désactiver la fonctionnalité de l'outil Service d'assistance.
KeyboardLayoutSync	`true` ou `false`	`true`	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 des postes de travail Horizon Agent pour Linux. 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.
LogCnt	Un entier	-1	Utilisez cette option pour définir le nombre de fichiers journaux réservés dans `/tmp/vmware-root`. ■ -1 : tout conserver ■ 0 : tout supprimer ■ > 0 : nombre de journaux réservés.
NetbiosDomain	Une chaîne de texte en lettres majuscules		Lorsque vous configurez l'authentification unique réelle, utilisez cette option pour définir le nom NetBIOS du domaine de votre organisation.
OfflineJoinDomain	`pbis` ou `samba`	`pbis`	Utilisez cette option pour définir la jonction de domaine hors connexion Instant Clone. Les méthodes disponibles pour exécuter une jonction de domaine hors ligne sont l'authentification PBISO (PowerBroker Identity Services Open) et la jonction de domaine hors ligne Samba. Si cette propriété a une valeur autre que `pbis` ou `samba`, la jonction de domaine hors ligne est ignorée.

Tableau 6-2. Options de configuration dans `/etc/vmware/viewagent-custom.conf` (suite)

Option	Valeur	Valeur par défaut	Description
RunOnceScript			Utilisez cette option pour joindre la machine virtuelle clonée à Active Directory. Définissez l'option `RunOnceScript` après avoir modifié le nom d'hôte. Le script spécifié est exécuté une seule fois après le changement du premier nom d'hôte. Le script est exécuté avec l'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 Active Directory avec winbind, puis définir cette option sur un chemin de script. Le script 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 Active Directory.
RunOnceScriptTimeout		120	Utilisez cette option pour définir le délai d'expiration en secondes de l'option RunOnceScript. Par exemple, définissez `RunOnceScriptTimeout=120`
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.

Tableau 6-2. Options de configuration dans `/etc/vmware/viewagent-custom.conf` (suite)

Option	Valeur	Valeur par défaut	Description
SSODesktopType	`UseGnomeClassic` ou `UseGnomeFlashback` ou `UseGnomeUbuntu` ou `UseMATE` ou `UseKdePlasma`	S/O	Cette option spécifie l'environnement de poste de travail à utiliser, au lieu de l'environnement de poste de travail par défaut, lorsque l'authentification unique est activée. Vous devez d'abord vérifier que l'environnement de poste de travail sélectionné est installé sur votre poste de travail avant de spécifier son utilisation. Lorsque cette option est définie sur un poste de travail Ubuntu 16.04/18.04, elle s'applique indépendamment, que la fonctionnalité d'authentification unique soit activée ou non. Si cette option est spécifiée dans un poste de travail RHEL.x/CentOS 7.x, l'environnement de poste de travail sélectionné est utilisé uniquement si l'authentification unique est activée. **Note** Cette option n'est pas prise en charge sur les postes de travail RHEL/CentOS 8.0 et RHEL/CentOS 6.x. Horizon 7 prend uniquement en charge l'environnement de poste de travail Gnome sur des postes de travail RHEL/CentOS 8.0. Reportez-vous à la section Environnement de poste de travail pour obtenir plus d'informations sur la configuration de KDE comme environnement de poste de travail par défaut lorsque l'authentification unique est activée sur les postes de travail RHEL/CentOS 6.x.
SSOEnable	`true` ou `false`	`true`	Définissez cette option pour activer/désactiver l'authentification unique (SSO).
SSOUserFormat	Une chaîne de texte	[username]	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. Voici des exemples de formats de nom de connexion : ■ SSOUserFormat=[domain]\\[username] ■ SSOUserFormat=[domain]+[username] ■ SSOUserFormat=[username]@[domain]
Sous-réseau	Une valeur au format d'adresse IP CIDR	[subnet]	Définissez cette option sur un sous-réseau que d'autres machines peuvent utiliser pour se connecter à Horizon Agent for Linux. S'il existe plusieurs adresses IP locales avec différents sous-réseaux, l'adresse IP locale dans le sous-réseau configuré est utilisée pour la connexion à Horizon Agent for Linux. Vous devez spécifier la valeur au format d'adresse IP CIDR. Par exemple, Subnet=123.456.7.8/24.

Tableau 6-2. Options de configuration dans `/etc/vmware/viewagent-custom.conf` (suite)

Option	Valeur	Valeur par défaut	Description
UEMEnable	`true` ou `false`	`false`	Définissez cette option pour activer ou désactiver les stratégies de carte à puce Dynamic Environment Manager. Si l'option est définie sur Activer, et que la condition dans la stratégie de carte à puce Dynamic Environment Manager est remplie, les stratégies sont appliquées.
UEMNetworkPath	Une chaîne de texte		Cette option doit être définie sur le chemin de réseau qui est défini dans la Console Dynamic Environment Manager. Le chemin d'accès doit suivre le format `//10.111.22.333/view/LinuxAgent/UEMConfig`.

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.

Utilisation de Stratégies de carte à puce

Vous pouvez utiliser des Stratégies de carte à puce pour créer des stratégies qui contrôlent le comportement des fonctionnalités de redirection USB, de redirection du Presse-papiers et de redirection du lecteur client sur des postes de travail Linux distants spécifiques.

Vous pouvez créer des stratégies pour les paramètres d'environnement utilisateur qui contrôlent le comportement de la redirection USB, l'impression virtuelle, la redirection du Presse-papiers, la redirection du lecteur client, les fonctionnalités de transfert de fichiers Web et Chrome, ainsi que les profils de bande passante dans une application ou un poste de travail publié. Les stratégies de carte à puce Horizon pour les paramètres d'environnement utilisateur sont appliquées lors de la connexion et peuvent être actualisées lors de la reconnexion d'une session. Pour réappliquer les stratégies de carte à puce Horizon lorsqu'un utilisateur se reconnecte à une session, vous pouvez configurer une tâche déclenchée.

Vous pouvez créer des stratégies pour les paramètres d'environnement de l'ordinateur que Dynamic Environment Manager applique lorsque les ordinateurs des utilisateurs finaux démarrent. Ces stratégies de carte à puce Horizon contrôlent le comportement de la redirection multimédia Flash, de l'impression intégrée et de la redirection USB. Les stratégies de carte à puce Horizon pour les paramètres d'environnement ordinateur sont appliquées lors du démarrage de l'ordinateur et peuvent être actualisées lors de la reconnexion d'une session.

Avec Stratégies de carte à puce, vous pouvez créer des stratégies qui ne prennent effet que si certaines conditions sont respectées. Par exemple, vous pouvez configurer une stratégie qui désactive la fonctionnalité de redirection du lecteur client si un utilisateur se connecte à un poste de travail distant depuis l'extérieur du réseau d'entreprise.

Configuration requise pour les Stratégies de carte à puce

Pour utiliser des Stratégies de carte à puce, votre environnement Horizon 7 doit satisfaire une certaine configuration requise.

- Vous devez installer Horizon Agent 7.5 ou version ultérieure et VMware Dynamic Environment Manager 9.4 ou version ultérieure sur les postes de travail distants que vous voulez gérer avec des Stratégies de carte à puce.
- Les utilisateurs doivent utiliser Horizon Client 4.8 ou version ultérieure pour se connecter à des postes de travail Linux distants que vous gérez avec des Stratégies de carte à puce.
- L'option `DEMEnable` doit être activée et l'option `DEMNetworkPath` doit être définie dans le fichier `/etc/vmware/viewagent-custom.conf`. Reportez-vous à la section Définir des options dans des fichiers de configuration sur un poste de travail Linux.
- Vous devez installer les modules clients pour accéder au stockage réseau partagé. Sur un système Ubuntu 18.04, par exemple, installez le module `nfs-common` pour le stockage partagé activé par NFS et le module `cifs-utils` pour le stockage activé par Samba.

Installation de Dynamic Environment Manager

Pour utiliser HorizonStratégies de carte à puce afin de contrôler le comportement des fonctionnalités de poste de travail distant sur un poste de travail Linux distant, vous devez installer Dynamic Environment Manager 9.4 ou version ultérieure sur le poste de travail Windows distant.

Vous pouvez télécharger le programme d'installation de Dynamic Environment Manager sur la page de téléchargement de VMware. Vous pouvez installer le composant Console de gestion Dynamic Environment Manager sur les postes de travail Windows à partir desquels vous voulez gérer l'environnement Dynamic Environment Manager. Depuis la Console de gestion Dynamic Environment Manager sur un poste de travail Windows, vous pouvez contrôler le comportement des fonctionnalités de poste de travail distant sur un poste de travail Linux distant.

Pour un pool de postes de travail RDS, vous installez Dynamic Environment Manager sur l'hôte RDS qui fournit les sessions de poste de travail publié.

Pour voir des instructions sur la configuration système requise et sur l'installation complète de Dynamic Environment Manager, consultez le document *Installation et configuration de VMware Dynamic Environment Manager*.

Configuration d'Dynamic Environment Manager

Vous devez configurer Dynamic Environment Manager avant de pouvoir l'utiliser pour créer des stratégies de carte à puce pour des fonctionnalités de poste de travail distant.

Pour configurer Dynamic Environment Manager, suivez les instructions de configuration dans le *Guide d'administration de VMware Dynamic Environment Manager*.

Paramètres de stratégie de carte à puce Horizon

Vous contrôlez le comportement de fonctionnalités distantes dans Dynamic Environment Manager en créant une stratégie de carte à puce Horizon.

Vous pouvez créer des stratégies pour les paramètres d'environnement utilisateur qui contrôlent le comportement de la redirection USB, l'impression virtuelle, la redirection du Presse-papiers, la redirection du lecteur client, les fonctionnalités de transfert de fichiers Web et Chrome, ainsi que les profils de bande passante dans une application ou un poste de travail publié. Les stratégies de carte à puce Horizon pour les paramètres d'environnement utilisateur sont appliquées lors de la connexion et peuvent être actualisées lors de la reconnexion d'une session. Pour réappliquer les stratégies de carte à puce Horizon lorsqu'un utilisateur se reconnecte à une session, vous pouvez configurer une tâche déclenchée. Reportez-vous à la liste complète des stratégies dans la rubrique « Configurer les stratégies de carte à puce Horizon pour les paramètres d'environnement utilisateur » dans le *Guide d'administration de VMware Dynamic Environment Manager*.

Vous pouvez créer des stratégies pour les paramètres d'environnement de l'ordinateur que Dynamic Environment Manager applique lorsque les ordinateurs des utilisateurs finaux démarrent. Ces stratégies de carte à puce Horizon contrôlent le comportement de la redirection multimédia Flash, de l'impression intégrée et de la redirection USB. Les stratégies de carte à puce Horizon pour les paramètres d'environnement ordinateur sont appliquées lors du démarrage de l'ordinateur et peuvent être actualisées lors de la reconnexion d'une session. Reportez-vous à la liste complète des stratégies dans la rubrique « Configurer les stratégies de carte à puce Horizon pour les paramètres d'environnement de l'ordinateur » dans le *Guide d'administration de VMware Dynamic Environment Manager*.

En général, les paramètres de stratégie de carte à puce Horizon que vous configurez pour les fonctionnalités distantes dans Dynamic Environment Manager remplacent les paramètres de clé de Registre et de stratégie de groupe équivalents.

Ajout de conditions à des définitions de stratégie de carte à puce Horizon

Lorsque vous définissez une stratégie de carte à puce Horizon dans Dynamic Environment Manager, vous pouvez ajouter des conditions qui doivent être satisfaites pour que la stratégie prenne effet. Par exemple, vous pouvez ajouter une condition qui désactive la fonctionnalité de redirection du lecteur client uniquement si un utilisateur se connecte au poste de travail distant depuis l'extérieur du réseau d'entreprise.

Important Vous devez ajouter les conditions suivantes à une définition de stratégie de carte à puce Horizon pour que les paramètres de stratégie pris en charge prennent effet dans un poste de travail Linux distant. Ce sont les seules conditions actuellement prises en charge. Si d'autres conditions sont définies, le résultat final de l'évaluation de la condition est false.

Tableau 6-3. Conditions requises pour les postes de travail Linux distants

Condition	Description
`Operating System Architeacture`	Vérifie l'architecture du système d'exploitation. La valeur doit être définie sur Linux.
`Endpoint IP address`	Vérifie si l'adresse IP du point de terminaison se trouve dans la plage spécifiée ou non. Les champs vides au début de la plage sont interprétés comme étant égaux à 0 et ceux à la fin comme étant égaux à 255.

Toutefois, vous pouvez définir plusieurs conditions `Endpoint IP address` comme indiqué dans l'exemple suivant.

```
Operating system is Linux
AND Endpoint IP address is in range 11.22.33.44 – 11.22.33.54
OR Endpoint IP address is in range 11.22.33.66 – 11.22.33.77
```

Pour plus d'informations sur l'ajout et la modification des conditions dans la console de gestion Dynamic Environment Manager, consultez le *Guide d'administration de VMware Dynamic Environment Manager*.

Créer une stratégie de carte à puce Horizon dans Dynamic Environment Manager

Vous utilisez la console de gestion Dynamic Environment Manager pour créer une stratégie de carte à puce Horizon dans Dynamic Environment Manager. Lorsque vous définissez une stratégie de carte à puce Horizon, vous pouvez ajouter des conditions qui doivent être satisfaites pour que la stratégie prenne effet.

Conditions préalables

- Installez et configurez Dynamic Environment Manager. Reportez-vous aux sections Installation de Dynamic Environment Manager et Configuration d'Dynamic Environment Manager.
- Familiarisez-vous avec les conditions que vous pouvez ajouter à des définitions de stratégie de carte à puce Horizon. Reportez-vous à la section Ajout de conditions à des définitions de stratégie de carte à puce Horizon.
- Activez l'option `DEMEnable` et configurez l'option `DEMNetworkPath` dans le fichier `/etc/vmware/viewagent-custom.conf`. Reportez-vous à la section Définir des options dans des fichiers de configuration sur un poste de travail Linux.

Note Dans un réseau à forte latence, après avoir enregistré votre nouvelle stratégie de carte à puce ou celle mise à jour, accordez à Dynamic Environment Manager au moins une minute pour terminer le traitement des modifications avant de dire aux utilisateurs finaux qu'ils peuvent se connecter aux postes de travail affectés.

Vous pouvez créer des stratégies pour les paramètres d'environnement utilisateur qui contrôlent le comportement de la redirection USB, l'impression virtuelle, la redirection du Presse-papiers, la redirection du lecteur client, les fonctionnalités de transfert de fichiers Web et Chrome, ainsi que les profils de bande passante dans une application ou un poste de travail publié. Les stratégies de carte à puce Horizon pour les paramètres d'environnement utilisateur sont appliquées lors de la connexion et peuvent être actualisées lors de la reconnexion d'une session. Pour réappliquer les stratégies de carte à puce Horizon lorsqu'un utilisateur se reconnecte à une session, configurez une tâche déclenchée.

Vous pouvez créer des stratégies pour les paramètres d'environnement de l'ordinateur que Dynamic Environment Manager applique lorsque les ordinateurs des utilisateurs finaux démarrent. Ces stratégies de carte à puce Horizon contrôlent le comportement de la redirection multimédia Flash, de l'impression intégrée et de la redirection USB. Les stratégies de carte à puce Horizon pour les paramètres d'environnement ordinateur sont appliquées lors du démarrage de l'ordinateur et peuvent être actualisées lors de la reconnexion d'une session.

Pour obtenir des informations complètes sur l'utilisation de la console de gestion Dynamic Environment Manager, consultez le document *Guide d'administration de VMware Dynamic Environment Manager*.

Procédure

1. Dans la console de gestion de Dynamic Environment Manager, sélectionnez l'environnement utilisateur pour créer une stratégie pour les paramètres d'environnement utilisateur ou l'onglet **Environnement informatique** pour créer une stratégie pour les paramètres d'environnement de l'ordinateur.

   Les définitions de stratégie de carte à puce Horizon existantes, le cas échéant, apparaissent dans le volet Stratégies de carte à puce Horizon.

2. Sélectionnez **Stratégies de carte à puce Horizon** et cliquez sur **Créer** pour créer une nouvelle stratégie de carte à puce.

3. Sélectionnez l'onglet **Paramètres** et définissez les paramètres de stratégie de carte à puce.

   a. Dans la section Paramètres généraux, entrez un nom pour la stratégie de carte à puce dans la zone de texte **Nom**.

      Par exemple, si la stratégie de carte à puce affecte la fonctionnalité de redirection du lecteur client, vous pouvez nommer la stratégie de carte à puce CDR.

   b. Dans la section Paramètres de stratégie de carte à puce Horizon, sélectionnez les fonctionnalités et les paramètres de poste de travail distant à inclure dans la stratégie de carte à puce.

      Vous pouvez sélectionner plusieurs fonctionnalités de poste de travail distant.

4 Ajoutez les conditions requises pour utiliser la nouvelle stratégie de carte à puce avec des postes de travail Linux distants.

   a Sélectionnez l'onglet **Conditions**, cliquez sur **Ajouter** et sélectionnez la condition **Architecture du système d'exploitation**.

   b Définissez la valeur sur **`Linux`**.

   ```
   Operating System is Linux
   ```

   c Cliquez sur **Ajouter** et sélectionnez la condition **Adresse IP du point de terminaison**.

   L'opérateur **ET** est ajouté par défaut.

   d Dans la boîte de dialogue Adresse IP du point de terminaison, définissez la plage d'adresses IP du point de terminaison, puis cliquez sur **OK**.

   Voici un exemple d'énoncé de condition.

   ```
   Operating System is Linux
   AND Endpoint IP address is in range 11.22.33.44 – 11.22.33.54
   ```

5 Cliquez sur **Enregistrer** pour enregistrer la stratégie de carte à puce.

Dynamic Environment Manager traite la stratégie de carte à puce Horizon chaque fois qu'un utilisateur se connecte ou se reconnecte au poste de travail distant.

Dynamic Environment Manager traite plusieurs stratégies de carte à puce dans l'ordre alphabétique en fonction du nom de la stratégie de carte à puce. Les stratégies de carte à puce Horizon apparaissent dans l'ordre alphabétique dans le volet Stratégies de carte à puce Horizon. En cas de conflit de stratégies de carte à puce, la dernière stratégie de carte à puce traitée est prioritaire. Par exemple, s'il existe une stratégie de carte à puce nommée Sophie qui active la redirection USB pour l'utilisatrice Sophie et une autre stratégie de carte à puce nommée Pool qui désactive la redirection USB pour le pool de postes de travail Ubuntu1604, la fonctionnalité de redirection USB est activée lorsque Sophie se connecte à un poste de travail distant dans le pool de postes de travail Ubuntu1604.

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 6-4. 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.

```
cdrserver.forcedByAdmin=true
cdrserver.sharedFolders=d:\ebooks,;c:\spreadsheets,
cdrserver.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 `cdrserver.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**.

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

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
- Pool de postes de travail flottant Instant Clone

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 7 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.

Pour créer un pool de postes de travail flottant Instant Clone, vous devez installer l'agent Horizon 7 sur une machine virtuelle Linux avec une configuration d'environnement PBIS Open et créer un modèle à partir de celui-ci. Ensuite, utilisez l'assistant de création de pool de postes de travail de serveur de connexion pour créer le pool de postes de travail flottant Instant Clone.

Ce chapitre contient les rubriques suivantes :

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.

La procédure suivante fournit des instructions pour configurer les paramètres obligatoires pour un pool de postes de travail manuel basé sur Linux. Pour plus d'informations sur la création de pools de postes de travail manuels, reportez-vous à *Configuration de postes de travail virtuels dans Horizon Console*.

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 VMware vCenter Server est ajouté à Horizon Connection Server.

Procédure

1 Dans Horizon Console, ajoutez un pool de postes de travail manuel.

Sélectionnez **Inventaire > Postes de travail > Ajouter**.

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

2 Sélectionnez **Pool de postes de travail manuel**.

3 Sélectionnez les machines virtuelles qui sont gérées ou non gérées par vCenter Server 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 Suivez les invites de l'assistant pour créer le pool.

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 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.

6 Après avoir créé le pool de postes de travail, accordez aux utilisateurs des droits d'accès aux machines du pool de postes de travail. Dans Horizon Console, 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 les pools de postes de travail 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 pouvez 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 Horizon 7, 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	■ Ne prendre aucune action d'alimentation ■ S'assurer que les machines sont toujours sous tension ■ Interrompre ■ Désactiver
Fermeture de session automatique après la déconnexion	■ Immédiatement ■ Jamais ■ Après n minutes
Autoriser les utilisateurs à réinitialiser/redémarrer leurs machines	■ Oui ■ Non
Autoriser l'utilisateur à ouvrir des sessions séparées depuis différents périphériques clients	■ Oui ■ Non
« Supprimer la machine après la fermeture de session » pour un pool de postes de travail automatisé avec un clone complet et flottant	■ Oui ■ Non

Prise en charge des opérations d'Horizon Console

- 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 Horizon PowerCLI.

- Update-UserOwnership
- Remove-UserOwnership

Note Ne modifiez pas les paramètres **Protocole d'affichage distant**. Ces paramètres doivent rester les mêmes que ceux spécifiés lors de 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	■ Gérer à l'aide de vSphere Client pour 2D ou vDGA ■ NVIDIA GRID vGPU

Pour plus d'informations, consultez la documentation *Administration de VMware Horizon Console*.

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.

La procédure suivante fournit des instructions pour configurer les paramètres obligatoires pour un pool de postes de travail de clone complet automatisé basé sur Linux. Pour plus d'informations sur la création de pools de postes de travail de clone complet automatisés, reportez-vous à la section *Configuration de postes de travail virtuels dans Horizon Console*.

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.
- Avant d'effectuer le clonage d'une machine virtuelle, créez un modèle de machine virtuelle sur lequel les clones sont basés. Reportez-vous à la section Créer un modèle de machine virtuelle pour cloner des machines de poste de travail 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.
Domaine	Spécifiez le domaine de l'environnement Horizon 7.
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 Console, ajoutez un pool de postes de travail automatisé.

Sélectionnez **Inventaire > Postes de travail > Ajouter**.

3 Sélectionnez **Pool de postes de travail automatisé** et cliquez sur **Suivant**.

4 Sélectionnez **Machines virtuelles complètes**, sélectionnez l'instance de vCenter Server et cliquez sur **Suivant**.

5 Suivez les invites de l'assistant pour créer le pool.

a 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 ou vDGA, et de NVIDIA GRID vGPU pour les postes de travail vGPU

b Lorsque vous y êtes invité, définissez les options d'**attribution de nom aux machines virtuelles**.

Option	Description
Spécifier des noms manuellement	Entrez des noms manuellement.
Mode d'attribution de nom	Par exemple, spécifiez `LinuxVM-{n}`. Vous devez également spécifier les options de dimensionnement du pool de postes de travail suivantes : ■ Nombre maximal de machines ■ Nombre de machines de rechange sous tension

c Lorsque vous y êtes invité, sélectionnez les paramètres de vCenter Server dans l'ordre.

Vous ne pouvez pas ignorer un paramètre de vCenter Server :

1 Modèle

2 Emplacement du dossier de machine virtuelle

3 Host or cluster (Hôte ou cluster)

4 Resource pool (Pool de ressources)

5 Magasins de données

6 Après avoir créé le pool de postes de travail, accordez aux utilisateurs des droits d'accès aux machines du pool de postes de travail. Dans Horizon Console, sélectionnez le pool de postes de travail, puis **Droits** > **Ajouter un droit** et ajoutez des utilisateurs ou des groupes.

7 Attendez que toutes les machines virtuelles Linux du pool de postes de travail soient disponibles.

Créer un pool de postes de travail flottant Instant Clone pour Linux

Vous pouvez créer un pool de postes de travail flottant Instant Clone pour les machines virtuelles Linux à l'aide de l'assistant **Ajouter un pool de postes de travail**. Après avoir créé un pool de postes de travail flottant Instant Clone, vous pouvez utiliser les machines virtuelles Linux en tant que postes de travail distants dans un déploiement Horizon 7.

L'agent Horizon 7 pour Linux prend en charge les pools de postes de travail Instant Clone uniquement sur les systèmes avec Ubuntu 18.04/16.04, RHEL 7.1 ou version ultérieure, RHEL 8.0 ou SLED/SLES 12.x.

Note Les capacités graphiques de vGPU ne sont pas prises en charge sur les pools de postes de travail Instant Clone créés depuis des postes de travail Linux.

La procédure suivante fournit des instructions pour configurer les paramètres obligatoires pour un pool de postes de travail Instant Clone basé sur Linux. Pour plus d'informations sur la création de pools de postes de travail Instant Clone, reportez-vous à *Configuration de postes de travail virtuels dans Horizon Console*.

Conditions préalables

- Familiarisez-vous avec les étapes de création de machines virtuelles dans vCenter Server et l'installation de systèmes d'exploitation Linux. Pour plus d'informations, reportez-vous à la section Créer une machine virtuelle et installer Linux.
- Familiarisez-vous avec les étapes de l'intégration AD à l'aide de la solution d'authentification PBISO ou de la jonction hors ligne Samba Winbind. Pour plus d'informations, reportez-vous à la section Configurer l'authentification PBISO (PowerBroker Identity Services Open) ou Configurer la jonction de domaine hors ligne Samba .

  Note Pour créer un pool de postes de travail Instant Clone à partir d'une machine virtuelle Linux exécutant RHEL 8.0, procédez à l'intégration AD à l'aide de la jonction hors ligne Samba Winbind. Les pools de postes de travail Instant Clone ne sont pas pris en charge pour les machines virtuelles RHEL 8.0 qui utilisent l'authentification PBISO.
- Familiarisez-vous avec les étapes d'installation d'Horizon 7 Agent pour Linux. Pour plus d'informations, reportez-vous à la section Installer Horizon Agent sur une machine virtuelle Linux.
- Familiarisez-vous avec les étapes de prise d'un snapshot d'une machine virtuelle Linux hors tension à l'aide de VMware vSphere Web Client. Reportez-vous à la section « Prendre un snapshot dans VMware Host Client » dans *Gestion des hôtes uniques vSphere - VMware Host Client*.
- Vérifiez que vCenter Server est ajouté au serveur de connexion Horizon.

Procédure

1. Créez une machine virtuelle (VM) Linux sur laquelle Ubuntu 18.04/16.04, RHEL 7.1 ou version ultérieure, RHEL 8.0, ou SLED/SLES 12.x est installé.

   Pour plus d'informations, reportez-vous à la section Créer une machine virtuelle et installer Linux.
2. Installez manuellement Open VMware Tools (OVT) sur votre machine Ubuntu 18.04/16.04 à l'aide de la commande suivante :

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

   Pour plus d'informations, reportez-vous à Préparer une machine Linux pour un déploiement de postes de travail distants.

3 Installez les modules de dépendance qui sont requis pour la distribution Linux.

Pour plus d'informations, reportez-vous à la section Installer des modules de dépendance pour Horizon Agent.

4 Installez Horizon Agent for Linux dans la machine virtuelle Linux.

```
# sudo ./install_viewagent.sh –A yes
```

Reportez-vous à la section Installer Horizon Agent sur une machine virtuelle Linux pour plus d'informations.

5 Intégrez votre machine virtuelle Linux à Active Directory.

- Pour utiliser la solution d'authentification PBISO, procédez comme suit :
  a Téléchargez PBIS Open 8.5.6 ou version ultérieure depuis `https://www.beyondtrust.com/products/powerbroker–identity–services–open/` et installez-le sur votre machine virtuelle Linux.

  ```
  # sudo ./pbis–open–8.5.6.2029.linux.x86_64.deb.sh
  ```

  b Intégrez votre VM Linux à Active Directory en utilisant les informations de la section Authentification PBISO (PowerBroker Identity Services Open) dans Intégration de Linux à Active Directory.
- Pour utiliser la jonction hors ligne Samba Winbind, définissez `OfflineJoinDomain` sur **`samba`** dans le fichier `/etc/vmware/viewagent–custom.conf`.

  Note Vous devez utiliser Samba Winbind pour intégrer une machine virtuelle RHEL 8.0 à Active Directory. Sinon, la création du pool de postes de travail flottant d'Instant Clone échoue.
- Pour désactiver la jonction de domaine hors ligne, vous devez définir l'option `OfflineJoinDomain` sur **`Aucune`** dans le fichier `/etc/vmware/viewagent–custom.conf`. Sinon, la création du pool de postes de travail flottant d'Instant Clone échoue.

6 Si votre serveur DHCP n'effectue aucune diffusion vers un serveur DNS, spécifiez un serveur DNS pour votre système Linux.

Un nouvel adaptateur réseau virtuel est ajouté lorsqu'une nouvelle machine virtuelle Instant Clone est créée. Tout paramètre dans l'adaptateur réseau, par exemple le serveur DNS, dans le modèle de machine virtuelle est perdu lorsque le nouvel adaptateur réseau est ajouté à la machine virtuelle Instant Clone. PBISO nécessite un serveur DNS valide et le mappage de nom de domaine complet dans `/etc/hosts` n'est pas acceptable. Pour éviter de perdre le paramètre de serveur DNS lorsque le nouvel adaptateur réseau est ajouté à la machine virtuelle clonée, vous devez spécifier un serveur DNS dans votre système Linux. Par exemple, dans un système Ubuntu 16.04, spécifiez le serveur DNS en ajoutant les lignes suivantes dans le fichier `/etc/resolvconf/resolv.conf.d/head`.

```
nameserver 10.10.10.10
search mydomain.org
```

7 (Facultatif) Si vous souhaitez ajouter un montage NFS dans le fichier `/etc/fstab` de l'agent principal Instant Clone VDI Linux, utilisez l'une des méthodes suivantes.

   - Ajoutez un indicateur « logiciel » dans `/etc/fstab`, tel que :

     ```
     10.111.222.333:/share     /home/nfsmount    nfs
     rsize=8192,wsize=8192,timeo=14,soft,intr,tcp
     ```

   - Si vous ne souhaitez pas utiliser l'indicateur « logiciel » dans `/etc/fstab`, vous ne pouvez pas configurer `/etc/fstab` dans l'image principale de la machine virtuelle Linux. Vous pouvez écrire un script de mise hors tension pour configurer le fichier `/etc/fstab`, puis spécifier ce script de mise hors tension pour l'outil ClonePrep. Pour plus d'informations, reportez-vous au document *Administration de VMware Horizon Console*.

8 Arrêtez la machine virtuelle Linux et créez une image principale en créant un snapshot de votre machine virtuelle Linux hors tension à l'aide de VMware vSphere® Web Client.

   Pour plus d'informations, reportez-vous à la section « Prendre un snapshot dans VMware Host Client » dans *Gestion des hôtes uniques vSphere - VMware Host Client*.

9 Dans Horizon Console, ajoutez un pool de postes de travail automatisé.

   Sélectionnez **Inventaire > Postes de travail > Ajouter**.

10 Sélectionnez **Pool de postes de travail automatisé** et cliquez sur **Suivant**.

11 Sélectionnez **Instant Clones**, sélectionnez l'instance de vCenter Server et cliquez sur **Suivant**.

12 Suivez les invites de l'assistant pour créer le pool.

a Lorsque vous y êtes invité, définissez les options d'**attribution de nom aux machines virtuelles**.

Option	Description
Activer l'approvisionnement	Sélectionnez cette option.
Arrêter l'approvisionnement en cas d'erreur	Sélectionnez cette option.
Mode d'attribution de nom	Spécifiez un modèle que Horizon 7 utilisera en tant que préfixe dans tous les noms de machines virtuelles de poste de travail, suivi d'un numéro unique. Par exemple, spécifiez **`LinuxVM-{n}`**.
Nombre max. de machines	Spécifiez le nombre total de machines dans le pool.
Nombre de machines de rechange (sous tension)	Spécifiez le nombre de machines virtuelles de poste de travail à garder disponibles pour les utilisateurs.
Provisionner toutes les machines à l'avance	Sélectionnez cette option afin qu'Horizon 7 provisionne le nombre de machines virtuelles spécifiées dans **Nombre max. de machines**.

b Lorsque vous y êtes invité, sélectionnez **Utiliser VMware Virtual SAN** pour la stratégie de gestion du stockage.

c Lorsque vous y êtes invité, spécifiez le paramètre de domaine, le conteneur Active Directory et d'éventuels scripts de personnalisation supplémentaires à exécuter une fois que la machine virtuelle est clonée.

Important Lorsque vous utilisez des scripts de mise hors tension ou de postsynchronisation ClonePrep, assurez-vous que ces scripts sont situés dans le dossier `/var/userScript`, appartenant à l'utilisateur racine, et que leurs autorisations de fichier sont définies sur 700.

Dans Horizon Console, vous pouvez afficher les machines virtuelles de poste de travail telles qu'elles sont ajoutées au pool en sélectionnant **Inventaire** > **Postes de travail**.

Après avoir créé le pool, ne supprimez pas l'image principale ou ne la retirez pas de l'inventaire de vCenter Server tant que le pool existe. Si vous supprimez la machine virtuelle d'image maître de l'inventaire de vCenter Server par erreur, vous devez la rajouter et réaliser une image de transfert à l'aide de l'image actuelle.

Étape suivante

Autorisez les utilisateurs à accéder au pool. Reportez-vous à la section « Ajouter des droits aux pools de postes de travail » dans *Configuration de postes de travail virtuels dans Horizon Console*.

Commandes PowerCLI Broker

Les cmdlets Horizon PowerCLI, qui sont utilisés pour effectuer de nombreuses tâches administratives sur le Serveur de connexion et un poste de travail Windows, peuvent également être utilisés pour les postes de travail Linux.

Créer un pool de postes de travail manuel

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

Les options et les valeurs suivantes sont obligatoires pour le poste de travail Linux.

- `DefaultProtocol Blast`
- `AllowProtocolOverride $false`
- `threedRender usevc|vgpu`. Pour un poste de travail vGPU, utilisez `-threedRender vgpu` et, pour un poste de travail 2D/DGA, utilisez `-threedRender 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 -threedRender 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 -threedRender 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 -
  threedRender usevc -Pool_id LinuxDesktop
  ```

Créer un pool de postes de travail automatisé de clone complet

```
Add-AutomaticPool -DefaultProtocol Blast -AllowProtocolOverride $false -threedRender 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]
```

Les options et les valeurs suivantes sont obligatoires pour les postes de travail Linux.

- `DefaultProtocol Blast`

- `AllowProtocolOverride $false`
- `threedRender usevc|vgpu` Pour un poste de travail vGPU, utilisez `–threedRender vgpu` ; pour un poste de travail 2D, utilisez `–threedRender usevc`.

Exemple

```
Add–AutomaticPool –DefaultProtocol Blast –AllowProtocolOverride $false –threedrender 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 un 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'un 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 l'utilisateur **`myuser`** à la 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 l'utilisateur **`myuser`** de la 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 PowerCLI Broker, reportez-vous à la section « Utilisation du module HorizonPowerCLI » dans *Intégration d'Horizon 7*.

Déploiement en bloc d'Horizon 7 pour des pools de postes de travail manuels

8

Avec Horizon Console, 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

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.	■ Pour Ubuntu, vous devez installer le serveur SSH avec la commande `sudo apt-get install openssh-server`. 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 `pscp.exe` et `plink.exe` 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 Horizon 7.
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.	■ 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.
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.	Le profil et les données utilisateur sont conservés.

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 (vRAM) requises pour les écrans que vous devez utiliser avec la machine virtuelle. Reportez-vous à la section Paramètres de machine virtuelle pour les graphiques 2D.
- 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. Reportez-vous à la section Chapitre 5 Installation d'Horizon Agent.
- Si nécessaire, familiarisez-vous avec les étapes de configuration des options à l'aide des fichiers de configuration d'Horizon 7. 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.

      Suivez les instructions sur les vCPU et la taille de la mémoire virtuelle dans le guide d'installation de votre distribution Linux.

      Par exemple, Ubuntu 18.04 indique 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, 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.

      Suivez les instructions de la section Paramètres de machine virtuelle pour les graphiques 2D. 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/CentOS 8.x, RHEL/CentOS 7.x ou SLED/SLES 12.x, installez VMware Tools.

Open VM Tools est installé par défaut sur RHEL/CentOS 8.0, RHEL/CentOS 7.x et SLED/SLES 12.x.

8 Installez et configurez les modules de dépendance.

a Si la distribution Linux exécute une version d'Open VM Tools antérieure à 9.10, installez le plug-in deployPkg.

Les instructions sont disponibles à l'adresse http://kb.vmware.com/kb/2075048.

b Si la distribution Linux est Ubuntu, consultez les articles suivants de la base de connaissances afin de déterminer les modules de dépendance à installer et à configurer dans la machine virtuelle.

- Consultez les articles https://kb.vmware.com/s/article/2051469 et https://kb.vmware.com/s/article/59687 de la base de connaissances pour Ubuntu 18.04 et 16.04.
- Pour Ubuntu 18.04, reportez-vous également à l'article https://kb.vmware.com/s/article/56409 de la base de connaissances.

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 Installez Horizon Agent.

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

Reportez-vous à la section Chapitre 5 Installation d'Horizon Agent.

13 Exécutez des configurations supplémentaires à l'aide des fichiers de configuration de Horizon 7.

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,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
linux-002,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
linux-003,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
linux-004,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
linux-005,Ubuntu1804x64,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://docs.vmware.com/fr/VMware-Horizon-7/index.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, qui peut uniquement être complet
- S'il faut désactiver une console VM vSphere

Contenu du script

```
<#
Create Clones from a Master VM

The Tool supports creation of Full clone from Master VM.
#>
#-------------------------- 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 -------------------------

$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
$cloneType = GetInput -prompt 'Clone Type ("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 full clone
if (($CloneType.length >0) -and ($CloneType -ne "full"))
{
    write-host  -ForeGroundColor Red "Clone type supports only '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
    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<"Full"> : Full
Disable vSphere VM Console ("yes" or "no", recommend "yes") : yes
```

La durée du processus de 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"

.DESCRIPTION
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
""
"`nPlease 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

.DESCRIPTION
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
""
"`nPlease 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'
$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
"-----------------------------------------------------"

$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 PowerCLI 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://docs.vmware.com/fr/VMware-Horizon-7/index.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 d'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 Horizon 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
}
$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
"-----------------------------------------------------"
$agentInstaller = GetInput -prompt 'Type the Horizon 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";
        $cmd = "tar -xzvf VMware-*-linux-*.tar.gz"
        Write-Host "Run cmd '$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 Horizon 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: HorizonUser
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
}
$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
"----------------------------------------------------"
$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 :

Utilisation d'Horizon Help Desk Tool dans la Horizon Console

Horizon Help Desk Tool est une application Web que vous pouvez utiliser pour obtenir l'état des sessions utilisateur Horizon 7 et effectuer des opérations de dépannage et de maintenance.

Dans Horizon Help Desk Tool, vous pouvez rechercher des sessions utilisateur pour résoudre des problèmes et exécuter des opérations de maintenance de poste de travail, telles que redémarrer ou réinitialiser des postes de travail.

Pour configurer Horizon Help Desk Tool, vous devez respecter les exigences suivantes :

- Licence d'édition d'Horizon Enterprise ou licence d'édition avancée d'Horizon Apps pour Horizon 7. Pour vérifier que vous disposez de la licence correcte, consultez le document *Administration d'Horizon 7*.
- Base de données d'événements pour stocker des informations sur les composants Horizon 7. Pour plus d'informations sur la configuration d'une base de données d'événements, reportez-vous au document *Administration d'Horizon 7*.
- Rôle Administrateur du service d'assistance ou rôle Administrateur du service d'assistance (lecture seule) pour se connecter à Horizon Help Desk Tool. Pour plus d'informations sur ces rôles, reportez-vous au document *Administration d'Horizon 7*.

- Activez le profileur de minutage sur chaque instance du Serveur de connexion pour afficher les segments d'ouverture de session.

  Pour ce faire, utilisez la commande `vdmadmin` suivante :

  ```
  vdmadmin –I –timingProfiler –enable
  ```

  Utilisez la commande `vdmadmin` suivante pour activer le profileur de minutage sur une instance du Serveur de connexion qui utilise un port de gestion :

  ```
  vdmadmin –I –timingProfiler –enable –server {ip/server}
  ```

- Activez l'option `HelpDeskEnable`dans le fichier de configuration `/etc/vmware/viewagent–custom.conf`.

Démarrer Horizon Help Desk Tool dans la Horizon Console

Horizon Help Desk Tool est intégré à la Horizon Console. Vous pouvez rechercher un utilisateur pour lequel vous voulez résoudre des problèmes dans Horizon Help Desk Tool.

Procédure

1. Vous pouvez rechercher un nom d'utilisateur dans la zone de texte Recherche d'utilisateur ou accéder directement à l'outil Horizon Help Desk Tool.
   - Dans la Horizon Console, entrez un nom d'utilisateur dans la zone de texte Recherche d'utilisateur.
   - Sélectionnez **Surveiller > Service d'assistance** et entrez un nom d'utilisateur dans la zone de texte Recherche d'utilisateur.

   La Horizon Console affiche une liste d'utilisateurs dans les résultats de recherche. La recherche peut renvoyer jusqu'à 100 résultats correspondants.
2. Sélectionnez un nom d'utilisateur.

   Les informations d'utilisateur s'affichent dans une fiche utilisateur.

Étape suivante

Pour résoudre les problèmes, cliquez sur les onglets associés dans la fiche utilisateur.

Résolution des problèmes des utilisateurs dans Horizon Help Desk Tool

Dans Horizon Help Desk Tool, vous pouvez afficher des informations utilisateur de base dans une fiche utilisateur. Vous pouvez cliquer sur les onglets de la fiche utilisateur pour obtenir plus d’informations sur des composants spécifiques.

Les détails utilisateur peuvent parfois s'afficher dans des tableaux. Vous pouvez trier ces détails utilisateur dans des colonnes.

- Pour trier une colonne dans l'ordre croissant, cliquez une fois sur la colonne.

- Pour trier une colonne dans l'ordre décroissant, cliquez deux fois sur la colonne.
- Pour ne pas trier la colonne, cliquez trois fois sur la colonne.

Informations utilisateur de base

Affiche les informations utilisateur de base, telles que le nom, le numéro de téléphone et l'adresse e-mail de l'utilisateur, et indique si l'utilisateur est connecté ou déconnecté. Si l'utilisateur a ouvert une session de poste de travail, l'état de l'utilisateur est Connecté. Dans le cas contraire, son état est Déconnecté.

Vous pouvez cliquer sur l'adresse e-mail pour envoyer un message à l'utilisateur.

Sessions

L'onglet **Sessions** affiche des informations sur les sessions de poste de travail auxquelles l'utilisateur est connecté.

Vous pouvez utiliser la zone de texte **Filtre** pour filtrer les sessions de poste de travail.

Note L'onglet **Sessions** n'affiche pas les informations de session pour les sessions qui accèdent à des VM virtuelles depuis vSphere Client ou ESXi.

L'onglet **Sessions** contient les informations suivantes :

Tableau 9-1. Onglet Sessions

Option	Description
État	Affiche des informations sur l'état de la session de poste de travail ■ S'affiche en vert si la session est connectée. ■ L, si la session est une session locale ou une session en cours d'exécution dans l'espace local.
Nom de l'ordinateur	Nom de la session de postes de travail. Cliquez sur le nom pour ouvrir les informations de session dans une fiche. Vous pouvez cliquer sur les onglets dans la carte de session pour afficher des informations supplémentaires : ■ L'onglet **Détails** affiche les informations utilisateur, telles que des informations sur la VM et l'utilisation du CPU ou de la mémoire. ■ L'onglet **Processus** affiche des informations sur les processus liés au CPU et à la mémoire.
Protocole	Protocole d'affichage de la session de poste de travail.
Type	Indique si le poste de travail est un poste de travail publié ou un poste de travail de machine virtuelle.
Heure d'ouverture de session	Heure à laquelle la session s'est connectée au Serveur de connexion.
Durée de la session	Durée de la connexion de la session au Serveur de connexion.

Postes de travail

L'onglet **Postes de travail** affiche des informations sur les postes de travail publiés ou les postes de travail virtuels que l'utilisateur est autorisé à utiliser.

Tableau 9-2. Postes de travail

Option	Description
État	Affiche des informations sur l'état de la session de poste de travail ■ S'affiche en vert si la session est connectée.
Nom du pool de postes de travail	Nom du pool de postes de travail de la session.
Type de poste de travail	Indique si le poste de travail est un poste de travail publié ou un poste de travail de machine virtuelle. **Note** N'affiche pas d'informations si la session est en cours d'exécution dans un espace différent de la fédération d'espaces.
Type	Affiche des informations sur le type d'autorisation de poste de travail. ■ Locale, pour une autorisation locale.
vCenter	Affiche le nom de la machine virtuelle dans vCenter Server. **Note** N'affiche pas d'informations si la session est en cours d'exécution dans un espace différent de la fédération d'espaces.
Protocole par défaut	Protocole d'affichage par défaut de la session de poste de travail.

Activités

L'onglet **Activités** affiche les informations de journal des événements sur les activités de l'utilisateur. Vous pouvez filtrer les activités selon un intervalle de temps, tel que les 12 dernières heures ou les 30 derniers jours, ou selon le nom de l'administrateur. Cliquez sur **Événement Service d'assistance uniquement** pour filtrer uniquement selon les activités d'Horizon Help Desk Tool. Cliquez sur l'icône d'actualisation pour actualiser le journal des événements. Cliquez sur l'icône d'exportation pour exporter le journal des événements en tant que fichier.

Note Le journal des événements n'est pas affiché pour les utilisateurs dans un environnement Architecture Cloud Pod.

Tableau 9-3. Activités

Option	Description
Heure	Sélectionnez un intervalle de temps. La valeur par défaut est les 12 dernières heures. ■ **12 dernières heures** ■ **24 dernières heures** ■ **7 derniers jours** ■ **30 derniers jours** ■ **Tout**
Administrateurs	Nom de l'utilisateur administrateur.
Message	Affiche les messages d'un utilisateur ou d'un administrateur qui sont spécifiques aux activités effectuées par l'utilisateur ou l'administrateur.
Nom de la ressource	Affiche les informations sur le nom du pool de postes de travail ou de la machine virtuelle sur lequel l'activité a été effectuée.

Détails de session d'Horizon Help Desk Tool

Les détails de session s'affichent dans l'onglet **Détails** lorsque vous cliquez sur un nom d'utilisateur dans l'option **Nom de l'ordinateur** dans l'onglet **Sessions**. Vous pouvez afficher les détails d'Horizon Client, le poste de travail virtuel ou publié et les détails du CPU et de la mémoire.

Client

Affiche des informations qui varient en fonction du type de client Horizon Client, ainsi que des détails tels que le nom d'utilisateur, la version d'Horizon Client, l'adresse IP et le système d'exploitation de la machine cliente.

Note Si vous avez mis Horizon Agent à niveau, vous devez également mettre à niveau Horizon Client vers la dernière version. Sinon, aucune version n'est affichée pour Horizon Client. Pour plus d'informations sur la mise à niveau d'Horizon Client, reportez-vous au document *Mises à niveau d'Horizon 7*.

VM

Affiche des informations sur les postes de travail virtuels ou publiés.

Tableau 9-4. Détails de la machine virtuelle

Option	Description
Nom de l'ordinateur	Nom de la session de postes de travail.
Version d'agent	Version de l'agent Horizon Agent.
Version du SE	Version du système d'exploitation.
Serveur de connexion	Serveur de connexion auquel la session se connecte.
Pool	Nom du pool de postes de travail.
vCenter	Adresse IP de vCenter Server.

Tableau 9-4. Détails de la machine virtuelle (suite)

Option	Description
État de session	État de la session de postes de travail. Les états de session peuvent être connecté ou déconnecté.
Durée de la session	Durée de connexion de la session au Serveur de connexion.
Durée de l'état	Durée de persistance de la session dans l'état.
Heure d'ouverture de session	Heure d'ouverture de session de l'utilisateur connecté à la session.
Durée d'ouverture de session	Durée pendant laquelle l'utilisateur est connecté au poste de travail Linux.

Mesures de l'expérience utilisateur

Affiche les détails de performances d'une session de poste de travail virtuel ou publié qui utilise le protocole d'affichage VMware Blast. Pour afficher ces détails sur les performances, cliquez sur **Plus**. Pour actualiser ces détails, cliquez sur l'icône d'actualisation.

Tableau 9-5. Détails du protocole d'affichage Blast

Option	Description
Fréquence d'images	Fréquence d'images, en images par seconde, dans une session Blast.
État de Skype	Pour les sessions de poste de travail Linux, cette option indique S/O.
Compteurs de session Blast	■ **Bande passante estimée (liaison montante)**. Bande passante estimée pour un signal de liaison montante. ■ **Perte de paquets (liaison montante)**. Pourcentage de perte de paquets pour un signal de liaison montante.
Compteurs d'imagerie Blast	■ **Octets transmis**. Nombre total d'octets pour les données d'imagerie qui ont été transmis pour une session Blast. ■ **Octets reçus**. Nombre total d'octets pour les données d'imagerie qui ont été reçus pour une session Blast.
Compteurs audio Blast	■ **Octets transmis**. Nombre total d'octets pour les données audio qui ont été transmis pour une session Blast. ■ **Octets reçus**. Nombre total d'octets pour les données audio qui ont été reçus pour une session Blast.
Compteurs CDR Blast	■ **Octets transmis**. Nombre total d'octets pour les données de redirection du lecteur client qui ont été transmis pour une session Blast. ■ **Octets reçus**. Nombre total d'octets pour les données de redirection du lecteur client qui ont été reçus pour une session Blast.

Utilisation du CPU et de la mémoire et performances du réseau et du disque

Affiche des graphiques de l'utilisation du CPU et de la mémoire du poste de travail virtuel ou publié et des performances du réseau ou du disque pour le protocole d'affichage ou Blast.

Note Suite à un démarrage ou un redémarrage d'Horizon Agent sur le poste de travail, les graphiques de performances peuvent ne pas afficher immédiatement la chronologie. La chronologie s'affiche après quelques minutes.

Tableau 9-6. Utilisation du CPU

Option	Description
CPU de la session	Utilisation du CPU de la session actuelle.
CPU de l'hôte	Utilisation du CPU de la machine virtuelle à laquelle la session est attribuée.

Tableau 9-7. Utilisation de la mémoire

Option	Description
Mémoire de la session	Utilisation de la mémoire de la session actuelle.
Mémoire de l'hôte	Utilisation de la mémoire de la machine virtuelle à laquelle la session est attribuée.

Tableau 9-8. Performances du réseau

Option	Description
Latence	Affiche un graphique de la latence pour la session PCoIP ou Blast. Le temps de latence est la durée de l'aller-retour en millisecondes. Le compteur de performances qui suit ce temps de latence est **Compteurs de session VMware Blast > RTT**.

Tableau 9-9. Performances du disque

Option	Description
Lecture	Nombre d'opérations d'entrée/sortie de lecture par seconde.
Écriture	Nombre d'opérations d'entrée/sortie d'écriture par seconde.
Latence de disque	Affiche un graphique de la latence de disque. La latence de disque est la durée en millisecondes des données IOPS (opérations d'entrée/sortie par seconde) récupérées depuis les compteurs de performances Windows.
Lecture moyenne	Nombre moyen d'opérations d'entrée/sortie de lecture aléatoire par seconde.
Écriture moyenne	Nombre moyen d'opérations d'entrée/sortie d'écriture aléatoire par seconde.
Latence moyenne	Temps de latence moyenne en millisecondes des données IOPS récupérées depuis les compteurs de performances Windows.

Segments d'ouverture de session

Affiche les segments de durée et d'utilisation de l'ouverture de session qui sont créés lors de l'ouverture de session.

Tableau 9-10. Segments d'ouverture de session

Option	Description
Durée d'ouverture de session	Durée calculée entre le moment où l'utilisateur clique sur le pool de postes de travail et le moment où l'utilisateur s'est connecté au poste de travail Linux.
Heure d'ouverture de session	Durée de la connexion de l'utilisateur à la session.
Segments d'ouverture de session	Affiche les segments qui sont créés lors de l'ouverture de session. ■ **Intermédiation**. Délai total nécessaire au Serveur de connexion pour traiter une connexion ou une reconnexion à une session. Mesuré entre le moment où l'utilisateur clique sur le pool de postes de travail et le moment où la connexion par tunnel est configurée. Inclut les délais des tâches du Serveur de connexion, tels que l'authentification d'utilisateur, la sélection de machine et la préparation de la machine pour la configuration de la connexion par tunnel. ■ **Interactif**. Délai total nécessaire à l'agent Horizon Agent pour traiter une connexion ou une reconnexion à une session. Calculé entre le moment où Blast Extreme utilise la connexion par tunnel et le moment où l'utilisateur s'est connecté au poste de travail Linux. ■ **Connexion au protocole**. Durée totale nécessaire pour la connexion du protocole PCoIP ou Blast pendant le processus d'ouverture de session. ■ **Script d'ouverture de session**. Durée totale nécessaire pour l'exécution complète d'un script d'ouverture de session. ■ **Authentification**. Temps total dont dispose le Serveur de connexion pour authentifier la session. ■ **Démarrage de VM**. Temps total nécessaire pour démarrer une machine virtuelle. Cette durée inclut le temps de démarrage du système d'exploitation, la reprise d'une machine suspendue et le temps nécessaire à Horizon Agent pour signaler qu'il est prêt pour une connexion.

Processus de session pour Horizon Help Desk Tool

Les processus de session s'affichent dans l'onglet **Processus** lorsque vous cliquez sur un nom d'utilisateur dans l'option **Nom de l'ordinateur** dans l'onglet **Sessions**.

Processus

Pour chaque session, vous pouvez afficher des détails supplémentaires sur les processus liés au CPU et à la mémoire. Par exemple, si vous remarquez que l'utilisation du CPU et de la mémoire pour une session est anormalement élevée, vous pouvez afficher les détails pour le processus dans l'onglet **Processus**.

Pour les sessions hôtes RDS, l'onglet **Processus** affiche les processus de sessions hôtes RDS actuelles démarrés par l'utilisateur actuel ou le processus système actuel.

Tableau 9-11. Détails de processus de session

Option	Description
Nom du processus	Nom du processus de session. Par exemple, chrome.exe.
CPU	Utilisation du CPU du processus en pourcentage.
Mémoire	Utilisation de la mémoire du processus en Ko.
Disque	IOPS du disque de mémoire. Calculées avec la formule suivante : (Nombre total d'octets d'E/S de l'heure actuelle) - (Nombre total d'octets d'E/S une seconde avant l'heure actuelle). Ce calcul peut afficher une valeur de 0 Ko par seconde si le Gestionnaire des tâches affiche une valeur positive.
Nom d'utilisateur	Nom de l'utilisateur propriétaire du processus.
CPU de l'hôte	Utilisation du CPU de la machine virtuelle à laquelle la session est attribuée.
Mémoire de l'hôte	Utilisation de la mémoire de la machine virtuelle à laquelle la session est attribuée.
Processus	Nombre de processus dans la machine virtuelle
Actualiser	L'icône d'actualisation actualise la liste des processus.
Terminer le processus	Arrête un processus en cours d'exécution. **Note** Vous devez disposer du rôle Administrateur du service d'assistance pour terminer un processus. Pour mettre fin à un processus, sélectionnez un processus et cliquez sur le bouton **Terminer le processus**. Vous ne pouvez pas mettre fin aux processus critiques tels que les principaux processus Windows pouvant être répertoriés dans l'onglet **Processus**. Si vous arrêtez un processus critique, Horizon Help Desk Tool affiche un message indiquant qu'il ne peut pas terminer le processus système.

Résoudre les problèmes de sessions de poste de travail Linux dans Horizon Help Desk Tool

Dans Horizon Help Desk Tool, vous pouvez résoudre les problèmes de sessions de poste de travail Linux en fonction de l'état de la connexion de l'utilisateur.

Conditions préalables

- Démarrez Horizon Help Desk Tool.

Procédure

1 Dans la fiche utilisateur, cliquez sur l'onglet **Sessions**.

Une fiche de performances indique l'utilisation du CPU et de la mémoire et contient des informations sur Horizon Client et le poste de travail virtuel ou publié.

2 Choisissez une option de dépannage.

Option	Action
Envoyer un message	Envoie un message à l'utilisateur sur le poste de travail publié ou le poste de travail virtuel. Vous pouvez choisir le niveau de gravité du message à inclure, à savoir Info, Avertissement ou Erreur. Cliquez sur **Envoyer un message**, entrez le type de gravité et les détails du message, puis cliquez sur **Envoyer**.
Redémarrer	Lance le processus de redémarrage sur le poste de travail virtuel. Cette fonctionnalité n'est pas disponible pour une session de poste de travail publié. Cliquez sur **Redémarrer VDI**.
Se déconnecter	Déconnecte la session de poste de travail ou d'application. Cliquez sur **Plus > Se déconnecter**.
Fermer la session	Initie le processus de déconnexion d'un poste de travail publié ou d'un poste de travail virtuel. Cliquez sur **Plus > Fermer la session**.
Réinitialiser	Initie une réinitialisation de la machine virtuelle. Cette fonctionnalité n'est pas disponible pour un poste de travail publié. Cliquez sur **Plus > Réinitialiser la VM**. **Note** L'utilisateur peut perdre le travail non enregistré.

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).

Horizon Agent ne se déconnecte pas d'Horizon Client sur iPad Pro

La connexion Horizon 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. Horizon Agent ne parvient pas à se déconnecter.

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

SLES 12 SP1 ne s'actualise pas automatiquement en mode moniteurs multiples lorsque vous faites glisser un terminal GNOME.

Problème

Lorsque vous démarrez SLES 12 SP1 en mode moniteurs multiples 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.

Solution

1. Terminez la session Shell GNOME.

```
kill -9 <process id of gnome-shell>
```

2 Redémarrez la session Shell GNOME.

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 l'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.