Utilisation de VMware Horizon Client pour Linux

Horizon Client 4.3

Ce document prend en charge la version de chacun des produits répertoriés, ainsi que toutes les versions publiées par la suite jusqu'au remplacement dudit document par une nouvelle édition. Pour rechercher des éditions plus récentes de ce document, rendez-vous sur : http://www.vmware.com/fr/support/pubs.

FR-002318-00

vmware®

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

http://www.vmware.com/fr/support/

Le site Web de VMware propose également les dernières mises à jour des produits.

N'hésitez pas à nous transmettre tous vos commentaires concernant cette documentation à l'adresse suivante :

docfeedback@vmware.com

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

VMware, Inc.
100-101 Quartier Boieldieu
92042 Paris La Défense
France
www.vmware.com/fr

Table des matières

Utilisation de VMware Horizon Client pour Linux

Ce guide intitulé *Utilisation de VMware Horizon Client pour Linux* fournit des informations sur l'installation et l'utilisation du logiciel VMware Horizon® Client™ sur un système client Linux pour une connexion à un poste de travail View dans le centre de données.

Ce document contient des informations sur la configuration système requise et des instructions sur l'installation et l'utilisation d'Horizon Client pour Linux.

Ces informations sont destinées aux administrateurs qui doivent configurer un déploiement d'View comportant des systèmes clients Linux. Les informations sont rédigées pour des administrateurs système expérimentés qui connaissent parfaitement la technologie des machines virtuelles et les opérations de datacenter.

Remarque Ce document concerne principalement Horizon Client pour Linux que VMware met à disposition. En outre, plusieurs partenaires VMware offrent des périphériques clients léger et zéro pour les déploiements d'View. Les fonctionnalités disponibles pour chaque périphérique client léger ou zéro, et les systèmes d'exploitation pris en charge, sont mises en œuvre en fonction du fournisseur, du modèle et de la configuration qu'une entreprise choisit d'utiliser. Pour plus d'informations sur les fournisseurs et les modèles de ces périphériques clients, consultez le Guide de compatibilité VMware, disponible sur le site Web de VMware.

Configuration système requise et installation

1

Les systèmes client doivent répondre à certaines exigences matérielles et logicielles. Le processus d'installation d' Horizon Client est semblable à celui d'autres applications.

Ce chapitre aborde les rubriques suivantes :

Configuration système requise pour les systèmes clients Linux

L'ordinateur de bureau ou le portable Linux sur lequel vous installez Horizon Client, et les périphériques qu'il utilise, doit respecter une certaine configuration système.

Remarque Cette configuration système requise concerne Horizon Client pour Linux que VMware met à disposition. En outre, plusieurs partenaires VMware offrent des périphériques clients léger et zéro pour les déploiements d'View. Les fonctionnalités disponibles pour chaque périphérique client léger ou zéro, et les systèmes d'exploitation pris en charge, sont mises en œuvre en fonction du fournisseur, du modèle et de la configuration qu'une entreprise choisit d'utiliser. Pour plus d'informations sur les fournisseurs et les modèles de ces périphériques clients, consultez le Guide de compatibilité VMware, disponible sur le site Web de VMware.

Remarque

- À partir de la version 7.0, View Agent est renommé Horizon Agent.
- VMware Blast, le protocole d'affichage disponible à partir d'Horizon Client 4.0 et Horizon Agent 7.0, est également appelé VMware Blast Extreme.

Architecture

i386, x86_64, ARM

Mémoire

Au moins 2 Go de RAM

Système d'exploitation

Système d'exploitation	Version
Ubuntu	12.04, 14.04
Ubuntu 64 bits	12.04, 14.04
Red Hat Enterprise Linux (RHEL)	6.8
Red Hat Enterprise Linux (RHEL) 64 bits	6.8, 7.2
SUSE Linux Enterprise Desktop (SLED)	11 SP4
CentOS	6.8

Configuration requise pour OpenSSL

Horizon Client requiert une version spécifique d'OpenSSL. La version correcte est automatiquement téléchargée et installée.

Serveur de connexion View, serveur de sécurité et View Agent ou Horizon Agent

Dernière version de maintenance de View 5.3.x et versions ultérieures.

Si les systèmes clients se connectent en dehors du pare-feu d'entreprise, VMware recommande d'utiliser un serveur de sécurité. Avec un serveur de sécurité, les systèmes client ne requièrent pas de connexion VPN.

Les applications distantes (hébergées) sont disponibles uniquement sur les serveurs Horizon 6.0 (ou version ultérieure) avec View.

Protocole d'affichage

- VMware Blast (requiert Horizon Agent 7.0 ou version ultérieure)
- PCoIP
- RDP

Résolution d'écran sur le système client

Minimale : 1 024 x 768 pixels

Exigences matérielles pour VMware Blast et PCoIP

- Un processeur x86 ou x64 avec extensions SSE2, avec une vitesse de processeur d'au moins 800 MHz.

- RAM disponible supérieure à la configuration requise pour prendre en charge plusieurs configurations d'écran. Utilisez la formule suivante comme indicateur général :

  ```
  20MB + (24 * (# monitors) * (monitor width) * (monitor height))
  ```

  Comme indicateur rapide, vous pouvez utiliser les calculs suivants :

  ```
  1 monitor: 1600 x 1200: 64MB
  2 monitors: 1600 x 1200: 128MB
  3 monitors: 1600 x 1200: 256MB
  ```

Exigences matérielles pour RDP

- Un processeur x86 ou x64 avec extensions SSE2, avec une vitesse de processeur d'au moins 800 MHz.
- RAM de 128 Mo.

Exigences logicielles pour Microsoft RDP

Pour Ubuntu 12.04, utilisez rdesktop 1.7.0.

Exigences logicielles pour FreeRDP

Si vous prévoyez d'utiliser une connexion RDP vers des postes de travail View et que vous préférez utiliser un client FreeRDP pour la connexion, vous devez installer la version correcte de FreeRDP et tous les correctifs applicables. Reportez-vous à la section « Installer et configurer FreeRDP », page 47.

Autres exigences logicielles

Horizon Client a également d'autres exigences logicielles en fonction de la distribution Linux utilisée. Assurez-vous de permettre à l'assistant d'installation d'Horizon Client d'analyser la compatibilité et les dépendances de la bibliothèque de votre système. La liste suivante de configurations requises ne s'applique qu'aux distributions Ubuntu.

- `libudev0`

  Remarque À partir d'Horizon Client 4.2, `libudev0` est requis pour lancer Horizon Client. Par défaut, `libudev0` n'est pas installé dans Ubuntu 14.04.

- Pour prendre charge les délais d'expiration des sessions inactives : `libXsso.so.1`.
- Pour prendre en charge la redirection d'URL Flash : `libexpat.so.1`. (Le fichier `libexpat.so.0` n'est plus requis.)
- Activez Xinerama pour améliorer les performances lorsque vous utilisez plusieurs moniteurs.

Configuration système requise pour l'Audio/Vidéo en temps réel

L'Audio/Vidéo en temps réel fonctionne avec des webcams standard, des périphériques audio USB et analogiques ainsi qu'avec les applications de conférence standard telles que Skype, WebEx et Google Hangouts. Pour prendre en charge l'Audio/Vidéo en temps réel, le déploiement de votre View doit satisfaire certaines exigences matérielles et logicielles.

Poste de travail distant View

View Agent 5.2 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure, doit être installé sur les postes de travail. S'agissant des postes de travail View Agent 5.2, la version correspondante de Remote Experience Agent doit également être installée sur les postes de travail. Par exemple, si View Agent 5.2 est installé, vous devez également installer Remote

Experience Agent à partir de View 5.2 Feature Pack 2. Consultez le document *Installation et administration de View Feature Pack* pour View. Si vous disposez de View Agent 6.0 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure, aucun Feature Pack n'est requis. Pour utiliser l'Audio/Vidéo en temps réel avec des postes de travail RDS et des applications distantes, vous devez disposer d'Horizon Agent 7.0.2 ou version ultérieure.

Ordinateur Horizon Client ou périphérique d'accès client

- L'Audio/Vidéo en temps réel est pris en charge sur les périphériques x86 et x64. Cette fonctionnalité n'est pas prise en charge par les processeurs ARM. Le système client doit répondre aux exigences matérielles minimales suivantes.

Résolution	Fréquence d'images	CPU	Mémoire requise
320 x 240	15 ips	2 cœurs, 1 800 MHz	105 Mo
640 x 480	15 ips	2 cœurs, 2 700 MHz	150 Mo
1 280 x 720	15 ips	4 cœurs, 3 400 MHz	210 Mo

- Horizon Client requiert les bibliothèques suivantes :
  - `Video4Linux2`
  - `libv4l`
  - `Pulse Audio`

  Le fichier plug-in (`/usr/lib/pcoip/vchan_plugins/libviewMMDevRedir.so`) présente les contraintes suivantes :

  ```
  libuuid.so.1
  libv4l2.so.0
  libspeex.so.1
  libudev0
  libtheoradec.so.1
  libtheoraenc.so.1
  libv4lconvert.so.0
  libjpeg.so.8
  ```

  Tous ces fichiers doivent se trouver sur le système client, sinon la fonction Audio/Vidéo en temps réel n'est pas opérationnelle. Ces contraintes s'ajoutent aux exigences requises par Horizon Client lui-même.
- Les pilotes des webcams et des périphériques audio doivent être installés, et la webcam ainsi que le périphérique audio doivent être opérationnels sur l'ordinateur client. Pour utiliser l'Audio/Vidéo en temps réel, vous n'avez pas à installer les pilotes des périphériques sur le système d'exploitation du poste de travail où l'agent est installé.

Protocole d'affichage pour View

- PCoIP
- VMware Blast (requiert Horizon Agent 7.0 ou version ultérieure)

L'Audio/Vidéo en temps réel n'est pas pris en charge par les sessions postes de travail RDP.

Configuration requise pour la redirection multimédia (MMR)

La redirection multimédia (MMR) permet de traiter le flux multimédia, c'est-à-dire de le décoder. Le système client effectue la lecture du contenu multimédia, réduisant ainsi la charge sur l'hôte ESXi.

Poste de travail distant View

- View Agent 6.0.2 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure, doit être installé sur les postes de travail mono-utilisateur.
- View Agent 6.1.1 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure, doit être installé sur l'hôte RDS des postes de travail basés sur des sessions.
- Pour plus d'informations sur les exigences de système d'exploitation, les exigences logicielles et les paramètres de configuration de l'application ou du poste de travail distant, consultez les rubriques sur la Redirection multimédia Windows Media dans *Configuration de pools de postes de travail et d'applications dans View* .

Ordinateur Horizon Client ou périphérique d'accès client

Comme MMR décharge le traitement multimédia depuis le serveur vers le client, le client présente les exigences matérielles minimales suivantes.

Processeur :	Intel Pentium 4 ou AMD Athlon à deux cœurs
Vitesse du processeur :	1,5 GHz pour une utilisation normale ou 1,8 GHz pour Full HD
Mémoire :	2 Go de RAM
Adaptateur vidéo :	Matériel accéléré

Pour éviter les problèmes de lecture de vidéos, vous devez installer l'une des bibliothèques suivantes :

- Bibliothèque principale GStreamer et gstreamer-ffmpeg 0.10
- Bibliothèque principale GStreamer et Fluendo 0.10

Sur SLED 11 SP4, si vous rencontrez des problèmes de lecture de vidéos tels qu'un écran noir, supprimez la bibliothèque libvdpau.

Sur les clients légers HP, vous devez supprimer le fichier `/usr/lib/gstreamer-0.10/libgstfluvadec.so` pour éviter les problèmes de lecture de vidéos tels qu'un incident de Horizon Client ou un écran noir.

Sur les clients légers Dell Wyse, il se peut que la lecture de vidéos ne fonctionne pas avec la bibliothèque Fluendo préinstallée. Pour résoudre le problème, contactez le support Dell pour obtenir la dernière version de la bibliothèque Fluendo.

Formats multimédias pris en charge

Les formats multimédia pris en charge sont ceux que prend en charge Lecteur Windows Media. Par exemple : M4V ; MOV ; MP4 ; WMP ; MPEG-4 Part 2 ; WMV 7, 8 et 9 ; WMA ; AVI ; ACE ; MP3 ; WAV.

Remarque Le contenu protégé par DRM n'est pas redirigé via la Redirection multimédia du Lecteur Windows Media.

MMR n'est pas activé par défaut. Pour l'activer, vous devez configurer l'option de configuration `view.enableMMR`. Pour plus d'informations, reportez-vous à la section « Paramètres de configuration et options de ligne de commande d'Horizon Client », page 29.

Conditions d'utilisation de la redirection d'URL flash

La diffusion de contenus Flash directement à partir d''Adobe Media Server vers les points de terminaison client soulage l'hôte ESXi du datacenter, supprime les routages supplémentaires via le datacenter et réduit la bande passante nécessaire pour écouter simultanément des événements vidéo en direct sur plusieurs points de terminaison client.

La fonctionnalité de redirection d'URL Flash utilise un JavaScript incorporé dans le HTML d'une page Web par l'administrateur de celle-ci. Chaque fois qu'un utilisateur de poste de travail virtuel clique sur le lien de l''URL désigné à partir d'une page Web, JavaScript intercepte et redirige le fichier ShockWave (SWF) à partir de la session du poste de travail virtuel au point de terminaison client. Le point de terminaison ouvre alors un projecteur VMware Flash local à l'extérieur de la session de poste de travail virtuel et lance la lecture du flux multimédia en local. La multidiffusion ou la monodiffusion sont prises en charge.

Cette fonctionnalité est disponible lorsqu'elle est utilisée avec la version correcte du logiciel agent. Pour View 5.3, cette fonctionnalité est incluse dans Remote Experience Agent, qui fait partie du pack de fonctionnalités View. Pour View 6.0 et versions ultérieures, cette fonctionnalité est incluse dans View Agent ou Horizon Agent.

Pour utiliser cette fonctionnalité, vous devez configurer votre page Web et vos périphériques client. Les systèmes client doivent satisfaire certaines exigences matérielles et logicielles :

- Cette fonctionnalité est prise en charge uniquement pour PCoIP. Cette fonctionnalité n'est pas prise en charge par les processeurs ARM.
- Les systèmes client doivent avoir une connectivité IP au serveur Web d'Adobe hébergeant le fichier Shockwave (SWF) qui initie les flux de multidiffusion ou de monodiffusion. Si nécessaire, configurez votre pare-feu pour ouvrir les ports appropriés afin de permettre aux périphériques client d'accéder à ce serveur.
- Les systèmes client doivent avoir le plug-in Flash approprié installé.
  a Installez le fichier `libexpat.so.1`, ou assurez-vous que ce fichier est déjà installé.

    Vérifiez que le fichier est installé dans le répertoire `/usr/lib` ou `/usr/local/lib`.

  b Installez le fichier `libflashplayer.so`, ou assurez-vous que ce fichier est déjà installé.

    Assurez-vous que le fichier est installé dans le répertoire du plug-in Flash approprié de votre système d'exploitation Linux.

  c Installez le programme `wget`, ou assurez-vous que le fichier de ce programme est déjà installé.
- `libffi.so.5` est requis sur Ubuntu 14.04 pour que la redirection d'URL Flash fonctionne, mais Ubuntu 14.04 ne contient que `libffi.so.6` par défaut. Vous pouvez résoudre cette limite en créant un lien symbolique entre `libffi.so.6` et `libffi.so.5`.

Pour consulter la liste des exigences qu'un poste de travail distant doit satisfaire pour la redirection d'URL Flash, et pour obtenir des instructions sur la configuration d'une page Web afin qu'elle fournisse un flux de multidiffusion ou de monodiffusion, reportez-vous à la documentation View.

Exigences de l'authentification par carte à puce

Les systèmes client qui utilisent une carte à puce pour l'authentification utilisateur doivent satisfaire certaines exigences.

Chaque système client qui utilise une carte à puce pour l'authentification utilisateur doit avoir les logiciels et matériels suivants :

- Horizon Client
- Un lecteur de carte à puce compatible
- Des pilotes d'application spécifiques du produit

Vous devez également installer des pilotes d'application spécifiques du produit sur les postes de travail distants ou l'hôte RDS Microsoft.

Les utilisateurs qui s'authentifient avec des cartes à puce doivent posséder une carte à puce et chaque carte à puce doit contenir un certificat utilisateur.

Outre le respect de ces exigences pour les systèmes Horizon Client, les autres composants d'View doivent également respecter certaines exigences de configuration pour prendre en charge les cartes à puce :

- Pour plus d'informations sur la configuration du Serveur de connexion pour prendre en charge l'utilisation des cartes à puce, consultez la section « Configuration de l'authentification par carte à puce » du document *Administration de View*.

  Vous devez ajouter tous les certificats d'autorité de certification applicables pour tous les certificats d'utilisateur de confiance à un fichier de magasin d'approbations de serveur sur l'hôte du Serveur de connexion ou du serveur de sécurité. Ces certificats incluent des certificats racines et doivent inclure des certificats intermédiaires si le certificat de carte à puce de l'utilisateur a été délivré par une autorité de certification intermédiaire.
- Pour plus d'informations sur les tâches que vous pouvez effectuer dans Active Directory afin d'implémenter l'authentification par carte à puce, consultez la section « Configuration de l'authentification par carte à puce » du document *Administration de View*.

Activation du champ Aide-mémoire du nom d'utilisateur dans Horizon Client

Dans certains environnements, les utilisateurs de carte à puce peuvent utiliser un seul certificat de carte à puce pour s'authentifier sur plusieurs comptes d'utilisateur. Les utilisateurs entrent leur nom d'utilisateur dans le champ **Aide-mémoire du nom d'utilisateur** lors de la connexion par carte à puce.

Pour que le champ **Aide-mémoire du nom d'utilisateur** apparaisse dans la boîte de dialogue de connexion d'Horizon Client, vous devez activer la fonctionnalité d'aide-mémoire du nom d'utilisateur de carte à puce pour l'instance du Serveur de connexion dans View Administrator. La fonctionnalité d'aide-mémoire du nom d'utilisateur de carte à puce n'est prise en charge qu'avec les serveurs et les agents Horizon 7 version 7.0.2 et versions ultérieures. Pour plus d'informations sur l'activation de la fonctionnalité d'aide-mémoire du nom d'utilisateur de carte à puce, consultez la section « Configuration de l'authentification par carte à puce » du document *Administration de View*.

Si votre environnement utilise un dispositif Access Point plutôt qu'un serveur de sécurité pour sécuriser l'accès externe, vous devez configurer le dispositif Access Point pour qu'il prenne en charge la fonctionnalité d'aide-mémoire du nom d'utilisateur de carte à puce. La fonctionnalité d'aide-mémoire du nom d'utilisateur de carte à puce n'est prise en charge qu'avec Access Point 2.7.2 et versions ultérieures. Pour plus d'informations sur l'activation de la fonctionnalité d'aide-mémoire du nom d'utilisateur de carte à puce dans Access Point, consultez le document *Déploiement et configuration d'Access Point*.

Remarque Horizon Client prend toujours en charge les certificats de carte à puce de compte unique lorsque la fonctionnalité d'aide-mémoire du nom d'utilisateur de carte à puce est activée.

Configurer Horizon Client pour l'authentification par carte à puce

Vous devez exécuter certaines étapes de configuration pour utiliser une carte à puce dans Horizon Client.

Prérequis

- Installez Horizon Client.
- (Facultatif) Pour que le champ **Aide-mémoire du nom d'utilisateur** apparaisse dans la boîte de dialogue de connexion d'Horizon Client, activez la fonctionnalité Aide-mémoire du nom d'utilisateur de carte à puce dans le Serveur de connexion. Pour plus d'informations, consultez la section « Configuration de l'authentification par carte à puce » du document *Administration de View*.

Procédure

1 Créez le dossier `/usr/lib/vmware/view/pkcs11`.

2 Créez un lien symbolique vers la bibliothèque pkcs11 qui est utilisée pour l'authentification par carte à puce.

Par exemple, exécutez la commande suivante :

```
sudo ln –s /usr/lib/pkcs11/libgtop11dotnet.so
                /usr/lib/vmware/view/pkcs11
```

Systèmes d'exploitation de poste de travail pris en charge

Les administrateurs créent des machines virtuelles avec un système d'exploitation invité et installent le logiciel agent sur le système d'exploitation invité. Les utilisateurs finaux peuvent ouvrir une session sur ces machines virtuelles à partir d'un périphérique client.

Pour obtenir une liste des systèmes d'exploitation invités Windows pris en charge, reportez-vous à la rubrique « Systèmes d'exploitation pris en charge pour View Agent » dans la documentation d'installation de View 5.x ou 6.x. Consultez la rubrique « Systèmes d'exploitation pris en charge pour Horizon Agent » dans la documentation d'installation d'Horizon 7.

Certains systèmes d'exploitation invités Linux sont également pris en charge si vous possédez View Agent 6.1.1 ou version ultérieure ou Horizon Agent 7.0 ou version ultérieure. Pour plus d'informations sur la configuration requise, la configuration de machines virtuelles Linux pour une utilisation dans Horizon 6 ou Horizon 7, et une liste des fonctionnalités prises en charge, consultez *Configuration de postes de travail Horizon 6 for Linux*, qui fait partie de la documentation d'Horizon 6, version 6.1, ou consultez *Configuration de postes de travail Horizon 7 for Linux*.

Préparation du Serveur de connexion pour Horizon Client

Les administrateurs doivent effectuer des tâches spécifiques pour permettre aux utilisateurs finaux de se connecter à des applications ou des postes de travail distants.

Pour que les utilisateurs finaux puissent se connecter au Serveur de connexion ou à un serveur de sécurité et accéder à une application ou à un poste de travail distant, vous devez configurer un certain nombre de paramètres de pool et de sécurité :

- Si vous prévoyez d'utiliser Access Point, configurez le Serveur de connexion pour qu'il fonctionne avec Access Point. Reportez-vous à *Déploiement et configuration d'Access Point*. Les dispositifs Access Point remplissent le même rôle que celui précédemment joué uniquement par des serveurs de sécurité.
- Si vous utilisez un serveur de sécurité, assurez-vous de disposer des dernières versions de maintenance du Serveur de connexion 5.3.x et du Serveur de sécurité 5.3.x ou versions ultérieures. Pour plus d'informations, reportez-vous au document *Installation de View*.

- Si vous prévoyez d'utiliser une connexion tunnel sécurisée pour des périphériques client et si la connexion sécurisée est configurée avec un nom d'hôte DNS pour le Serveur de connexion ou un serveur de sécurité, vérifiez que le périphérique client peut résoudre ce nom DNS.

  Pour activer ou désactiver le tunnel sécurisé, dans View Administrator, allez à la boîte de dialogue Modifier les paramètres du Serveur de connexion View et cochez la case **Utiliser une connexion tunnel sécurisée vers le poste de travail**.

- Vérifiez qu'un pool de postes de travail ou d'applications a été créé et que le compte d'utilisateur que vous souhaitez utiliser est autorisé à accéder au pool.

  Pour le Serveur de connexion 5.3.x, consultez les rubriques sur la création de pools de postes de travail dans le document *Administration de View*. Pour le Serveur de connexion 6.0 et versions ultérieures, consultez les rubriques sur la création de pools de postes de travail et d'applications dans le document *Configuration de pools de postes de travail et d'applications dans View* .

- Pour pouvoir utiliser une authentification à deux facteurs, telle que l'authentification RSA SecurID ou RADIUS, avec Horizon Client, vous devez activer cette fonctionnalité sur le Serveur de connexion. Pour plus d'informations, consultez les rubriques concernant l'authentification à deux facteurs dans le document *Administration de View*.

Options d'installation

Au cours du processus d'installation d'Horizon Client, vous êtes invité à confirmer l'installation de plusieurs composants. Tous les composants sont inclus dans l'installation par défaut.

Le tableau suivant fournit un résumé de chaque composant optionnel.

Tableau 1-1. Options d'installation d' Horizon Client pour Linux

Option	Description
Redirection USB	Donne aux utilisateurs un accès à des périphériques USB connectés en local sur leurs postes de travail. La fonctionnalité Redirection USB est prise en charge sur les postes de travail distants qui sont déployés sur des machines mono-utilisateur. Les fichiers du composant sont installés dans `/usr/lib/vmware/view/usb/`. Les services `vmware-usbarbitrator` et `vmware-view-usbd` s'exécutent automatiquement si vous autorisez le programme d'installation à enregistrer et à démarrer les services installés après l'installation. Sinon, vous pouvez démarrer manuellement les deux services en exécutant `vmware-usbarbitrator` et `vmware-view-usbd` sous `/usr/lib/vmware/view/usb/`. **Remarque** Vous pouvez utiliser les paramètres de stratégie de groupe pour désactiver une redirection USB pour des utilisateurs spécifiques.
Audio/Vidéo en temps réel	Permet de rediriger la webcam et les périphériques audio connectés au système client pour qu'ils puissent être utilisés sur le poste de travail distant. Le fichier du composant est installé dans `/usr/lib/pcoip/vchan_plugins/`.
Impression virtuelle	Permet aux utilisateurs d'imprimer sur n'importe quelle imprimante disponible sur leurs ordinateurs clients. Les utilisateurs n'ont pas à installer des pilotes supplémentaires sur leurs postes de travail distants. Les fichiers du composant sont installés dans `/usr/lib/vmware/view/virtualPrinting/`. Après avoir installé le client, vous n'avez pas à configurer manuellement cette fonctionnalité si vous autorisez le programme d'installation à enregistrer et à démarrer les services installés après l'installation. Sinon, vous pouvez configurer et activer cette fonctionnalité en suivant les instructions dans « Activer la fonctionnalité d'impression virtuelle sur un client Linux », page 19. Dans Horizon 6.0.2 et versions ultérieures, l'impression virtuelle est prise en charge sur les applications et les postes de travail distants suivants : ■ Postes de travail qui sont déployés sur des machines mono-utilisateur. ■ Postes de travail qui sont déployés sur des hôtes RDS, où les hôtes RDS sont des machines virtuelles. ■ Applications distantes qui sont fournies par les hôtes RDS. ■ Applications distantes qui sont lancées à partir d'Horizon Client sur des postes de travail distants (sessions imbriquées).

Tableau 1-1. Options d'installation d' Horizon Client pour Linux (suite)

Option	Description
Redirection multimédia (MMR)	Redirige le flux multimédia depuis le poste de travail vers la machine cliente, où le flux est traité. Le fichier du composant est installé dans `/usr/lib/vmware/view/vdpService/`.
Carte à puce	Permet aux utilisateurs de s'authentifier avec des cartes à puce lorsqu'ils utilisent le protocole d'affichage VMware Blast ou PCoIP. Même si cette option est sélectionnée par défaut dans le programme d'installation du client, elle ne l'est pas lorsque vous exécutez le programme d'installation de View Agent sur le poste de travail à distance. La carte à puce est prise en charge sur les postes de travail distants qui sont déployés sur des machines mono-utilisateur et sur les hôtes RDS. Pour la prise en charge de la carte à puce sur les hôtes RDS, vous devez posséder View Agent 6.1.1 ou version ultérieure. Les fichiers du composant sont installés dans `/usr/lib/pcoip/vchan_plugins/`.
Redirection de lecteur client	Permet aux utilisateurs de partager des dossiers et des lecteurs sur l'ordinateur client avec des applications et des postes de travail distants. Les lecteurs peuvent comporter des lecteurs montés et des périphériques de stockage USB. Les fichiers du composant sont installés dans `/usr/lib/vmware/view/vdpService/`.

Installer ou mettre à niveau Horizon Client pour Linux depuis les téléchargements de produits VMware

Vous pouvez télécharger et exécuter un bundle de programmes d'installation Horizon Client depuis la page de téléchargement de produits VMware. Ce programme d'installation contient les modules pour les fonctionnalités telles que la redirection USB, l'impression virtuelle, l'Audio/Vidéo en temps réel, la carte à puce et la redirection du lecteur client.

Remarque Sur la plupart des distributions Linux, le bundle de programmes d'installation de Horizon Client lance un assistant sous forme d'interface graphique utilisateur. Sur les distributions Linux de SUSE, le bundle de programmes d'installation lance un assistant par ligne de commande. Vous pouvez également exécuter le programme d'installation avec l'option `--console` pour lancer l'assistant par ligne de commande.

Prérequis

- Vérifiez que le système client exécute un système d'exploitation pris en charge. Reportez-vous à la section « Configuration système requise pour les systèmes clients Linux », page 8.
- Familiarisez-vous avec les options d'installation. Reportez-vous à la section « Options d'installation », page 15.
- Vérifiez que vous disposez d'un accès racine au système hôte.
- Vérifiez que VMware Workstation n'est pas installé sur le système client.
- Si vous prévoyez d'utiliser le protocole d'affichage RDP pour vous connecter à un poste de travail View, vérifiez que le client RDP approprié est installé. Reportez-vous à la section « Configuration système requise pour les systèmes clients Linux », page 8.
- Désinstallez toute version antérieure du logiciel Horizon Client. Reportez-vous à la section « Désinstaller Horizon Client pour Linux », page 78.
- Si vous prévoyez d'utiliser le programme d'installation à partir de la ligne de commande, familiarisez-vous avec les options d'installation à partir de la ligne de commande Linux. Reportez-vous à la section « Options d'installation à partir de la ligne de commande du client Linux », page 18.
- Sur les distributions SUSE Linux, exécutez `sudo zypper install python-curses` pour installer la bibliothèque `curses`.

Au cours du processus d'installation, le programme d'installation exécute une analyse des bibliothèques système afin de déterminer si le système est compatible avec Horizon Client ; vous avez toutefois la possibilité d'ignorer cette analyse.

Procédure

1 Sur le système client Linux, téléchargez le fichier du programme d'installation Horizon Clientdepuis la page de téléchargement de produits Horizon Client à l'adresse http://www.vmware.com/go/viewclients.

Le nom du fichier est `VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle`, où *x.x.x* est le numéro de version, *yyyyyyy* est le numéro de build et *arch* est `x86` ou `x64`.

2 Ouvrez une fenêtre Terminal, remplacez le répertoire par celui qui contient le fichier d'installation et exécutez le programme d'installation avec la commande appropriée.

Option	vdmadmin
Pour l'assistant sous forme d'interface graphique utilisateur, si vous avez défini des autorisations exécutables	`sudo ./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle`
Pour l'assistant sous forme d'interface graphique utilisateur, si vous n'avez pas défini des autorisations exécutables	`sudo sh ./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle`
Pour le programme d'installation par ligne de commande	`sudo ./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle --console`

L'assistant du programme d'installation s'affiche et vous invite à accepter le contrat de licence utilisateur final.

3 Suivez les invites pour terminer l'installation.

Important Vous êtes invité à autoriser le programme d'installation à enregistrer et à démarrer les services installés après l'installation. Autoriser le programme d'installation à effectuer ces tâches signifie que vous n'avez pas à démarrer manuellement les services de redirection USB chaque fois que vous redémarrez, et vous n'avez plus à activer manuellement la fonction d'impression virtuelle.

4 Une fois l'installation terminée, indiquez si vous souhaitez exécuter l'analyse des bibliothèques dont dépendent plusieurs composants de la fonctionnalité.

L'analyse système affiche une valeur de résultat de compatibilité pour chaque bibliothèque.

Valeur de résultat	Description
Opération réussie	Toutes les bibliothèques requises ont été trouvées.
Échec	La bibliothèque spécifiée est introuvable.

Les informations de journalisation relatives à l'installation sont enregistrées dans `/tmp/vmware-root/vmware-installer-pid.log`.

Suivant

Démarrez Horizon Client et vérifiez que vous pouvez vous connecter au poste de travail virtuel correct. Reportez-vous à la section « Connexion à une application ou un poste de travail distant », page 51.

Options d'installation à partir de la ligne de commande du client Linux

Vous pouvez utiliser les options d'installation de ligne de commande pour installer Horizon Client sur un système Linux.

Installez Horizon Client de manière silencieuse à l'aide de l'option `--console` en conjonction avec d'autres options de ligne de commande et des paramètres de variables d'environnement. Avec l'installation silencieuse, vous pouvez déployer efficacement des composants View dans une grande entreprise.

Le tableau suivant répertorie les options que vous pouvez utiliser lorsque vous exécutez le fichier du programme d'installation `VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle`.

Tableau 1-2. Options d'installation de ligne de commande Linux

Option	Description
`--help`	Affiche des informations sur l'utilisation.
`--console`	Vous permet d'utiliser le programme d'installation de ligne de commande dans une fenêtre de terminal.
`--custom`	Affiche toutes les questions relatives à l'installation, même si les réponses par défaut ont été scriptées, par exemple à l'aide des options `--set-setting`. L'option par défaut est `--regular`, ce qui signifie que seules les questions pour lesquelles il n'existe pas de réponse par défaut s'affichent.
`--eulas-agreed`	Accepte le contrat de licence d'utilisateur final VMware.
`--gtk`	Ouvre le programme d'installation de VMware basé sur l'interface graphique, ce qui est l'option par défaut. Si l'interface graphique ne peut pas s'afficher ou se charger pour quelque raison que ce soit, le mode console est utilisé.
`--ignore-errors` ou `-I`	Permet à l'installation de se poursuivre, même si une erreur se produit dans un des scripts du programme d'installation. Cependant, comme la partie contenant une erreur ne s'effectue pas, il est possible que le composant ne soit pas configuré correctement.
`--regular`	Affiche les questions relatives à l'installation qui n'ont pas encore reçu de réponse ou qui sont requises. Il s'agit de l'option par défaut.
`--required`	Affiche l'invite de contrat de licence uniquement, puis poursuit l'installation du client. L'option par défaut est `--regular`, ce qui signifie que seules les questions pour lesquelles il n'existe pas de réponse par défaut s'affichent.
`--set-setting vmware-horizon-smartcard smartcardEnable yes`	Installe le composant de carte à puce.
`--set-setting vmware-horizon-rtav rtavEnable yes`	Installe le composant Audio/Vidéo en temps réel.
`--set-setting vmware-horizon-usb usbEnable yes`	Installe la fonctionnalité de redirection USB.
`--set-setting vmware-horizon-virtual-printing tpEnable yes`	Installe la fonctionnalité d'impression virtuelle.
`--set-setting vmware-horizon-tsdr tsdrEnable yes`	Installe la fonctionnalité de redirection du lecteur client.
`--set-setting vmware-horizon-mmr mmrEnable yes`	Installe la fonctionnalité de redirection multimédia (MMR).
`--stop-services`	N'enregistrez pas et ne démarrez pas les services installés.

Outre les options répertoriées dans le tableau, vous pouvez définir les variables d'environnement suivantes.

Tableau 1-3. Paramètres d'installation des variables d'environnement Linux

Variable	Description
`TERM=dumb`	Affiche une interface utilisateur texte très basique.
`VMWARE_EULAS_AGREED=yes`	Vous permet d'accepter les CLUF des produits de manière silencieuse.
`VMIS_LOG_LEVEL=`*value*	Remplacez *value* par l'une des valeurs suivantes : ■ `NOTSET` ■ `DEBUG` ■ `INFO` ■ `WARNING` ■ `ERROR` ■ `CRITICAL` Les informations de journalisation sont enregistrées dans `/tmp/vmware-root/vmware-installer-`*`pid`*`.log`.

Exemple : Commandes d'installation silencieuse

L'exemple ci-dessous explique comment installer Horizon Client de manière silencieuse et spécifie si chaque composant doit être installé ou non.

```
sudo env TERM=dumb VMWARE_EULAS_AGREED=yes \

./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle --console \

--set-setting vmware-horizon-usb usbEnable no \

--set-setting vmware-horizon-virtual-printing tpEnable yes \

--set-setting vmware-horizon-smartcard smartcardEnable no\

--set-setting vmware-horizon-rtav rtavEnable yes \

--set-setting vmware-horizon-tsdr tsdrEnable yes
```

L'exemple suivant montre comment effectuer une installation silencieuse d'Horizon Client avec les paramètres par défaut.

```
sudo env TERM=dumb VMWARE_EULAS_AGREED=yes \
./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle --console --required
```

Activer la fonctionnalité d'impression virtuelle sur un client Linux

Le bundle de programmes d'installation d'Horizon Client 3.2 et versions ultérieures inclut un composant d'impression virtuelle. Si vous possédez Horizon Client 3.2, vous devez créer un fichier de configuration et définir des variables d'environnement pour activer la fonction.

La fonction d'impression virtuelle permet aux utilisateurs finaux d'utiliser des imprimantes locales ou réseau à partir d'un poste de travail distant sans avoir à installer de pilotes d'imprimante supplémentaires sur ce dernier.

Important En général, il n'est pas nécessaire d'exécuter cette procédure si vous possédez Horizon Client 3.4 ou version ultérieure, car vous pouvez spécifier pendant l'installation du client que le programme d'installation doit enregistrer et démarrer les services installés après l'installation. Lorsque l'utilisateur lance le client, un fichier de configuration est automatiquement créé et placé dans le répertoire `home` de l'utilisateur.

Prérequis

Vous devez utiliser le bundle du programme d'installation fourni par VMware pour installer Horizon Client 3.2 ou version ultérieure. Le composant d'impression virtuelle est ensuite installé par défaut.

Procédure

1 Ouvrez une fenêtre de terminal et entrez une commande pour créer un dossier nommé `.thnuclnt` dans le répertoire `home`.

```
$ mkdir ~/.thnuclnt/
```

Remarque Comme ce fichier est créé dans le répertoire de base d'un utilisateur spécifique, le fichier doit être créé pour chaque utilisateur qui utilise le système client Linux.

2 À l'aide d'un éditeur de texte, créez un fichier de configuration appelé `thnuclnt.conf` dans le dossier `~/.thnuclnt`, puis ajoutez-y le texte suivant :

```
autoupdate = 15
automap = true
autoid = 0
updatecount = 1
editcount = 0

connector svc {
   protocol = listen
   interface = /home/user/.thnuclnt/svc
   setdefault = true
}
```

Dans ce texte, remplacez la variable *user* par le nom de l'utilisateur.

3 Enregistrez et fermez le fichier.

4 Entrez une commande qui démarre le processus `thnuclnt`.

```
$ thnuclnt –fg
```

5 Entrez les commandes appropriées afin de définir les variables d'environnement pour les composants d'impression virtuelle.

```
$ export TPCLIENTADDR=/home/user/.thnuclnt/svc
$ export THNURDPIMG=/usr/bin/thnurdp
```

6 Pour lancer Horizon Client, démarrez le processus `vmware-view`.

Désormais, les imprimantes qui s'affichent normalement sur le client sont également redirigées. Elles s'affichent alors dans les boîtes de dialogue d'impression sur votre poste de travail distant.

7 (Facultatif) Si à un moment donné vous souhaitez désactiver la fonctionnalité d'impression virtuelle, suivez la procédure ci-dessous :

a Entrez une commande qui interrompt le processus `thnuclnt`.

```
$ killall thnuclnt
```

b Déconnectez-vous du poste de travail distant, puis reconnectez-vous au poste de travail.

Les imprimantes ne sont plus redirigées.

Installer Horizon Client pour Linux depuis le centre logiciel Ubuntu

Si vous utilisez un système Ubuntu, vous pouvez installer le client depuis le centre logiciel Ubuntu comme alternative à l'installation de la version fournie sur le site Web des téléchargements VMware. Si vous utilisez le centre logiciel Ubuntu, installez le client à l'aide de Synaptic Package Manager.

Cette rubrique fournit les instructions permettant d'obtenir le logiciel client du centre logiciel Ubuntu. Vous pouvez également obtenir le logiciel Horizon Client sur le site Web de téléchargement de produits VMware, comme indiqué dans « Installer ou mettre à niveau Horizon Client pour Linux depuis les téléchargements de produits VMware », page 16.

Important Les clients qui utilisent des clients légers basés sur Linux doivent contacter le fournisseur de leur client léger pour les mises à jour d'Horizon Client. Les clients qui ont correctement créé leurs propres points de terminaison basés sur Linux et mis à jour le client doivent contacter leur représentant commercial VMware.

Prérequis

- Vérifiez que le système client utilise un système d'exploitation pris en charge. Reportez-vous à la section « Configuration système requise pour les systèmes clients Linux », page 8.
- Vérifiez que la version correcte d'OpenSSL est installée. Reportez-vous à la section « Configuration système requise pour les systèmes clients Linux », page 8.
- Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur le système client.
- Si vous prévoyez d'utiliser le protocole d'affichage RDP pour vous connecter à un poste de travail View, vérifiez que le client RDP approprié est installé. Reportez-vous à la section « Configuration système requise pour les systèmes clients Linux », page 8.
- Désinstallez toute version de View Client 1.x ou 2.x. Consultez « Désinstaller Horizon Client pour Linux », page 78.

Procédure

1 Sur votre ordinateur portable ou de bureau Linux, activez Partenaires Canonical.

   a Dans la barre de menu Ubuntu, sélectionnez **Système > Administration > Update Manager**.

   b Cliquez sur le bouton **Paramètres** et entrez le mot de passe pour réaliser des tâches administratives.

   c Dans la boîte de dialogue Sources logicielles, cliquez sur l'onglet **Autres logiciels** et cochez la case **Partenaires Canonical** pour sélectionner l'archive des logiciels que Canonical fournit à ses partenaires.

   d Cliquez sur **Fermer** et suivez les instructions pour mettre à jour la liste de packages.

2 Si vous disposez d'Ubuntu 12.04 ou 14.04, téléchargez et installez le package à partir du centre logiciel Ubuntu de la façon suivante.

   a Ouvrez une fenêtre Terminal et entrez la commande permettant d'obtenir de nouveaux packages :

   ```
   sudo apt-get update
   ```

   Les nouveaux packages sont téléchargés et une liste des packages s'affiche dans la fenêtre Terminal.

   b Ouvrez Update Manager, recherchez des mises à jour et installez-les.

c Ouvrez le centre logiciel Ubuntu et recherchez **vmware-view-client**.

d Installez l'application vmware-view-client.

Si vous utilisez le système d'exploitation Ubuntu 12.04 ou 14.04, la version la plus récente d'Horizon Client est installée.

Une icône d'application pour **VMware Horizon Client** s'affiche dans le lanceur d'application.

Suivant

Démarrez Horizon Client et vérifiez que vous pouvez vous connecter au poste de travail virtuel correct. Reportez-vous à la section « Connexion à une application ou un poste de travail distant », page 51.

Configurer des options VMware Blast

Vous pouvez configurer des options de décodage H.264 et de protocole réseau pour des sessions d'application et de poste de travail distant qui utilisent le protocole d'affichage VMware Blast.

La résolution maximale prise en charge dépend de la capacité du processeur graphique (GPU) sur le client. Un processeur graphique prenant en charge une résolution 4K pour JPEG/PNG peut ne pas prendre en charge une résolution 4K pour H.264. Si une résolution pour H.264 n'est pas prise en charge, Horizon Client utilise JPEG/PNG à la place.

Le décodage H.264 est pris en charge sur les processeurs graphiques AMD, NVIDIA et Intel. Pour les processeurs graphiques AMD et NVIDIA, le décodage H.264 requiert que la bibliothèque graphique OpenGL 3.2 ou version ultérieure soit installée.

Si vous prévoyez d'utiliser le décodage H.264 avec un processeur NVIDIA, installez VDPAU (Video Decode and Presentation API for Unix). VDPAU n'est plus inclus avec le dernier pilote NVIDIA et il doit être installé séparément.

Pour utiliser le décodage H.264 avec un processeur graphique Intel, le pilote VA-API d'Intel et les bibliothèques VA-API de GLX sont nécessaires. L'exécution de la commande `vainfo` affiche les profils H.264. Si la version du pilote VA-API est la version 1.2.x ou antérieure, vous devez ajouter l'entrée `mks.enableGLBasicRenderer = TRUE` à `/etc/vmware/config`, `/usr/lib/vmware/config` ou `~/.vmware/config`. Les fichiers de configuration sont traités dans l'ordre suivant :

1 `/etc/vmware/config`

2 `/usr/lib/vmware/config`

3 `~/.vmware/config`

Avec Red Hat 7.2, un processeur graphique Intel, une version du pilote Intel 1.2 ou antérieure, OpenGL 3.2 et H.264 activé, vous devez ajouter les entrées suivantes à l'un des trois fichiers de configuration pour éviter des problèmes d'affichage tels qu'un écran noir.

```
mks.enableGLRenderer=FALSE
mks.enableGLBasicRenderer=TRUE
```

H.264 n'est pas pris en charge sur SLED 11 SP4 avec un processeur graphique Intel, car la version de xorg est trop ancienne.

Prérequis

Cette fonctionnalité requiert Horizon Agent 7.0 ou version ultérieure.

Procédure

1 Dans la fenêtre du sélecteur de postes de travail et d'applications, sélectionnez **Connexion > Paramètres** ou cliquez sur l'icône Paramètres en haut à droite de la fenêtre et sélectionnez **VMware Blast** dans le volet gauche de la fenêtre Paramètres.

2 Configurez les options de décodage et de protocole réseau.

Option	Description
H.264	Sélectionnez cette option pour autoriser le décodage H.264 dans Horizon Client. Lorsque cette option est sélectionnée (paramètre par défaut), Horizon Client utilise le décodage H.264 si l'agent prend en charge le codage logiciel H.264. Si l'agent ne prend pas en charge le codage logiciel H.264, Horizon Client utilise le décodage JPG/PNG. Désélectionnez cette option pour utiliser le décodage JPG/PNG.
UDP	Sélectionnez cette option pour autoriser la mise en réseau UDP dans Horizon Client. Lorsque cette option est sélectionnée (paramètre par défaut), Horizon Client utilise la mise en réseau UDP si la connectivité UDP est disponible. Si la mise en réseau UDP est bloquée, Horizon Client utilise la mise en réseau TCP. Désélectionnez cette option pour utiliser la mise en réseau TCP. **Remarque** UDP est désactivé par défaut sur un poste de travail distant Horizon. Pour qu'UDP fonctionne, il doit être activé sur le poste de travail, le client et Blast Secure Gateway (BSG).

Vos modifications seront appliquées la prochaine fois qu'un utilisateur se connecte à une application ou un poste de travail distant et qu'il sélectionne le protocole d'affichage VMware Blast. Vos modifications n'ont pas d'incidence sur les sessions VMware Blast existantes.

Données Horizon Client collectées par VMware

Si votre entreprise participe au programme d'amélioration du produit, VMware collecte des données provenant de certains champs d'Horizon Client. Les champs contenant des informations sensibles restent anonymes.

VMware collecte des données sur les clients afin de hiérarchiser la compatibilité matérielle et logicielle. Si l'administrateur de votre entreprise a choisi de participer au programme d'amélioration du produit, VMware collecte des données anonymes sur votre déploiement afin d'améliorer la réponse de VMware aux exigences des clients. Aucune donnée permettant d'identifier votre organisation n'est collectée. Les informations d'Horizon Client sont envoyées d'abord au Serveur de connexion, puis à VMware, avec des données provenant des instances du Serveur de connexion, des pools de postes de travail et des postes de travail distants.

Bien que les informations soient chiffrées lors de leur transfert au Serveur de connexion, les informations sur le système client sont journalisées non chiffrées dans un répertoire propre à l'utilisateur. Les journaux ne contiennent aucune information d'identification personnelle.

L'administrateur qui installe le Serveur de connexion peut choisir de participer au programme d'amélioration du produit VMware lors de l'exécution de l'assistant d'installation du Serveur de connexion, ou un administrateur peut définir une option dans View Administrator après l'installation.

Tableau 1-4. Données collectées depuis Horizon Client pour le programme d'amélioration du produit

Description	Ce champ reste-t-il anonyme ?	Exemple
Entreprise ayant produit l'application Horizon Client	Non	VMware
Nom du produit	Non	VMware Horizon Client
Version du produit client	Non	(Le format est *x.x.x-yyyyyy*, où *x.x.x* est le numéro de version du client et *yyyyyy* est le numéro de build.)

Tableau 1-4. Données collectées depuis Horizon Client pour le programme d'amélioration du produit (suite)

Description	Ce champ reste-t-il anonyme ?	Exemple
Architecture binaire du client	Non	Exemples : ■ i386 ■ x86_64 ■ arm
Nom du build du client	Non	Exemples : ■ VMware-Horizon-Client-Win32-Windows ■ VMware-Horizon-Client-Linux ■ VMware-Horizon-Client-iOS ■ VMware-Horizon-Client-Mac ■ VMware-Horizon-Client-Android ■ VMware-Horizon-Client-WinStore
Système d'exploitation hôte	Non	Exemples : ■ Windows 8.1 ■ Windows 7, 64 bits Service Pack 1 (Build 7601) ■ iPhone OS 5.1.1 (9B206) ■ Ubuntu 12.04.4 LTS ■ Mac OS X 10.8.5 (12F45)
Noyau du système d'exploitation hôte	Non	Exemples : ■ Windows 6.1.7601 SP1 ■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X ■ Darwin 11.4.2 ■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012 ■ inconnu (pour Windows Store)
Architecture du système d'exploitation hôte	Non	Exemples : ■ x86_64 ■ i386 ■ armv71 ■ ARM
Modèle du système hôte	Non	Exemples : ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision WorkStation T3400 (A04 03/21/2008)
Processeur du système hôte	Non	Exemples : ■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH ■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH ■ inconnu (pour iPad)
Nombre de cœurs dans le processeur du système hôte	Non	Par exemple : 4
Mo de mémoire sur le système hôte	Non	Exemples : ■ 4096 ■ inconnu (pour Windows Store)
Nombre de périphériques USB connectés	Non	2 (la redirection de périphériques USB est prise en charge uniquement pour les clients Linux, Windows et Mac.)
Nombre maximal de connexions de périphériques USB simultanées	Non	2

Tableau 1-4. Données collectées depuis Horizon Client pour le programme d'amélioration du produit (suite)

Description	Ce champ reste-t-il anonyme ?	Exemple
ID de fournisseur de périphériques USB	Non	Exemples : ■ Kingston ■ NEC ■ Nokia ■ Wacom
ID de produit de périphérique USB	Non	Exemples : ■ DataTraveler ■ Gamepad ■ Disque de stockage ■ Souris sans fil
Famille de périphériques USB	Non	Exemples : ■ Sécurité ■ Périphérique d'interface humaine ■ Imagerie
Nombre d'utilisations du périphérique USB	Non	(Nombre de partages du périphérique)

Configuration d' Horizon Client pour les utilisateurs finaux 2

La configuration d'Horizon Client pour les utilisateurs finaux peut impliquer la construction d'URI, la définition du mode de vérification des certificats, la modification d'options TLS/SSL avancées, la configuration de clés spécifiques et de combinaisons de clés, la définition d'options de protocole d'affichage et l'activation du mode FIPS.

Ce chapitre aborde les rubriques suivantes :

Paramètres de configuration communs

Horizon Client offre plusieurs mécanismes de configuration permettant de simplifier les processus de connexion et de sélection d'un poste de travail pour les utilisateurs finaux et de renforcer les stratégies de sécurité.

Le tableau suivant ne présente qu'une partie des paramètres de configuration que vous pouvez définir de plusieurs manières.

Tableau 2-1. Paramètres de configuration communs

Paramètre	Mécanismes de configuration
Adresse du Serveur de connexion View	URI, propriété du fichier de configuration, ligne de commande
Nom d'utilisateur Active Directory	URI, propriété du fichier de configuration, ligne de commande
Nom de domaine	URI, propriété du fichier de configuration, ligne de commande
Nom affiché du poste de travail	URI, propriété du fichier de configuration, ligne de commande
Taille de fenêtre	URI, propriété du fichier de configuration, ligne de commande
Protocole d'affichage	URI, propriété du fichier de configuration, ligne de commande

Tableau 2-1. Paramètres de configuration communs (suite)

Paramètre	Mécanismes de configuration
Configuration de la vérification des certificats	Propriété du fichier de configuration
Configuration des protocoles et des algorithmes de chiffrement SSL	Propriété du fichier de configuration, ligne de commande

Utilisation de l'interface de ligne de commande et des fichiers de configuration d' Horizon Client

Vous pouvez configurer Horizon Client à l'aide d'options de ligne de commande ou de propriétés équivalentes dans un fichier de configuration.

Vous pouvez utiliser l'interface de ligne de commande de `vmware-view` ou définir des propriétés dans des fichiers de configuration pour choisir les valeurs par défaut que vos utilisateurs voient dans Horizon Client ou pour empêcher certaines boîtes de dialogue de demander des informations aux utilisateurs. Vous pouvez également spécifier des paramètres que vous ne voulez pas que les utilisateurs modifient.

Ordre de traitement des paramètres de configuration

Lorsque Horizon Client démarre, des paramètres de configuration sont traités depuis divers emplacements dans l'ordre suivant :

1 `/etc/vmware/view-default-config`

2 `~/.vmware/view-preferences`

3 Arguments de ligne de commande

4 `/etc/vmware/view-mandatory-config`

Si un paramètre est défini dans plusieurs emplacements, la valeur utilisée est la valeur du dernier fichier ou de la dernière option de ligne de commande lu(e). Par exemple, pour spécifier des paramètres qui remplacent les préférences des utilisateurs, définissez des propriétés dans le fichier `/etc/vmware/view-mandatory-config`.

Pour définir des valeurs par défaut que les utilisateurs peuvent modifier, utilisez le fichier `/etc/vmware/view-default-config`. Quand des utilisateurs modifient un paramètre, tous les paramètres modifiés sont enregistrés dans le fichier `~/.vmware/view-preferences` lorsqu'ils quittent Horizon Client.

Propriétés empêchant les utilisateurs de modifier des valeurs par défaut

Pour de nombreuses propriétés, vous pouvez définir une propriété `view.allow` correspondante qui contrôle si les utilisateurs sont autorisés à modifier le paramètre. Par exemple, si vous définissez la propriété `view.allowDefaultBroker` sur « FALSE » dans le fichier `/etc/vmware/view-mandatory-config`, les utilisateurs ne pourront pas modifier le nom du serveur lorsqu'ils se connectent en utilisant Horizon Client.

Syntaxe à utiliser dans l'interface de ligne de commande

Utilisez la forme suivante de la commande `vmware-view` dans une fenêtre de terminal.

`vmware-view [`*`command-line-option`* `[`*`argument`*`]] ...`

Par défaut, la commande `vmware-view` se trouve dans le répertoire `/usr/bin`.

Vous pouvez utiliser la forme abrégée ou la forme longue du nom d'option, même si toutes les options n'ont pas de forme abrégée. Par exemple, pour spécifier le domaine, vous pouvez utiliser `-d` (forme abrégée) ou `--domainName=` (forme longue). Vous pouvez choisir d'utiliser la forme longue pour faire un script plus lisible.

Vous pouvez utiliser l'option `--help` pour obtenir une liste d'options de ligne de commande et des informations sur l'utilisation.

Important Si vous devez utiliser un proxy, appliquez la syntaxe suivante :

`http_proxy=`*`proxy_server_URL:port`* `https_proxy=`*`proxy_server_URL:port`* `vmware-view` *`options`*

Cette solution palliative est nécessaire, car vous devez effacer les variables d'environnement déjà définies pour le proxy. Si vous n'exécutez pas cette action, le paramètre d'exception de proxy est inopérant dans Horizon Client. Vous pouvez configurer une exception de proxy pour l'instance du Serveur de connexion View.

Paramètres de configuration et options de ligne de commande d' Horizon Client

Par souci de commodité, presque tous les paramètres de configuration possèdent une propriété *key=value* et un nom d'option de ligne de commande correspondant. Pour quelques paramètres, il existe une option de ligne de commande mais pas de propriété correspondante que vous pouvez définir dans un fichier de configuration. Pour d'autres paramètres, vous devez définir une propriété car aucune option de ligne de commande n'est disponible.

Important Certaines options de ligne de commande et clés de configurations ne sont disponibles qu'avec la version de Horizon Client fournie par des fournisseurs tiers. Pour plus d'informations sur les partenaires client léger et zéro de VMware, consultez le *Guide de compatibilité VMware* à l'adresse http://www.vmware.com/resources/compatibility/search.php?deviceCategory=vdm.

Tableau 2-2. Options de ligne de commande et clés du fichier de configuration d' Horizon Client

Clé de configuration	Option de ligne de commande	Description
`view.allMonitors`	`--allmonitors`	Masque le système d'exploitation hôte et ouvre l'interface utilisateur de Horizon Client en mode plein écran sur tous les moniteurs connectés lors du démarrage du client. Si vous définissez la clé de configuration, spécifiez **« TRUE »** ou **« FALSE »**. La valeur par défaut est « FALSE ».
`view.allowDefaultBroker`	`-l`, `--lockServer`	L'utilisation de cette option de ligne de commande ou la définition de la propriété sur « FALSE » désactive le champ **Serveur** sauf si le client n'a jamais été connecté à un serveur et si aucune adresse de serveur n'est fournie sur la ligne de commande ou dans le fichier de préférences. Exemple d'utilisation de l'option de ligne de commande : `--lockServer -s view.company.com`

Tableau 2-2. Options de ligne de commande et clés du fichier de configuration d' Horizon Client (suite)

Clé de configuration	Option de ligne de commande	Description
`view.autoConnectBroker`	Aucune	Se connecte automatiquement au dernier serveur View Server utilisé sauf si la propriété de configuration `view.defaultBroker` est définie ou si l'option de ligne de commande `--serverURL=` est utilisée. Spécifiez **« TRUE »** ou **« FALSE »**. La valeur par défaut est « FALSE ». Définir cette propriété et la propriété `view.autoConnectDesktop` sur « TRUE » revient à définir la propriété `view.nonInteractive` sur « TRUE ».
`view.autoConnectDesktop`	Aucune	Se connecte automatiquement au dernier poste de travail View utilisé sauf si la propriété de configuration `view.defaultDesktop` est définie ou si l'option de ligne de commande `--desktopName=` est utilisée. Spécifiez **« TRUE »** ou **« FALSE »**. La valeur par défaut est « FALSE ». Définir cette propriété et la propriété `view.autoConnectBroker` sur « TRUE » revient à définir la propriété `view.nonInteractive` sur « TRUE ».
`view.autoDisconnectEmptyAppSession`	Aucune	Lorsque cette option est définie sur **« TRUE »** (par défaut), si la session d'application devient vide parce que l'utilisateur quitte toutes les applications, l'utilisateur final obtient un message. Ce message invite l'utilisateur à choisir entre la déconnexion de la session vide ou la poursuite de l'exécution de cette session. Lorsque cette option est définie sur **« FALSE »**, la session est fermée conformément au paramètre de délai d'attente utilisé dans View Administrator, qui prévoit par défaut une déconnexion après une minute d'inactivité.
`view.defaultAppHeight`	Aucune	Spécifie la hauteur par défaut de la fenêtre des applications distantes, en pixels. Utilisez cette propriété avec `view.defaultAppWidth` lors de la spécification d'une taille de poste de travail personnalisée (la propriété `view.defaultAppSize` est définie sur « 5 »). La valeur par défaut est « 480 ».
`view.defaultAppSize`	`--appSize=`	Définit la taille par défaut de la fenêtre des applications distantes : ■ Pour utiliser tous les moniteurs, spécifiez **« 1 »**. ■ Pour utiliser le mode plein écran sur un moniteur, spécifiez **« 2 »**. ■ Pour utiliser une grande fenêtre, spécifiez **« 3 »**. ■ Pour utiliser une petite fenêtre, spécifiez **« 4 »**. ■ Pour définir une taille personnalisée, spécifiez **« 5 »**, puis définissez également les propriétés `view.defaultAppWidth` et `view.defaultAppHeight`. La valeur par défaut est « 1 ».
`view.defaultAppWidth`	Aucune	Spécifie la largeur par défaut de la fenêtre pour les applications distantes, en pixels. Utilisez cette propriété avec `view.defaultAppHeight` lors de la spécification d'une taille de poste de travail personnalisée (la propriété `view.defaultAppSize` est définie sur « 5 »). La valeur par défaut est « 640 ».

Tableau 2-2. Options de ligne de commande et clés du fichier de configuration d' Horizon Client (suite)

Clé de configuration	Option de ligne de commande	Description

`view.defaultBroker`	`-s`, `--serverURL=`	Ajoute le nom que vous spécifiez au champ **Serveur** dans Horizon Client. Spécifiez un nom de domaine complet. Vous pouvez également spécifier un numéro de port si vous n'utilisez pas le port par défaut 443.
		Le port par défaut est la dernière valeur utilisée.
		Exemple d'utilisation de l'option de ligne de commande :
		`--serverURL=https://view.company.com`
		`-s view.company.com`
		`--serverURL=view.company.com:1443`

`view.defaultDesktop`	`-n`, `--desktopName=`	Spécifie quel poste de travail utiliser lorsque `autoConnectDesktop` est défini sur « TRUE » et que l'utilisateur a accès à plusieurs postes de travail. Il s'agit du nom que vous voyez dans la boîte de dialogue Sélectionner un poste de travail. En général, le nom est le nom de pool.
`view.defaultDesktopHeight`	Aucune	Spécifie la hauteur par défaut de la fenêtre pour le poste de travail View, en pixels. Utilisez cette propriété avec `view.defaultDesktopWidth` lors de la spécification d'une taille de poste de travail personnalisée (la propriété `view.defaultDesktopSize` est définie sur « 5 »).

`view.defaultDesktopSize`	`--desktopSize=`	Définit la taille par défaut de la fenêtre pour le poste de travail View :
		■ Pour utiliser tous les écrans, définissez la propriété sur **`"1"`** ou utilisez l'argument de ligne de commande **`"all"`**.
		■ Pour utiliser le mode plein écran sur un écran, définissez la propriété sur **`"2"`** ou utilisez l'argument de ligne de commande **`"full"`**.
		■ Pour utiliser une grande fenêtre, définissez la propriété sur **`"3"`** ou utilisez l'argument de ligne de commande **`"large"`**.
		■ Pour utiliser une petite fenêtre, définissez la propriété sur **`"4"`** ou utilisez l'argument de ligne de commande **`"small"`**.
		■ Pour définir une taille personnalisée, définissez la propriété sur **`"5"`** et définissez également les propriétés `view.defaultDesktopWidth` et `view.defaultDesktopHeight`. Vous pouvez également spécifier la largeur par hauteur en pixels, dans la ligne de commande en utilisant le format **`"widthxheight"`**.
		Exemple d'utilisation de l'option de ligne de commande :
		`--desktopSize="1280x800"`
		`--desktopSize="all"`

`view.defaultDesktopWidth`	Aucune	Spécifie la largeur par défaut de la fenêtre pour le poste de travail View, en pixels. Utilisez cette propriété avec `view.defaultDesktopHeight` lors de la spécification d'une taille de poste de travail personnalisée (la propriété `view.defaultDesktopSize` est définie sur « 5 »).

Tableau 2-2. Options de ligne de commande et clés du fichier de configuration d' Horizon Client (suite)

Clé de configuration	Option de ligne de commande	Description
`view.defaultDomain`	`-d`, `--domainName=`	Définit le nom de domaine qu'Horizon Client utilise pour toutes les connexions et ajoute le nom de domaine que vous spécifiez au champ **Nom de domaine** dans la boîte de dialogue d'authentification.
`view.defaultLogLevel`	Aucune	Définit le niveau de journalisation d'Horizon Client. Définit la propriété sur l'une des valeurs suivantes : ■ **« 0 »** signifie inclure tous les événements de journaux. ■ **« 1 »** signifie inclure les événements au niveau de la trace et les événements capturés pour les paramètres 2 à 6. ■ **« 2 »** signifie inclure les événements de débogage et les événements capturés pour les paramètres 3 à 6. ■ **« 3 »** (par défaut) signifie inclure les événements au niveau des informations et les événements capturés pour les paramètres 4 à 6. ■ **« 4 »** signifie inclure les événements d'avertissement, d'erreur et irrécupérables. ■ **« 5 »** signifie inclure les événements d'erreur et irrécupérables. ■ **« 6 »** signifie inclure les événements irrécupérables. La valeur par défaut est « 3 ».
`view.defaultPassword`	`-p "-"`, `--password="-"`	Pour les connexions VMware Blast, PCoIP et `rdesktop`, spécifiez toujours **`"-"`** pour lire le mot de passe à partir de `stdin`. Définit le mot de passe que Horizon Client utilise pour toutes les connexions et ajoute le mot de passe au champ **Mot de passe** dans la boîte de dialogue d'authentification si Serveur de connexion View accepte l'authentification par mot de passe. **Remarque** Vous ne pouvez pas utiliser un mot de passe vide. Cela signifie que vous ne pouvez pas spécifier --password=""
`view.defaultProtocol`	`--protocol=`	Spécifie quel protocole d'affichage utiliser. Spécifiez **`"PCOIP"`** ou **`"RDP"`**. Ces valeurs sont sensibles à la casse. Par exemple, si vous saisissez **`rdp`**, le protocole par défaut est utilisé. La valeur par défaut est le paramètre spécifié dans View Administrator dans les paramètres du pool. Si vous utilisez RDP et que vous voulez utiliser FreeRDP plutôt que `rdesktop`, vous devez également utiliser le paramètre `rdpClient`.
`view.defaultUser`	`-u`, `--userName=`	Définit le nom d'utilisateur qu'Horizon Client utilise pour toutes les connexions et ajoute le nom d'utilisateur que vous spécifiez dans le champ **Nom d'utilisateur** de la boîte de dialogue d'authentification. Pour le mode kiosque, le nom de compte peut être basé sur l'adresse MAC du client, ou il peut commencer par une chaîne de préfixe reconnue, telle que **`custom-`**.
`view.disableMaximizedApp`	`--disableMaximizedApp`	Si cette option est définie sur **« FALSE »** (par défaut), l'application est lancée en mode Plein écran.

Tableau 2-2. Options de ligne de commande et clés du fichier de configuration d' Horizon Client (suite)

Clé de configuration	Option de ligne de commande	Description
`view.enableMMR`	Aucune	Active la redirection multimédia (MMR). Spécifiez **« TRUE »** ou **« FALSE »**. La valeur par défaut est « FALSE ».
`view.fullScreen`	`--fullscreen`	Masque le système d'exploitation hôte et ouvre l'interface utilisateur de Horizon Client en mode plein écran sur un moniteur. Cette option n'affecte pas le mode d'affichage de la session de poste de travail. Si vous définissez la clé de configuration, spécifiez **« TRUE »** ou **« FALSE »**. La valeur par défaut est « FALSE ».

`view.kbdLayout`	`-k`, `--kbdLayout=`	Spécifie quels paramètres régionaux utiliser pour la disposition de clavier.
		Remarque `rdesktop` utilise des codes de paramètres régionaux, tels que **`"fr"`** et **`"de"`**, alors que `freerdp` utilise des ID de disposition de clavier. Pour obtenir une liste de ces ID, utilisez la commande suivante :
		`xfreerdp --kbd-list`
		Exemple d'utilisation de l'option de ligne de commande pour rdesktop :
		`--kbdLayout="en-us"`
		`-k "fr"`
		Exemple d'utilisation de l'option de ligne de commande pour freerdp :
		`-k "0x00010407"`

`view.kioskLogin`	`--kioskLogin`	Spécifie qu'Horizon Client va procéder à l'authentification en utilisant un compte en mode Kiosque. Si vous définissez la clé de configuration, spécifiez **« TRUE »** ou **« FALSE »**. La valeur par défaut est « FALSE ». Pour voir des exemples, reportez-vous à l'exemple de mode Kiosque qui suit ce tableau.
`view.mmrPath`	`-m`, `--mmrPath=`	(Disponible uniquement avec les distributions de fournisseurs tiers) Spécifie le chemin d'accès au répertoire qui contient les bibliothèques Wyse MMR (redirection multimédia). Exemple d'utilisation de l'option de ligne de commande : `--mmrPath="/usr/lib/altmmr"`

Tableau 2-2. Options de ligne de commande et clés du fichier de configuration d' Horizon Client (suite)

Clé de configuration	Option de ligne de commande	Description
`view.monitors`	`--monitors=` *numbered list*	Vous permet de spécifier quels moniteurs adjacents utiliser pour Horizon Client. Utilisez `--allmonitors` (ou `view.allMonitors`) pour indiquer que vous souhaitez utiliser tous les moniteurs en plein écran et utiliser la *liste numérotée* de `--monitors=` pour spécifier quel sous-ensemble de moniteurs sera utilisé. Exemple d'utilisation de ligne de commande pour spécifier le premier et le deuxième écran dans une configuration de trois écrans installés côte à côte. `--allmonitors --monitors="1,2" ` ` Pour aider à distinguer quel moniteur physique est associé à une icône de moniteur dans l'interface utilisateur du client, un rectangle s'affiche dans le coin supérieur gauche du moniteur physique que vous avez choisi d'utiliser. Le rectangle contient la couleur et le numéro correspondants utilisés dans l'icône pour le moniteur choisi.
`view.nomenubar`	`--nomenubar`	Supprime la barre de menus d'Horizon Client lorsque le client est en mode Plein écran, afin que les utilisateurs ne puissent pas accéder aux options de menu pour fermer une session d'un poste de travail View, le réinitialiser ou s'en déconnecter. Utilisez cette option lorsque vous configurez le mode kiosque. Si vous définissez la clé de configuration, spécifiez **« TRUE »** ou **« FALSE »**. La valeur par défaut est « FALSE ».

`view.nonInteractive`	`-q`, `--nonInteractive`	Masque les étapes d'interface utilisateur inutiles pour les utilisateurs finaux en ignorant les écrans spécifiés dans la ligne de commande ou les propriétés de configuration.
		Si vous définissez la clé de configuration, spécifiez **« TRUE »** ou **« FALSE »**. La valeur par défaut est « FALSE ».
		Définir cette propriété sur « TRUE » revient à définir les propriétés `view.autoConnectBroker` et `view.autoConnectDesktop` sur « TRUE ».
		Exemple d'utilisation de l'option de ligne de commande :
		`--nonInteractive`
		`--serverURL="https://view.company.com"`
		`--userName="user1" --password="-"`
		`--domainName="xyz"`
		`--desktopName="Windows 7"`

`view.once`	`--once`	Spécifie que vous ne souhaitez pas qu'Horizon Client retente la connexion en cas d'erreur. En général, vous devez spécifier cette option si vous utilisez le mode kiosque et utiliser le code de sortie pour traiter l'erreur. Sinon, il peut vous sembler difficile de tuer le processus `vmware-view` à distance. Si vous définissez la clé de configuration, spécifiez **« TRUE »** ou **« FALSE »**. La valeur par défaut est « FALSE ».

Tableau 2-2. Options de ligne de commande et clés du fichier de configuration d' Horizon Client (suite)

Clé de configuration	Option de ligne de commande	Description
`view.rdesktopOptions`	`--rdesktopOptions=`	(Disponible si vous utilisez le protocole d'affichage Microsoft RDP) Spécifie des options de ligne de commande à transmettre à l'application rdesktop. Pour plus d'informations sur les options rdesktop, consultez la documentation sur rdesktop. Exemple d'utilisation de l'option de ligne de commande : `--rdesktopOptions="-f -m"`
Aucune	`-r`, `--redirect=`	(Disponible si vous utilisez le protocole d'affichage Microsoft RDP) Spécifie un périphérique local que vous voulez que rdesktop redirige vers le poste de travail View. Spécifiez les informations du périphérique que vous voulez transmettre à l'option `-r` de rdesktop. Vous pouvez définir plusieurs options de périphérique dans une seule commande. Exemple d'utilisation de l'option de ligne de commande : `--redirect="sound:off"`
`view.rdpClient`	`--rdpclient=`	(Disponible si vous utilisez le protocole d'affichage Microsoft RDP) Spécifie quel type de client RDP utiliser. L'option par défaut est `rdesktop`. Pour utiliser FreeRDP à la place, spécifiez `xfreerdp`. **Remarque** Pour utiliser FreeRDP, la version correcte de FreeRDP doit être installée, ainsi que tous les correctifs applicables. Pour plus d'informations, reportez-vous à la section « Installer et configurer FreeRDP », page 47.
Aucune	`--save`	Enregistre le nom d'utilisateur et le nom de domaine utilisés lors de la dernière ouverture de session, ce qui vous évite d'avoir à les ressaisir la prochaine fois que vous les informations d'identification de connexion vous sont demandées.
`view.sendCtrlAltDelToLocal`	Aucune	(Disponible si vous utilisez le protocole d'affichage VMware Blast ou PCoIP) Lorsque cette option est définie sur **« TRUE »**, le système envoie la combinaison de touches Ctrl+Alt+Suppr au système client plutôt que d'ouvrir une boîte de dialogue qui invite l'utilisateur à se déconnecter du poste de travail View. La valeur par défaut est « FALSE ». **Remarque** Si vous utilisez le protocole d'affichage Microsoft RDP, vous pouvez utiliser cette fonctionnalité grâce à l'option `-K`, par exemple, `vmware-view -K`. Cette option a la même priorité que le paramètre du fichier `/etc/vmware/view-keycombos-config`.
`view.sendCtrlAltDelToVM`	Aucune	(Disponible si vous utilisez le protocole d'affichage VMware Blast ou PCoIP) Lorsque cette option est définie sur **« TRUE »**, le système envoie la combinaison de touches Ctrl+Alt+Suppr au poste de travail virtuel plutôt que d'ouvrir une boîte de dialogue qui invite l'utilisateur à se déconnecter du poste de travail View. La valeur par défaut est « FALSE ». Cette option a une priorité plus élevée que le paramètre du fichier `/etc/vmware/view-keycombos-config`.

Tableau 2-2. Options de ligne de commande et clés du fichier de configuration d' Horizon Client (suite)

Clé de configuration	Option de ligne de commande	Description
`view.sendCtrlAltInsToVM`	Aucune	(Disponible si vous utilisez le protocole d'affichage VMware Blast ou PCoIP) Lorsque cette option est définie sur **« TRUE »**, le système envoie la combinaison de touches Ctrl+Alt+ Inser au poste de travail virtuel plutôt que d'envoyer Ctrl+Alt+Suppr. La valeur par défaut est « FALSE ». **Remarque** Pour utiliser cette fonctionnalité, vous devez également définir l'objet stratégie de groupe côté agent appelée « Utiliser une autre touche pour l'envoi de séquence de touches de sécurité », disponible dans le modèle `pcoip.adm`. Reportez-vous à la rubrique intitulée « Variables de session View PCoIP pour le clavier » dans le chapitre « Configuration des stratégies » du document *Configuration de pools de postes de travail et d'applications dans View* . Cette option a une priorité plus faible que le paramètre du fichier `/etc/vmware/view-keycombos-config`.
`view.shareRemovableStorage`	Aucune	Lorsque cette option est définie sur **« TRUE »**, active l'option **Autoriser l'accès au stockage amovible**. La valeur par défaut est « TRUE ».
`view.sslCipherString`	`--sslCipherString=`	Configure la liste de chiffrements pour limiter l'utilisation de certains algorithmes de chiffrement avant l'établissement d'une connexion SSL chiffrée. Pour une liste de chaînes de chiffrement, reportez-vous à http://www.openssl.org/docs/apps/ciphers.html. La chaîne de chiffrement par défaut d'Horizon Client est « !aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES ».
`view.sslProtocolString`	`--sslProtocolString=`	Configure la liste de chiffrements pour limiter l'utilisation de certains protocoles de chiffrement avant l'établissement d'une connexion SSL chiffrée. Les protocoles pris en charge sont SSLv3/SSLv3.0, TLSv1.0/TLSv1, TLSv1.1 et TLSv1.2. La liste de chiffrements est composée d'une ou de plusieurs chaînes de protocole séparées par des deux-points. Les chaînes ne sont pas sensibles à la casse. La valeur par défaut est « TLSv1.0:TLSv1.1:TLSv1.2 ».
`view.sslVerificationMode`	Aucune	Définit le mode de vérification des certificats de serveur. Spécifiez **"1"** pour refuser des connexions lorsque le certificat échoue des vérifications, **"2"** pour avertir mais autoriser les connexions qui utilisent un certificat auto-signé ou **"3"** pour autoriser des connexions non vérifiables. Si vous spécifiez **"3"**, aucune vérification n'est effectuée. La valeur par défaut est "2".
`view.usbAutoConnectAtStartup`	`--usbAutoConnectAtStartUp=`	Connecte automatiquement les périphériques USB au démarrage d'Horizon Client. Spécifiez **« TRUE »** ou **« FALSE »**. La valeur par défaut est « TRUE ».
`view.usbAutoConnectOnInsert`	`--usbAutoConnectOnInsert=`	Connecte automatiquement les périphériques USB lorsqu'un périphérique USB est inséré. Spécifiez **« TRUE »** ou **« FALSE »**. La valeur par défaut est « TRUE ».

Tableau 2-2. Options de ligne de commande et clés du fichier de configuration d' Horizon Client (suite)

Clé de configuration	Option de ligne de commande	Description
`view.xfreerdpOptions`	`--xfreerdpOptions=`	(Disponible si vous utilisez le protocole d'affichage Microsoft RDP) Spécifie des options de ligne de commande à transmettre au programme `xfreerdp`. Pour plus d'informations sur les options `xfreerdp`, consultez la documentation de `xfreerdp`. **Remarque** Pour utiliser FreeRDP, la version correcte de FreeRDP doit être installée, ainsi que tous les correctifs applicables. Pour plus d'informations, reportez-vous à la section « Installer et configurer FreeRDP », page 47.
Aucune	`--enableNla`	(S'applique si vous utilisez FreeRDP pour les connexion RDP) Active l'authentification de niveau réseau (NLA). Vous devez utiliser cette option avec l'option `--ignore-certificate`. Pour plus d'informations, reportez-vous à la section « Utilisation de FreeRDP pour des connexions RDP », page 46. NLA est désactivé par défaut si vous utilisez FreeRDP. La version correcte de FreeRDP doit être installée, ainsi que tous les correctifs applicables. Pour plus d'informations, reportez-vous à la section « Installer et configurer FreeRDP », page 47. **Remarque** Le programme `rdesktop` ne prend pas en charge NLA.
Aucune	`--printEnvironmentInfo`	Affiche des informations sur l'environnement d'un périphérique client, y compris son adresse IP, son adresse MAC, le nom de la machine et le nom de domaine. Pour le mode kiosque, vous pouvez créer un compte pour le client basé sur l'adresse MAC. Pour afficher l'adresse MAC, vous devez utiliser cette option avec l'option `-s`. Exemple d'utilisation de l'option de ligne de commande : `--printEnvironmentInfo -s view.company.com`
Aucune	`--usb=`	Spécifie quelle option utiliser pour la redirection USB. Reportez-vous à la section « Configuration système requise pour la redirection USB », page 81.
Aucune	`--version`	Affiche des informations de version sur Horizon Client.

Exemple : Exemple du mode kiosque

Les utilisateurs de kiosque peuvent être les clients d'une station d'enregistrement pour compagnies aériennes, les étudiants dans une salle de classe ou une bibliothèque, le personnel médical utilisant une station de travail de saisie de données médicales ou les clients d'un point libre-service. Les comptes sont associés à des périphériques clients plutôt qu'à des utilisateurs car les utilisateurs n'ont pas à ouvrir de session pour utiliser le périphérique client ou le poste de travail View. Il peut toujours être demandé aux utilisateurs de fournir des informations d'identification d'authentification pour certaines applications.

Pour configurer le mode kiosque, vous devez utiliser l'interface de ligne de commande `vdmadmin` sur l'instance de Serveur de connexion View et effectuer plusieurs procédures décrites dans le chapitre sur le mode kiosque dans le document *Administration de View*. Une fois le mode kiosque configuré, vous pouvez utiliser la commande `vmware-view` sur un client Linux pour vous connecter à un poste de travail View en mode kiosque.

Pour vous connecter à des postes de travail View depuis des clients Linux en mode kiosque, vous devez, au minimum, inclure les clés de configuration ou options de ligne de commande suivantes.

Clé de configuration	Options de ligne de commande équivalentes
`view.kioskLogin`	`--kioskLogin`
`view.nonInteractive`	`-q`, `--nonInteractive`
`view.fullScreen`	`--fullscreen`
`view.nomenubar`	`--nomenubar`
`view.defaultBroker`	`-s`, `--serverURL=`

L'omission de l'un de ces paramètres de configuration n'est pas prise en charge en mode kiosque. Si Serveur de connexion View est configuré pour exiger un nom d'utilisateur de kiosque non défini par défaut, vous devez également définir la propriété `view.defaultUser` ou utiliser l'option de ligne de commande `-u` ou `--userName=`. Si aucun nom d'utilisateur défini par défaut n'est requis et si vous ne spécifiez pas de nom d'utilisateur, Horizon Client peut dériver et utiliser le nom d'utilisateur de kiosque par défaut.

Remarque Si vous définissez la clé de configuration `view.sslVerificationMode`, veillez à la définir dans le fichier `/etc/vmware/view-mandatory-config`. Lorsque le client est exécuté en mode kiosque, il ne regarde pas dans le fichier `view-preferences`.

La commande indiquée dans cet exemple exécute Horizon Client sur un système client Linux et possède les caractéristiques suivantes :

- Le nom du compte d'utilisateur est basé sur l'adresse MAC du client.
- Horizon Client s'exécute en mode Plein écran sans barre de menus de Horizon Client.
- Les utilisateurs sont automatiquement connectés à l'instance de Serveur de connexion View et au poste de travail View spécifiés et ils ne sont pas invités à fournir des informations d'identification d'ouverture de session.
- Si une erreur de connexion se produit, en fonction du code d'erreur renvoyé, un script peut s'exécuter ou un programme de surveillance du kiosque peut gérer l'erreur. Par conséquent, le système client peut, par exemple, afficher un écran hors service ou peut attendre un certain temps avant de tenter de se connecter de nouveau à Serveur de connexion View.

```
./vmware-view --kioskLogin --nonInteractive --once --fullscreen --nomenubar
--serverURL="server.mycomany.com" --userName="CM-00:11:22:33:44:55:66:77" --password="mypassword"
```

Important Si un message de pré-connexion a été configuré pour apparaître avant d'autoriser Horizon Client à se connecter à un poste de travail View, l'utilisateur doit accepter le message avant de pouvoir accéder au poste de travail. Pour éviter ce problème, utilisez View Administrator afin de désactiver les messages de pré-connexion.

Utilisation d'URI pour configurer Horizon Client

Les URI (Uniform Resource Identifiers) vous permettent de créer une page Web ou un e-mail contenant des liens sur lesquels les utilisateurs finaux peuvent cliquer pour démarrer Horizon Client, se connecter à un serveur et ouvrir un poste de travail ou une application spécifique avec des options de configuration particulières.

Vous pouvez simplifier le processus de connexion à une application ou à un poste de travail distant en créant des pages Web ou des e-mails contenant des liens pour les utilisateurs finaux. Vous pouvez créer ces liens en construisant des URI qui fournissent tout ou partie des informations suivantes, afin d'éviter à vos utilisateurs finaux de devoir le faire.

- Adresse du Serveur de connexion

- Numéro de port du Serveur de connexion
- Nom d'utilisateur Active Directory
- Nom de domaine
- Nom affiché du poste de travail ou de l'application
- Taille de fenêtre
- Actions incluant la réinitialisation, la déconnexion et le démarrage d'une session
- Protocole d'affichage

Pour construire un URI, vous pouvez utiliser le schéma d'URI `vmware-view` avec des éléments de chemin et de requête propres à Horizon Client.

Remarque Vous pouvez utiliser les URI pour démarrer Horizon Client uniquement si le logiciel client est déjà installé sur des ordinateurs clients.

Syntaxe pour la création d'URI vmware-view

La syntaxe comprend le schéma d'URI `vmware-view`, un chemin d'accès spécifiant le poste de travail ou l'application et, en option, une requête permettant de spécifier des actions de poste de travail ou d'application, ou des options de configuration.

Spécification d'URI

Lorsque vous créez une URI, vous appelez essentiellement `vmware-view` avec la chaîne d'URI View complète comme argument.

Utilisez la syntaxe suivante pour créer des URI pour démarrer Horizon Client :

`vmware-view://[`*`authority-part`*`][/`*`path-part`*`][?`*`query-part`*`]`

Le seul élément requis est le schéma d'URI, `vmware-view`. Pour certaines versions de certains systèmes d'exploitation client, le nom du schéma est sensible à la casse. Il faut ainsi utiliser `vmware-view`.

Important Pour tous les éléments, les caractères non ASCII doivent d'abord être encodés en UTF-8 [STD63], puis chaque octet de la séquence UTF-8 correspondante doit être codé en pourcentage pour être représenté en tant que caractères URI.

Pour plus d'informations sur l'encodage de caractères ASCII, consultez la référence d'encodage d'URL sur http://www.utf8-chartable.de/.

authority-part

Spécifie l'adresse du serveur et, éventuellement, un nom d'utilisateur, un numéro de port non défini par défaut, ou bien les deux. Les traits de soulignement (_) ne sont pas pris en charge dans les noms de serveur. Les noms de serveur doivent être conformes à la syntaxe DNS.

Pour spécifier un nom d'utilisateur, utilisez la syntaxe suivante :

`user1@`*`server-address`*

Vous ne pouvez pas spécifier d'adresse UPN, ce qui inclut le domaine. Pour spécifier le domaine, vous pouvez utiliser la partie de requête `domainName` de l'URI.

Pour spécifier un numéro de port, utilisez la syntaxe suivante :

server-address:*port-number*

path-part

Spécifie le poste de travail ou l'application. Utilise le nom d'affichage du poste de travail ou de l'application. Ce nom est celui spécifié dans View Administrator lorsque le pool de postes de travail ou d'applications a été créé. Si le nom affiché contient un espace, utilisez le mécanisme de codage **%20** pour représenter l'espace.

query-part

Spécifie les options de configuration à utiliser ou les actions du poste de travail ou de l'application à effectuer. Les requêtes ne sont pas sensibles à la casse. Pour utiliser plusieurs requêtes, utilisez une esperluette (&) entre les requêtes. En cas de conflit entre des requêtes, la dernière requête de la liste est utilisée. Utilisez la syntaxe suivante :

query1=*value1*[&*query2*=*value2*...]

Requêtes prises en charge

Cette rubrique répertorie les requêtes prises en charge pour ce type d'Horizon Client. Si vous créez des URI pour plusieurs types de clients, tels que des clients de postes de travail et des clients mobiles, reportez-vous au guide *Utilisation de VMware Horizon Client* pour chaque type de système client.

action

Tableau 2-3. Valeurs pouvant être utilisées avec la requête d'action

Valeur	Description
`browse`	Affiche une liste des postes de travail ou applications disponibles hébergées sur le serveur spécifié. Il ne vous est pas demandé de spécifier un poste de travail ou une application pour l'utilisation de cette action.
`start-session`	Ouvre l'application ou le poste de travail spécifié. Si aucune requête d'action n'est fournie et que le nom du poste de travail ou de l'application est fourni, `start-session` est l'action par défaut.
`reset`	Éteint puis redémarre le poste de travail spécifié ou l'application distante. Les données non enregistrées sont perdues. La réinitialisation d'un poste de travail distant équivaut à appuyer sur le bouton Réinitialiser d'un ordinateur physique.
`logoff`	Déconnecte l'utilisateur du système d'exploitation invité sur le poste de travail distant. Si vous spécifiez une application, l'action est ignorée ou l'utilisateur final voit le message d'avertissement « Action d'URI non valide ».

args

Spécifie des arguments de ligne de commande à ajouter au lancement d'applications distantes. Utilisez la syntaxe `args=`*value*, où *value* est une chaîne. Utilisez l'encodage avec pourcentage pour les caractères suivants :

- Pour un deux-points (:), utilisez **%3A**
- Pour une barre oblique inversée (\), utilisez **%5C**
- Pour un espace ( ), utilisez **%20**
- Pour un guillemet double ("), utilisez **%22**

Par exemple, pour spécifier le nom de fichier `"My new file.txt"` pour l'application Notepad++, utilisez **%22My%20new%20file.txt%22**.

appProtocol Pour les applications distantes, les valeurs valides sont **`PCOIP`** et **`BLAST`**. Par exemple, pour spécifier le protocole PCoIP, utilisez la syntaxe **`appProtocol=PCOIP`**.

desktopLayout Définit la taille de la fenêtre qui affiche un poste de travail distant. Pour utiliser cette requête, vous devez paramétrer la requête `action` sur **`start-session`** ou ne pas utiliser de requête `action`.

Tableau 2-4. Valeurs valides pour la requête desktopLayout

Valeur	Description
`fullscreen`	Un moniteur affiche son contenu en plein écran. Il s'agit de la valeur par défaut.
`multimonitor`	Tous les moniteurs affichent leur contenu en plein écran.
`windowLarge`	Fenêtre de grande taille.
`windowSmall`	Fenêtre de petite taille.
*W*x*H*	Personnalisez la résolution, spécifiez la largeur et la hauteur en pixels. Exemple de syntaxe : **`desktopLayout=1280x800`**.

desktopProtocol Pour les postes de travail distants, les valeurs valides sont **`RDP`**, **`PCOIP`** et **`BLAST`**. Par exemple, pour spécifier le protocole PCoIP, utilisez la syntaxe **`desktopProtocol=PCOIP`**.

domainName Nom de domaine NETBIOS associé à l'utilisateur qui se connecte à l'application ou au poste de travail distant. Utilisez par exemple `monentreprise` plutôt que `monentreprise.com`.

useExisting Si cette option est définie sur **`true`**, il n'est possible d'exécuter qu'une seule instance d'Horizon Client. Si des utilisateurs tentent de se connecter à un deuxième serveur, ils doivent se déconnecter du premier serveur, ce qui entraîne la déconnexion des sessions d'application et de poste de travail. Si cette option est définie sur **`false`**, il est possible d'exécuter plusieurs instances d'Horizon Client et les utilisateurs peuvent se connecter à plusieurs serveurs en même temps. La valeur par défaut est **`true`**. Exemple de syntaxe : **`useExisting=false`**.

Exemples d'URI de vmware-view

Vous pouvez créer des liens hypertextes ou des boutons avec le schéma URI `vmware-view` et inclure ces liens dans des e-mails ou sur une page Web. Vos utilisateurs finaux peuvent cliquer sur ces liens pour, par exemple, ouvrir un poste de travail distant particulier avec les options de démarrage que vous spécifiez.

Exemples de syntaxe URI

Chaque exemple d'URI est suivi d'une description de ce que l'utilisateur final voit après avoir cliqué sur le lien URI.

1 `vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session`

Horizon Client démarre et se connecte au serveur `view.mycompany.com`. La boîte de dialogue de connexion invite l'utilisateur à fournir un nom d'utilisateur, un nom de domaine et un mot de passe. Après l'ouverture de session, le client se connecte au poste de travail dont le nom d'affichage est **Poste de travail principal**, et l'utilisateur voit sa session ouverte sur le système d'exploitation client.

Remarque Le protocole d'affichage et la taille de fenêtre par défaut sont utilisés. Le protocole d'affichage par défaut est PCoIP. La taille de fenêtre par défaut est plein écran.

Vous pouvez modifier les valeurs par défaut. Reportez-vous à la section « Utilisation de l'interface de ligne de commande et des fichiers de configuration d'Horizon Client », page 28.

---

2 `vmware-view://view.mycompany.com:7555/Primary%20Desktop`

Cet URI a le même effet que l'exemple précédent, sauf qu'il utilise le port non défini par défaut 7555 pour le Serveur de connexion. (Le port par défaut est 443.) Comme un identificateur de poste de travail est fourni, le poste de travail s'ouvre même si l'action `start-session` n'est pas incluse dans l'URI.

3 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?desktopProtocol=PCOIP`

Horizon Client démarre et se connecte au serveur `view.mycompany.com`. Dans la boîte de dialogue de connexion, la zone de texte **Nom d'utilisateur** contient le nom **fred**. L'utilisateur doit fournir le nom de domaine et le mot de passe. Après l'ouverture de session, le client se connecte au poste de travail dont le nom d'affichage est **Poste de travail Finance**, et l'utilisateur voit sa session ouverte sur le système d'exploitation client. La connexion utilise le protocole d'affichage PCoIP.

4 `vmware-view://view.mycompany.com/Calculator?action=start-session&appProtocol=BLAST`

Horizon Client démarre et se connecte au serveur `view.mycompany.com`. Dans la boîte de dialogue de connexion, l'utilisateur doit fournir le nom d'utilisateur, le nom de domaine et le mot de passe. Après l'ouverture de session, le client se connecte à l'application dont le nom complet affiché est **Calculatrice**. La connexion utilise le protocole d'affichage VMware Blast.

5 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?domainName=mycompany`

Horizon Client démarre et se connecte au serveur `view.mycompany.com`. Dans la boîte de dialogue de connexion, la zone de texte **Nom d'utilisateur** contient le nom **fred** et la zone de texte **Domaine** contient **mycompany**. L'utilisateur doit fournir uniquement un mot de passe. Après l'ouverture de session, le client se connecte au poste de travail dont le nom d'affichage est **Poste de travail Finance**, et l'utilisateur voit sa session ouverte sur le système d'exploitation client.

6 `vmware-view://view.mycompany.com/`

Horizon Client démarre et l'utilisateur est dirigé vers l'invite d'ouverture de session pour se connecter au serveur `view.mycompany.com`.

7 `vmware-view://view.mycompany.com/Primary%20Desktop?action=reset`

Horizon Client démarre et se connecte au serveur `view.mycompany.com`. La boîte de dialogue de connexion invite l'utilisateur à fournir un nom d'utilisateur, un nom de domaine et un mot de passe. Après l'ouverture de session, Horizon Client affiche une boîte de dialogue qui invite l'utilisateur à confirmer l'opération de réinitialisation pour Poste de travail principal. Après la réinitialisation, en fonction du type de client utilisé, l'utilisateur peut voir un message indiquant la réussite de l'opération.

Remarque Cette action n'est disponible que si un administrateur View a activé cette fonctionnalité pour les utilisateurs finaux.

---

8 `vmware-view://`

Horizon Client démarre et l'utilisateur est dirigé vers la page pour entrer l'adresse d'un serveur.

9 `vmware-view://10.10.10.10/My%20Notepad++?args=%22My%20new%20file.txt%22`

Lance My Notepad++ sur le serveur 10.10.10.10 et transmet l'argument `My new file.txt` dans la commande de lancement d'application. Le nom de fichier est entre guillemets, car il contient des espaces.

10 `vmware-view://10.10.10.10/Notepad++%2012?args=a.txt%20b.txt`

Lance Notepad++ 12 sur le serveur 10.10.10.10 et transmet l'argument `a.text b.txt` dans la commande de lancement d'application. Comme l'argument n'est pas entre guillemets, un espace sépare les noms de fichier et les deux fichiers sont ouverts séparément dans Notepad++.

Remarque Les applications peuvent différer dans leur manière d'utiliser des arguments de ligne de commande. Par exemple, si vous transmettez l'argument `a.txt b.txt` à Wordpad, Wordpad n'ouvre qu'un seul fichier, `a.txt`.

Exemples de code HTML

Vous pouvez utiliser des URI pour faire des liens hypertextes et des boutons à inclure dans des e-mails ou sur des pages Web. Les exemples suivants montrent comment utiliser l'URI du premier exemple d'URI pour coder un lien hypertexte qui dit **Test Link** et un bouton qui dit **TestButton**.

```
<html>
<body>

<a href="vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session">Test
Link</a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session'"></form> <br>

</body>
</html>
```

Configuration de la vérification des certificats pour les utilisateurs finaux

Les administrateurs peuvent configurer le mode de vérification des certificats afin que, par exemple, une vérification complète soit toujours effectuée.

La vérification des certificats se produit pour les connexions SSL entre le Serveur de connexion et Horizon Client. Les administrateurs peuvent configurer le mode de vérification pour utiliser l'une des stratégies suivantes :

- Les utilisateurs finaux sont autorisés à choisir le mode de vérification. Le reste de cette liste décrit les trois modes de vérification.
- (Pas de vérification) Aucune vérification de certificat n'est effectuée.
- (Avertir) Les utilisateurs sont avertis si un certificat auto-signé est présenté par le serveur. Les utilisateurs peuvent choisir d'autoriser ou pas ce type de connexion.
- (Sécurité complète) Une vérification complète est effectuée et les connexions qui ne passent pas de vérification complète sont rejetées.

Pour plus d'informations sur les types de vérifications effectuées, reportez-vous à la section « Définition du mode de vérification de certificats pour Horizon Client », page 56.

Utilisez la propriété `view.sslVerificationMode` pour définir le mode de vérification par défaut :

- **1** implémente `Full Verification`.
- **2** implémente `Warn If the Connection May Be Insecure`.

- **3** implémente `No Verification Performed`.

Pour configurer le mode afin que les utilisateurs finaux ne puissent pas modifier le mode, définissez la propriété `view.allowSslVerificationMode` sur **`"False"`** dans le fichier `/etc/vmware/view-mandatory-config` sur le système client. Reportez-vous à la section « Paramètres de configuration et options de ligne de commande d'Horizon Client », page 29.

Configuration des options TLS/SSL avancées

Vous pouvez sélectionner les protocoles de sécurité et les algorithmes de chiffrement qui sont utilisés pour chiffrer les communications entre Horizon Client et les serveurs Horizon ou entre Horizon Client et l'agent dans le poste de travail distant.

Ces options sont également utilisées pour chiffrer le canal USB (communication entre le démon du service USB et l'agent).

Avec le paramètre par défaut, les suites de chiffrement utilisent la spécification AES 128 ou 256 bits, suppriment les algorithmes DH anonymes, puis trient la liste de chiffrements actuels par longueur de clé de chiffrement.

Par défaut, TLS v1.0, TLS v1.1 et TLS v1.2 sont activés. SSL v2.0 et v3.0 ne sont pas pris en charge.

Remarque Si TLS v1.0 et RC4 sont désactivés, la redirection USB ne fonctionne pas lorsque des utilisateurs sont connectés à des postes de travail Windows XP. Sachez qu'il existe des risques de sécurité si vous choisissez d'utiliser cette fonctionnalité en activant TLS v1.0 et RC4.

Si vous configurez un protocole de sécurité pour Horizon Client qui n'est pas activé sur le serveur View Server auquel le client se connecte, une erreur TLS/SSL se produit et la connexion échoue.

Important Au moins un des protocoles que vous activez dans Horizon Client doit également être activé sur le poste de travail distant. Sinon, les périphériques USB ne peuvent pas être redirigés vers le poste de travail distant.

Sur le système client, vous pouvez utiliser des propriétés du fichier de configuration ou des options de ligne de commande pour ces paramètres :

- Pour utiliser les propriétés du fichier de configuration, utilisez les propriétés `view.sslProtocolString` et `view.sslCipherString`.
- Pour utiliser des options de configuration de ligne de commande, utilisez les options `--sslProtocolString` et `--sslCipherString`.

Pour plus d'informations, reportez-vous à « Utilisation de l'interface de ligne de commande et des fichiers de configuration d'Horizon Client », page 28 et recherchez les noms de propriétés et d'options dans le tableau de la section « Paramètres de configuration et options de ligne de commande d'Horizon Client », page 29.

Configuration de touches et de combinaisons de touches spécifiques à envoyer au système local

À partir d'Horizon Client, si vous utilisez PCoIP, ou, à partir d'Horizon Client 4.0, si vous utilisez VMware Blast ou PCoIP, vous pouvez créer un fichier `view-keycombos-config` pour spécifier les touches individuelles et les combinaisons de touches qui ne doivent pas être transmises au poste de travail distant.

Lorsque vous travaillez sur un poste de travail distant, vous pouvez préférer que certaines combinaisons de touches soient traitées par votre système client local. Vous pouvez, par exemple, utiliser une combinaison de touches particulière pour lancer l'économiseur d'écran sur votre ordinateur client. Vous pouvez créer un fichier situé dans `/etc/vmware/view-keycombos-config` et spécifier les combinaisons de touches et les touches individuelles.

Placez chaque touche ou combinaison de touches sur une nouvelle ligne en utilisant le format suivant :

<modName>scanCode
scanCode

Le premier exemple concerne une combinaison de touches. Le deuxième exemple concerne une touche isolée. La valeur de *scanCode* correspond au code de touche enfoncée du clavier, en hexadécimal.

Dans cet exemple, *modName* est l'une des quatre touches de modification : `ctrl`, `alt`, `maj` et `super`. La touche Super est propre aux claviers. Par exemple, la touche Super correspond généralement à la touche Windows sur un clavier Microsoft Windows, et à la touche Cmd sur un clavier Mac OS X. Vous pouvez également utiliser `<any>` comme caractère générique pour *modName*. Par exemple, `<any>0x153` spécifie toutes les combinaisons de la touche Supprimer, ainsi que la touche Supprimer individuelle du clavier américain. La valeur que vous utilisez pour *modName* n'est pas sensible à la casse.

Spécification du code d'analyse d'une touche

La valeur de *scanCode* doit être au format hexadécimal. Pour déterminer le code à utiliser, ouvrez le fichier correspondant à la langue et au clavier appropriés dans le répertoire `lib/vmware/xkeymap` sur votre système client. Outre les codes de touches répertoriés dans ce fichier, vous pouvez également utiliser les codes suivants :

Tableau 2-5. Touches multimédias

Nom de la touche	Code d'analyse
PREVIOUS_TRACK	0x110
NEXT_TRACK	0x119
MUTE	0x120
CALCULATOR	0x121
PLAY_PAUSE	0x122
STOP	0x124
VOLUME_DOWN	0x12e
VOLUME_UP	0x130
BROWSER_HOME	0x132
BROWSER_SEARCH	0x165
BROWSER_FAVORITES	0x166
BROWSER_REFRESH	0x167
BROWSER_STOP	0x168
BROWSER_FORWARD	0x169
BROWSER_BACK	0x16A
MY_COMPUTER	0x16B
MAIL	0x16C
MEDIA_SELECT	0x16D

Tableau 2-6. Touches Hangul et Hanja

Nom de la touche	Code d'analyse
HANGUL_EN	0x72
HANJA_EN	0x71
HANGUL_KO	0x172

Tableau 2-6. Touches Hangul et Hanja (suite)

Nom de la touche	Code d'analyse
HANJA_KO	0x171
HANGUL	0xF2
HANJA	0xF1

Tableau 2-7. Touches Veille système, Sortie de veille et Marche/Arrêt

Nom de la touche	Code d'analyse
SYSTEM_SLEEP	0x15F
SYSTEM_WAKE	0x163
SYSTEM_POWER	0x15e

La liste suivante montre un exemple de contenu d'un fichier `/etc/vmware/view-keycombos-config`. Les commentaires de code sont précédés du symbole #.

```
<ctrl>0x152      #block ctrl-insert
<alt>15          #block alt-tab
<Ctrl><Alt>0x153 #block ctrl-alt-del
<any>0x137       #block any combinations of the Print key
0x010               #block the individual Q key in a US English keyboard
                 #or block the individual A key in a French keyboard
0x03b            #block the individual F1 key
0x04f            #block the individual 1 key in a numeric keypad
```

Utilisation de FreeRDP pour des connexions RDP

Si vous prévoyez d'utiliser RDP au lieu de VMware Blast ou PCoIP pour les connexions à des postes de travail View, vous pouvez choisir d'utiliser un client `rdesktop` ou `xfreerdp`, la mise en œuvre open source du protocole RDP (Remote Desktop Protocol), publiée sous la licence Apache.

Comme le programme `rdesktop` n'est plus activement développé, Horizon Client peut également exécuter l'exécutable `xfreerdp` si votre machine Linux dispose de la version et des correctifs requis pour FreeRDP.

Important Si vous prévoyez de vous connecter à des applications ou à des postes de travail distants sur un hôte Microsoft RDS, si cet hôte est configuré avec le mode de gestion des licences par périphérique, vous devez utiliser `xfreerdp` ou opter pour le mode de licence par utilisateur. Cela est dû au fait que le mode de gestion des licences par périphérique oblige le client RDP à fournir un ID de client, alors que `rdesktop` ne fournit pas cet ID, tandis que `xfreerdp` le fournit.

La version correcte de FreeRDP doit être installée, ainsi que tous les correctifs applicables. Pour plus d'informations, reportez-vous à la section « Installer et configurer FreeRDP », page 47.

Syntaxe générale

Vous pouvez utiliser l'interface de ligne de commande `vmware-view` ou certaines propriétés dans des fichiers de configuration afin de spécifier des options pour `xfreerdp`, comme vous le faites pour `rdesktop`.

- Pour spécifier que Horizon Client doit exécuter `xfreerdp` plutôt que `rdesktop`, utilisez l'option de ligne de commande ou la clé de configuration appropriée.

Option de ligne de commande :	`--rdpclient="xfreerdp"`
Clé de configuration :	`view.rdpClient="xfreerdp"`

- Pour spécifier des options à transmettre au programme `xfreerdp`, utilisez l'option de ligne de commande ou la clé de configuration appropriée, et spécifiez les options FreeRDP.

Option de ligne de commande :	`--xfreerdpOptions`
Clé de configuration :	`view.xfreerdpOptions`

Pour plus d'informations sur l'utilisation de l'interface de ligne de commande `vmware-view` et des fichiers de configuration, reportez-vous à la section « Utilisation de l'interface de ligne de commande et des fichiers de configuration d'Horizon Client », page 28.

Syntaxe pour l'authentification au niveau du réseau

Plusieurs options de configuration pour le programme `rdesktop` sont les mêmes que pour le programme `xfreerdp`. Une différence importante est que `xfreerdp` prend en charge l'authentification au niveau du réseau (NLA). La NLA est désactivée par défaut. Vous devez utiliser l'option de ligne de commande suivante pour activer l'authentification au niveau du réseau :

```
--enableNla
```

En outre, vous devez ajouter l'option `/cert-ignore` pour que le processus de vérification de certificat aboutisse. Voici un exemple de la syntaxe appropriée :

```
vmware-view --enableNla --rdpclient=xfreerdp --xfreerdpOptions="/p:password /cert-ignore /u:user-name /d:domain-name /v:server"
```

Si le mot de passe contient des caractères spéciaux, faites-les précéder d'un caractère d'échappement (par exemple : **\$**).

Syntaxe spécifique de l'utilisation de FreeRDP avec Horizon Client

Gardez à l'esprit les directives suivantes :

- Vous devez faire précéder d'un caractère d'échappement les caractères spéciaux que vous placez normalement entre guillemets. Par exemple, la commande suivante ne fonctionne pas, car le caractère spécial $ dans pa$$word n'est pas précédé d'un caractère d'échappement :

  (incorrect)
  ```
  vmware-view --rdpclient=xfreerdp --xfreerdpOptions="/p:'pa$$word' /u:'crt\administrator'"
  ```

  Vous devez plutôt utiliser :

  (correct)
  ```
  vmware-view --rdpclient=xfreerdp --xfreerdpOptions="/p:'pa\$\$word' /u:'crt\administrator'"
  ```

- Si les utilisateurs emploient une mise en œuvre session-en-session d'Horizon Client, vous devez utiliser l'option `/rfx`. Vous avez une mise en œuvre session-en-session lorsqu'un utilisateur se connecte à Horizon Client sur un client léger, de telle sorte que l'interface d'Horizon Client est la seule que voit l'utilisateur final, et que ce dernier lance une version imbriquée d'Horizon Client pour utiliser l'application distante fournie par un hôte RDS. Dans ce cas, si vous n'utilisez pas l'option `/rfx`, l'utilisateur final ne pourra pas voir les icônes des applications et des postes de travail distants dans le sélecteur de postes de travail et d'applications du client imbriqué.

Installer et configurer FreeRDP

Pour utiliser un client FreeRDP pour des connexions RDP à des postes de travail View, votre machine Linux doit inclure la version requise de FreeRDP.

Pour obtenir une liste des packages dont `xfreerdp` dépend dans Ubuntu, allez sur https://github.com/FreeRDP/FreeRDP/wiki/Compilation.

Prérequis

Sur votre machine cliente Linux, téléchargez FreeRDP 1.1 depuis GitHub, à l'adresse https://github.com/FreeRDP/FreeRDP.

Procédure

1 Appliquez le correctif avec le fichier `freerdp-1.1.0.patch`, à l'aide des commandes de correctif suivantes :

```
cd /client-installation-directory/patches/FreeRDP-stable-1.1
patch -p1 < freerdp-1.1.0.patch
patch -p1 < freerdp-1.1.0-tls.patch
```

Ici *client-installation-directory* est le chemin d'accès à `VMware-Horizon-View-Client-x.x.x-yyyyyy.i386`, où *x.x.x* est le numéro de version et *yyyyyy* le numéro de build. Le fichier `freerdp-1.1.0-tls.patch` permet la connexion TLSv1.2 dans `xfreerdp`. Pour plus d'informations sur le fichier `freerdp-1.1.0.patch`, reportez-vous au fichier `README.patches` dans le même répertoire *client-installation-directory*`/patches`.

2 Exécutez la commande suivante :

```
cmake -DWITH_SSE2=ON -DWITH_PULSEAUDIO=ON -DWITH_PCSC=ON -DWITH_CUPS=ON .
```

3 Exécutez la commande suivante :

```
make
```

4 Exécutez la commande suivante, qui installe le fichier binaire `xfreerdp` créé dans un répertoire sur le chemin d'exécution pour que Horizon Client puisse exécuter le programme en exécutant `xfreerdp` :

```
sudo make install
```

5 (Facultatif) Vérifiez que le module d'impression virtuelle peut se charger.

a Pour vérifier que `tprdp.so` peut être chargé par FreeRDP 1.1, exécutez la commande suivante :

```
sudo ln -s /usr/lib/vmware/rdpvcbridge/tprdp.so /usr/local/lib/i386-linux-
gnu/freerdp/tprdp-client.so
```

b Pour démarrer Horizon Client avec la fonctionnalité d'impression virtuelle activée, exécutez la commande suivante :

```
vmware-view --rdpclient=xfreerdp --xfreerdpOptions='/cert-ignore /vc:tprdp'
```

Remarque La fonctionnalité d'impression virtuelle est disponible si vous utilisez VMware Blast ou PCoIP.

Activation du mode FIPS

Vous pouvez activer le mode FIPS (Federal Information Processing Standard) pour que le client utilise des algorithmes cryptographiques compatibles FIPS lorsqu'il communique avec des postes de travail distants.

Important Si vous activez le mode FIPS sur le client, il doit également être activé sur le poste de travail distant. Le mode mixte, où le mode FIPS n'est activé que sur le client, ou que sur le poste de travail, n'est pas pris en charge.

Pour activer le mode FIPS, apportez les modifications suivantes à la configuration :

1 Modifiez le fichier `/etc/vmware/config` et ajoutez les lignes suivantes :

```
usb.enableFIPSMode = "TRUE"
mks.enableFIPSMode = “TRUE”
```

2 Modifiez le fichier `/etc/vmware/view-mandatory-config` et ajoutez la ligne suivante :

```
View.fipsMode = "TRUE"
```

3 Modifiez le fichier `/etc/teradici/pcoip_admin.conf` et ajoutez la ligne suivante :

```
pcoip.enable_fips_mode = 1
```

Configuration du cache d'images client PCoIP

Le cache d'images client PCoIP stocke le contenu des images sur le client pour éviter la retransmission. Cette fonctionnalité est activée par défaut pour réduire la bande passante.

Le cache d'images PCoIP capture la redondance spatiale et temporelle. Par exemple, lorsque vous faites défiler un document PDF, le nouveau contenu apparaît depuis le bas de la fenêtre et le contenu le plus ancien disparaît du haut de la fenêtre. L'autre contenu reste constant et remonte. Le cache d'images PCoIP peut détecter cette redondance spatiale et temporelle.

Comme pendant le défilement, les informations d'écran envoyées au périphérique client sont constituées principalement d'une séquence d'index de cache, l'utilisation du cache d'images permet d'économiser un quantité significative de bande passante. Ce défilement efficace offre des avantages dans un réseau LAN et dans un réseau WAN.

- Dans un réseau LAN, où la bande passante est relativement illimitée, le cache d'image client permet d'économiser une quantité significative de bande passante.
- Dans un réseau WAN, pour rester dans les limites de bande passante disponible, le défilement est souvent dégradé sauf si la mise en cache client est utilisée. Dans cette situation, la mise en cache client peut économiser la bande passante et permettre de faire défiler les données d'une manière fluide et avec grande réactivité.

Cette fonctionnalité est activée par défaut pour que le client stocke des portions de l'affichage ayant déjà été transmises. La taille du cache par défaut est de 250 Mo. Une taille de cache supérieure réduit la bande passante mais requiert plus de mémoire sur le client. Une taille de cache inférieure requiert plus de bande passante. Par exemple, un client léger avec peu de mémoire requiert une taille de cache inférieure.

Définition de la propriété de configuration

Pour configurer la taille du cache, vous pouvez définir la propriété `pcoip.image_cache_size_mb`. Par exemple, le paramètre suivant configure la taille du cache sur 50 Mo :

```
pcoip.image_cache_size_mb = 50
```

Utilisez un espace avant et après le signe égal (=).

Si vous spécifiez une valeur inférieure à la quantité de mémoire disponible divisée par 2, la valeur est arrondie au multiple de 10 le plus proche. La valeur minimale est de 50. Toute valeur inférieure à 50 est ignorée.

Si vous spécifiez une valeur supérieure à la quantité de mémoire disponible divisée par 2, la valeur est définie à la quantité de mémoire disponible divisée par 2 et arrondie au multiple de 10 le plus proche.

Vous pouvez définir cette propriété dans un des différents fichiers. Lorsque Horizon Client démarre, le paramètre est traité depuis divers emplacements dans l'ordre suivant :

1 `/etc/teradici/pcoip_admin_defaults.conf`

2 `~/.pcoip.rc`

3 `/etc/teradici/pcoip_admin.conf`

Si un paramètre est défini dans plusieurs emplacements, la valeur utilisée est la valeur du dernier fichier lu.

Remarque Vous pouvez définir la propriété suivante pour afficher une indication visuelle que le cache d'images fonctionne :

```
pcoip.show_image_cache_hits = 1
```

Avec cette configuration, pour chaque carreau (32 x 32 pixels) dans une image qui provient du cache d'images, vous pouvez voir un rectangle autour du carreau.

Gestion des connexions aux applications et postes de travail distants

3

Horizon Client vous permet de vous connecter au Serveur de connexion ou à un serveur de sécurité et d'ouvrir ou de fermer une session sur un poste de travail distant, mais également d'utiliser des applications distantes. À des fins de dépannage, il vous permet également de réinitialiser les applications et postes de travail distants.

En fonction de la façon dont l'administrateur configure les stratégies de postes de travail distants, les utilisateurs finaux peuvent être en mesure d'exécuter plusieurs opérations sur leurs postes de travail.

Ce chapitre aborde les rubriques suivantes :

Connexion à une application ou un poste de travail distant

Une fois connecté à un serveur View Server, vous pouvez utiliser les applications et postes de travail distants que vous êtes autorisé à utiliser.

Avant de laisser vos utilisateurs finaux accéder à leurs applications et postes de travail distants, vérifiez que vous pouvez vous connecter à une application ou à un poste de travail distant à partir d'un périphérique client. Vous devez spécifier un serveur et fournir des informations d'identification pour votre compte d'utilisateur.

Pour utiliser les applications distantes, vous devez vous connecter au Serveur de connexion View 6.0 ou versions ultérieures.

Prérequis

- Procurez-vous les informations d'identification pour ouvrir une session, telles que le nom d'utilisateur et le mot de passe, le nom d'utilisateur et le code secret RSA SecurID, le nom d'utilisateur et le code secret pour l'authentification RADIUS ou le numéro d'identification personnel (PIN) de carte à puce.
- Obtenez le nom de domaine NETBIOS pour ouvrir une session. Utilisez par exemple `monentreprise` plutôt que `monentreprise.com`.
- Effectuez les tâches administratives décrites dans « Préparation du Serveur de connexion pour Horizon Client », page 14.

- Si vous vous trouvez à l'extérieur du réseau d'entreprise et si vous n'utilisez pas de serveur de sécurité pour accéder au poste de travail distant, vérifiez que votre périphérique client est configuré pour utiliser une connexion VPN et activez cette connexion.

  Important VMware vous recommande d'utiliser un serveur de sécurité plutôt qu'un VPN.

- Vérifiez que vous disposez du nom de domaine complet (FQDN) du serveur qui fournit l'accès à l'application ou au poste de travail distant. Les traits de soulignement (_) ne sont pas pris en charge dans les noms de serveur. Vous avez également besoin du numéro de port si le port n'est pas 443.
- Si vous prévoyez d'utiliser le protocole d'affichage RDP pour vous connecter à un poste de travail distant, vérifiez que le paramètre de stratégie de groupe AllowDirectRDP de l'agent est activé.

Procédure

1 Ouvrez une fenêtre de terminal et entrez `vmware-view` ou recherchez les applications pour **VMware Horizon Client**, et double-cliquez sur l'icône.

2 Double-cliquez sur le bouton **+ Ajouter un serveur** si aucun serveur n'a encore été ajouté ou cliquez sur le bouton **+ Nouveau serveur** dans la barre de menus, et entrez le nom du Serveur de connexion View ou d'un serveur de sécurité, puis cliquez sur **Connecter**.

   Les connexions entre Horizon Client et le Serveur de connexion View utilisent toujours SSL. Le port par défaut pour les connexions SSL est 443. Si le Serveur de connexion View n'est pas configuré pour utiliser le port par défaut, utilisez le format indiqué dans cet exemple : `view.company.com:1443`.

   Vous pouvez voir un message que vous devez confirmer avant que la boîte de dialogue de connexion apparaisse.

   Remarque Lorsque la connexion a réussi, une icône de ce serveur est enregistrée sur l'écran d'accueil d'Horizon Client. Lors de la prochaine ouverture de Horizon Client pour vous connecter à ce serveur, vous pouvez double-cliquer sur l'icône, ou, si vous utilisez seulement ce serveur, vous pouvez cliquer avec le bouton droit sur l'icône du serveur et sélectionner **Se connecter automatiquement à ce serveur** dans le menu contextuel.

3 Si un message demande les informations d'identification RSA SecurID ou les informations d'identification de l'authentification RADIUS, entrez le nom d'utilisateur et le code secret, puis cliquez sur **OK**.

4 Entrez votre nom d'utilisateur et mot de passe, sélectionnez un domaine et cliquez sur **OK**..

   Vous pouvez voir un message que vous devez confirmer avant que la boîte de dialogue de connexion apparaisse.

5 Si l'indicateur de sécurité de poste de travail devient rouge et qu'un message d'avertissement apparaît, répondez à l'invite.

   Généralement, cet avertissement indique que le Serveur de connexion n'a pas envoyé d'empreinte numérique de certificat au client. L'empreinte numérique est un hachage de la clé publique du certificat et elle est utilisée comme abréviation de la clé publique.

6 (Facultatif) Pour configurer les paramètres d'affichage des postes de travail distants, cliquez avec le bouton droit de la souris sur une icône de poste de travail ou sélectionnez une icône de poste de travail et cliquez sur l'icône **Paramètres** (en forme d'engrenage) en regard du nom de serveur dans la partie supérieure de l'écran.

Option	Description
Protocole d'affichage	Si votre administrateur l'a autorisé, vous pouvez utiliser la liste **Connecter via** pour sélectionner le protocole d'affichage. VMware Blast requiert Horizon Agent 7.0 ou version ultérieure.
Disposition de l'affichage	Utilisez la liste **Affichage** pour sélectionner une taille de fenêtre ou pour utiliser plusieurs écrans.

7 (Facultatif) Pour marquer une application ou un poste de travail distant comme favori, cliquez avec le bouton droit de la souris sur l'icône du poste de travail ou de l'application en question et sélectionnez **Marquer comme favori** dans le menu contextuel qui apparaît.

Une icône étoile apparaît dans l'angle supérieur droit du nom du poste de travail ou de l'application. Lors de votre prochaine connexion, vous pourrez cliquer sur le bouton **Afficher les favoris** pour trouver rapidement l'application ou le poste de travail en question.

8 Double-cliquez sur une application ou un poste de travail distant pour vous connecter.

Si vous vous connectez à un poste de travail distant basé sur la session qui est hébergé sur un hôte RDS Microsoft et si le poste de travail est déjà configuré pour utiliser un protocole d'affichage différent, vous ne pourrez pas vous connecter immédiatement. Vous serez invité à utiliser le protocole actuellement configuré ou vous devrez demander au système de fermer votre session au système d'exploitation distant afin qu'une connexion puisse être établie avec le protocole sélectionné.

Une fois la connexion établie, la fenêtre client s'affiche.

Si l'authentification sur le Serveur de connexion View échoue ou si le client ne peut pas se connecter à une application ou à un poste de travail distant, effectuez les tâches suivantes :

- Déterminez si le Serveur de connexion View est configuré pour ne pas utiliser SSL. Le logiciel client nécessite des connexions SSL. Vérifiez si le paramètre général dans View Administrator de la case **Use SSL for client connections (Utiliser SSL pour les connexions client)** est désélectionné. Si c'est le cas, vous devez cocher la case pour que SSL soit utilisé ou configurer votre environnement de sorte que les clients puissent se connecter à un équilibreur de charge activé pour HTTPS ou à un autre périphérique intermédiaire configuré pour établir une connexion HTTP vers Serveur de connexion View.
- Vérifiez que le certificat de sécurité pour le Serveur de connexion View fonctionne correctement. Si ce n'est pas le cas, dans View Administrator, vous pouvez également voir que View Agent sur des postes de travail n'est pas accessible. Il s'agit de symptômes de problèmes de connexion supplémentaires causés par des problèmes de certificat.
- Vérifiez que les balises définies sur l'instance de Serveur de connexion View autorisent les connexions depuis cet utilisateur. Reportez-vous au document *Administration de View*.
- Vérifiez que l'utilisateur est autorisé à accéder à ce poste de travail ou à cette application. Reportez-vous au document *Configuration de pools de postes de travail et d'applications dans View*.
- Si vous utilisez le protocole d'affichage RDP pour vous connecter à un poste de travail distant, vérifiez que le système client distant autorise les connexions à des postes de travail distants.

Partager l'accès aux dossiers et lecteurs locaux

Vous pouvez configurer Horizon Client pour partager les dossiers et les lecteurs sur votre système local avec des applications et des postes de travail distants. Les lecteurs peuvent comporter des lecteurs mappés et des périphériques de stockage USB. Cette fonctionnalité est appelée redirection de lecteur client.

Dans un poste de travail distant Windows, les dossiers et les lecteurs partagés apparaissent dans la section **Périphériques et lecteurs** du dossier **Ce PC**, ou dans la section **Autre** du dossier **Ordinateur**, en fonction de la version du système d'exploitation Windows. Dans une application distante, par exemple le bloc-notes, vous pouvez rechercher et ouvrir un fichier situé dans un dossier ou un lecteur partagé. Les dossiers et les lecteurs sélectionnés pour le partage apparaissent dans le système de fichiers comme des lecteurs réseau utilisant le format de nom ***nom* sur *NOM-DE-LA-MACHINE***.

Il n'est pas nécessaire d'être connecté à une application ou à un poste de travail distant pour configurer les paramètres de la redirection de lecteur client. Ces paramètres s'appliquent à toutes les applications et à tous les postes de travail distants. Cela signifie qu'il n'est pas possible de configurer les paramètres pour que les dossiers du client local soient partagés avec une application ou un poste de travail distant uniquement.

La fonction de redirection de lecteur client requiert que les fichiers de bibliothèque suivants soient installés. Sur certaines machines clientes légères, il est possible que ces fichiers de bibliothèque ne soient pas installés par défaut.

- `libsigc-2.0.so.0`
- `libglibmm-2.4.so.1`

Configurer le navigateur sur le système client afin d'utiliser un serveur proxy peut réduire les performances de la redirection de lecteur client si le tunnel sécurisé est activé sur l'instance du Serveur de connexion. Pour obtenir les meilleures performances de redirection du lecteur client, configurez le navigateur afin qu'il n'utilise pas un serveur proxy ou qu'il détecte automatiquement les paramètres du réseau local.

Prérequis

Pour partager des dossiers et des lecteurs avec une application ou un poste de travail distant, vous devez activer la fonctionnalité de redirection de lecteur client. Cette tâche inclut l'installation de View Agent 6.1.1 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure, et l'activation de l'option de l'agent **Redirection de lecteur client**. Elle peut également inclure la configuration de stratégies ou des paramètres de registre pour contrôler le comportement de la redirection de lecteur client. Pour plus d'informations, reportez-vous au document *Configuration de pools de postes de travail et d'applications dans View* .

Procédure

1 Ouvrez la boîte de dialogue Paramètres lorsque le volet Partage est affiché.

Option	Description
Dans la fenêtre de sélection des postes de travail et applications	Cliquez avec le bouton droit sur une icône de poste de travail ou d'application, sélectionnez **Paramètres** et cliquez sur **Partage**. Vous pouvez également sélectionner **Connexion > Paramètres** dans la barre de menus et cliquer sur **Partage**.
Dans la boîte de dialogue Partage lors de la connexion à un poste de travail ou une application	Cliquez sur **Autoriser** pour partager ou sur **Refuser** pour ne pas partager votre répertoire de base.
À partir de l'OS du poste de travail	Sélectionnez **Connexion > Paramètres** dans la barre de menus et cliquez sur **Partage**.

2 Configurez les paramètres de la redirection de lecteur client.

Option	Action
Partager un dossier ou un lecteur spécifique avec des applications et des postes de travail distants	Cliquez sur le bouton **Ajouter**, recherchez et sélectionnez le dossier ou le lecteur à partager, puis cliquez sur **OK**. **Remarque** Il n'est pas possible de partager un dossier sur un périphérique USB si le périphérique est déjà connecté à une application ou un poste de travail distant à l'aide de la fonction de redirection USB.
Arrêter le partage d'un dossier ou d'un lecteur spécifique	Sélectionnez le dossier ou le lecteur dans la liste des dossiers et cliquez sur le bouton **Supprimer**.
Autoriser les applications et les postes de travail distants à accéder à des fichiers de votre répertoire de base	Cochez la case **Partager votre répertoire de base :** *home-directory*.
Partager des périphériques de stockage USB avec des postes de travail distants	Cochez la case **Autoriser l'accès au stockage amovible**. La fonction de redirection de lecteur client partage automatiquement tous les périphériques de stockage USB insérés dans votre système client et tous les lecteurs externes connectés via FireWire et Thunderbolt. Il n'est pas nécessaire de sélectionner un périphérique spécifique à partager. **Remarque** Les périphériques de stockage USB déjà connectés à un poste de travail distant avec la fonctionnalité de redirection USB ne sont pas partagés. Si cette case est décochée, vous pouvez utiliser la fonctionnalité de redirection USB pour connecter des périphériques de stockage USB à des postes de travail distants.
Ne pas afficher la boîte de dialogue Partage lorsque vous vous connectez à une application ou à un poste de travail distant	Cochez la case **Ne pas afficher la boîte de dialogue lors de la connexion à un poste de travail ou à une application**. Si cette case n'est pas cochée, la boîte de dialogue Partage s'affiche lorsque vous vous connectez pour la première fois à un poste de travail ou à une application après une connexion à un serveur. Par exemple, si vous ouvrez une session sur un serveur avant de vous connecter à un poste de travail, la boîte de dialogue Partage s'affiche. Si vous vous connectez ensuite à une autre application ou un autre poste de travail, cette boîte de dialogue ne s'affiche plus. Pour afficher de nouveau cette boîte de dialogue, vous devez vous déconnecter du serveur puis rouvrir une session.

Suivant

Vérifiez que vous pouvez voir les dossiers partagés depuis l'application ou le poste de travail distant :

- Dans un poste de travail distant Windows, ouvrez l'Explorateur de fichiers et regardez dans la section **Périphériques et lecteurs** du dossier **Ce PC** ou ouvrez l'Explorateur Windows et regardez dans la section **Autre** du dossier **Ordinateur**.
- Depuis une application distante, si applicable, sélectionnez **Fichier > Ouvrir** ou **Fichier > Enregistrer sous** et naviguez vers le dossier ou le lecteur qui s'affiche dans le système de fichiers comme lecteur réseau utilisant le format de nom ***nom-dossier* sur *NOM-DE-LA-MACHINE***.

Partager des dossiers en modifiant un fichier de configuration

En plus de partager des dossiers via la boîte de dialogue Paramètres, vous pouvez partager des dossiers en modifiant un fichier de configuration.

Procédure

1 Créez un fichier de configuration nommé `config` s'il n'existe pas dans les emplacements suivants :

- `$HOME/.vmware/`
- `/usr/lib/vmware/`
- `/etc/vmware/`

2 Ajoutez la ligne suivante pour chaque dossier que vous voulez partager :

```
tsdr.share=Folder Path
```

Par exemple, pour partager les dossiers `/` et `/home/user1`, créez le fichier `/etc/vmware/config` et ajoutez les lignes suivantes :

```
tsdr.share=/
tsdr.share=/home/user1
```

Les dossiers qui sont partagés dans un fichier de configuration ne sont pas répertoriés dans le volet Partage de la boîte de dialogue Paramètres. Vous pouvez modifier le fichier de configuration pour arrêter le partage de dossiers ou pour partager des dossiers supplémentaires.

Définition du mode de vérification de certificats pour Horizon Client

Les administrateurs, et parfois les utilisateurs finaux, peuvent configurer le rejet des connexions client si une ou plusieurs vérifications de certificats de serveur échouent.

La vérification des certificats se produit pour les connexions SSL entre le Serveur de connexion et Horizon Client. La vérification de certificat inclut les vérifications suivantes :

- Le certificat a-t-il un autre but que de vérifier l'identité de l'expéditeur et de chiffrer les communications du serveur ? Autrement dit, s'agit-il du bon type de certificat ?
- Le certificat a-t-il expiré, ou est-il valide uniquement dans le futur ? Autrement dit, le certificat est-il valide en fonction de l'horloge de l'ordinateur ?
- Le nom commun sur le certificat correspond-il au nom d'hôte du serveur qui l'envoie ? Une incompatibilité peut se produire si l'équilibrage de charge redirige Horizon Client vers un serveur disposant d'un certificat qui ne correspond pas au nom d'hôte entré dans Horizon Client. Une incompatibilité peut également se produire si vous entrez une adresse IP plutôt qu'un nom d'hôte dans le client.

- Le certificat est-il signé par une autorité de certification inconnue ou non approuvée ? Les certificats auto-signés sont un type d'autorité de certification non approuvée.

  Pour que cette vérification aboutisse, la chaîne d'approbation du certificat doit être associée à une racine dans le magasin de certificats local.

Remarque Pour plus d'informations sur la distribution d'un certificat racine auto-signé que les utilisateurs peuvent installer sur leurs systèmes clients Linux, consultez la documentation Ubuntu.

Horizon Client utilise les certificats au format PEM stockés dans le répertoire `/etc/ssl/certs` du système client. Pour plus d'informations sur l'importation d'un certificat racine stocké à cet emplacement, consultez « Importing a Certificate into the System-Wide Certificate Authority Database » (Importation d'un certificat dans la base de données de l'autorité de certification à l'échelle du système) dans le document à l'adresse https://help.ubuntu.com/community/OpenSSL.

Outre la présentation d'un certificat de serveur, le Serveur de connexion envoie une empreinte numérique de certificat à Horizon Client. L'empreinte numérique est un hachage de la clé publique du certificat et elle est utilisée comme abréviation de la clé publique. Si le Serveur de connexion n'envoie pas d'empreinte numérique, un avertissement s'affiche pour indiquer que la connexion n'est pas autorisée.

Si votre administrateur l'a autorisé, vous pouvez définir le mode de vérification des certificats. Sélectionnez **Fichier > Préférences** dans la barre de menus. Vous avez trois possibilités :

- **Ne jamais se connecter à des serveurs non autorisés**. Si l'une des vérifications de certificat échoue, le client ne peut pas se connecter au serveur. Un message d'erreur répertorie les vérifications qui ont échoué.
- **Signaler avant de se connecter à des serveurs non autorisés**. Si une vérification de certificat échoue car le serveur utilise un certificat auto-signé, vous pouvez cliquer sur **Continuer** pour ignorer l'avertissement. Pour les certificats auto-signés, le nom du certificat ne doit pas nécessairement correspondre au nom du serveur que vous avez entré dans Horizon Client.
- **Ne pas vérifier les certificats d'identité des serveurs**. Ce paramètre signifie qu'aucune vérification des certificats n'a lieu.

Basculer entre des postes de travail ou des applications

Si vous êtes connecté à un poste de travail distant, vous pouvez basculer vers un autre poste de travail. Vous pouvez également vous connecter à des applications distantes si vous êtes connecté à un poste de travail distant.

Procédure

- Sélectionnez une application ou un poste de travail distant à partir du même serveur ou d'un autre serveur.

Option	Action
Choisir une autre application ou un autre poste de travail sur le même serveur	Effectuez l'une des opérations suivantes : ■ Si vous êtes connecté à un poste de travail distant et que vous souhaitez passer à une autre application ou un autre poste de travail distant qui s'exécute déjà sur votre client, sélectionnez le poste de travail ou l'application dans le menu **View**. ■ Si vous êtes connecté à une application ou un poste de travail distant et que vous souhaitez basculer vers une autre application ou un autre poste de travail qui n'est pas en cours d'exécution, sélectionnez **Fichier > Revenir à la liste des postes de travail et des applications** dans la barre de menus, puis lancez le poste de travail ou l'application à partir de la fenêtre de sélection. ■ Dans la fenêtre de sélection des postes de travail et applications, double-cliquez sur l'icône de l'autre poste de travail ou application. Ce poste de travail ou cette application s'ouvre dans une nouvelle fenêtre de manière à pouvoir disposer de plusieurs fenêtres ouvertes et à basculer entre elles.
Choisir une application ou un poste de travail sur un serveur différent	Effectuez l'une des opérations suivantes : ■ Si vous souhaitez maintenir l'application ou le poste de travail actuel ouvert et vous connecter également à une application ou un poste de travail distant sur un autre serveur, démarrez une nouvelle instance d'Horizon Client et connectez-vous à l'autre poste de travail ou application. ■ Si vous souhaitez fermer le poste de travail actuel et vous connecter à un poste de travail sur un autre serveur, accédez à la fenêtre de sélection de postes de travail, cliquez sur l'icône **Se déconnecter** dans l'angle supérieur gauche de la fenêtre, puis confirmez que vous souhaitez fermer votre session sur ce poste de travail. Vous serez déconnecté du serveur actuel et de toutes les sessions ouvertes de poste de travail ou d'application. Vous pouvez ensuite vous connecter à un autre serveur.

Fermer une session ou se déconnecter

Avec certaines configurations, si vous vous déconnectez d'un poste de travail distant sans fermer votre session, les applications du poste de travail peuvent rester ouvertes. Vous pouvez également vous déconnecter d'un serveur tout en gardant des applications distantes en cours d'exécution.

Même si vous n'avez aucun poste de travail distant ouvert, vous pouvez fermer la session du système d'exploitation du poste de travail distant. Utiliser cette fonction a le même résultat que d'envoyer Ctrl+Alt +Del au poste de travail et de cliquer sur **Fermer la session**.

Procédure

- Déconnectez-vous sans fermer de session.

Option	Action
Quittez également Horizon Client	Cliquez sur le bouton **Fermer** dans le coin de la fenêtre ou sélectionnez **Fichier > Quitter** dans la barre de menus.
Choisir un autre poste de travail distant sur le même serveur	Sélectionnez **Poste de travail > Déconnecter** dans la barre de menus.
Choisir un poste de travail distant sur un autre serveur	Sélectionnez **Fichier > Se déconnecter du serveur** dans la barre de menus.

Remarque Votre administrateur View peut configurer votre poste de travail pour que la session soit fermée automatiquement lors de la déconnexion. Dans ce cas, tous les programmes ouverts sur votre poste de travail sont arrêtés.

- Fermer une session et se déconnecter d'un poste de travail distant.

Option	Action
À partir de l'OS du poste de travail	Utilisez le menu **Démarrer** de Windows pour fermer la session.
À partir de la barre de menus	Sélectionnez **Poste de travail > Se déconnecter et fermer la session**. Si vous utilisez cette procédure, les fichiers ouverts sur le poste de travail distant seront fermés sans être enregistrés.

- Fermez la session lorsqu'aucun poste de travail distant n'est ouvert.
  a Dans l'écran d'accueil avec les raccourcis de poste de travail, choisissez le poste de travail, puis sélectionnez **Poste de travail > Fermer la session** dans la barre de menus.
  b Si vous y êtes invité, entrez les informations d'identification pour accéder au poste de travail distant.

  Si vous utilisez cette procédure, les fichiers ouverts sur le poste de travail distant seront fermés sans être enregistrés.

Utilisation d'un poste de travail ou d'une application Microsoft Windows sur un système Linux

4

Horizon Client pour Linux prend en charge de nombreuses fonctionnalités.

Ce chapitre aborde les rubriques suivantes :

Matrice de prise en charge des fonctions pour Linux

Certaines fonctionnalités sont prises en charge sur un type d'Horizon Client, mais pas sur un autre.

Lorsque vous prévoyez quel protocole d'affichage et quelles fonctionnalités seront disponibles pour vos utilisateurs finaux, utilisez les informations suivantes pour déterminer quels systèmes d'exploitation clients prennent cette fonctionnalité en charge.

Tableau 4-1. Fonctionnalités de poste de travail distant prises en charge sur les clients Linux

Fonction	Poste de travail Windows XP (View Agent 6.0.2 et versions antérieures)	Poste de travail Windows Vista (View Agent 6.0.2 et versions antérieures)	Poste de travail Windows 7	Poste de travail Windows 8.x	Poste de travail Windows 10	Poste de travail Windows Server 2008/2012 R2 ou Windows Server 2016
redirection USB	Limité	Limité	X	X	X	X
Audio/Vidéo en temps réel (RTAV)	Limité	Limité	X	X	X	X
Redirection de scanner						
Redirection de port série						

Tableau 4-1. Fonctionnalités de poste de travail distant prises en charge sur les clients Linux (suite)

Fonction	Poste de travail Windows XP (View Agent 6.0.2 et versions antérieures)	Poste de travail Windows Vista (View Agent 6.0.2 et versions antérieures)	Poste de travail Windows 7	Poste de travail Windows 8.x	Poste de travail Windows 10	Poste de travail Windows Server 2008/2012 R2 ou Windows Server 2016
Protocole d'affichage RDP	Limité	Limité	X	X	X	X
Protocole d'affichage PCoIP	Limité	Limité	X	X	X	X
Protocole d'affichage VMware Blast			X	X	X	X
Gestion de persona						
Wyse MMR	Systèmes client partenaires seulement et seulement avec RDP	Systèmes client partenaires seulement et seulement avec RDP				
Redirection multimédia (MMR) Windows Media			X	X	X	
Impression basée sur l'emplacement	Limité	Limité	X	X	X	X
Impression virtuelle	Limité	Limité	X	X	X	X
Cartes à puce	Limité	Limité	X	X	X	X
RSA SecurID ou RADIUS	Limité	Limité	X	X	X	X
Authentification unique	Limité	Limité	X	X	X	X
Plusieurs écrans	Limité	Limité	X	X	X	X
Redirection de lecteur client			X	X	X	X

Les postes de travail Windows 10 requièrent View Agent 6.2 ou version ultérieure. Les postes de travail Windows Server 2012 R2 requièrent View Agent 6.1 ou version ultérieure. Les postes de travail Windows Server 2016 requièrent Horizon Agent 7.0.2 ou version ultérieure.

VMware Blast requiert Horizon Agent 7.0 ou version ultérieure.

Important View Agent 6.1 et les versions ultérieures ne prennent pas en charge les postes de travail Windows XP et Windows Vista. View Agent 6.0.2 est la dernière version de View qui prend en charge ces systèmes d'exploitation. Les clients qui disposent d'un contrat de support étendu avec Microsoft pour Windows XP et Vista, ainsi qu'un contrat de support étendu avec VMware pour ces systèmes d'exploitation invités, peuvent déployer l'instance de View Agent 6.0.2 de leurs postes de travail Windows XP et Vista avec le Serveur de connexion View 6.1.

Fonctionnalités prises en charge pour les postes de travail basés sur des sessions sur les hôtes RDS

Les hôtes RDS sont des ordinateurs serveurs sur lesquels View Agent ou Horizon Agent et les services Bureau à distance Windows sont installés. Plusieurs utilisateurs peuvent avoir plusieurs sessions de poste de travail simultanément sur un hôte RDS. Un hôte RDS peut être une machine physique ou une machine virtuelle.

Remarque Le tableau suivant contient des lignes uniquement pour les fonctionnalités prises en charge. Lorsque le texte spécifie une version minimale de View Agent, le texte « et versions ultérieures » s'entend « inclure Horizon Agent 7.0.x et versions ultérieures ».

Tableau 4-2. Fonctionnalités prises en charge par les hôtes RDS avec View Agent 6.0.x ou version ultérieure, ou Horizon Agent 7.0.x ou version ultérieure, installé

Fonction	Hôte RDS Windows Server 2008 R2	Hôte RDS Windows Server 2012	Hôte RDS Windows Server 2016
RSA SecurID ou RADIUS	X	X	Horizon Agent 7.0.2 et versions ultérieures
Carte à puce	View Agent 6.1 et versions ultérieures	View Agent 6.1 et versions ultérieures	Horizon Agent 7.0.2 et versions ultérieures
Authentification unique	X	X	Horizon Agent 7.0.2 et versions ultérieures
Protocole d'affichage RDP (pour les clients de poste de travail)	X	X	Horizon Agent 7.0.2 et versions ultérieures
Protocole d'affichage PCoIP	X	X	Horizon Agent 7.0.2 et versions ultérieures
Protocole d'affichage VMware Blast	Horizon Agent 7.0 et version ultérieure	Horizon Agent 7.0 et version ultérieure	Horizon Agent 7.0.2 et versions ultérieures
HTML Access	View Agent 6.0.2 et versions ultérieures (machine virtuelle uniquement)	View Agent 6.0.2 et versions ultérieures (machine virtuelle uniquement)	Horizon Agent 7.0.2 et versions ultérieures
Redirection multimédia (MMR) Windows Media	View Agent 6.1.1 et versions ultérieures	View Agent 6.1.1 et versions ultérieures	Horizon Agent 7.0.2 et versions ultérieures
Redirection de lecteur client	View Agent 6.1.1 et versions ultérieures	View Agent 6.1.1 et versions ultérieures	Horizon Agent 7.0.2 et versions ultérieures
Impression virtuelle (pour clients de poste de travail)	View Agent 6.0.1 et versions ultérieures (machine virtuelle uniquement)	View Agent 6.0.1 et versions ultérieures (machine virtuelle uniquement)	Horizon Agent 7.0.2 et versions ultérieures (machine virtuelle uniquement)
Impression basée sur l'emplacement	View Agent 6.0.1 et versions ultérieures (machine virtuelle uniquement)	View Agent 6.0.1 et versions ultérieures (machine virtuelle uniquement)	Horizon Agent 7.0.2 et versions ultérieures (machine virtuelle uniquement)
Plusieurs moniteurs (pour clients de poste de travail)	X	X	Horizon Agent 7.0.2 et versions ultérieures
Unity Touch (pour les clients Chrome OS et mobiles)	X	X	Horizon Agent 7.0.2 et versions ultérieures
Audio/Vidéo en temps réel (RTAV)	Horizon Agent 7.0.2 et versions ultérieures	Horizon Agent 7.0.2 et versions ultérieures	Horizon Agent 7.0.3 et versions ultérieures

Pour savoir quelles éditions de chaque système d'exploitation invité et quels Service Packs sont pris en charge, consultez la rubrique « Systèmes d'exploitation pris en charge pour View Agent » dans la documentation d'installation de View 5.x ou 6.x. Consultez la rubrique « Systèmes d'exploitation pris en charge pour Horizon Agent » dans la documentation d'installation d'Horizon 7.

Limitations de certaines fonctionnalités

Les restrictions suivantes s'appliquent aux fonctionnalités prises en charge sur les postes de travail Windows avec Horizon Client pour Linux.

Tableau 4-3. Configuration requise pour des fonctionnalités spécifiques

Fonction	Configuration requise
Audio/Vidéo en temps réel	■ Pour les logiciels clients de fournisseurs tiers, cette fonctionnalité requiert View 5.2 avec Feature Pack 2 ou version ultérieure. ■ Pour Horizon Client de VMware, cette fonctionnalité requiert View Agent 6.0.2 ou version ultérieure. Requiert le protocole d'affichage VMware Blast ou PCoIP.
Impression virtuelle et impression basée sur l'emplacement pour les postes de travail Windows Server 2008 R2, les postes de travail RDS (sur hôtes RDS de machine virtuelle) et les applications distantes	■ Pour les logiciels clients de fournisseurs tiers, cette fonctionnalité requiert Horizon 6.0.1 avec View ou version ultérieure. ■ Pour Horizon Client de VMware, cette fonctionnalité requiert View Agent 6.0.2 ou version ultérieure. Requiert le protocole d'affichage VMware Blast ou PCoIP.
redirection USB	■ Pour les logiciels clients de fournisseurs tiers, cette fonctionnalité requiert View 5.1 ou version ultérieure. ■ Pour Horizon Client de VMware, cette fonctionnalité requiert View Agent 6.0.2 ou version ultérieure. Requiert le protocole d'affichage VMware Blast ou PCoIP.
Cartes à puce	Pour les postes de travail de machine virtuelle mono-utilisateur, cette fonctionnalité requiert View Agent 6.0.2 ou version ultérieure. Pour les postes de travail basés sur une session fournis par des hôtes RDS, cette fonctionnalité requiert View Agent 6.1 ou version ultérieure.
Redirection de lecteur client	View Agent 6.1.1 ou version ultérieure.

Remarque Vous pouvez également utiliser Horizon Client pour accéder en toute sécurité aux applications Windows distantes, en plus des postes de travail distants. La sélection d'une application dans Horizon Client ouvre une fenêtre pour cette application sur le périphérique client local et l'application se présente et se comporte comme si elle était installée localement.

Vous ne pouvez utiliser des applications distantes que si vous êtes connecté à un Serveur de connexion 6.0 ou version ultérieure. Pour plus d'informations concernant les systèmes d'exploitation pris en charge pour l'hôte RDS (session Bureau à distance) qui fournit les applications distantes et les postes de travail basés sur une session, consultez la rubrique « Systèmes d'exploitation pris en charge par Horizon Agent » dans la documentation d'installation de View 5.x ou 6.x. Consultez la rubrique « Systèmes d'exploitation pris en charge pour Horizon Agent » dans la documentation d'installation d'Horizon 7.

Remarque Les fonctions disponibles pour chaque périphérique de client léger sont déterminées par le fournisseur, le modèle et la configuration qu'une entreprise choisit d'utiliser. Pour plus d'informations sur les fournisseurs et les modèles de périphériques de client léger, consultez le *Guide de compatibilité de VMware* sur http://www.vmware.com/resources/compatibility/search.php?deviceCategory=vdm.

Pour une description de ces fonctionnalités et de leurs limites, consultez le document *Planification de View*.

Fonctions prises en charge pour les postes de travail Linux

Certains systèmes d'exploitation invités Linux sont pris en charge si vous disposez de View Agent 6.1.1 ou version ultérieure. Pour voir une liste des systèmes d'exploitation Linux pris en charge et des informations sur les fonctions prises en charge, consultez *Configuration des postes de travail Horizon 6 for Linux*, qui fait partie de la documentation d'Horizon 6, version 6.1.

Internationalisation

L'interface utilisateur et la documentation sont disponibles en anglais, allemand, français, japonais, chinois simplifié, chinois traditionnel, coréen et espagnol.

Si vous utilisez un système client Linux Ubuntu 10.4 et voulez afficher l'interface utilisateur client dans une autre langue que l'anglais, vous devez définir le système client pour utiliser un paramètre régional qui utilise le codage UTF-8.

Claviers et moniteurs

Vous pouvez utiliser plusieurs moniteurs et tous les types de claviers avec un poste de travail distant. Certains paramètres permettent d'optimiser l'expérience utilisateur.

Meilleures pratiques d'utilisation de plusieurs moniteurs

Suivez les recommandations ci-dessous pour utiliser efficacement plusieurs moniteurs avec un poste de travail distant :

- Définissez le moniteur situé en bas à l'extrême gauche en tant que moniteur principal.
- Activez Xinerama. Si vous n'activez pas Xinerama, l'affichage principal risque de ne pas être identifié correctement.
- La barre de menus s'affichera sur le moniteur situé en haut à l'extrême gauche. Par exemple, si vous disposez de deux moniteurs côte à côte et si le haut du moniteur gauche est plus bas que le haut du moniteur droit, la barre de menus s'affichera sur le moniteur droit, car ce dernier est toujours le moniteur situé en haut à l'extrême gauche.
- Vous pouvez utiliser jusqu'à 4 moniteurs si vous disposez de suffisamment de mémoire RAM vidéo.

  Pour pouvoir utiliser plus de 2 moniteurs pour afficher votre poste de travail distant sur un système client Ubuntu, vous devez correctement configurer le paramètre `kernel.shmmax`. Utilisez la formule suivante :

  max horizontal resolution X *max vertical resolution* X *max number of monitors* X 4

  Par exemple, si vous affectez manuellement au paramètre `kernel.shmmax` la valeur 65536000, vous pouvez utiliser quatre moniteurs avec la résolution d'écran 2 560 x 1 600.
- Horizon Client utilise la configuration de moniteur employée lors du démarrage d'Horizon Client. Si vous basculez un moniteur du mode Paysage au mode Portrait ou si vous connectez un moniteur supplémentaire au système client lors de l'exécution d'Horizon Client, vous devez redémarrer Horizon Client afin de pouvoir utiliser la nouvelle configuration de moniteur.

Horizon Client prend en charge les configurations de moniteur suivantes :

- Si vous utilisez 2 moniteurs, il n'est pas nécessaire que les moniteurs soient dans le même mode. Par exemple, si vous utilisez un ordinateur portable connecté à un moniteur externe, le moniteur externe peut être en mode portrait ou en mode paysage.

- Si vous disposez d'une version d'Horizon Client antérieure à la version 4.0, et si vous utilisez plus de 2 moniteurs, ils doivent être réglés sur le même mode et disposer de la même résolution d'écran. Autrement dit, si vous utilisez 3 moniteurs, les 3 moniteurs doivent être soit en mode portrait, soit en mode paysage et ils doivent tous avoir la même résolution d'écran.
- Les moniteurs peuvent être placés côte à côte, associés 2 par 2, ou empilés verticalement, seulement si vous utilisez 2 moniteurs.
- Si vous spécifiez que vous souhaitez utiliser tous les moniteurs et si vous utilisez le protocole d'affichage VMware Blast ou PCoIP, vous pouvez spécifier un sous-ensemble de moniteurs adjacents à utiliser en cliquant avec le bouton droit sur le poste de travail dans la fenêtre de sélection de poste de travail, en sélectionnant **Plein écran - Tous les moniteurs** dans la liste déroulante **Affichage**, puis en cliquant sur les moniteurs que vous souhaitez utiliser.

Remarque Si vous disposez d'un système client Ubuntu, vous devez sélectionner le moniteur situé le plus à gauche de la partie supérieure comme l'un des moniteurs. Par exemple, si vous avez 4 moniteurs répartis deux par deux, vous devez sélectionner soit les deux moniteurs situés en haut, soit les deux moniteurs situés à gauche.

Résolution de l'écran

Suivez les instructions ci-dessous pour définir les résolutions d'écran :

- Si vous ouvrez un poste de travail distant sur un moniteur secondaire, puis changez la résolution d'écran sur ce moniteur, le poste de travail distant utilise le moniteur principal.
- Avec PCoIP, si vous utilisez deux moniteurs, vous pouvez régler la résolution de chacun d'eux séparément, avec une résolution pouvant aller jusqu'à 2 560 x 1 600 par affichage. Si vous utilisez plus de 2 moniteurs, les moniteurs doivent avoir la même résolution d'écran.
- Avec le protocole d'affichage VMware Blast ou PCoIP, la résolution d'écran de poste de travail distant de 4K (3 840 x 2 160) est prise en charge. Le nombre d'écrans 4K pris en charge dépend de la version matérielle de la machine virtuelle de poste de travail et de la version de Windows.

Version du matériel	Version Windows	Nombre d'écrans 4K pris en charge
10 (compatible avec ESXi 5.5.x)	7, 8, 8.x, 10	1
11 (compatible avec ESXi 6.0)	7 (fonction de rendu 3D désactivée et Windows Aero désactivé)	3
11	7 (fonction de rendu 3D activée)	1
11	8, 8.x, 10	1

View Agent 6.2 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure, doit être installé sur le poste de travail distant. Pour de meilleures performances, la machine virtuelle doit disposer d'au moins 2 Go de RAM et de 2 vCPU. Cette fonction peut nécessiter de bonnes conditions de réseau, telles qu'une bande passante de 1 000 Mbit/s avec une faible latence du réseau et un taux de perte de paquets réduit.

Remarque Lorsque la résolution d'écran de poste de travail distant est définie sur 3 840 x 2 160 (4K), les éléments sur l'écran peuvent sembler plus petits, et il peut vous être impossible d'utiliser la boîte de dialogue Résolution d'écran sur le poste de travail distant pour agrandir le texte et les autres éléments.

- Avec RDP si vous disposez de plusieurs moniteurs, vous ne pouvez pas régler la résolution de chaque moniteur séparément.

Limitations de clavier

En règle générale, les claviers fonctionnent aussi bien avec un poste de travail distant qu'avec un ordinateur physique. Vous trouverez ci-dessous la liste des limitations auxquelles vous pouvez être confronté en fonction des types des périphériques et des logiciels sur le système client :

- Si vous utilisez le protocole d'affichage PCoIP et si vous voulez que le poste de travail distant détecte le mappage de clavier utilisé par votre système client, par exemple, un clavier japonais ou allemand, vous devez définir un objet de stratégie de groupe (GPO) dans View Agent. Utilisez la stratégie **Activer la synchronisation des langues de saisie par défaut PCoIP de l'utilisateur** disponible dans le fichier de modèle View PCoIP Session Variables ADM. Pour plus d'informations, reportez-vous au document *Configuration de pools de postes de travail et d'applications dans View* .
- Certaines touches multimédia sur un clavier multimédia peuvent ne pas fonctionner. Par exemple, la touche Musique et Poste de travail peuvent ne pas fonctionner.
- Si vous vous connectez à un poste de travail utilisant RDP, utilisez le gestionnaire de fenêtres Fluxbox et avez activé un écran de veille sur le poste de travail distant, le clavier peut ne pas fonctionner après une période d'inactivité.

  Quel que soit le gestionnaire de fenêtres que vous utilisez, VMware vous recommande de désactiver l'écran de veille sur un poste de travail distant et de ne pas définir de minuteur de mise en veille.

Connecter des périphériques USB

Vous pouvez accéder à des périphériques USB connectés localement, tels que des lecteurs USB, des appareils photo et des imprimantes, à partir d'un poste de travail distant. Cette fonctionnalité est appelée redirection USB.

Avec cette fonctionnalité, la plupart des périphériques USB connectés au système client local sont disponibles à partir d'un menu d'Horizon Client. Vous pouvez utiliser le menu pour connecter et déconnecter les périphériques.

L'utilisation de périphériques USB avec des postes de travail distants est soumise aux limitations suivantes :

- Lorsque vous accédez à un périphérique USB à partir d'un menu d'Horizon Client et que vous utilisez le périphérique dans un poste de travail distant, vous ne pouvez pas accéder au périphérique sur l'ordinateur local.
- Les périphériques USB qui ne sont pas affichés dans le menu, mais qui sont disponibles dans un poste de travail distant, incluent des périphériques d'interface humaine, tels que des claviers et des dispositifs de pointage. Le poste de travail distant et l'ordinateur local utilisent ces périphériques en même temps. L'interaction avec ces périphériques peut parfois être lente à cause de la latence du réseau.
- Des lecteurs de disques USB de taille importante peuvent nécessiter plusieurs minutes avant d'apparaître sur le poste de travail.
- Certains périphériques USB requièrent des pilotes spécifiques. Si un pilote requis n'est pas déjà installé sur un poste de travail distant, vous pouvez être invité à l'installer lorsque vous connectez le périphérique USB au poste de travail distant.
- Si vous prévoyez d'ajouter des périphériques USB qui utilisent des pilotes MTP, tels que des smartphones et des tablettes Samsung fonctionnant sous Android, vous devez configurer Horizon Client afin qu'il connecte automatiquement des périphériques USB à votre poste de travail distant. Dans le cas contraire, si vous tentez de rediriger manuellement le périphérique USB à l'aide d'un élément de menu, le périphérique ne sera pas redirigé, sauf si vous le débranchez avant de le brancher de nouveau.

- Les webcams ne sont pas prises en charge pour la redirection USB via le menu **Connecter le périphérique USB**. Pour utiliser une webcam ou un périphérique d'entrée audio, vous devez utiliser la fonctionnalité Audio/Vidéo en temps réel. Cette fonctionnalité est disponible quand elle est utilisée avec View 5.2 Feature Pack 2 ou version ultérieure. Reportez-vous à la section « Utilisation de la fonctionnalité Audio/Vidéo en temps réel pour webcams et microphones », page 69.
- La redirection de périphériques audio USB dépend de l'état du réseau et n'est pas fiable. Certains périphériques requièrent un débit de données élevé même lorsqu'ils sont inactifs. Si vous disposez de la fonctionnalité Audio/Vidéo en temps réel intégrée à View 5.2 Feature Pack 2 ou version ultérieure, les périphériques d'entrée/sortie audio fonctionneront correctement et vous n'aurez pas besoin d'utiliser la redirection USB pour ces périphériques.

Vous pouvez connecter des périphériques USB à un poste de travail distant manuellement ou automatiquement.

Remarque Ne redirigez pas des périphériques USB, tels que les périphériques Ethernet USB et les périphériques à écran tactile, vers le poste de travail distant. Si vous redirigez un périphérique Ethernet USB, votre système client perdra la connectivité réseau. Si vous redirigez un périphérique à écran tactile, le poste de travail distant recevra une entrée tactile mais pas une entrée de clavier. Si vous avez défini votre poste de travail virtuel afin de connecter automatiquement des périphériques USB, vous pouvez configurer une stratégie pour exclure des périphériques spécifiques. Reportez-vous à la rubrique « Configurer les paramètres de stratégie de filtre pour les périphériques USB » dans le document *Configuration des pools de postes de travail et d'applications dans View*.

Important Cette procédure décrit comment utiliser le menu d'Horizon Client pour connecter des périphériques USB et configurer la connexion automatique des périphériques USB. Vous pouvez également configurer la redirection USB en utilisant un fichier de configuration ou en créant une stratégie de groupe. Pour plus d'informations sur l'utilisation d'un fichier de configuration, consultez « Configuration système requise pour la redirection USB », page 81. Pour plus d'informations sur la création de stratégies de groupe, reportez-vous au document *Configuration des pools de postes de travail et d'applications dans View*.

Prérequis

- Pour utiliser des périphériques USB avec un poste de travail distant, l'administrateur View doit avoir activé la fonctionnalité USB pour le poste de travail distant.

  Cette tâche inclut l'installation du composant **Redirection USB** de l'agent, et peut inclure la configuration de stratégies concernant la redirection USB. Pour plus d'informations, consultez le document *Administration de View* si vous utilisez un Serveur de connexion et Agent 5.3.x. Consultez *Configuration des pools de postes de travail et d'applications dans View* si vous utilisez un Serveur de connexion et Agent 6.0 ou version ultérieure.
- Lors de l'installation d'Horizon Client, le composant **Redirection USB** doit avoir été installé. Si vous n'avez pas inclus ce composant dans l'installation, désinstallez le client et exécutez de nouveau le programme d'installation pour inclure le composant **Redirection USB**.

Procédure

- Connectez et déconnectez manuellement un périphérique USB.

  a Dans la barre de menus Horizon Client, cliquez sur **Connecter le périphérique USB**.

  b Sélectionnez ou désélectionnez le périphérique USB.
- Dans le menu **Connecter le périphérique USB**, sélectionnez ou désélectionnez **Connexion automatique au démarrage** pour configurer la connexion des périphériques USB lors du démarrage d'Horizon Client.

  Cette option est sélectionnée par défaut.

- Dans le menu **Connecter le périphérique USB**, sélectionnez ou désélectionnez **Connexion automatique lors de l'insertion** pour configurer la connexion d'un périphérique USB lorsque vous l'insérez dans le système client.

  Activez cette option si vous prévoyez de connecter des périphériques qui utilisent des pilotes MTP, tels que les smartphones et tablettes Samsung fonctionnant sous Android. Cette option est sélectionnée par défaut.

Vous pouvez également configurer la connexion automatique de périphériques USB à l'aide des options `view.usbAutoConnectAtStartup` et `view.usbAutoConnectOnInsert` du fichier de configuration. Pour plus d'informations, consultez « Paramètres de configuration et options de ligne de commande d'Horizon Client », page 29.

Si le périphérique USB n'apparaît pas sur le poste de travail après plusieurs minutes, déconnectez, puis reconnectez le périphérique à l'ordinateur client.

Suivant

Si vous rencontrez des problèmes avec la redirection USB, consultez la rubrique sur la résolution de problèmes de redirection USB dans le document *Configuration des pools de postes de travail et d'applications dans View*.

Utilisation de la fonctionnalité Audio/Vidéo en temps réel pour webcams et microphones

La fonctionnalité Audio/vidéo en temps réel vous permet d'utiliser une webcam ou un microphone de votre ordinateur local sur votre poste de travail distant. L'Audio/Vidéo en temps réel est compatible avec les applications de conférence standard et les applications vidéo basées sur navigateur, et prend en charge les webcams, les périphériques audio USB standard et l'entrée audio analogique.

Pour plus d'informations sur la configuration de la fonction Audio/Vidéo en temps réel, de la fréquence et de la résolution d'image sur un poste de travail distant, consultez le document *Installation et administration de VMware Horizon View Feature Pack* (pour les postes de travail View 5.3.x) ou le document *Configuration de pools de postes de travail et d'applications dans View* (pour les postes de travail Horizon 6.0 avec View et versions ultérieures). Pour plus d'informations sur la configuration des paramètres sur les systèmes clients, consultez l'article de la base de connaissances VMware *Configuration de la fréquence et de la résolution d'images pour l'Audio/Vidéo en temps réel sur les clients Horizon View*, à l'adresse http://kb.vmware.com/kb/2053644.

Pour télécharger une application de test qui vérifie l'installation et le fonctionnement de la fonctionnalité Audio/Vidéo en temps réel, accédez à http://labs.vmware.com/flings/real-time-audio-video-test-application. Cette application de test est disponible sous la forme d'un « fling » VMware et ne bénéficie donc d'aucun support technique.

Remarque Cette fonctionnalité est disponible uniquement avec la version d'Horizon Client pour Linux fournie par des fournisseurs tiers ou avec le logiciel Horizon Client disponible sur le site Web des téléchargements de produits VMware.

Conditions d'utilisation de votre Webcam

Vous pouvez utiliser sur votre poste de travail une webcam intégrée ou connectée à votre ordinateur local si un administrateur View a configuré la fonctionnalité Audio/vidéo en temps réel et si le protocole d'affichage VMware Blast ou PCoIP est utilisé. Vous pouvez utiliser la webcam dans les applications de conférences telles que Skype, Webex ou Google Hangouts.

Lors de l'installation d'une application telle que Skype, Webex ou Google Hangouts sur votre poste de travail distant, vous pouvez choisir des périphériques d'entrée et de sortie dans les menus de l'application. Pour les postes de travail de machine virtuelle, vous pouvez choisir Microphone virtuel VMware et Webcam virtuelle VMware. Pour les postes de travail RDS, vous pouvez choisir Périphérique audio distant et Webcam virtuelle VMware.

Cette fonction marche avec plusieurs applications, et la sélection d'un périphérique d'entrée ne sera pas nécessaire.

Si la webcam est utilisée par votre ordinateur local, elle ne peut pas être utilisée simultanément par le poste de travail distant. De même, si la webcam est utilisée par le poste de travail distant, elle ne peut pas être utilisée par votre ordinateur local en même temps.

Important Si vous utilisez une webcam USB, votre administrateur ne doit pas configurer le client pour une transmission automatique des périphériques via la redirection USB. La connexion de la webcam via la redirection USB dégrade les performances des conversations vidéo.

Si plusieurs webcams sont connectées à votre ordinateur local, vous pouvez configurer une webcam préférée à utiliser sur votre poste de travail distant.

Sélectionner un microphone par défaut sur un système client Linux

Si plusieurs microphones sont connectés à votre système client, un seul d'entre eux peut être utilisé sur votre poste de travail View. Pour spécifier le microphone par défaut, vous pouvez utiliser le contrôle du son de votre système client.

Avec la fonctionnalité Audio/Vidéo en temps réel, les périphériques d'entrée audio et les périphériques de sortie audio fonctionnent sans qu'il soit nécessaire d'utiliser la redirection USB, et la bande passante réseau nécessaire est considérablement réduite. Les périphériques d'entrée audio analogique sont également pris en charge.

Cette procédure explique comment sélectionner un microphone par défaut depuis l'interface utilisateur du système client. Les administrateurs peuvent également configurer un microphone préféré en modifiant un fichier de configuration. Reportez-vous à la section « Sélectionner une webcam ou un microphone préféré sur un système client Linux », page 71.

Prérequis

- Assure-vous que vous disposez d'un microphone USB ou un autre type installé et opérationnel sur votre système client.
- Vérifiez que vous utilisez le protocole d'affichage VMware Blast ou PCoIP pour votre poste de travail distant.

Procédure

1. Dans l'interface graphique Ubuntu, sélectionnez **Système > Préférences > Son**.

   Vous pouvez également cliquer sur l'icône **Son** à droite de la barre d'outils en haut de l'écran.
2. Cliquez sur l'onglet **Entrée** dans la boîte de dialogue Préférences de son.
3. Sélectionnez le périphérique préféré et cliquez sur **Fermer**.

Sélectionner une webcam ou un microphone préféré sur un système client Linux

Avec la fonctionnalité Audio/Vidéo en temps réel, si vous disposez de plusieurs webcams et microphones sur votre système client, vous ne pouvez en utiliser qu'un seul sur votre poste de travail View. Pour désigner la webcam et le microphone préférés, vous pouvez modifier un fichier de configuration.

Selon sa disponibilité, la webcam ou le microphone préféré est utilisé sur le poste de travail distant ; sinon, une autre webcam ou un autre microphone sera utilisé.

Avec la fonctionnalité Audio/Vidéo en temps réel, les webcams, les périphériques d'entrée audio et les périphériques de sortie audio fonctionnent sans nécessiter l'utilisation de la redirection USB, et la bande passante du réseau nécessaire est considérablement réduite. Les périphériques d'entrée audio analogique sont également pris en charge.

Pour définir les propriétés dans le fichier `/etc/vmware/config` et indiquer un périphérique préféré, vous devez déterminer les valeurs de certains champs. Vous pouvez rechercher dans le fichier journal les valeurs de ces champs.

- Pour les webcams, vous définissez la propriété `rtav.srcWCamId` sur la valeur du champ `UserId` pour la webcam et la propriété `rtav.srcWCamName` sur la valeur du champ `Name` pour la webcam.

  La propriété `rtav.srcWCamName` a une priorité plus élevée que la propriété `rtav.srcWCamId`. Les deux propriétés doivent spécifier la même webcam. Si les propriétés spécifient des webcams différentes, la webcam spécifiée par `rtav.srcWCamName` est utilisée, si elle existe. Si elle n'existe pas, la webcam spécifiée par `rtav.srcWCamId` est utilisée. Si les deux webcams sont introuvables, la webcam par défaut est utilisée.

- Pour les périphériques audio, affectez à la propriété `rtav.srcAudioInId` la valeur du champ Pulse Audio `device.description`.

Prérequis

Selon que vous configurez une webcam préférée, un micro préféré ou les deux, exécutez les tâches préalables appropriées :

- Assurez-vous qu'une webcam USB est installée et opérationnelle sur votre système client.
- Assure-vous que vous disposez d'un microphone USB ou un autre type installé et opérationnel sur votre système client.
- Vérifiez que vous utilisez le protocole d'affichage VMware Blast ou PCoIP pour votre poste de travail distant.

Procédure

1 Lancez le client et démarrez une application de webcam ou de microphone pour déclencher une énumération de périphériques vidéo ou audio dans le journal client.

   a Connectez la webcam ou le périphérique audio que vous souhaitez utiliser.

   b Utilisez la commande `vmware-view` pour démarrer Horizon Client.

   c Démarrez un appel, puis arrêtez-le.

   Ce processus crée un fichier journal.

2 Recherchez les entrées relatives à la webcam ou au microphone.

a Ouvrez le fichier journal de débogage avec un éditeur de texte.

Le fichier journal contenant les messages de journal audio-vidéo en temps réel se trouve dans `/tmp/vmware-<username>/vmware-RTAV-<pid>.log`. Le journal client se trouve dans `/tmp/vmware-<username>/vmware-view-<pid>.log`.

b Recherchez dans le fichier journal les entrées qui renvoient aux webcams et aux microphones raccordés.

L'exemple suivant montre un extrait de la sélection de webcams :

```
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - 3 Device(s) found
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=UVC Camera (046d:
0819)   UserId=UVC Camera (046d:0819)#/sys/devices/pci0000:00/0000:00:1a.
7/usb1/1-3/1-3.4/1-3.4.5   SystemId=/dev/video1
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=gspca main driver
UserId=gspca main driver#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.4/1-3.4.7
SystemId=/dev/video2
main| I120: RTAV: static void VideoInputBase::LogDevEnum() -
Name=Microsoft® LifeCam HD-6000 for Notebooks   UserId=Microsoft® LifeCam HD-6000 for
Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6   SystemId=/dev/video0
main| W110: RTAV: static bool AudioCaptureLin::EnumCaptureDevices(MMDev::DeviceList&) -
enumeration data unavailable
```

L'exemple suivant montre un extrait de la sélection de périphériques audio et le niveau sonore actuel de chacun d'entre eux :

```
vthread-18| I120: RTAV: bool AudioCaptureLin::TriggerEnumDevices() - Triggering
enumeration
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - PulseAudio Get Source (idx=1 'alsa_output.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-stereo.monitor' 'Monitor of Logitech USB
Headset Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - channel:0 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - channel:1 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - PulseAudio Get Source (idx=2 'alsa_input.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-mono' 'Logitech USB Headset Analog Mono')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - channel:0 vol:98304
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - PulseAudio Get Source (idx=3 'alsa_output.usb-
Microsoft_Microsoft_LifeChat_LX-6000-00-LX6000.analog-stereo.monitor' 'Monitor of
Microsoft LifeChat LX-6000 Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - channel:0 vol:65536
```

Des avertissements s'affichent si l'un des niveaux sonores source du périphérique sélectionné ne respecte pas les critères PulseAudio lorsque la source n'est pas définie à 100 % (0 dB) ou si le périphérique source sélectionné est muet :

```
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel volume: 0:  67%
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel is muted
```

3 Copiez la description du périphérique et utilisez-la pour définir la propriété appropriée dans le fichier `/etc/vmware/config`.

Comme exemple de webcam, copiez `Microsoft® LifeCam HD-6000 for Notebooks` et `Microsoft® LifeCam HD-6000 for Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6` pour spécifier la webcam Microsoft comme webcam préférée et définissez les propriétés comme suit :

```
rtav.srcWCamName = "Microsoft® LifeCam HD-6000 for Notebooks"
rtav.srcWCamId = "Microsoft® LifeCam HD-6000 for
Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6"
```

Dans cet exemple, vous pourriez aussi définir la propriété `rtav.srcWCamId` sur `"Microsoft"`. La propriété `rtav.srcWCamId` prend en charge les correspondances partielles et exactes. La propriété `rtav.srcWCamName` ne prend en charge qu'une correspondance exacte.

Pour un exemple de périphérique audio, copiez `Logitech USB Headset Analog Mono` pour désigner le casque Logitech comme périphérique audio préféré et définissez la propriété comme suit :

```
rtav.srcAudioInId="Logitech USB Headset Analog Mono"
```

4 Enregistrez les modifications et fermez le fichier de configuration `/etc/vmware/config`.

5 Fermez la session du poste de travail et démarrez une nouvelle session.

Enregistrement de documents dans une application distante

Vous pouvez créer et enregistrer des documents avec certaines applications distantes, telles que Microsoft Word ou WordPad. L'emplacement dans lequel vous enregistrez ces documents dépend de l'environnement réseau de votre société. Par exemple, vos documents peuvent être enregistrés sur un partage d'accueil de votre ordinateur local.

Les administrateurs peuvent utiliser un fichier de modèle ADMX pour définir une stratégie de groupe qui spécifie à quel endroit les documents sont enregistrés. Cette stratégie se nomme « Définir le répertoire de base de l'utilisateur des services Bureau à distance ». Pour plus d'informations, consultez la rubrique « Paramètres des profils RDS » dans le document *Configuration de pools de postes de travail et d'applications dans View* .

Définir les préférences d'impression pour la fonction d'impression virtuelle sur un poste de travail distant

La fonction d'impression virtuelle permet aux utilisateurs finaux d'utiliser des imprimantes locales ou réseau à partir d'un poste de travail distant sans avoir à installer de pilotes d'imprimante supplémentaires sur ce dernier. Pour chaque imprimante disponible via cette fonction, vous pouvez définir des préférences pour la compression des données, la qualité d'impression, l'impression recto verso, la couleur, etc.

Important La fonctionnalité d'impression virtuelle n'est disponible qu'avec Horizon Client 3.2 ou version ultérieure, disponible sur le site Web de téléchargement de produits VMware, ou avec la version d'Horizon Client pour Linux fournie par des fournisseurs tiers.

Cette fonction a également les exigences suivantes :

- View Agent 6.0.2 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure, doit être installé sur le poste de travail distant.
- Vous devez utiliser le protocole d'affichage VMware Blast ou PCoIP.

Pour plus d'informations sur les partenaires client léger et zéro de VMware, consultez le *Guide de compatibilité VMware* à l'adresse http://www.vmware.com/resources/compatibility/search.php?deviceCategory=vdm. Pour le logiciel client fourni par des fournisseurs tiers, vous devez utiliser le protocole d'affichage VMware Blast, PCoIP ou FreeRDP. Cette fonction n'est pas opérationnelle avec rdesktop.

Après l'ajout d'une imprimante sur l'ordinateur local, Horizon Client l'ajoute à la liste des imprimantes disponibles sur le poste de travail distant. Aucune configuration supplémentaire n'est requise. Les utilisateurs qui disposent des privilèges d'administrateur peuvent toujours installer des pilotes d'imprimante sur le poste de travail distant sans créer de conflit avec le composant d'impression virtuelle.

Important Cette fonction n'est pas disponible pour les types d'imprimantes suivants :

- Les imprimantes USB qui utilisent la fonction de redirection USB pour se connecter à un port USB virtuel dans le poste de travail distant.

  Dans ce cas, vous devez déconnecter l'imprimante USB du poste de travail distant pour utiliser la fonction d'impression virtuelle avec celle-ci.

- La fonction Windows pour imprimer vers un fichier.

  Il n'est pas possible de cocher la case **Print to file (Imprimer vers fichier)** dans une boîte de dialogue Print (Impression). Il est possible d'utiliser un pilote d'imprimante qui crée un fichier. Par exemple, vous pouvez utiliser un logiciel de création de PDF pour imprimer vers un fichier PDF.

Cette procédure concerne un poste de travail distant disposant d'un système d'exploitation Windows 7 ou Windows 8.x (de bureau). La procédure est similaire mais n'est pas identique pour Windows Server 2008 et Windows Server 2012.

Prérequis

Vérifiez que le composant d'impression virtuelle de l'agent est installé sur le poste de travail distant. Dans le système de fichiers du poste de travail distant, assurez-vous que le dossier suivant existe : `C:\Program Files\Common Files\ThinPrint`.

Pour utiliser l'impression virtuelle, l'administrateur View doit avoir activé la fonctionnalité d'impression virtuelle pour le poste de travail distant. Cette tâche inclut l'activation de l'option d'installation de l'impression virtuelle dans le programme d'installation de l'agent, et peut inclure la configuration de stratégies concernant le comportement de l'impression virtuelle. Pour plus d'informations, consultez le document *Administration de View* si vous utilisez un Serveur de connexion et View Agent 5.x ou version antérieure. Consultez *Configuration des pools de postes de travail et d'applications dans View* si vous utilisez Horizon 6 ou version ultérieure.

Procédure

1 Dans le poste de travail distant Windows 7 ou Windows 8.x, cliquez sur **Démarrer > Périphériques et imprimantes**.

2 Dans la fenêtre Périphériques et imprimantes, cliquez avec le bouton droit sur l'imprimante par défaut, sélectionnez **Propriétés de l'imprimante** dans le menu contextuel et choisissez l'imprimante.

   Les imprimantes virtuelles apparaissent sous la forme *<printer_name>* dans les postes de travail de machine virtuelle mono-utilisateur et sous la forme *<printer_name>(s<session_ID>)* dans les postes de travail basés sur une session sur des hôtes RDS si View Agent 6.2 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure, est installé. Si View Agent 6.1 ou version antérieure est installé sur le poste de travail distant, les imprimantes virtuelles apparaissent sous la forme *<printer_name>#:<number>*.

3 Dans la fenêtre Propriétés de l'imprimante, cliquez sur l'onglet **Installation du périphérique** et spécifiez les paramètres à utiliser.

4 Dans l'onglet **Général**, cliquez sur **Préférences**, puis spécifiez les paramètres à utiliser.

5 Dans la boîte de dialogue Options d'impression, sélectionnez les différents onglets et précisez les paramètres à utiliser.

   Pour les paramètres avancés **Mise en page**, VMware recommande de conserver ceux par défaut.

6 Cliquez sur **OK**.

Copier et coller du texte

Il est possible de copier du texte sur et depuis des applications et des postes de travail distants. Votre administrateur View peut définir cette fonctionnalité pour que les opérations copier et coller soient autorisées uniquement depuis votre système client vers une application ou un poste de travail distant ou uniquement depuis une application ou un poste de travail distant vers votre système client, ou les deux, ou aucun.

Cette fonctionnalité est disponible si vous utilisez le protocole d'affichage VMware Blast ou PCoIP. Les applications distantes sont prises en charge avec Horizon 6.0 ou version ultérieure.

Les administrateurs configurent la fonctionnalité de copier-coller à l'aide d'objets de stratégie de groupe (GPO) qui appartiennent à View Agent ou Horizon Agent dans des postes de travail distants. Pour plus d'informations, consultez le chapitre sur la configuration de stratégies dans le document *Configuration de postes de travail et d'applications dans View*.

Vous pouvez copier du texte depuis Horizon Client sur une application ou un poste de travail distant, ou l'inverse, mais le texte collé est du texte brut.

Vous ne pouvez pas copier-coller des graphiques. Il est également impossible de copier et coller des fichiers entre un poste de travail distant et le système de fichiers de votre ordinateur client.

Configuration de la taille de la mémoire du Presse-papiers du client

Dans la version 7.0.1 et les versions ultérieures d'Horizon 7 et dans la version 4.1 et les versions ultérieures d'Horizon Client, la taille de mémoire du Presse-papiers est configurable pour le serveur et pour le client.

Lorsqu'une session PCoIP ou VMware Blast est établie, le serveur envoie la taille de la mémoire de son Presse-papiers au client. La taille de mémoire effective du Presse-papiers est la plus petite des valeurs de taille de mémoire du Presse-papiers du serveur et du client.

Pour définir la taille de la mémoire du Presse-papiers du client, ajoutez le paramètre suivant à l'un des trois fichiers de configuration : `~/.vmware/config`, `/usr/lib/vmware/config`, ou `/etc/vmware/config`.

`mksvchan.clipboardSize=`*`value`*

value correspond à la taille, en kilo-octets (Ko), de la mémoire du Presse-papiers du client. Vous pouvez spécifier une valeur maximale de 16 384 Ko. Si vous spécifiez 0 ou si vous ne spécifiez aucune valeur, la taille par défaut de la mémoire du Presse-papiers du client est de 8 192 Ko (8 Mo).

Horizon Client recherche la taille de la mémoire du Presse-papiers dans les fichiers de configuration dans l'ordre suivant et s'arrête dès qu'il trouve une valeur non nulle.

1 `~/.vmware/config`

2 `/usr/lib/vmware/config`

3 `/etc/vmware/config`

En fonction de votre réseau, une taille importante de la mémoire du Presse-papiers peut avoir un impact négatif sur les performances. VMware recommande de ne pas définir la taille de la mémoire du Presse-papiers à une valeur supérieure à 16 Mo.

Résolution des problèmes d' Horizon Client 5

La plupart des problèmes liés à Horizon Client peuvent être résolus en réinitialisant le poste de travail ou en réinstallant l'application VMware Horizon Client.

Ce chapitre aborde les rubriques suivantes :

Problèmes avec la saisie au clavier

Lorsque vous tapez dans une application ou un poste de travail distant, si aucune des séquences de touches ne semble fonctionner, le problème peut provenir du logiciel de sécurité sur votre système client local.

Problème

Quand vous êtes connecté à une application ou un poste de travail distant, aucun caractère ne s'affiche lorsque vous tapez. Vous pouvez également remarquer qu'une seule touche se répète sans cesse.

Cause

Certains logiciels de sécurité, tels que Norton 360 Total Security, incluent une fonction qui détecte les programmes enregistreurs de frappe et bloque la journalisation des séquences de touches. Cette fonction de sécurité permet de protéger le système contre les logiciels espions indésirables qui, par exemple, volent les mots de passe et les numéros de carte de crédit. Malheureusement, ce logiciel de sécurité peut empêcher Horizon Client d'envoyer des séquences de touches à l'application ou au poste de travail distant.

Solution

- Sur le système client, désactivez la fonction de détection des enregistreurs de frappe de votre antivirus ou de votre logiciel de sécurité.

Réinitialiser une application ou un poste de travail distant

Vous devrez peut-être réinitialiser un poste de travail ou une application si le système d'exploitation de l'application ou du poste de travail cesse de répondre. La réinitialisation d'un poste de travail distant arrête et redémarre le poste de travail. La réinitialisation de vos applications distantes arrête les applications. Les données non enregistrées sont perdues.

La réinitialisation d'un poste de travail distant équivaut à appuyer sur le bouton Réinitialiser d'un ordinateur physique pour le forcer à redémarrer. Tous les fichiers ouverts sur le poste de travail distant seront fermés sans être enregistrés.

La réinitialisation d'applications équivaut à quitter toutes les applications distantes sans enregistrer les données non enregistrées. Toutes les applications ouvertes sont fermées, même si les applications proviennent de batteries de serveurs RDS différentes.

Vous pouvez réinitialiser un poste de travail distant uniquement si votre administrateur a activé cette fonction.

Procédure

- Utilisez la commande **Réinitialiser**.

Option	Action
Réinitialiser un poste de travail distant à partir du poste de travail	Sélectionnez **Connexion > Réinitialiser** dans la barre de menus.
Réinitialiser un poste de travail distant depuis la fenêtre de sélection des postes de travail et applications	Sélectionnez le poste de travail distant et sélectionnez **Connexion > Réinitialiser** dans la barre de menus.
Réinitialiser des applications distantes depuis la fenêtre de sélection des postes de travail et applications	Cliquez sur le bouton **Paramètres** (icône engrenage) dans le coin supérieur droit de la fenêtre, sélectionnez **Applications** dans le volet de gauche, cliquez sur **Réinitialiser**, puis sur **Continuer**.

Pour un poste de travail distant, le système d'exploitation du poste de travail distant est redémarré. Le client se déconnecte du poste de travail. En ce qui concerne les applications distantes, celles-ci sont fermées.

Suivant

Il convient d'observer un temps d'attente suffisant pour le démarrage du système avant de tenter de se connecter au poste de travail distant.

Désinstaller Horizon Client pour Linux

Vous pouvez parfois résoudre des problèmes liés à Horizon Client en désinstallant et en réinstallant l'application Horizon Client.

La méthode que vous utilisez pour désinstaller Horizon Client pour Linux dépend de la version et de la méthode que vous avez utilisées pour installer le logiciel client.

Prérequis

Vérifiez que vous avez un accès root sur le système client Linux.

Procédure

- Si vous avez Horizon Client 3.1 ou une version antérieure, ou si vous avez installé le client à partir du centre logiciel Ubuntu, sélectionnez **Applications > Centre Logiciel Ubuntu**, et dans la section **Logiciel Installé**, sélectionnez **vmware-view-client** et cliquez sur **Supprimer.**
- Si vous avez Horizon Client 3.2 ou une version ultérieure, que vous avez installée à partir du site Web des téléchargements de produit VMware, ouvrez une fenêtre de terminal, modifiez les répertoires vers le répertoire qui contient le fichier du programme d'installation, et exécutez la commande d'installation avec l'option –u.

```
sudo env VMWARE_KEEP_CONFIG=yes \

./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle -u vmware-horizon-client
```

Dans le nom de fichier, *x.x.x* est le numéro de version, *yyyyyyy* est le numéro de build et *arch* est `x86` ou `x64`. Utiliser le paramètre `VMWARE_KEEP_CONFIG=yes` signifie conserver les paramètres de configuration lorsque le client est désinstallé. Si cette variable d'environnement n'est pas définie, vous êtes invité à spécifier si vous souhaitez enregistrer les paramètres de configuration.

Suivant

Vous pouvez réinstaller le client ou installer une nouvelle version. Reportez-vous à la section « Installer ou mettre à niveau Horizon Client pour Linux depuis les téléchargements de produits VMware », page 16.

Configuration de la redirection USB sur le client

6

Avec la fonctionnalité de redirection USB, vous pouvez utiliser un fichier de configuration sur le système client pour spécifier quels périphériques USB peuvent être redirigés vers un poste de travail distant.

Par exemple, vous pouvez limiter les types de périphériques USB qu'Horizon Client rend disponibles pour la redirection, configurer View Agent pour qu'il empêche le transfert de certains périphériques USB depuis un ordinateur client et spécifier si Horizon Client doit diviser des périphériques USB composites en composants séparés pour la redirection.

Ce chapitre aborde les rubriques suivantes :

Configuration système requise pour la redirection USB

La fonctionnalité de redirection USB n'est disponible que pour certaines versions du logiciel client.

Pour les logiciels Horizon Client fournis par des fournisseurs tiers, la configuration requise pour la fonctionnalité de redirection USB comprend les exigences suivantes :

- La version de View Agent et du Serveur de connexion View doit être View 5.1 ou ultérieure.
- Les fonctionnalités de filtre USB et de fractionnement de périphérique décrites dans ce document sont disponibles avec le Serveur de connexion View 5.1 et versions ultérieures.

Pour plus d'informations sur les partenaires de clients légers et de clients zéro de VMware, consultez le guide VMware Compatibility Guide (Guide de compatibilité VMware). Pour utiliser les composants USB disponibles pour des fournisseurs tiers, certains fichiers doivent être installés dans certains emplacements et certains processus doivent être configurés pour démarrer avant le lancement d'Horizon Client. Ces détails n'entrent pas dans le cadre de ce document.

Pour Horizon Client, la fonctionnalité de redirection USB présente les exigences suivantes :

- View Agent 6.0.2 ou version ultérieure doit être installé sur le poste de travail à distance.
- Vous devez utiliser le protocole d'affichage VMware Blast ou PCoIP.

Si vous utilisez Horizon 6.0.1 et version ultérieure, vous pouvez connecter des périphériques USB 3.0 à des ports USB 3.0. Les périphériques USB 3.0 sont uniquement pris en charge avec un flux unique. Comme la prise en charge multi-flux n'est pas encore mise en œuvre, les performances du périphérique USB ne sont pas améliorées. Notez que sur le système client Linux, les processeurs i386 sont pris en charge, tandis que les architectures armel et armhf ne le sont pas. La version du noyau Linux doit être 2.6.35 ou version ultérieure.

Fichiers journaux USB spécifiques

Horizon Client envoie des informations USB à des fichiers journaux.

À des fins de dépannage, vous pouvez augmenter la quantité d'informations envoyées dans des journaux USB spécifiques en utilisant les commandes suivantes :

```
vmware-usbarbitrator --verbose
```

```
vmware-view-usbd -o log:trace
```

Pour obtenir une liste d'informations sur l'utilisation, utilisez la commande suivante :

```
vmware-usbarbitrator -h
```

Définition de propriétés de configuration USB

Vous pouvez définir des propriétés de configuration USB dans les fichiers de configuration `/etc/vmware/config`, `/usr/lib/vmware/config` et `~/.vmware/config`.

Le service `vmware-view-usbd` examine ces fichiers de configuration dans l'ordre suivant :

1. `/etc/vmware/config`. Si des propriétés de configuration USB sont définies dans ce fichier, ces propriétés sont utilisées.
2. `/usr/lib/vmware/config`. Si les propriétés USB sont introuvables dans `/etc/vmware/config`, le fichier `/usr/lib/vmware/config` est vérifié.
3. `~/.vmware/config`. Si les propriétés USB sont introuvables dans les autres fichiers, le fichier `~/.vmware/config` est vérifié.

Utilisez la syntaxe suivante pour définir des propriétés de configuration USB dans les fichiers de configuration.

```
viewusb.property1 = "value1"
```

Avec les propriétés de configuration USB, vous pouvez contrôler si certains types de périphériques sont redirigés. Des propriétés de filtrage sont également disponibles pour vous permettre d'inclure ou d'exclure certains types de périphériques. Pour les clients Linux version 1.7 et ultérieure, et pour les clients Windows, des propriétés pour fractionner des périphériques composites sont également fournies.

Certaines valeurs de propriété nécessitent le VID (ID du fournisseur) et le PID (ID du produit) pour un périphérique USB. Pour connaître le VID et le PID, vous pouvez rechercher le nom du produit sur Internet, associé à `vid` et `pid`. Vous pouvez également consulter le fichier `/tmp/vmware-root/vmware-view-usbd-*.log` après avoir connecté le périphérique USB au système local lorsque Horizon Client est en cours d'exécution. Pour définir l'emplacement de ce fichier, utilisez la propriété `view-usbd.log.fileName` dans le fichier `/etc/vmware/config`, par exemple :

```
view-usbd.log.fileName = "/tmp/usbd.log"
```

Important Lors de la redirection de périphériques audio, vérifiez que la version de noyau de votre système Ubuntu est 3.2.0-27.43 ou version ultérieure. Ubuntu 12.04 inclut la version de noyau 3.2.0-27.43. Si vous ne pouvez pas effectuer la mise à niveau vers cette version de noyau, vous pouvez également désactiver l'accès de l'hôte vers le périphérique audio. Par exemple, vous pouvez ajouter la ligne « `blacklist snd-usb-audio` » à la fin du fichier `/etc/modprobe.d/blacklist.conf`. Si votre système ne respecte pas ces exigences, le système client peut se bloquer lorsque Horizon Client tente de rediriger le périphérique audio. Par défaut, les périphériques audio sont redirigés.

Le tableau suivant décrit les propriétés de configuration USB disponibles.

Tableau 6-1. Configuration des propriétés pour la redirection USB

Nom et propriété de la stratégie	Description
Autoriser le fractionnement automatique de périphérique Propriété : `viewusb.AllowAutoDeviceSplitting`	Autorise le fractionnement automatique de périphériques USB composites. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Exclude Vid/Pid Device From Split Propriété : `viewusb.SplitExcludeVidPid`	Exclut un périphérique USB composite spécifié par des ID de fournisseur et de produit du fractionnement. Le format du paramètre est `vid-`*xxx1*`_pid-`*yyy1*`[;vid-`*xxx2*`_pid-`*yyy2*`]...` Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (**`*`**) à la place de chiffres dans un ID. Par exemple : **`vid-0781_pid-55**`** La valeur par défaut n'est pas définie.
Split Vid/Pid Device Propriété : `viewusb.SplitVidPid`	Traite les composants d'un périphérique USB composite spécifiés par des ID de fournisseur et de produit en tant que périphériques séparés. Le format du paramètre est `vid-`*xxxx*`_pid-`*yyyy*`([exintf:`*zz*`[;exintf:`*ww*`]])[;...]` Vous pouvez utiliser le mot-clé `exintf` pour exclure des composants de la redirection en spécifiant leur numéro d'interface. Vous devez spécifier les numéros d'ID au format hexadécimal et les numéros d'interface au format décimal en incluant les zéros à gauche. Vous pouvez utiliser le caractère générique (**`*`**) à la place de chiffres dans un ID. Par exemple : **`vid-0781_pid-554c(exintf:01;exintf:02)`** **Remarque** Si le périphérique composite comprend des composants qui sont automatiquement exclus, tels qu'une souris ou un clavier, View n'inclut alors pas automatiquement les composants que vous n'avez pas explicitement exclus. Vous devez spécifier une règle de filtre telle que `Include Vid/Pid Device` pour inclure ces composants. La valeur par défaut n'est pas définie.
Allow Audio Input Devices Propriété : `viewusb.AllowAudioIn`	Permet la redirection de périphériques d'entrée audio. La valeur par défaut n'est pas définie, ce qui correspond à **`false`**, car la fonctionnalité Audio/Vidéo en temps réel est utilisée pour les périphériques d'entrée audio et vidéo, mais la redirection USB ne l'est pas par défaut.
Allow Audio Output Devices Propriété : `viewusb.AllowAudioOut`	Permet la redirection de périphériques de sortie audio. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.

Tableau 6-1. Configuration des propriétés pour la redirection USB (suite)

Nom et propriété de la stratégie	Description
Autoriser HID Propriété : `viewusb.AllowHID`	Autoriser la redirection des périphériques d'entrée autres que les claviers et les souris. La valeur par défaut est indéfinie, ce qui correspond à **`true`**.
Allow HIDBootable Propriété : `viewusb.AllowHIDBootable`	Permet la redirection de périphériques d'entrée autres que des claviers et des souris qui sont disponibles au démarrage (ou périphériques démarrables par HID). La valeur par défaut est indéfinie, ce qui correspond à **`true`**.
Autoriser la description de périphérique a sécurité intégrée Propriété : `viewusb.AllowDevDescFailsafe`	Autorise la redirection des périphériques même si Horizon Client ne parvient pas à obtenir les descripteurs de configuration/périphérique. Pour autoriser un périphérique même si config/desc échoue, incluez-le dans les filtres d'inclusion tels que `IncludeVidPid` ou `IncludePath`. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Allow Keyboard and Mouse Devices Propriété : `viewusb.AllowKeyboardMouse`	Permet la redirection de claviers avec périphériques de pointage intégrés (souris, Trackball ou pavé tactile). La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Allow Smart Cards Propriété : `viewusb.AllowSmartcard`	Permet la redirection de périphériques à carte à puce. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Allow Video Devices Propriété : `viewusb.AllowVideo`	Permet la redirection de périphériques vidéo. La valeur par défaut n'est pas définie, ce qui correspond à **`false`**, car la fonctionnalité Audio/Vidéo en temps réel est utilisée pour les périphériques d'entrée audio et vidéo, mais la redirection USB ne l'est pas par défaut.
Disable Remote Configuration Download Propriété : `viewusb.DisableRemoteConfig`	Désactive l'utilisation de paramètres de View Agent lors de l'exécution du filtrage de périphérique USB. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Exclude All Devices Propriété : `viewusb.ExcludeAllDevices`	Exclut 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 `Exclude All Devices` sur **`true`** sur View Agent, et si ce paramètre est transmis à Horizon Client, le paramètre de View Agent remplace celui d'Horizon Client. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Exclude Device Family Propriété : `viewusb.ExcludeFamily`	Exclut des familles de périphériques de la redirection. Le format du paramètre est *family_name_1*[`;`*family_name_2*]… Par exemple : **`bluetooth;smart-card`** Si vous avez activé le fractionnement automatique de périphérique, View 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, View examine la famille de périphérique de l'ensemble du périphérique USB composite. La valeur par défaut n'est pas définie.
Exclude Vid/Pid Device Propriété : `viewusb.ExcludeVidPid`	Exclut des périphériques avec des ID de fournisseur et de produit spécifiés de la redirection. Le format du paramètre est `vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*] … Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (**`*`**) à la place de chiffres dans un ID. Par exemple : **`vid-0781_pid-****;vid-0561_pid-554c`** La valeur par défaut n'est pas définie.

Tableau 6-1. Configuration des propriétés pour la redirection USB (suite)

Nom et propriété de la stratégie	Description
Exclude Path Propriété : `viewusb.ExcludePath`	Exclut des périphériques dans des chemins de concentrateur ou de port spécifiés de la redirection. Le format du paramètre est `bus-`*x1*`[/`*y1*`]...-port-`*z1*`[;bus-`*x2*`[/`*y2*`]...-port-`*z2*`]…` 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 : **`bus-1/2/3_port-02;bus-1/1/1/4_port-ff`** La valeur par défaut n'est pas définie.
Include Device Family Propriété : `viewusb.IncludeFamily`	Inclut des familles de périphériques pouvant être redirigées. Le format du paramètre est *family_name_1*`[;`*family_name_2*`]…` Par exemple : **`storage`** La valeur par défaut n'est pas définie.
Include Path Propriété : `viewusb.IncludePath`	Inclut des périphériques dans des chemins de concentrateur ou de port spécifiés pouvant être redirigés. Le format du paramètre est `bus-`*x1*`[/`*y1*`]...-port-`*z1*`[;bus-`*x2*`[/`*y2*`]...-port-`*z2*`]…` 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 : **`bus-1/2_port-02;bus-1/7/1/4_port-0f`** La valeur par défaut n'est pas définie.
Include Vid/Pid Device Propriété : `viewusb.IncludeVidPid`	Inclut des périphériques avec des ID de fournisseur et de produit spécifiés pouvant être redirigés. Le format du paramètre est `vid-`*xxx1*`_pid-`*yyy2*`[;vid-`*xxx2*`_pid-`*yyy2*`]…` Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (`*`) à la place de chiffres dans un ID. Par exemple : **`vid-0561_pid-554c`** La valeur par défaut n'est pas définie.

Exemples de redirection USB

Chaque exemple est suivi d'une description de l'effet sur la redirection USB.

- Inclure la plupart des périphériques dans la famille de souris.

  ```
  viewusb.IncludeFamily = "mouse"
  viewusb.ExcludeVidPid = "Vid-0461_Pid-0010;Vid-0461_Pid-4d20"
  ```

  La première propriété dans cet exemple indique à Horizon Client d'autoriser la redirection des souris vers un poste de travail View. La deuxième propriété remplace la première et indique à Horizon Client de maintenir deux souris spécifiques en mode local et de ne pas les rediriger.

- Activer le fractionnement automatique de périphérique, mais exclure un périphérique particulier du fractionnement. Pour un autre périphérique particulier, laisser un de ses composants local et rediriger les autres composants vers le poste de travail distant :

  ```
  viewusb.AllowAutoDeviceSplitting = "True"
  viewusb.SplitExcludeVidPid = "Vid-03f0_Pid-2a12"
  viewusb.SplitVidPid = "Vid-0911_Pid-149a(exintf:03)"
  viewusb.IncludeVidPid = "Vid-0911_Pid-149a"
  ```

  Les périphériques USB composites sont composés de deux périphériques ou plus, tels qu'un périphérique d'entrée vidéo et un périphérique de stockage. La première propriété de cet exemple active le fractionnement automatique des périphériques composites. La deuxième propriété exclut le périphérique USB composite spécifié (`Vid-03f0_Pid-2a12`) du fractionnement.

  La troisième ligne indique à Horizon Client de traiter les différents composants d'un autre périphérique composite (`Vid-0911_Pid-149a`) comme étant différents périphériques et d'exclure de la redirection le composant de numéro d'interface 03. Ce composant est conservé en mode local.

Du fait que ce périphérique composite inclut un composant qui est normalement exclu par défaut, tel qu'une souris ou un clavier, la quatrième ligne est nécessaire de façon à ce que les autres composants du périphérique composite `Vid-0911_Pid-149a` puissent être redirigés vers le poste de travail View.

Les trois premières propriétés sont des propriétés de fractionnement. La dernière propriété est une propriété de filtrage. Les propriétés de filtrage s'effectuent avant les propriétés de fractionnement.

Important Ces propriétés de configuration du client peuvent être fusionnées avec, ou remplacées par, des stratégies correspondantes, paramétrées pour View Agent sur le poste de travail distant. Pour plus d'informations sur le fonctionnement des propriétés de fractionnement et de filtrage USB sur le client en association avec les stratégies USB de View Agent, consultez les rubriques sur l'utilisation de stratégies pour contrôler la redirection USB dans le document *Administration de View.*

Familles de périphériques USB

Vous pouvez spécifier une famille lorsque vous créez des règles de filtrage USB pour Horizon Client ou pour View Agent ou Horizon Agent.

Remarque Certains périphériques ne lisent pas certaines familles de périphériques.

Tableau 6-2. Familles de périphériques USB

Nom de la famille de périphériques	Description
`audio`	Tout périphérique d'entrée ou de sortie audio.
`audio-in`	Périphériques d'entrée audio, tels que des microphones.
`audio-out`	Périphériques de sortie audio, tels que des haut-parleurs et des écouteurs.
`bluetooth`	Périphériques connectés par Bluetooth.
`comm`	Périphériques de communication, tels que des modems et des adaptateurs réseau filaires.
`hid`	Périphériques d'interface humaine, à l'exclusion des claviers et des pointeurs.
`hid-bootable`	Périphériques d'interface humaine disponibles au démarrage, à l'exclusion des claviers et des pointeurs.
`imaging`	Périphériques graphiques tels que des scanners.
`keyboard`	Périphérique de type clavier.
`mouse`	Périphérique de pointage tel qu'une souris.
`other`	Famille non spécifiée.
`pda`	Assistants numériques personnels.
`physical`	Périphériques à retour de force, tels que les joysticks à retour de force.
`printer`	Périphériques d'impression.
`security`	Périphériques de sécurité, tels que des lecteurs d'empreintes digitales.
`smart-card`	Périphériques à carte à puce.
`storage`	Périphériques de stockage de masse tels que des disques à mémoire flash et des disques durs externes.
`unknown`	Famille inconnue.
`vendor`	Périphériques disposant de fonctions spécifiques au fournisseur.
`video`	Périphériques d'entrée vidéo.
`wireless`	Adaptateurs réseau sans fil.
`wusb`	Périphériques USB sans fil.

Index