Utilisation de VMware Horizon View Client pour Linux

Janvier 2014

Horizon View

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-001162-03

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 View Client pour Linux

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

Ce document contient des informations quant aux configurations système requises ainsi que des instructions quant à l'installation et l'utilisation d'Horizon View Client pour Linux.

Ces informations sont conçues pour les administrateurs qui doivent configurer un déploiement d' Horizon 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 Horizon View Client pour Linux que VMware met à disposition sur Ubuntu. En outre, plusieurs partenaires VMware offrent des périphériques de client léger pour les déploiements d'Horizon View. Les fonctions disponibles pour chaque périphérique de client léger, et les systèmes d'exploitation pris en charge, sont déterminés 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 VMware Compatibility Guide (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 de View Client est semblable à l'installation de la plupart des applications.

Configuration système requise

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

Remarque Cette configuration système concerne Horizon View Client pour Linux que VMware met à disposition sur Ubuntu. En outre, plusieurs partenaires VMware offrent des périphériques de client léger pour les déploiements d'Horizon View. Les fonctions disponibles pour chaque périphérique de client léger, et les systèmes d'exploitation pris en charge, sont déterminés 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 VMware Compatibility Guide (Guide de compatibilité VMware), disponible sur le site Web de VMware.

Modèle	Ordinateur de bureau ou portable à processeur Intel
Mémoire	Au moins 2 Go de RAM
Systèmes d'exploitation	■ View Client 2.0 et versions supérieures : Ubuntu Linux 12.04 32 bits ■ View Client 1.6 et 1.7 : Ubuntu Linux 10.04 ou 12.04 32 bits ■ View Client 1.5 : Ubuntu Linux 10.04 ou 10.10 32 bits
Serveur de connexion View, serveur de sécurité et View Agent	Dernière version de maintenance de VMware View 4.6.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.
Protocole d'affichage pour Horizon View	PCoIP ou RDP **Important** Bien qu'Horizon View Client pour Linux prenne en charge le protocole d'affichage RDP, le client RDP particulier intégré à votre distribution d'Ubuntu peut ne pas fonctionner avec Horizon View Client.
Résolution d'écran sur le système client	Minimum : 1 024 X 768 pixels

Exigences matérielles pour PCoIP	■ Un processeur x86 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 :
	`20 Mo + (24 * (nb d'écrans) * (largeur d'écran) * (hauteur d'écran))`
	Comme indicateur rapide, vous pouvez utiliser les calculs suivants :
	`1 écran : 1600 x 1200 : 64 Mo`
	`2 écrans : 1600 x 1200 : 128 Mo`
	`3 écrans : 1600 x 1200 : 256 Mo`

Exigences matérielles pour RDP	■ Un processeur x86 avec extensions SSE2, avec une vitesse de processeur d'au moins 800 MHz. ■ RAM de 128 Mo.

Configuration logicielle requise pour Microsoft RDP

- Pour Ubuntu 12.04, utilisez rdesktop 1.7.0.
- Pour Ubuntu 10.04, utilisez rdesktop 1.6.0.

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 34.

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 Horizon View doit satisfaire certaines exigences matérielles et logicielles.

Poste de travail distant Horizon View

View Agent 5.2 ou version ultérieure doit être installé sur les postes de travail. La version correspondante de Remote Experience Agent doit également être installée sur les postes de travail. Par exemple, si View Agent 5.3 est installé, vous devez aussi installer Remote Experience Agent depuis Horizon View 5.3 Feature Pack 1. Consultez le document *Installation et administration de VMware Horizon View Feature Pack* pour VMware Horizon View

Logiciel Horizon View Client

Horizon View Client 2.2 pour Linux ou version ultérieure. Notez que cette fonction n'est accessible qu'avec la version d'Horizon View Client pour Linux fournie par certains partenaires.

Ordinateur Horizon View Client ou périphérique d'accès client

- L'Audio/Vidéo en temps réel est pris en charge sur les périphériques x86. Cette fonctionnalité n'est pas prise en charge par les processeurs ARM. Le processeur du système client doit avoir au moins deux cœurs.
- Horizon View Client requiert les bibliothèques suivantes :
  - `Video4Linux2`
  - `libv4l`
  - `Pulse Audio`

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

  ```
  libuuid.so.1
  libv4l2.so.0
  libspeex.so.1
  libudev.so.0
  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 View 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 View Agent est installé.
Protocole d'affichage pour Horizon View	PCoIP L'Audio/Vidéo en temps réel n'est pas pris en charge par les sessions postes de travail RDP.

Systèmes d'exploitation de poste de travail pris en charge

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

Pour obtenir la liste des systèmes d'exploitation invités, consultez la rubrique « Systèmes d'exploitation pris en charge par View Agent » dans la documentation d'installation d'Horizon View 4.6.x ou 5.x.

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.

Cette fonctionnalité est disponible lorsqu'elle est utilisée avec la version correcte de VMware Horizon View Feature Pack.

- La prise en charge de la multidiffusion requiert VMware Horizon View 5.2 Feature Pack 2 ou version ultérieure.
- La prise en charge de la monodiffusion requiert VMware Horizon View 5.3 Feature Pack 1 ou version ultérieure.

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

- Pour la prise en charge de la multidiffusion, les systèmes client doivent utiliser Horizon View Client 2.1 ou version ultérieure. Pour la prise en charge de la monodiffusion, les systèmes client doivent utiliser Horizon View Client 2.2 ou version ultérieure.

  Remarque Cette fonctionnalité n'est prise en charge que par la version d'Horizon View Client fournie par les partenaires et uniquement sur les périphériques client légers x86. 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.0` 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.

Pour consulter la liste des exigences qu'un poste de travail View 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 au document *Installation et administration de VMware Horizon View Feature Pack*.

Préparation du Serveur de connexion View pour Horizon View Client

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

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

- Si vous utilisez un serveur de sécurité comme le recommande VMware, assurez-vous de disposer des dernières versions de maintenance du Serveur de connexion View 4.6.x et du Serveur de sécurité View 4.6.x ou versions ultérieures. Consultez la documentation *Installation de VMware Horizon 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 View 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 a été créé et que le compte d'utilisateur que vous souhaitez utiliser est autorisé à accéder au poste de travail distant. Consultez les rubriques sur la création de pools de postes de travail dans la documentation *Administration de VMware Horizon View*.
- Pour pouvoir utiliser une authentification à deux facteurs, telle que l'authentification RSA SecurID ou RADIUS, avec Horizon View Client, vous devez activer cette fonctionnalité sur le Serveur de connexion View. L'authentification RADIUS est disponible avec View 5.1 et les versions supérieures et le Serveur de connexion View. Pour plus d'informations, consultez les rubriques concernant l'authentification à 2 facteurs dans la documentation *Administration de VMware Horizon View*.

Installer Horizon View Client pour Linux

Les utilisateurs finaux ouvrent Horizon View Client pour se connecter à des postes de travail distants à partir d'une machine physique. Horizon View Client pour Linux s'exécute sur des systèmes Ubuntu 12.04 et vous l'installez à l'aide de Synaptic Package Manager.

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 View 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 », 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 », page 8.

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 Téléchargez le package sur le centre logiciel d'Ubuntu, en procédant de la façon suivante.

   a Dans la barre de menus Ubuntu, sélectionnez **Système > Administration > Synaptic Package Manager**.

   b Cliquez sur **Rechercher** et recherchez `vmware`.

   c Dans la liste de packages trouvés, cochez la case à côté de **vmware-view-client** et sélectionnez **Marquer pour l'installation**.

   d Cliquez sur **Appliquer** dans la barre d'outils.

   Si vous utilisez le système d'exploitation Ubuntu 12.04, la version la plus récente d' Horizon View Client est installée. Si vous utilisez le système d'exploitation Ubuntu 10.04, View Client pour Linux 1.7 est installé.

3 Pour savoir si l'installation est réussie, vérifiez que l'icône d'application **VMware Horizon View** apparaît dans le menu **Applications > Internet**.

Suivant

Démarrez Horizon View Client et vérifiez que vous pouvez vous connecter au poste de travail virtuel correct. Reportez-vous à la section « Première connexion à un poste de travail distant », page 39.

Configurer les liens de téléchargement de View Client affichés dans View Portal

Par défaut, lorsque vous ouvrez un navigateur et entrez l'URL d'une instance de Serveur de connexion View, la page de portail qui apparaît contient des liens vers le site de téléchargement de VMware pour télécharger Horizon View Client. Vous pouvez modifier les valeurs par défaut.

Les liens par défaut d'Horizon View Client sur la page de portail garantissent que vous êtes dirigé vers les derniers programmes d'installation d'Horizon View Client compatibles. Toutefois, dans certains cas, il est possible que vous vouliez que les liens pointent vers un serveur Web interne ou que vous vouliez rendre des versions de client spécifiques disponibles sur votre propre Serveur de connexion View. Vous pouvez reconfigurer la page pour pointer vers une URL différente.

Lorsque vous créez des liens pour les systèmes clients Mac OS X, Linux et Windows, le lien propre au système d'exploitation correct est affiché sur la page de portail. Par exemple, si vous naviguez jusqu'à la page de portail depuis un système Windows, vous ne voyez que le ou les liens des programmes d'installation Windows. Vous pouvez créer des liens distincts pour les programmes d'installation 32 bits et 64 bits. Vous pouvez également créer des liens pour les systèmes iOS et Android, mais ces systèmes d'exploitation ne sont pas détectés automatiquement, de sorte que si vous accédez à la page de portail depuis un iPad, par exemple, vous voyez les liens pour iOS et Android, si vous créez des liens pour les deux.

IMPORTANT Si vous personnalisez les liens de la page de portail, comme décrit dans cette rubrique, et que vous installez VMware Horizon View HTML Access ultérieurement sur le serveur, votre page de portail personnalisée est remplacée par une page HTML Access. Pour plus d'informations sur la personnalisation de cette page, reportez-vous à *Utilisation de VMware Horizon View HTML Access*.

Prérequis

- Téléchargez les fichiers du programme d'installation d'Horizon View Client que vous voulez utiliser dans votre environnement. L'URL vers la page de téléchargement du client est https://www.vmware.com/go/viewclients.
- Déterminez quel serveur HTTP hébergera les fichiers du programme d'installation. Les fichiers peuvent résider sur une instance de Serveur de connexion View ou sur un autre serveur HTTP.

Procédure

1 Sur le serveur HTTP sur lequel les fichiers du programme d'installation résideront, créez un dossier pour ces fichiers.

  Par exemple, pour placer les fichiers dans un dossier `downloads` sur l'hôte de Serveur de connexion View, dans le répertoire d'installation par défaut, utilisez le chemin suivant :

  ```
  C:\Program Files\VMware\VMware View\Server\broker\webapps\downloads
  ```

  Les liens vers les fichiers doivent utiliser des URL avec le format `https://`*`server-name`*`/downloads/`*`client-installer-file-name`*. Par exemple, un serveur avec le nom `view.mycompany.com` utilise l'URL suivante pour View Client pour Windows : `https://view.mycompany.com/downloads/VMware-Horizon-View-Client.exe`. Dans cet exemple, le dossier `downloads` se trouve dans le dossier racine `webapps`.

2 Copiez les fichiers du programme d'installation dans le dossier.

  Si le dossier réside sur Serveur de connexion View, vous pouvez remplacer les fichiers dans ce dossier sans avoir à redémarrer le service Serveur de connexion VMware View.

3 Sur la machine Serveur de connexion View, copiez les fichiers `portal-links.properties` et `portal.properties` situés dans *`install-path`*`\Server\Extras\PortalExamples`.

4 Créez un dossier `portal` dans le répertoire `C:\ProgramData\VMware\VDM` et copiez les fichiers `portal-links.properties` et `portal.properties` dans le dossier `portal`.

5 Modifiez le fichier `C:\ProgramData\VMware\VDM\portal\portal-links.properties` pour qu'il pointe vers le nouvel emplacement des fichiers du programme d'installation.

Vous pouvez modifier les lignes dans ce fichier et en ajouter si vous devez créer plus de liens. Vous pouvez également supprimer des lignes.

Les exemples suivants montrent des propriétés pour créer deux liens pour View Client pour Windows et deux liens pour View Client pour Linux :

```
link.win=https://<varname id="VARNAME_B2B27F517DB04754B1CCF5F1411BA59E">server-
name</varname>/downloads/VMware-Horizon-View-Client-x86_64-<varname
id="VARNAME_7CD50CBABC614BCD976B2575FEDEF1F2">y.y.y-XXXX</varname>.exe#win
link.win.1=https://<varname id="VARNAME_8243922EA8B44DC3A2E9A360C4DDC304">server-
name</varname>/downloads/VMware-Horizon-View-Client-<varname
id="VARNAME_9D2A6519E01D4ADA9B701FDB8785B141">y.y.y-XXXX</varname>.exe#win
link.linux=https://<varname id="VARNAME_C62EA29FFF1047D1A350C57AD8006223">server-
name</varname>/downloads/VMware-Horizon-View-Client-x86_64-<varname
id="VARNAME_B664011E02154BBD9479411042551944">y.y.y-XXXX</varname>.rpm#linux
link.linux.1=https://<varname id="VARNAME_C498001B66334F39A59E2610D499EAA8">server-
name</varname>/downloads/VMware-Horizon-View-Client-<varname
id="VARNAME_D5652EFD7B75490F873921D2AFF8D9B0">y.y.y-XXXX</varname>.tar.gz#linux
```

Dans cet exemple, *`y.y.y-XXXX`* indique la version et le numéro de build. Le texte `win` à la fin de la ligne indique que ce lien doit apparaître dans le navigateur si le client dispose d'un système d'exploitation Windows. Utilisez `win` pour Windows, `linux` pour Linux et `mac` pour Mac OS X. Pour les autres systèmes d'exploitation, utilisez `unknown`.

6 Modifiez le fichier `C:\ProgramData\VMware\VDM\portal\portal.properties` pour spécifier le texte à afficher pour les liens.

Ces lignes apparaissent dans la section du fichier intitulé `# keys based on key names in portal-links.properties`.

L'exemple suivant indique le texte qui correspond aux liens spécifiés pour `link.win` et `link.win.1` :

```
text.win=View Client pour utilisateurs de clients Windows 32 bits
text.win.1=View Client pour utilisateurs de clients Windows 64 bits
```

7 Redémarrez le service Serveur de connexion VMware View.

Lorsque des utilisateurs finaux entrent l'URL pour Serveur de connexion View, ils voient des liens avec le texte que vous avez spécifié. Les liens pointent vers les emplacements que vous avez spécifiés.

Données Horizon View Client collectées par VMware

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

Remarque Cette fonctionnalité est disponible uniquement si votre déploiement Horizon View utilise le Serveur de connexion View 5.1 ou versions supérieures. Les informations client sont envoyées pour les clients View Client 1.7 et versions supérieures.

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 View Client sont envoyées d'abord au Serveur de connexion View, puis à VMware, avec des données provenant des serveurs, des pools de postes de travail et des postes de travail distants Horizon View.

Bien que les informations soient chiffrées lors de leur transfert au Serveur de connexion View, 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.

Pour participer au programme d'amélioration du produit de VMware, l'administrateur qui installe le Serveur de connexion View peut s'inscrire tout en exécutant l'Assistant d'installation du Serveur de connexion View, ou il peut définir une option dans View Administrator après l'installation.

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

Description	Ce champ reste-t-il anonyme ?	Exemple
Entreprise ayant produit l'application Horizon View Client	Non	VMware
Nom du produit	Non	VMware Horizon View 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* le numéro de build.
Architecture binaire du client	Non	Exemples : ■ i386 ■ x86_64 ■ arm
Nom du build du client	Non	Exemples : ■ VMware-Horizon-View-Client-Win32-Windows ■ VMware-Horizon-View-Client-Linux ■ VMware-Horizon-View-Client-iOS ■ VMware-Horizon-View-Client-Mac ■ VMware-Horizon-View-Client-Android ■ VMware-Horizon-View-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 10.04.4 LTS ■ Mac OS X 10.7.5 (11G63)
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)

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

Description	Ce champ reste-t-il anonyme ?	Exemple
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)

Configuration d' Horizon View Client pour les utilisateurs finaux 2

Horizon View 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 présente certains des paramètres de configuration que vous pouvez définir de plusieurs façons. Pour de nombreux autres paramètres de configuration, vous devez utiliser un mécanisme particulier. Par exemple, pour définir le paramètre Désactiver les notifications toast, vous devez utiliser un paramètre de stratégie de groupe.

Tableau 2-1. Paramètres de configuration communs

Paramètre	Mécanismes de configuration
Adresse du Serveur de connexion View	URI, Stratégie de groupe, Ligne de commande, Registre Windows
Nom d'utilisateur Active Directory	URI, Stratégie de groupe, Ligne de commande, Registre Windows
Se connecter en tant qu'utilisateur actuel	Stratégie de groupe, Ligne de commande
Nom de domaine	URI, Stratégie de groupe, Ligne de commande, Registre Windows
Nom affiché du poste de travail	URI, Stratégie de groupe, Ligne de commande
Taille de fenêtre	URI, Stratégie de groupe, Ligne de commande
Protocole d'affichage	URI, Ligne de commande
Options pour la redirection des périphériques USB	URI, Stratégie de groupe, Ligne de commande
Configuration de la vérification des certificats	Stratégie de groupe, Registre Windows
Configuration des protocoles et des algorithmes de chiffrement SSL	Stratégie de groupe, Registre Windows

Ce chapitre aborde les rubriques suivantes :

Utilisation d'URI pour configurer Horizon View 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 lancer Horizon View Client, se connecter au Serveur de connexion View et démarrer un poste de travail spécifique avec des options de configuration particulières.

Vous pouvez simplifier le processus de connexion 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 View
- Numéro de port pour le Serveur de connexion View
- Nom d'utilisateur Active Directory
- Nom de domaine
- Nom affiché du poste de travail
- Taille de fenêtre
- Actions sur le poste de travail, notamment réinitialisation, fermeture d'une session et 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 View Client.

Remarque Vous pouvez utiliser des URI permettant de lancer Horizon View Client uniquement si le logiciel client est déjà installé sur les ordinateurs clients des utilisateurs finaux.

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 et, en option, une requête permettant de spécifier les actions du poste de travail ou les options de configuration.

Spécification d'URI pour VMware Horizon View

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 permettant de lancer Horizon View Client :

```
vmware-view://[<varname id="VARNAME_E0F8F9951BC4471D9871655A18782C9E">authority-part</varname>]
[/<varname id="VARNAME_7B21DCA6CDE942BBB914ADD20452590B">path-part</varname>][?<varname
id="VARNAME_217F9AF17A3745369FD8E2154505D735">query-part</varname>]
```

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 noms de serveur doivent être conformes à la syntaxe DNS.

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

```
user1@<varname id="VARNAME_640D14F5E64B44E189F204DC09A8248B">server-address</varname>
```

Veuillez remarquer que vous ne pouvez pas spécifier d'adresse UPN, ce qui inclut le nom 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 :

```
<varname id="VARNAME_1BAB6153D2834B1490509093A1961D1F">server-address</varname>:<varname id="VARNAME_2296A4E54893485C852FFE94067114D7">port-number</varname>
```

path-part

Spécifie le poste de travail. Utilisez le nom affiché du poste de travail. Si le nom affiché contient un espace, utilisez le mécanisme d'encodage **`%20`** pour représenter l'espace.

query-part

Spécifie les options de configuration à utiliser ou les actions du poste de travail à effectuer. Les requêtes ne sont pas sensibles à la casse. Pour utiliser des requêtes multiples, 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 :

```
<varname id="VARNAME_48A6B3A0E1184943BC1206017B78B9D5">query1</varname>=<varname id="VARNAME_9B9916FF3D3540D4AA5622F9C828F072">value1</varname>[&<varname id="VARNAME_6BCA2912EC454A5683D586754BF89DCE">query2</varname>=<varname id="VARNAME_F698C39E83D34D639C943ACDF828BAFE">value2</varname>...]
```

Requêtes prises en charge

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

action

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

Valeur	Description
`browse`	Affiche une liste des postes de travail disponibles hébergés sur le serveur spécifié. Il ne vous est pas demandé de spécifier un poste de travail pour l'utilisation de cette action.
`start-session`	Lance le poste de travail spécifié. Si aucune requête d'action n'est fournie et que le nom du poste de travail est fourni, `start-session` est l'action par défaut.
`réinitialiser`	Éteint puis redémarre le poste de travail spécifié. 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.
`rollback`	Ignore les modifications du poste de travail spécifié apportées lors de son emprunt pour une utilisation en mode local, sur un PC Windows ou sur un ordinateur portable.

connectUSBOnInsert

(Le composant USB n'est inclus qu'avec la version d'Horizon View Client disponible auprès de fournisseurs tiers.) Connecte un périphérique USB au poste de travail au premier plan lorsque vous branchez le périphérique. Cette requête est paramétrée de façon implicite si vous spécifiez la requête `unattended`. Pour utiliser cette requête, vous devez paramétrer la requête `action` sur **`start-session`** ou ne pas utiliser de requête `action`. Les valeurs valides sont **`yes`** et **`no`**. Exemple de syntaxe : **`connectUSBOnInsert=yes`**.

connectUSBOnStartup

(Le composant USB n'est inclus qu'avec la version d'Horizon View Client disponible auprès de fournisseurs tiers.) Redirige tous les périphériques USB vers les postes de travail actuellement connectés au système client. Cette requête est paramétrée de façon implicite si vous spécifiez la requête `unattended`. Pour utiliser cette requête, vous devez paramétrer la requête `action` sur **`start-session`** ou ne pas utiliser de requête `action`. Les valeurs valides sont **`yes`** et **`no`**. Exemple de syntaxe : **`connectUSBOnStartup=yes`**.

desktopLayout

Définit la taille de la fenêtre qui affiche le 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 2-3. Valeurs valides pour la requête desktopLayout

Valeur	Description
`fullscreen`	Un moniteur affiche son contenu en plein écran. Il s'agit du réglage par défaut.
`multimonitor`	Tous les moniteurs affichent leur contenu en plein écran.
`windowLarge`	Fenêtre de grande taille.

Tableau 2-3. Valeurs valides pour la requête desktopLayout (suite)

Valeur	Description
`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 Les valeurs valides sont **`RDP`** et **`PCoIP`**. Par exemple, pour spécifier le protocole PCoIP, utilisez la syntaxe **`desktopProtocol=PCoIP`**.

domainName Domaine associé à l'utilisateur qui se connecte au poste de travail distant.

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, lancer 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 View 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 de View Client et des fichiers de configuration », page 22.

---

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 Serveur de connexion View. (Le port par défaut est 443.) Comme un identificateur de poste de travail est fourni, le poste de travail est lancé 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 View 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://fred@view.mycompany.com/Finance%20Desktop?domainName=mycompany`

Horizon View 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.

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

Horizon View Client démarre et l'utilisateur est dirigé vers l'invite lui permettant de se connecter au serveur `view.mycompany.com`.

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

Horizon View 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. Une fois la connexion établie, Horizon View Client affiche une boîte de dialogue invitant l'utilisateur à confirmer l'opération de réinitialisation du 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 l'administrateur View a activé cette fonction pour les utilisateurs finaux.

7 `vmware-view://`

Horizon View Client démarre et l'utilisateur est dirigé vers une page sur laquelle il peut entrer l'adresse d'une instance du Serveur de connexion View.

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>
```

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

Vous pouvez configurer View 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 `vmware-view` ou des propriétés définies dans des fichiers de configuration pour définir les valeurs par défaut que vos utilisateurs voient dans View 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 View Client démarre, des paramètres de configuration sont traités depuis plusieurs 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 View Client.

Propriétés empêchant les utilisateurs de modifier des valeurs par défaut

Pour chaque propriété, 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 dans le champ **Server Name (Nom du serveur)** lorsqu'ils utilisent View 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 n'entre pas en vigueur dans View 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 de View 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 configuration, telles que celles de la redirection USB et de MMR, sont disponibles uniquement avec la version de View 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 2-4. Options de ligne de commande et clés du fichier de configuration de View 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 View Client en mode plein écran sur tous les écrans connectés lors du démarrage de View Client. Si vous définissez la clé de configuration, spécifiez **"TRUE"** ou **"FALSE"**. La valeur par défaut est "FALSE".

`view.allowDefaultBroker`	`-l`, `--lockServer`
	Exemple :
	`--lockServer -s view.company.com`
		Utiliser cette option de ligne de commande, ou définir la propriété sur "FALSE", désactive le champ **Nom de serveur** sauf si le client ne s'est jamais connecté à aucun serveur, et si aucune adresse de serveur n'est fournie dans la ligne de commande ou dans le fichier de préférences.

`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.defaultBroker`	`-s`, `--serverURL=`
	Exemples :
	`--serverURL=https://view.company.com`
	`-s view.company.com`
	`--serverURL=view.company.com:1443`
		Ajoute le nom que vous spécifiez au champ **Nom de serveur** dans View 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.

`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.

Tableau 2-4. Options de ligne de commande et clés du fichier de configuration de View Client (suite)

Clé de configuration	Option de ligne de commande	Description
`view.defaultDesktopHeight`	Aucune	Spécifie la hauteur par défaut de la fenêtre pour le poste de travail View, en pixels.

`view.defaultDesktopSize`	`--desktopSize=`
	Exemples :
	`--desktopSize="1280x800"`
	`--desktopSize="all"`
		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"`**.

`view.defaultDesktopWidth`	Aucune	Spécifie la largeur par défaut de la fenêtre pour le poste de travail View, en pixels.
`view.defaultDomain`	`-d`, `--domainName=`	Définit le nom de domaine que View 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 de View Client.
`view.defaultPassword`	`-p "-"`, `--password="-"`	Pour les connexions PCoIP et `rdesktop`, spécifiez toujours **`"-"`** pour lire le mot de passe à partir de `stdin`. Définit le mot de passe que View Client utilise pour toutes les connexions et ajoute le mot de passe au champ **Mot de passe** dans la boîte de dialogue d'authentification de View Client 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=""

Tableau 2-4. Options de ligne de commande et clés du fichier de configuration de View Client (suite)

Clé de configuration	Option de ligne de commande	Description
`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 que View Client utilise pour toutes les connexions et ajoute le nom d'utilisateur que vous spécifiez au champ **Nom d'utilisateur** dans la boîte de dialogue d'authentification de View Client. 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.fullScreen`	`--fullscreen`	Masque le système d'exploitation hôte et ouvre l'interface utilisateur de View Client en mode plein écran sur un écran. 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=`
	Exemples de `rdesktop` :
	`--kbdLayout="en-us"`
	`-k "fr"`
	Exemple de `freerdp` :
	`-k "0x00010407"`
		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`

`view.kioskLogin`	`--kioskLogin` Exemple : Voir l'exemple du mode kiosque présenté après ce tableau.	Spécifie que View Client est sur le point de s'authentifier à l'aide d'un compte en mode kiosque. Si vous définissez la clé de configuration, spécifiez **`"TRUE"`** ou **`"FALSE"`**. La valeur par défaut est "FALSE".

`view.mmrPath`	`-m`, `--mmrPath=`
	Exemple :
	`--mmrPath="/usr/lib/altmmr"`
		(Disponible uniquement avec les distributions de fournisseurs tiers) Spécifie le chemin d'accès au répertoire qui contient les bibliothèques Wyse MMR (redirection multimédia).

Tableau 2-4. Options de ligne de commande et clés du fichier de configuration de View Client (suite)

Clé de configuration	Option de ligne de commande	Description
`view.nomenubar`	`--nomenubar`	Supprime la barre de menu View Client lorsque View Client est en mode plein écran pour que les utilisateurs ne puissent pas accéder aux options de menu pour fermer une session, réinitialiser ou se déconnecter d'un poste de travail View. 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`
	Exemple :
	`--nonInteractive`
	`--serverURL="https://view.company.com"`
	`--userName="user1" --password="-"`
	`--domainName="xyz"`
	`--desktopName="Windows 7"`
		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".

`view.once`	`--once`	Spécifie que vous ne voulez pas que View Client essaie de nouveau de se connecter en cas d'erreur. Utilisez `--once` si vous voulez obtenir un flux de travail similaire vers le client View 4.6. Cette option force View Client à quitter après que l'utilisateur s'est déconnecté ou a fermé une session sur un poste de travail. 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".

`view.rdesktopOptions`	`--rdesktopOptions=`
	Exemple :
	`--rdesktopOptions="-f -m"`
		(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.

Aucune	`-r`, `--redirect=`
	Exemple :
	`--redirect="sound:off"`
		(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.

Tableau 2-4. Options de ligne de commande et clés du fichier de configuration de View Client (suite)

Clé de configuration	Option de ligne de commande	Description
`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 34.
Aucune	`--save`	(Disponible si vous utilisez View Client 2.2 ou version ultérieure) Enregistre le nom d'utilisateur et le nom de domaine utilisés lors de la dernière connexion, ce qui vous évite d'avoir à les ressaisir lors de la prochaine connexion.
`view.sendCtrlAltDelToLocal`	Aucune	(Disponible si vous utilisez le protocole d'affichage PCoIP et View Client 2.1 ou version ultérieure) Lorsqu'il est défini sur **"TRUE"**, envoie la combinaison de touches Ctrl+Alt+Delete 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 réaliser cette fonction en utilisant l'option `–K` ; par exemple, `vmware–view –K`. Vous pouvez également configurer cette combinaison de touches en utilisant le fichier `view–keycombos–config`, comme indiqué dans la section « Configuration de touches et de combinaisons de touches spécifiques à envoyer au système local », page 31.
`view.sendCtrlAltInsToVM`	Aucune	(Disponible si vous utilisez le protocole d'affichage PCoIP et View Client 2.1 ou version ultérieure) Lorsqu'il est défini sur **"TRUE"**, envoie la combinaison de touches Ctrl+Alt+Ins 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 *Administration de VMware Horizon View*.

Tableau 2-4. Options de ligne de commande et clés du fichier de configuration de View Client (suite)

Clé de configuration	Option de ligne de commande	Description
`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.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 34.
Aucune	`--enableNla`	(S'applique si vous utilisez FreeRDP pour les connexion RDP) Active l'authentification de niveau réseau (NLA). 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 34. **Remarque** Le programme `rdesktop` ne prend pas en charge NLA.

Aucune	`--printEnvironmentInfo`
	Exemple :
	`--printEnvironmentInfo -s view.company.com`
		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`.

Tableau 2-4. Options de ligne de commande et clés du fichier de configuration de View Client (suite)

Clé de configuration	Option de ligne de commande	Description
Aucune	`--usb=`	(Disponible uniquement avec les distributions de fournisseurs tiers et uniquement pour View Client 1.5) Spécifie les options à utiliser pour la redirection USB. Reportez-vous à la section « Utilisation de l'option de ligne de commande View Client 1.5 pour rediriger les périphériques USB », page 63. Pour configurer des options USB avec View Client 1.6 et supérieur, reportez-vous à Chapitre 6, « Configuration de la redirection USB sur le client », page 57.
Aucune	`--version`	Affiche des informations de version sur View 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 VMware Horizon 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 un nom d'utilisateur de kiosque non défini par défaut n'est pas requis et si vous ne spécifiez pas de nom d'utilisateur, View 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 View 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.
- View Client s'exécute en mode plein écran sans barre de menus de View 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 View 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.

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

Si vous utilisez le protocole d'affichage PCoIP avec Horizon View Client 2.2 ou une version ultérieure, vous pouvez créer un fichier `view-keycombos-config` pour spécifier les combinaisons de touches à ne pas transmettre au poste de travail distant. Si vous utilisez Horizon View Client 2.3, vous pouvez également spécifier des touches individuelles.

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. À partir de la version 2.2 d'Horizon View Client, vous pouvez créer un fichier situé dans `/etc/vmware/view-keycombos-config` et spécifier les combinaisons de touches. Si vous utilisez Horizon View Client 2.3 ou une version ultérieure, vous pouvez également spécifier des touches individuelles.

Placez chaque touche ou combinaison de touches sur une nouvelle ligne en respectant le format indiqué dans le tableau suivant.

Tableau 2-5. Format pour spécifier les touches à ne pas transmettre aux postes de travail distants

Version du client	Format
Horizon View Client 2.2	`<<varname id="VARNAME_2FEB13F2EAB54854AB592728157B01DA">modName</varname>><varname id="VARNAME_5599ABEB8A9C40008FC8DBB35ADD0553">keyName</varname>` **IMPORTANT** Cette fonctionnalité est destinée aux combinaisons de touches et non aux touches isolées. Par exemple, vous ne pouvez pas spécifier uniquement *<modName>* ou uniquement *keyName*.
Horizon View Client 2.3 ou version ultérieure	`<<varname id="varname_8B31DEC6FAAD4DF2A2459399C4FFF8CA">modName</varname>><varname id="varname_2775AC593B6F46689C5FF2164A58AA80">scanCode</varname><varname id="varname_3947E08F92424A659F8F601D8399F92B">scanCode</varname>` 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* correspond à 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. Si vous utilisez Horizon View Client 2.3 ou une version ultérieure, vous pouvez également utiliser `<any>` en tant que 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'une touche enfoncée dans Horizon View Client 2.3 ou une version ultérieure

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.

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      #pour bloquer ctrl-insert
<alt>15          #pour bloquer alt-tab
<Ctrl><Alt>0x153 #pour bloquer ctrl-alt-suppr
<any>0x137       #pour bloquer toutes les combinaisons de la touche d'impression
0x010               #pour bloquer la touche Q individuelle sur un clavier américain
                 #ou pour bloquer la touche A individuelle sur un clavier français
0x03b            #pour bloquer la touche F1 individuelle
0x04f            #pour bloquer la touche 1 individuelle sur un clavier numérique
```

Spécification d'un nom de touche dans Horizon View Client 2.2

La valeur *keyName* est sensible à la casse et peut avoir n'importe laquelle des valeurs suivantes : les chiffres `0` à `9`, les touches de fonction `F1` à `F12`, les lettres minuscules ou majuscules `A` à `Z`, ou n'importe laquelle des autres touches dans la liste qui suit.

Remarque Dans la liste qui suit, les touches dotées du préfixe `KP`, telles que `KP_Enter`, représentent des touches du pavé numérique.

BackSpace	Execute	KP_Page_Down	quotedbl	asciicircum
Tab	Insert	KP_End	numbersign	underscore
Linefeed	Undo	KP_Begin	dollar	grave
Clear	Redo	KP_Insert	percent	quoteleft
Return	Menu	KP_Delete	ampersand	braceleft
Pause	Find	KP_Equal	apostrophe	bar
Scroll_Lock	Cancel	KP_Multiply	quoteright	braceright
Sys_Req	Help	KP_Add	quoteleft	asciitilde
Escape	Break	KP_Separator	parenleft	
Delete	Num_Lock	KP_Subtract	parenright	
Multi_key	KP_Space	KP_Decimal	asterisk	
Codeinput	KP_Tab	KP-Divide	plus	
Home	KP_Enter	KP_0	comma	
Left	KP_F1	KP_1	minus	
Up	KP_F2	KP_2	period	

Right	KP_F3	KP_3	slash
Down	KP_F4	KP_4	colon
Prior	KP_Home	KP_5	less
Page_Up	KP_Left	KP_6	equal
Next	KP_UP	KP_7	greater
Page_Down	KP_Right	KP_8	question
End	KP_Down	KP_9	at
Begin	KP_Prior	Caps_Lock	bracketleft
Select	KP_Page_Up	space	backslash
Print	KP_Next	exclam	bracketright

La liste suivante montre un exemple de contenu d'un fichier `/etc/vmware/view-keycombos-config` :

```
<ctrl><alt>Delete
<alt>Tab
<alt>1
<alt>h
<ctrl>1
<ctrl>S
<ctrl>h
<super>h
<shift>h
<ctrl>space
<Ctrl>KP_Enter
<Ctrl>Up
```

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 s'exécute pour les connexions SSL entre le Serveur de connexion View et Horizon View 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 « Modes de vérification des certificats pour Horizon View Client », page 41.

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

- **1** implémente `Vérification complète`.
- **2** implémente `Avertir si la connexion peut être non sécurisée`.
- **3** implémente `Aucune vérification effectuée`.

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 de View Client », page 23.

Utilisation de FreeRDP pour des connexions RDP

Si vous prévoyez d'utiliser RDP au lieu de 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, View Client 1.7 et supérieur peut également exécuter l'exécutable `xfreerdp` si votre machine Linux dispose de la version et des correctifs requis pour FreeRDP.

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 View Client doit exécuter `xfreerdp` au lieu de `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`

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
```

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 de View Client et des fichiers de configuration », page 22.

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 34.

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 et les correctifs requis concernant FreeRDP.

Vous devez disposer de FreeRDP 1.0.x et installer également les correctifs applicables pour que les options `--from-stdin` et `-X` fonctionnent correctement.

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

Procédure

1 Sur votre machine cliente Linux, téléchargez FreeRDP 1.0.x depuis GitHub, à l'adresse https://github.com/FreeRDP/FreeRDP.

2 Si vous installez FreeRDP 1.0.1, appliquez le correctif avec le fichier `freerdp-1.0.1.patch`, à l'aide de la commande de correctif suivante :

```
patch -p1 < freerdp-1.0.1.patch
```

3 Pour créer et installer FreeRDP, ouvrez une fenêtre de terminal et exécutez les commandes suivantes.

a Exécutez la commande suivante :

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

b Exécutez la commande suivante :

```
make
```

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

```
sudo make install
```

Activation du mode FIPS sur le client

Vous pouvez définir une propriété de configuration pour que le client utilise uniquement des algorithmes et des protocoles cryptographiques approuvés par FIPS (Federal Information Processing Standard) 140-2 pour établir une connexion PCoIP distante.

Remarque Le mode FIPS PCoIP de View ne prend pas en charge les algorithmes de chiffrement AES-256.

Ce paramètre s'applique à la fois au serveur et au client. Vous pouvez configurer un ou les deux points de terminaison pour qu'ils fonctionnent en mode FIPS. La configuration d'un seul point de terminaison pour qu'il fonctionne en mode FIPS limite les algorithmes de chiffrement disponibles pour la négociation de session.

Important Si vous activez le mode FIPS sur un point de terminaison et que l'autre point de terminaison ne prend pas en charge les algorithmes cryptographiques approuvés par FIPS 140-2, la connexion échoue.

Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, le mode FIPS n'est pas utilisé.

Définition de la propriété de configuration

Pour activer ou désactiver le mode FIPS, vous pouvez définir la propriété `pcoip.enable_fips_mode`. Affectez la valeur **`1`** à la propriété pour activer le mode FIPS, ou la valeur **`0`** pour le désactiver. Par exemple, le paramètre suivant active le mode FIPS :

```
pcoip.enable_fips_mode = 1
```

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

Vous pouvez définir cette propriété dans n'importe quel fichier d'un groupe de fichiers. Lorsque View Client démarre, le paramètre est traité dans 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.

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.

IMPORTANT Cette fonction est disponible uniquement lorsque la version de View Agent et celle du Serveur de connexion View correspondent à la version View 5.0 ou une version supérieure.

Le cache d'images PCoIP capture la redondance spatiale et temporaire. 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 temporaire.

Comme pendant le défilement, les informations d'écran envoyées au périphérique client sont constituées principalement d'une séquence d'index de cache, 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. Vous pouvez configurer la taille du cache d'images client, d'un minimum de 50 Mo à un maximum de 1 024 Mo pour View Client 1.7 et versions supérieures. La taille maximale pour les versions antérieures est de 300 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 un nombre inférieur à 50, le nombre est converti sur 50. Si vous spécifiez un nombre supérieur au maximum, le nombre est converti sur le maximum.

Vous pouvez définir cette propriété dans un des différents fichiers. Lorsque View Client démarre, le paramètre est traité depuis plusieurs 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 de serveur et des postes de travail 3

Horizon View Client vous permet de vous connecter au Serveur de connexion View ou à un serveur de sécurité et d'ouvrir ou de fermer une session sur un poste de travail distant. À des fins de dépannage, il vous permet également de réinitialiser un poste de travail distant qui vous est affecté.

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.

- Première connexion à un poste de travail distant page 39

  Avant de laisser vos utilisateurs finaux accéder à leur poste de travail distant, vérifiez que vous pouvez vous connecter à un poste de travail distant à partir du système client.

- Modes de vérification des certificats pour Horizon View Client page 41

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

- Basculer entre postes de travail page 42

  Si vous êtes connecté à un poste de travail, vous pouvez basculer vers un autre poste de travail.

- Fermer une session ou se déconnecter d'un poste de travail page 42

  Si vous vous déconnectez d'un poste de travail distant sans fermer votre session, des applications restent ouvertes.

- Restaurer un poste de travail page 43

  La restauration ignore les modifications réalisées sur un poste de travail virtuel que vous avez emprunté pour l'utiliser en mode local sur un PC ou un ordinateur portable Windows.

Première connexion à un poste de travail distant

Avant de laisser vos utilisateurs finaux accéder à leur poste de travail distant, vérifiez que vous pouvez vous connecter à un poste de travail distant à partir du système client.

Prérequis

- Obtenez les informations d'identification dont vous avez besoin pour ouvrir une session, telles que le nom d'utilisateur et le mot de passe Active Directory, le nom d'utilisateur et le code secret RSA SecurID ou le nom d'utilisateur et le code secret pour l'authentification RADIUS.
- Obtenez le nom de domaine pour ouvrir une session.
- Effectuez les tâches administratives décrites dans « Préparation du Serveur de connexion View pour Horizon View Client », page 11.

- 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 au poste de travail distant. 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 View Agent est activé.
- Si votre administrateur l'a autorisé, vous pouvez configurer le mode de vérification des certificats pour le certificat SSL que le serveur View server présente. Reportez-vous à la section « Modes de vérification des certificats pour Horizon View Client », page 41.

Procédure

1 Ouvrez une fenêtre du terminal et entrez `vmware-view`, ou sélectionnez **Applications > Internet > VMware Horizon View Client** à partir de la barre de menu Ubuntu.

2 Entrez le nom de serveur et un numéro de port si nécessaire, puis cliquez sur **Continuer**.

Voici un exemple d'utilisation d'un port non défini comme port par défaut : `view.company.com:1443`.

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

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 View 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. Le Serveur de connexion View 4.6.1, 5.0.1 et les versions supérieures envoient des informations d'empreinte numérique, contrairement aux versions antérieures.

6 (Facultatif) Sélectionnez le protocole d'affichage et la taille de fenêtre à utiliser.

Option	Description
Protocole d'affichage	L'option par défaut est **PCoIP**. Pour utiliser plutôt Microsoft RDP, cliquez sur **PCoIP** sous le nom de poste de travail à définir et sélectionnez **Microsoft RDP**.
Taille de fenêtre	L'option par défaut est **Plein écran - Tous les moniteurs**. Pour choisir une autre taille de fenêtre, cliquez sur l'une des autres options sous le nom de poste de travail, telle que **Grand écran** ou **Personnaliser la taille**.

7 Double-cliquez sur un raccourci de poste de travail distant pour vous connecter.

Une fois la connexion établie, la fenêtre client s'affiche. Si Horizon View Client ne parvient pas à se connecter au poste de travail, effectuez les tâches suivantes :

- Déterminez si le Serveur de connexion View est configuré pour ne pas utiliser SSL. Horizon View Client requiert 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.
- Vérifiez que les balises définies sur l'instance de Serveur de connexion View autorisent les connexions depuis cet utilisateur. Consultez le document *VMware Horizon View Administration*.
- Vérifiez que l'utilisateur est autorisé à accéder à ce poste de travail. Consultez le document *VMware Horizon View Administration*.
- Si vous utilisez le protocole d'affichage RDP pour vous connecter à un poste de travail distant, vérifiez que l'ordinateur client autorise les connexions à des postes de travail distants.

Modes de vérification des certificats pour Horizon View 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 s'exécute pour les connexions SSL entre le Serveur de connexion View et Horizon View 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 View Client vers un serveur disposant d'un certificat qui ne correspond pas au nom d'hôte entré dans Horizon View 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 client Linux, consultez la documentation Ubuntu.

Horizon View Client utilise les certificats de 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 la procédure intitulée « 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 View 4.6.1, 5.0.1 et versions ultérieures envoient une empreinte numérique de certificat à Horizon View 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 View server 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 menu VMware Horizon View Client ou dans la barre de menu du poste de travail View. 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 de certificat ne doit pas correspondre au nom du Serveur de connexion View que vous avez entré dans Horizon View Client.
- **Ne pas vérifier les certificats d'identité des serveurs**. Ce paramètre signifie que View n'effectue aucune vérification de certificat.

Basculer entre postes de travail

Si vous êtes connecté à un poste de travail, vous pouvez basculer vers un autre poste de travail.

Procédure

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

Option	Action
Choisir un autre poste de travail distant sur le même serveur	Sélectionnez **Poste de travail > Se déconnecter** dans la barre de menu.
Choisir un poste de travail distant sur un autre serveur	Sélectionnez **Fichier > Déconnexion du serveur** dans la barre de menus.

Fermer une session ou se déconnecter d'un poste de travail

Si vous vous déconnectez d'un poste de travail distant sans fermer votre session, des applications restent ouvertes.

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 View 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 > Se déconnecter** dans la barre de menu.
Choisir un poste de travail distant sur un autre serveur	Sélectionnez **Fichier > Déconnexion 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.

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, sélectionnez le poste de travail et **Poste de travail > Fermer la session** dans la barre de menus.
  b Si vous y êtes invité, entrez des 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.

Restaurer un poste de travail

La restauration ignore les modifications réalisées sur un poste de travail virtuel que vous avez emprunté pour l'utiliser en mode local sur un PC ou un ordinateur portable Windows.

Vous pouvez restaurer un poste de travail distant uniquement si votre administrateur View a activé cette fonctionnalité et uniquement si vous avez emprunté le poste de travail.

Avertissement Si des modifications ont été faites sur le poste de travail en mode local et que ces modifications n'ont pas été répliquées sur le serveur View server avant la restauration, les modifications sont perdues.

Prérequis

- Obtenez les informations d'identification dont vous avez besoin pour ouvrir une session, telles que le nom d'utilisateur et le mot de passe Active Directory, le nom d'utilisateur et le code secret RSA SecurID ou le nom d'utilisateur et le code secret pour l'authentification RADIUS.
- Sauvegardez le poste de travail sur le serveur pour conserver des données ou des fichiers.

  Vous pouvez utiliser View Administrator pour répliquer des données sur le serveur ou, si la règle est définie pour l'autoriser, vous pouvez utiliser View Client with Local Mode sur le client Windows sur lequel le poste de travail est actuellement emprunté.

Procédure

1 Si l'écran d'accueil Horizon View Client affiche l'invite **Serveur de connexion View**, entrez le nom du serveur et cliquez sur **Continuer**.

   a Si un message demande les informations d'identification RSA SecurID ou les informations d'identification pour l'authentification RADIUS, entrez le nom d'utilisateur et le code secret et cliquez sur **Continuer**.

   b Saisissez votre nom d'utilisateur et votre mot de passe dans la boîte de dialogue de connexion.

2 Sur l'écran d'accueil d'Horizon View Client qui affiche les raccourcis de postes de travail distants, sélectionnez le poste de travail et choisissez **Poste de travail >Restaurer le poste de travail** dans la barre de menus.

Une fois le poste de travail distant restauré, vous pouvez y ouvrir une session à partir du client Linux.

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

4

View Client pour Linux prend en charge certaines fonctions incluses dans View Client pour Windows.

Ce chapitre aborde les rubriques suivantes :

Matrice de prise en charge des fonctions pour Linux

Certaines fonctions sont prises en charge sur un type de View Client mais pas sur un autre. Par exemple, le mode local est pris en charge uniquement sur View Client pour Windows.

Tableau 4-1. Fonctions prises en charge sur les postes de travail Windows pour les clients Linux

Fonction	Poste de travail Windows 8.x	Poste de travail Windows 7	Poste de travail Windows Vista	Poste de travail Windows XP	Poste de travail Windows Server 2008 R2
RSA SecurID ou RADIUS	X	X	X	X	X
Authentification unique	X	X	X	X	X
Protocole d'affichage RDP	X	X	X	X	X
Protocole d'affichage PCoIP	X	X	X	X	X
Accès USB	Systèmes client partenaires seulement	Systèmes client partenaires seulement	Systèmes client partenaires seulement	Systèmes client partenaires seulement	Systèmes client partenaires seulement
Audio/Vidéo en temps réel (RTAV)	Systèmes client partenaires seulement	Systèmes client partenaires seulement	Systèmes client partenaires seulement	Systèmes client partenaires seulement	Systèmes client partenaires seulement

Tableau 4-1. Fonctions prises en charge sur les postes de travail Windows pour les clients Linux (suite)

Fonction	Poste de travail Windows 8.x	Poste de travail Windows 7	Poste de travail Windows Vista	Poste de travail Windows XP	Poste de travail Windows Server 2008 R2
Wyse MMR			Systèmes client partenaires seulement et seulement avec RDP	Systèmes client partenaires seulement et seulement avec RDP	
Redirection multimédia (MMR) Windows 7					
Impression virtuelle	Systèmes client partenaires seulement	Systèmes client partenaires seulement	Systèmes client partenaires seulement	Systèmes client partenaires seulement	
Impression basée sur l'emplacement	X	X	X	X	
Cartes à puce	Systèmes client partenaires seulement et seulement avec PCoIP	Systèmes client partenaires seulement	Systèmes client partenaires seulement	Systèmes client partenaires seulement	Systèmes client partenaires seulement
Plusieurs écrans	X	X	X	X	X
Mode local					

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

- Les postes de travail Windows 8.x sont uniquement pris en charge si vous disposez de serveurs et de postes de travail Horizon View 5.2 ou version ultérieure.
- La fonction Audio/Vidéo temps réel est uniquement prise en charge si vous disposez d' Horizon View 5.2 avec Feature Pack 2 ou version ultérieure.
- Les postes de travail Windows Server 2008 R2 sont pris en charge uniquement si vous possédez des serveurs et des postes de travail Horizon View 5.3 ou version ultérieure.

Pour des descriptions de ces fonctions et leurs limites, consultez le document *Planification de VMware Horizon View*.

Remarque Cette matrice de prise en charge des fonctions s'applique à View Client pour Linux que VMware met à disposition sur Ubuntu. En outre, plusieurs partenaires VMware offrent des périphériques de client léger pour les déploiements d'Horizon View. 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.

Internationalisation

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

Si vous utilisez un système client Ubuntu 10.4 Linux et voulez afficher l'interface utilisateur View 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.
- 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 View Client utilise la configuration de moniteur employée lors du démarrage d' Horizon View 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 View Client, vous devez redémarrer Horizon View Client afin de pouvoir utiliser la nouvelle configuration de moniteur.

Horizon View 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 utilisez plus de 2 moniteurs, les moniteurs doivent être dans le même mode et avoir 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.

Résolution d'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 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, consultez le document *Administration de VMware Horizon 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.

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.

Cette fonctionnalité est disponible quand elle est utilisée avec VMware Horizon View 5.2 Feature Pack 2 ou version ultérieure. Pour plus d'informations sur la configuration de la fonctionnalité Audio/Vidéo en temps réel, de la résolution et de la fréquence d'images sur un poste de travail distant, reportez-vous au guide *Installation et administration de VMware Horizon View Feature Pack*. 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 n'est accessible qu'avec la version d'Horizon View Client pour Linux fournie par certains partenaires.

Conditions d'utilisation de votre Webcam

Vous pouvez utiliser sur votre poste de travail une webcam intégrée ou connectée à votre ordinateur local si votre administrateur Horizon View a configuré la fonctionnalité Audio/vidéo EN temps réel et si le protocole d'affichage 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 VMware Virtual Microphone et VMware Virtual Webcam comme périphériques d'entrée et VMware Virtual Audio comme périphérique de sortie dans les menus de l'application. 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, votre administrateur peut configurer une webcam préférée qui sera utilisée sur votre poste de travail distant. Contactez votre administrateur Horizon View si vous n'êtes pas sûr de la webcam sélectionnée

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 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.

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 50.

Prérequis

- Assurez-vous qu'un microphone USB ou d'un autre type est installé et opérationnel sur votre système client.
- Assurez-vous que vous utilisez le protocole d'affichage 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 View ; 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 l'ID du périphérique.

- Pour les webcams, affectez à la propriété `rtav.srcWCamId` la valeur de la description de webcam figurant dans le fichier journal, comme indiqué dans la procédure suivante.
- Pour les périphériques audio, affectez à la propriété `rtav.srcAudioInId` la valeur du champ Pulse Audio `device.description`.

  Recherchez cette valeur dans le fichier journal, comme indiqué dans la procédure suivante.

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.
- Assurez-vous qu'un microphone USB ou d'un autre type est installé et opérationnel sur votre système client.
- Assurez-vous que vous utilisez le protocole d'affichage 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 View 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 audio-vidéo en temps réel se trouve dans `/tmp/vmware-<username>/vmware-mks-<pid>.log`. Le fichier journal client est situé 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`.

Pour un exemple de webcam, copiez `Microsoft® LifeCam HD-6000 for Notebooks` afin de désigner la webcam Microsoft comme webcam préférée et définissez la propriété comme suit :

```
rtav.srcWCamId="Microsoft® LifeCam HD-6000 for Notebooks"
```

Dans cet exemple, vous pourriez aussi définir la propriété sur `rtav.srcWCamId="Microsoft"`.

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 Monoo"
```

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

5 Démarrez un nouvel appel.

Définir les préférences d'impression de la fonction d'impression virtuelle

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 L'impression virtuelle n'est accessible qu'avec la version d'Horizon View Client pour Linux fournie par certains partenaires. 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. Cette fonction a également les exigences suivantes :

- La version d'Horizon View Client pour Linux doit être 2.1 ou ultérieure.
- La version de View Agent et du Serveur de connexion View doit être Horizon View 5.2 ou supérieure.
- Vous devez utiliser le protocole d'affichage PCoIP ou FreeRDP. Cette fonction n'est pas opérationnelle avec rdesktop.

Après l'ajout d'une imprimante sur l'ordinateur local, Horizon View 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 pas exactement la même pour Windows XP et Windows Vista.

Prérequis

Vérifiez que le composant d'impression virtuelle de View Agent est installé sur le poste de travail distant. Dans le système de fichiers de poste de travail distant, les pilotes se trouvent dans `C:\Program Files\Common Files\VMware\Drivers\Virtual Printer`.

L'installation de View Agent est l'une des tâches requises pour préparer une machine virtuelle à utiliser en tant que poste de travail distant. Pour plus d'informations, consultez le document *Administration de VMware Horizon View*.

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.

   Dans 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

Par défaut, vous pouvez copier-coller du texte depuis votre système client vers un poste de travail View distant. Si votre administrateur active la fonction, vous pouvez également copier-coller le texte depuis un poste de travail View sur votre système client ou entre deux postes de travail View. Certaines restrictions s'appliquent.

Si vous utilisez le protocole d'affichage PCoIP et un poste de travail View avec View 5.x ou ultérieur, votre administrateur View peut définir cette fonction pour que les opérations de copier-coller soient autorisées uniquement depuis votre système client sur un poste de travail View, ou uniquement depuis un poste de travail View vers votre système client, ou les deux, ou aucun.

Les administrateurs configurent le copier-coller à l'aide d'objets de stratégie de groupe (GPO) qui appartiennent à View Agent dans des postes de travail View. Pour plus d'informations, consultez la rubrique concernant les variables de session générale View PCoIP dans le document *Administration de VMware Horizon View*, se trouvant dans le chapitre sur les stratégies de configuration.

Vous pouvez copier du texte brut ou du texte formaté depuis View Client sur un poste de travail View, ou l'inverse, mais le texte collé est du texte brut.

Vous ne pouvez pas copier-coller des graphiques. Vous ne pouvez pas non plus copier-coller des fichiers entre un poste de travail View et le système de fichiers sur l'ordinateur client.

Résolution des problèmes d' Horizon View Client 5

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

Ce chapitre aborde les rubriques suivantes :

Réinitialiser un poste de travail

Vous devrez peut-être réinitialiser un poste de travail si le système d'exploitation du poste de travail cesse de répondre. La réinitialisation arrête et redémarre le poste de travail. 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.

Vous pouvez réinitialiser le poste de travail uniquement si votre administrateur View a activé cette fonction.

Procédure

- Utilisez la commande **Réinitialiser le poste de travail**.

Option	Action
À partir de l'OS du poste de travail	Sélectionnez **Poste de travail > Réinitialiser le poste de travail** dans la barre de menu.
À partir de l'écran d'accueil avec des icônes de poste de travail	Sélectionnez le poste de travail et choisissez **Poste de travail > Réinitialiser le poste de travail** dans la barre de menu.

Le système d'exploitation du poste de travail distant redémarre. Horizon View Client se déconnecte du poste de travail.

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.

Désinstallation d'Horizon View Client

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

Pour désinstaller Horizon View Client, vous pouvez utiliser la même méthode que celle que vous utilisez habituellement pour désinstaller n'importe quelle autre application.

Sélectionnez par exemple **Applications > Centre Logiciel Ubuntu** et, dans la partie **Logiciel Installé**, sélectionnez **vmware-view-client** et cliquez sur **Supprimer**.

Une fois la désinstallation terminée, vous pouvez réinstaller l'application.

Reportez-vous à la section « Installer Horizon View Client pour Linux », page 11.

Configuration de la redirection USB sur le client

6

Avec View Client 1.6, vous pouvez utiliser un fichier de configuration sur le système client pour spécifier quels périphériques USB peuvent être redirigés vers un poste de travail View. Notez que le composant USB est disponible uniquement avec la version de View Client pour Linux fournie par des fournisseurs tiers.

Il est possible de configurer des stratégies USB à la fois pour View Agent sur le poste de travail distant, et pour View Client sur le système local, afin d'atteindre les objectifs suivants :

- Restreindre les types de périphériques USB que View Client rend disponibles à la redirection.
- Faire en sorte que View Agent empêche certains périphériques USB d'être transférés depuis un ordinateur client.
- (View Client 1.7 et versions supérieures) Spécifier si View Client doit fractionner des périphériques USB composites en des composants distincts pour une redirection.

IMPORTANT La fonction de redirection USB n'est disponible que lorsque la version de View Agent et de Serveur de connexion View est View 4.6.1 ou supérieur et uniquement avec la version de View Client fournie par des fournisseurs tiers. Les fonctionnalités de filtre USB et de fractionnement automatique décrites dans ces rubriques sont disponibles avec le Serveur de connexion View 5.1 et versions supérieures. 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 de View Client 1.6 et supérieur, certains fichiers doivent être installés dans certains emplacements et certains processus doivent être configurés pour démarrer avant le lancement de View Client. Ces détails n'entrent pas dans le cadre de ce document.

Ce chapitre aborde les rubriques suivantes :

Définition de propriétés de configuration USB

Vous pouvez définir les propriétés USB dans n'importe quel fichier d'un groupe de fichiers de configuration.

1. `/etc/vmware/config`. Le service `vmware-view-usbd` examine d'abord ce fichier. 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 ces propriétés dans le fichier de configuration.

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

Remarque Avec ces propriétés, vous pouvez autoriser la redirection de certains types de périphériques. Des propriétés de filtrage sont également disponibles pour que vous puissiez exclure certains types de périphériques et en inclure d'autres. Pour les clients Linux version 1.7 et supérieure, et pour les clients Windows, des propriétés pour fractionner des périphériques composites sont également disponibles.

Certaines valeurs 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 branché le périphérique USB sur le système local lorsque View 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 En ce qui concerne la redirection des périphériques audio, vérifiez que la version de noyau de votre système Ubuntu est 3.2.0-27.43 ou supérieur. 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 planter lorsque View Client tente de rediriger le périphérique audio. Par défaut, les périphériques audio sont redirigés.

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

Nom et propriété de la stratégie	Description
Autoriser le fractionnement automatique du périphérique Propriété : `viewusb.AllowAutoDeviceSplitting`	(View Client 1.7 et versions supérieures) Autoriser le fractionnement automatique des périphériques USB composites. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Exclure le périphérique Vid/Pid du fractionnement Propriété : `viewusb.SplitExcludeVidPid`	(View Client 1.7 et versions supérieures) Exclut le fractionnement d'un périphérique USB composite spécifié par l'ID de produit et l'ID de fournisseur. Le format du paramètre est `vid-`*`xxx1`*`_pid-`*`yyy1`*`[;vid-`*`xxx2`*`_pid-`*`yyy2`*`].....` Vous devez spécifier les numéros d'ID sous forme hexadécimale. Vous pouvez utiliser le caractère générique (**`*`**) à la place du chiffre d'un ID. Par exemple : **`vid-0781_pid-55**`** La valeur par défaut est indéfinie.

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

Nom et propriété de la stratégie	Description
Fractionner le périphérique Vid/Pid. Propriété : `viewusb.SplitVidPid`	(View Client 1.7 et versions supérieures) Traite les composants d'un périphérique USB composite spécifié par l'ID de produit et l'ID de fournisseur comme des périphériques distincts. Le format de ce paramètre est : `vid-`*xxxx*`_pid-`*yyyy*`([exintf:`*zz*`[;exintf:`*ww*`]])[;...]` Vous pouvez utiliser le mot-clé `exintf` pour exclure les composants de la redirection en spécifiant leur numéro d'interface. Vous devez spécifier les numéros d'ID sous forme hexadécimale et les numéros d'interface sous forme décimale en incluant le ou les premiers zéros. Vous pouvez utiliser le caractère générique (*****) à la place du chiffre d'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 stratégie de filtre telle que `Include Vid/Pid Device` afin d'inclure ces composants. La valeur par défaut est indéfinie.
Autoriser les périphériques d'entrée audio Propriété : `viewusb.AllowAudioIn`	Autorise la redirection des périphériques d'entrée audio. La valeur par défaut est indéfinie, ce qui équivaut à **`false`** dans View Client 2.2 ou version ultérieure, mais à **`true`** dans View Client 2.1 et version antérieure. La valeur par défaut a été modifiée, car avec View Client 2.2, 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.
Autoriser les périphériques de sortie audio Propriété : `viewusb.AllowAudioOut`	Autorise la redirection des périphériques de sortie audio. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
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`**.
Autoriser HIDBootable Propriété : `viewusb.AllowHIDBootable`	Autorise la redirection des périphériques d'entrée autres que les claviers et les souris disponibles au moment du démarrage (également appelés périphériques hid-bootable). 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 View Client ne parvient pas à obtenir les descripteurs config/device. 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`**.
Autoriser les claviers et les souris Propriété : `viewusb.AllowKeyboardMouse`	Autoriser la redirection des claviers disposant de pointeurs intégrés (tels qu'une souris, une boule de commande ou un pavé tactile). La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Autoriser les cartes à puce Propriété : `viewusb.AllowSmartcard`	Autorise la redirection des périphériques à carte à puce. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Autoriser les périphériques vidéos Propriété : `viewusb.AllowVideo`	Autorise la redirection des périphériques vidéos. La valeur par défaut est indéfinie, ce qui équivaut à **`false`** dans View Client 2.2 ou version ultérieure, mais à **`true`** dans View Client 2.1 et version antérieure. La valeur par défaut a été modifiée car avec View Client 2.2, 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.

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

Nom et propriété de la stratégie	Description
Désactiver le téléchargement de configuration distante Propriété : `viewusb.DisableRemoteConfig`	Désactive l'utilisation des paramètres View Agent lors de l'exécution du filtrage du périphérique USB. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Exclure tous les périphériques Propriété : `viewusb.ExcludeAllDevices`	Exclut tous les périphériques USB de la redirection. Si ce paramètre est réglé sur **`true`**, vous pouvez utiliser d'autres paramètres de stratégie pour autoriser la redirection de périphériques ou de familles de périphériques spécifiques. Si ce paramètre est réglé sur **`false`**, vous pouvez utiliser d'autres paramètres de stratégie pour empêcher la redirection de périphériques ou de familles de périphériques spécifiques. Si vous paramétrez la valeur de `Exclude All Devices` sur **`true`** dans View Agent et que ce paramètre passe à View Client, le paramètre View Agent est prioritaire sur le paramètre View Client. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Exclure une famille de périphériques 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 des périphériques, View examine la famille du périphérique de chaque interface d'un périphérique USB composite afin de décider quelles interfaces exclure. Si vous avez désactivé le fractionnement automatique de périphérique, View examine la famille de périphérique de la totalité du périphérique USB composite. La valeur par défaut est indéfinie.
Exclure le périphérique Vid/Pid. Propriété : `viewusb.ExcludeVidPid`	Permet d'exclure de la redirection les périphériques associés à des ID de fournisseur et de produit donnés. Le format du paramètre est `vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]... Vous devez spécifier les numéros d'ID sous forme hexadécimale. Vous pouvez utiliser le caractère générique (**`*`**) à la place du chiffre d'un ID. Par exemple : **`vid-0781_pid-****;vid-0561_pid-554c`** La valeur par défaut est indéfinie.
Exclure un chemin Propriété : `viewusb.ExcludePath`	Permet d'exclure de la redirection des périphériques correspondant à des chemins de concentrateurs ou de ports spécifiques. Le format de ce paramètre est : `bus-`*x1*[`/`*y1*]...`_port-`*z1*[`;bus-`*x2*[`/`*y2*]...`_port-`*z2*]... Vous devez spécifier les numéros de bus et de port sous forme hexadécimale. Il n'est pas possible d'utiliser le caractère générique pour les chemins d'accès. Par exemple : **`bus-1/2/3_port-02;bus-1/1/1/4_port-ff`** La valeur par défaut est indéfinie.
Inclure des familles de périphériques Propriété : `viewusb.IncludeFamily`	Permet d'inclure 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 est indéfinie.

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

Nom et propriété de la stratégie	Description
Inclure un chemin Propriété : `viewusb.IncludePath`	Permet d'inclure des périphériques correspondant à des chemins de concentrateurs ou de ports spécifiques pouvant être redirigés. Le format du paramètre est `bus-`*x1*[*/y1*]...`_port-`*z1*[`;bus-`*x2*[*/y2*]...`_port-`*z2*]... Vous devez spécifier les numéros de bus et de port sous forme hexadécimale. Il n'est pas possible d'utiliser le caractère générique pour les chemins d'accès. Par exemple : **`bus-1/2_port-02;bus-1/7/1/4_port-0f`** La valeur par défaut est indéfinie.
Inclure le périphérique Vid/Pid. Propriété : `viewusb.IncludeVidPid`	Permet d'inclure des périphériques associés à des ID de fournisseur et de produit pouvant être redirigés. Le format du paramètre est `vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]... Vous devez spécifier les numéros d'ID sous forme hexadécimale. Vous pouvez utiliser le caractère générique (*****) à la place du chiffre d'un ID. Par exemple : **`vid-0561_pid-554c`** La valeur par défaut est indéfinie.

Exemples supplémentaires

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

1 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 View Client d'autoriser la redirection des souris vers un poste de travail View. La deuxième propriété remplace la première et indique à View Client de laisser deux souris spécifiques locales et de ne pas les rediriger.

2 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 View Client qu'il faut traiter les composants d'un périphérique composite différent (`Vid-0911_Pid-149a`) comme des périphériques distincts, mais qu'il faut exclure le composant suivant de la redirection : le composant dont le numéro d'interface est 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 VMware Horizon View*.

Familles de périphériques USB

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

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.
`autre`	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.
`sécurité`	Périphériques de sécurité, tels que des lecteurs d'empreintes digitales.
`smart-card`	Périphériques à carte à puce.
`stockage`	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.

Tableau 6-2. Familles de périphériques USB (suite)

Nom de la famille de périphériques	Description
`wireless`	Adaptateurs réseau sans fil.
`wusb`	Périphériques USB sans fil.

Remarque Pour les versions antérieures à 5.1, View Client pour Windows lit la famille du périphérique sur le pilote du périphérique que vous avez installé sur l'ordinateur client. Pour View 5.1, il n'est pas nécessaire d'installer le pilote du périphérique sur un ordinateur client Windows. View Client lit la famille du périphérique sur le périphérique lui-même et pas sur le pilote du périphérique. Le micrologiciel d'un périphérique USB définit généralement la famille du périphérique, ce qui décrit sa fonction, même si tous les périphériques n'indiquent pas la valeur correcte correspondant à la famille.

Les clients légers basés sur Linux lisent toujours la famille du périphérique sur le périphérique lui-même.

Utilisation de l'option de ligne de commande View Client 1.5 pour rediriger les périphériques USB

Vous pouvez utiliser la ligne de commande `--usb=` de la commande `vmnware-view` pour configurer les périphériques USB à rediriger vers un poste de travail View. Notez que l'option de ligne de commande USB n'est disponible qu'avec la version de View Client pour Linux fournit par des fournisseurs tiers et uniquement pour View Client 1.5.

Important Si vous disposez de View Client 1.6 ou d'une version supérieure, vous devez utiliser un fichier de configuration, plutôt que l'option de ligne de commande `--usb=`, afin de configurer la redirection USB. Reportez-vous à la section Chapitre 6, « Configuration de la redirection USB sur le client », page 57.

Les arguments de l'option `--usb=` sont envoyés à la commande de redirection USB `vmware-view-usb`.

L' exemple suivant active la journalisation au niveau de la trace :

```
vmware-view --usb=log:trace
```

Vous pouvez définir plusieurs instances de l'option `--usb` pour chaque option `vmware-view-usb` que vous spécifiez. L'exemple suivant active la journalisation au niveau du débogage et exclut un périphérique défini pas son ID :

```
 vmware-view --usb=log:debug
--usb=exid:vid0012pid0034
```

Le tableau suivant répertorie les arguments que vous pouvez utiliser avec l'option `--usb`.

Tableau 6-3. Options de redirection USB

Option	Description
`disable-boot-fwd`	Désactive la détection et le filtrage du périphérique d'amorçage par le client USB View. L'activation de cette option, redirige tous les périphériques USB, y compris celui depuis lequel le système client est démarré.

`ex:`*`device1`*`[,`*`device2`*`]...`	Exclut une liste de périphériques nommés à rediriger. Par exemple :
	`vmware-view`
	`--usb=ex:"flash 1"`

`exfa:`*`device-family1`*`[,`*`device-family2`*`]...`	Exclut une liste de familles de périphériques nommées de la redirection. Par exemple :
	`vmware-view`
	`--usb=exfa:storage`

Tableau 6-3. Options de redirection USB (suite)

Option	Description

`exid:`*device-ID1*`[,`*device-ID2*`]...`	Exclut une liste de périphériques de la redirection où les périphériques sont définis par les valeurs hexadécimales de leurs ID de fournisseur et de produit en utilisant le format `vid`*xxxx*`pid`*xxxx* . Par exemple :
	`vmware-view`
	`--usb=exid:vid1e2fpid5a1e`

`expt:`*device-path1*`[,`*device-path2*`]...`	Exclut une liste de périphériques de la redirection où les périphériques sont définis par les valeurs décimales de leur bus et leurs valeurs de port en utilisant le format `bus`*n*`port`*n*. Par exemple : `vmware-view --usb=expt:bus1port4,bus5port3`

`in:`*device1*`[,`*device2*`]...`	Inclut une liste de périphériques nommés à rediriger. Par exemple :
	`vmware-view`
	`--usb=in:"flash 1"`

`infa:`*device-family1*`[,`*device-family2*`]...`	Inclut une liste de familles de périphériques nommées à rediriger. Par exemple :
	`vmware-view`
	`--usb=infa:storage`

`inid:`*device-ID1*`[,`*device-ID2*`]...`	Inclut une liste de périphériques à rediriger où les périphériques sont définis par les valeurs hexadecimales de leurs ID de fournisseur et de produit en utilisant le format `vid`*xxxx*`pid`*xxxx* . Par exemple :
	`vmware-view`
	`--usb=inid:vid27f8pid2a1b`

`inpt:`*device-path1*`[,`*device-path2*`]...`	Inclut une liste de périphériques à rediriger où les périphériques sont définis par les valeurs décimales de leur bus et de leurs valeurs de port en utilisant le format format `bus`*n*`port`*n*. Par exemple :
	`vmware-view`
	`--usb=inpt:bus3port1,bus4port2`

`log:{debug|error|info|trace}`	Définit le niveau de journalisation `vmware-view-usb:trace`, `debug`, `info` (par défaut) ou `error` en ordre décroissant de détail. Le fichier journal (`backendLog.txt`) est écrit dans `/tmp/vmware-`*username*`/vmware-view-usb-`*pid*`.log`. Par exemple :
	`vmware-view`
	`--usb=log:error`

L'ordre de priorité d'inclusion ou d'exclusion des périphériques est le suivant, de la priorité la plus élevée à la priorité la plus basse :

1 `expt` (exclut les périphériques identifiés par le bus et le port)

2 `inpt` (inclut les périphériques identifiés par le bus et le port)

3 `ex` (exclut une liste de périphériques nommés)

4 `in` (inclut une liste de périphériques nommés)

5 `exid` (exclut les périphériques identifiés par les ID de fournisseur et de produit)

6 `inid` (inclut les périphériques identifiés par les ID de fournisseur et de produit)

7 `exfa` (exclut une liste de familles de périphériques nommées)

8 `infa` (inclut une liste de familles de périphériques nommées)

L'exemple suivant exclut toutes les familles de périphérique de stockage, à part un périphérique spécifié par son ID :

```
vmware-view --usb=exfa:storage
--usb=inid:vid1812pid1492
```

La liste suivante est une liste de catégories de familles de périphériques USB que vous pouvez utiliser avec les options `infa` et `exfa`.

`audio`	`printer`
`bluetooth`	`security`
`comm`	`smart-card`
`hid`	`storage`
`hid-bootable`	`unknown`
`hub`	`vendor`
`imaging`	`video`
`other`	`wireless`
`pda`	`wusb`
`physical`	

Index