

Utilisation de VMware Horizon Client pour Windows

Septembre 2015
Horizon Client

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-001497-04

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

Copyright © 2013–2015 VMware, Inc. Tous droits réservés. [Copyright et informations sur les marques.](#)

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

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

Table des matières

| | |
|---|-----------|
| Utilisation de VMware Horizon Client pour Windows | 5 |
| 1 Configuration système requise et configuration pour clients basés sur Windows | 7 |
| Configuration système requise pour les clients Windows | 8 |
| Configuration système requise pour l'Audio/Vidéo en temps réel | 10 |
| Configuration requise pour la redirection de scanner | 10 |
| Exigences de la redirection de port série | 11 |
| Exigences pour l'utilisation de la redirection multimédia (MMR) | 12 |
| Conditions d'utilisation de la redirection d'URL flash | 15 |
| Exigences pour l'utilisation de Microsoft Lync avec Horizon Client | 15 |
| Exigences de l'authentification par carte à puce | 17 |
| Systèmes d'exploitation de poste de travail pris en charge | 18 |
| Préparation du Serveur de connexion View pour Horizon Client | 18 |
| Données Horizon Client collectées par VMware | 19 |
| 2 Installation d' Horizon Client pour Windows | 21 |
| Installer Horizon Client pour Windows | 21 |
| Activation du mode FIPS sur le système d'exploitation client Windows | 23 |
| Installation silencieuse d' Horizon Client | 24 |
| Installer Horizon Client en silence | 24 |
| Propriétés de l'installation silencieuse pour Horizon Client | 25 |
| Options de la ligne de commande Microsoft Windows Installer | 27 |
| 3 Configuration d' Horizon Client pour les utilisateurs finaux | 31 |
| Utilisation d'URI pour configurer Horizon Client | 32 |
| Syntaxe pour la création d'URI vmware-view | 32 |
| Exemples d'URI de vmware-view | 35 |
| Configuration de la vérification des certificats pour les utilisateurs finaux | 37 |
| Modes de vérification des certificats pour Horizon Client | 38 |
| Configuration des options TLS/SSL avancées | 39 |
| Utilisation du modèle de stratégie de groupe pour configurer VMware Horizon Client pour Windows | 40 |
| Paramètres de définition de scripts des objets de stratégie de groupe (GPO) des clients | 40 |
| Paramètres de sécurité des objets de stratégie de groupe (GPO) des clients | 42 |
| Paramètres RDP des objets de stratégie de groupe (GPO) des clients | 46 |
| Paramètres généraux des objets de stratégie de groupe (GPO) de clients | 48 |
| Paramètres UBS des objets de stratégie de groupe (GPO) des clients | 50 |
| Paramètres de modèle d'administration pour les variables de session de client PCoIP de View | 52 |
| Exécution d' Horizon Client depuis la ligne de commande | 56 |
| Utilisation des commandes d' Horizon Client | 56 |

| | | |
|----------|--|-----------|
| | Consulter le fichier de configuration Horizon Client | 58 |
| | Utilisation du Registre Windows pour configurer Horizon Client | 59 |
| 4 | Gestion des connexions aux applications et postes de travail distants | 61 |
| | Connexion à une application ou un poste de travail distant | 61 |
| | Conseils pour l'utilisation de la fenêtre de sélection des postes de travail et des applications | 64 |
| | Partager l'accès aux dossiers et lecteurs locaux | 65 |
| | Masquer la fenêtre VMware Horizon Client | 67 |
| | Reconnexion à un poste de travail ou à une application | 67 |
| | Créer un raccourci de poste de travail ou d'application sur votre poste de travail client ou menu Démarrer | 68 |
| | Basculer entre des postes de travail ou des applications | 69 |
| | Fermer une session ou se déconnecter | 70 |
| 5 | Travail dans une application ou un poste de travail distant | 73 |
| | Matrice de prise en charge des fonctionnalités pour les clients Windows | 73 |
| | Internationalisation | 76 |
| | Utilisation d'un IME (éditeur de méthode d'entrée) local | 77 |
| | Activation de la prise en charge des claviers à l'écran | 78 |
| | Utilisation de plusieurs moniteurs | 78 |
| | Modifier le mode d'affichage lorsque la fenêtre d'un poste de travail est ouverte | 80 |
| | Connecter des périphériques USB | 80 |
| | Configurer les clients pour qu'ils se reconnectent lors du redémarrage de périphériques USB | 83 |
| | Utilisation de la fonctionnalité Audio/Vidéo en temps réel pour webcams et microphones | 84 |
| | Conditions d'utilisation de votre Webcam | 84 |
| | Sélectionner une webcam préférée sur un système client Windows | 85 |
| | Sélectionner un microphone par défaut sur un système client Windows | 86 |
| | Utilisation de scanners | 87 |
| | Utilisation de la redirection de port série | 88 |
| | Copier-coller du texte et des images | 89 |
| | Utilisation des applications distantes | 90 |
| | Enregistrement de documents dans une application distante | 90 |
| | Impression à partir d'une application ou d'un poste de travail distant | 90 |
| | Définir les préférences d'impression pour la fonction d'impression virtuelle sur un poste de travail distant | 91 |
| | Utilisation d'imprimantes USB | 92 |
| | Contrôler l'affichage d'Adobe Flash | 92 |
| | Utilisation de la fonction de souris relative pour des applications de CAO et 3D | 93 |
| | Raccourcis clavier | 94 |
| 6 | Résolution des problèmes d' Horizon Client | 97 |
| | Que faire si Horizon Client se ferme de façon inattendue | 97 |
| | Réinitialiser une application ou un poste de travail distant | 97 |
| | Désinstallation d' Horizon Client | 98 |

| | |
|-------|----|
| Index | 99 |
|-------|----|

Utilisation de VMware Horizon Client pour Windows

Ce guide, intitulé *Utilisation de VMware Horizon Client pour Windows*, fournit des informations concernant l'installation et l'utilisation du logiciel VMware Horizon™ Client™ sur un système client Microsoft Windows pour se connecter à une application ou à un poste de travail distant du centre de données.

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

Ces informations sont conçues pour les administrateurs qui doivent configurer un déploiement d'View comportant des systèmes clients Microsoft Windows, tels que des postes de travail et des ordinateurs portables. Les informations sont rédigées pour des administrateurs système expérimentés qui connaissent parfaitement la technologie des machines virtuelles et les opérations de datacenter.

Configuration système requise et configuration pour clients basés sur Windows

1

Les systèmes exécutant des composants Horizon Client doivent respecter certaines configurations matérielles et logicielles.

Horizon Client sur des systèmes Windows utilise les paramètres Internet de Microsoft Internet Explorer, notamment des paramètres proxy, lors de la connexion au Serveur de connexion View. Assurez-vous que vos paramètres Internet Explorer sont exacts et que vous pouvez accéder à l'URL de Serveur de connexion View via Internet Explorer.

Ce chapitre aborde les rubriques suivantes :

- [« Configuration système requise pour les clients Windows », page 8](#)
- [« Configuration système requise pour l'Audio/Vidéo en temps réel », page 10](#)
- [« Configuration requise pour la redirection de scanner », page 10](#)
- [« Exigences de la redirection de port série », page 11](#)
- [« Exigences pour l'utilisation de la redirection multimédia \(MMR\) », page 12](#)
- [« Conditions d'utilisation de la redirection d'URL flash », page 15](#)
- [« Exigences pour l'utilisation de Microsoft Lync avec Horizon Client », page 15](#)
- [« Exigences de l'authentification par carte à puce », page 17](#)
- [« Systèmes d'exploitation de poste de travail pris en charge », page 18](#)
- [« Préparation du Serveur de connexion View pour Horizon Client », page 18](#)
- [« Données Horizon Client collectées par VMware », page 19](#)

Configuration système requise pour les clients Windows

Vous pouvez installer Horizon Client pour Windows sur des ordinateurs de bureau ou portables qui utilisent un système d'exploitation Microsoft Windows pris en charge.

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

| | | | |
|---|--|----------------|--|
| Modèle | Ordinateur de bureau ou portable compatible x86 ou x86 64 bits standard Horizon Client 3.3 et versions ultérieures prennent également en charge les tablettes basées sur x86, telles que Windows Surface Pro. | | |
| Mémoire | Au moins 1 Go de RAM | | |
| Systèmes d'exploitation | <ul style="list-style-type: none"> Pour Horizon Client 3.5, les systèmes d'exploitation suivants sont pris en charge. | | |
| | OS | Versión | SP |
| | Windows 10 | 32 ou 64 bits | S/O |
| | Windows 8 ou 8.1 | 32 ou 64 bits | Aucun ou Update 2 |
| | Windows 7 | 32 ou 64 bits | SP1 |
| | | | Édition |
| | | | Enterprise |
| | | | Pro et Enterprise |
| | | | Home, Enterprise, Professional et Ultimate |
| | <ul style="list-style-type: none"> Pour Horizon Client 3.3 et 3.4, les systèmes d'exploitation suivants sont pris en charge. | | |
| | OS | Versión | SP |
| | Windows 8 ou 8.1 | 32 ou 64 bits | Aucun ou mise à jour |
| | Windows 7 | 32 ou 64 bits | SP1 |
| | | | Édition |
| | | | Pro et Enterprise |
| | | | Home, Enterprise, Professional et Ultimate |
| | <ul style="list-style-type: none"> Pour Horizon Client 3.0, 3.1 et 3.2, les systèmes d'exploitation suivants sont pris en charge. | | |
| | OS | Versión | SP |
| | Windows 8 ou 8.1 | 32 ou 64 bits | Aucun ou mise à jour |
| | Windows 7 | 32 ou 64 bits | Aucun ou SP1 |
| | Windows XP | 32 bits | SP3 |
| | Windows Vista | 32 bits | SP1 ou SP2 |
| | | | Édition |
| | | | Pro - Desktop et Enterprise - Desktop |
| | | | Home, Enterprise, Professional/Business et Ultimate. |
| | | | Home et Professional |
| | | | Home, Enterprise, Professional/Business et Ultimate. |
| Serveur de connexion View, serveur de sécurité et View Agent | Dernière version de maintenance de View 5.3.x et versions ultérieures. Si des systèmes clients se connectent en dehors du pare-feu d'entreprise, VMware vous recommande d'utiliser un serveur de sécurité ou un dispositif Access Point pour que les systèmes clients ne requièrent pas de connexion VPN. | | |

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

REMARQUE Les clients peuvent également se connecter au dispositif Access Point, qui est disponible avec Horizon 6, version 6.2.

Protocole d'affichage pour View

PCoIP ou RDP

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 :

$20\text{MB} + (24 * (\# \text{ monitors}) * (\text{monitor width}) * (\text{monitor height}))$

Comme indicateur rapide, vous pouvez utiliser les calculs suivants :

1 monitor: 1600 x 1200: 64MB

2 monitors: 1600 x 1200: 128MB

3 monitors: 1600 x 1200: 256MB

Exigences matérielles pour RDP

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

Exigences logicielles pour RDP

- (Pris en charge avec Horizon Client 3.0, 3.1 et 3.2 uniquement) Pour les systèmes Windows XP et Windows XP Embedded, utilisez Microsoft RDP 6.1.
- (Pris en charge avec Horizon Client 3.0, 3.1 et 3.2 uniquement) Windows Vista inclut RDP 6.1, mais RDP 7.1 est recommandé.
- Pour Windows 7, utilisez RDP 7.1 ou 8.0. Windows 7 comprend RDP 7.1. Windows 7 SP1 inclut RDP 7.1.
- Pour Windows 8, utilisez RDP 8.0. Pour Windows 8.1, utilisez RDP 8.1.
- Pour Windows 10, utilisez RDP 10.0.
- (Pris en charge avec View Agent 6.0.2 et versions antérieures uniquement) Pour les machines virtuelles de poste de travail Windows XP, vous devez installer les correctifs RDP répertoriés dans les articles 323497 et 884020 de la Base de connaissances de Microsoft. Si vous n'installez pas les correctifs RDP, le message Échec des sockets Windows risque de s'afficher sur le client.
- Le programme d'installation de View Agent configure la règle de pare-feu locale pour que les connexions RDP entrantes correspondent au port RDP actuel du système d'exploitation hôte, en général le port 3389. Si vous changez le numéro du port RDP, vous devez changer les règles de pare-feu associées.

Vous pouvez télécharger les versions de Remote Desktop Client sur le Centre de téléchargement de Microsoft.

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

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

Poste de travail distant View

View Agent 5.3 ou version ultérieure doit être installé sur les postes de travail. S'agissant des postes de travail View Agent 5.3, 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 View 5.3 Feature Pack 1. Reportez-vous au document *Installation et administration de View Feature Pack* pour View. Si vous disposez de View Agent 6.0 ou version ultérieure, aucun Feature Pack n'est requis. La fonctionnalité Audio/Vidéo en temps réel n'est pas prise en charge dans les applications distantes.

Ordinateur Horizon Client ou périphérique d'accès client

- L'Audio/Vidéo en temps réel est pris en charge par tous les systèmes d'exploitation client Windows qui utilisent Horizon Client pour Windows. Pour plus d'informations, reportez-vous à « [Configuration système requise pour les clients Windows](#) », page 8.
- 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 View

PCoIP

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

Configuration requise pour la redirection de scanner

Avec Horizon Client 3.2 et versions ultérieures, vous pouvez scanner des informations vers vos postes de travail à distance et applications distantes avec des scanners connectés à votre système client local.

Pour utiliser cette fonctionnalité, vos postes de travail à distance, vos applications et vos ordinateurs clients doivent répondre à certaines configurations système requises.

Poste de travail distant View

Les postes de travail à distance requièrent l'installation de View Agent 6.0.2 ou d'une version ultérieure, avec l'option de configuration de redirection de scanner, sur les machines virtuelles parentes ou modèles, ou sur les hôtes RDS. Sur les systèmes d'exploitation Windows et Windows Server, l'option de configuration de redirection de scanner de View Agent est désélectionnée par défaut.

Pour plus d'informations sur les systèmes d'exploitation invités pris en charge sur les machines virtuelles mono. utilisateur et sur les hôtes RDS, et sur la configuration de la redirection de scanner dans les postes de travail à distance et les applications, reportez-vous à « Configuration de redirection de scanner », dans *Configuration de pools de postes de travail et d'applications dans View*.

**Ordinateur
Horizon Client ou
périphérique d'accès
client**

- Horizon Client 3.2 ou version ultérieure doit être installé sur le système client.
- La redirection de scanner est prise en charge sur les systèmes d'exploitation Windows Vista 32 bits, Windows 7 32 ou 64 bits, et Windows 8/8.1 32 et 64 bits. Avec Horizon Client 3.5 ou version ultérieure, Windows 10 est également pris en charge.
- Les pilotes du scanner doivent être installés, et ce dernier doit être opérationnel sur l'ordinateur client. Vous n'avez pas besoin d'installer les pilotes du scanner sur le système d'exploitation du poste de travail à distance sur lequel View Agent est installé.

Norme de scanner

TWAIN ou WIA

**Protocole d'affichage
pour View**

PCoIP

La redirection de scanner n'est pas prise en charge dans les sessions de poste de travail RDP.

Exigences de la redirection de port série

Avec cette fonction, les utilisateurs peuvent rediriger des ports série (COM) connectés en local, tels que les ports RS232 intégrés ou les adaptateurs USB-série, vers leurs postes de travail distants. Pour prendre en charge la redirection de port série, votre déploiement de View doit répondre à certaines exigences matérielles et logicielles.

**Poste de travail distant
View**

Les postes de travail distants requièrent l'installation de View Agent 6.1.1 ou d'une version ultérieure, avec l'option d'installation de redirection de port série, sur les machines virtuelles parentes ou modèles. Cette option d'installation n'est pas sélectionnée par défaut.

Les systèmes d'exploitation invités suivants sont pris en charge sur les machines virtuelles mono-utilisateur :

- Windows 7 32 ou 64 bits
- Windows 8.x 32 ou 64 bits
- Windows 10 32 ou 64 bits
- Windows Server 2008 R2 configuré en tant que poste de travail
- Windows Server 2012 R2 configuré en tant que poste de travail

Cette fonction n'est pas actuellement prise en charge pour les hôtes RDS Windows Server.

Les pilotes du périphérique de port série n'ont pas à être installés sur le système d'exploitation du poste de travail où View Agent est installé.

REMARQUE Pour plus d'informations sur la configuration de la redirection de port série sur les postes de travail distants, reportez-vous à la section « Configuration de la redirection de port série » dans *Configuration de pools de postes de travail et d'applications dans View*.

**Ordinateur
Horizon Client ou
périphérique d'accès
client**

- Horizon Client pour Windows 3.4 ou version ultérieure doit être installé sur le système client.
- La redirection de port série est prise en charge sur les systèmes clients Windows 7 32 ou 64 bits, Windows 8.x 32 ou 64 bits et Windows 10 32 et 64 bits.
- Tous les pilotes du périphérique de port série nécessaires doivent être installés, et le port série doit être opérationnel sur l'ordinateur client. Vous n'avez pas besoin d'installer les pilotes du périphérique sur le système d'exploitation du poste de travail distant sur lequel View Agent est installé.

**Protocole d'affichage
pour View**

PCoIP

La redirection de port série VMware Horizon n'est pas prise en charge dans les sessions de poste de travail RDP.

Exigences pour l'utilisation de la redirection multimédia (MMR)

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

La fonctionnalité MMR étant mise en œuvre différemment selon les systèmes d'exploitation, les configurations système requises pour certains systèmes d'exploitation Windows diffèrent des configurations requises pour d'autres systèmes d'exploitation Windows antérieurs.

De même, les composants MMR installés avec certaines versions de View Agent diffèrent de ceux installés avec des versions antérieures de View Agent. La configuration requise pour les différentes combinaisons View Agent et système d'exploitation client est abordée dans d'autres sections de cette rubrique.

REMARQUE Pour découvrir la comparaison des composants MMR Windows Media, MMR de Windows 7 et MMR Wyse, ainsi qu'une matrice indiquant la prise en charge de plusieurs combinaisons de versions de client, de versions d'agent et de systèmes d'exploitation, reportez-vous à « Prise en charge de la redirection multimédia par les systèmes d'exploitation des postes de travail », dans le guide d'Horizon 6, version 6.0.2 intitulé *Configuration de pools de postes de travail et d'applications dans View*.

Configuration requise de MMR Windows Media pour Horizon Client 3.2 et versions ultérieures

Pour pouvoir utiliser la fonctionnalité MMR Windows Media sur les clients Windows 7 et 8.x, vos serveurs, postes de travail virtuels et ordinateurs clients doivent respecter certaines exigences de configuration.

Exigences logicielles de VMware pour postes de travail distants

- Pour utiliser cette fonctionnalité avec des postes de travail VDI qui sont déployés sur des machines virtuelles mono-utilisateur, View Agent 6.0.2 ou une version ultérieure doit être installé sur le poste de travail.

IMPORTANT Si vous utilisez Horizon Client 3.2 ou version ultérieure pour vous connecter à un poste de travail View sur lequel View Agent 6.0.1 ou une version antérieure est installé, ni la fonctionnalité MMR Windows Media, ni la fonctionnalité MMR Windows 7 ne fonctionneront.

- Pour utiliser cette fonctionnalité avec des postes de travail distants fournis par un hôte RDS, View Agent 6.1.1 ou une version ultérieure doit être installé sur l'hôte RDS.
- Pour plus d'informations sur les exigences de système d'exploitation, les exigences logicielles et les paramètres de configuration de l'application ou du poste de travail distant, consultez les rubriques sur la Redirection multimédia Windows Media dans *Configuration de pools de postes de travail et d'applications dans View* pour votre version spécifique d'Horizon 6.

Ordinateur Horizon Client ou périphérique d'accès client

- Les clients doivent exécuter des systèmes d'exploitation Windows 7 ou Windows 8/8.1 à 64 ou 32 bits.

Formats multimédias pris en charge

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

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

Exigences concernant la fonctionnalité MMR Horizon Client 3.0 et 3.1 pour les systèmes d'exploitation Windows 7

Pour pouvoir utiliser la fonctionnalité MMR à la place de la fonctionnalité MMR Windows Media sur des postes de travail View Windows 7 et des clients Windows 7 ou 8, vos serveurs, postes de travail virtuels et ordinateurs clients doivent respecter certaines exigences de configuration.

IMPORTANT Avec Horizon Client 3.0 et 3.1, les postes de travail à distance Windows 8 ne prennent pas en charge la fonctionnalité MMR. Pour ces agents View, utilisez la redirection multimédia de Windows incluse dans RDP 7 et versions ultérieures, ou mettez à niveau vers Horizon Client 3.2 ou version ultérieure et View Agent 6.0.2 ou version ultérieure.

Exigences logicielles VMware

- Les serveurs et les postes de travail View doivent posséder View 5.3 ou version ultérieure.

| | |
|---|---|
| | <ul style="list-style-type: none"> ■ Sur les postes de travail View 5.3 ou versions antérieures, vous devez également installer la dernière version de Remote Experience Agent. Reportez-vous au document <i>Installation et administration de View Feature Pack</i> pour View 5.3 Feature Pack 1. Pour View 6.0 ou 6.0.1, cet agent est inclus dans le programme d'installation de View Agent. ■ Pour obtenir des informations sur d'autres paramètres de configuration requis, consultez la documentation d'View. |
| Poste de travail View | <ul style="list-style-type: none"> ■ Les postes de travail doivent tourner sur des systèmes d'exploitation Windows 7, 64 ou 32 bits. ■ Le Rendu 3D doit être activé sur le pool de postes de travail. ■ La version du matériel virtuel des machines virtuelles poste de travail doit être 8 ou plus. ■ Les utilisateurs doivent effectuer la lecture de leurs vidéos avec Windows Media Player 12 ou version ultérieure. |
| Ordinateur Horizon Client ou périphérique d'accès client | <ul style="list-style-type: none"> ■ Les clients doivent tourner sur des systèmes d'exploitation Windows 7 ou Windows 8, 64 ou 32 bits. ■ Les clients doivent disposer de cartes vidéo compatibles DXVA (DirectX Video Acceleration) qui peuvent décoder les vidéos sélectionnées. ■ Windows Media Player 12 ou version ultérieure doit être installé sur les clients pour permettre la redirection vers le matériel local. |
| Formats multimédias pris en charge | <p>Les formats multimédias doivent être conformes à la norme de compression vidéo H.264. Les formats de fichiers M4V, MP4 et MOV sont pris en charge. Vos postes de travail virtuels doivent utiliser l'un de ces formats de fichiers et les décodeurs locaux de ces formats doivent exister sur les systèmes client.</p> |

Exigences concernant la fonctionnalité MMR Horizon Client 3.0, 3.1 et 3.2 pour les systèmes d'exploitation Windows Vista et Windows XP

Pour qu'il soit possible d'utiliser la fonctionnalité MMR sur des postes de travail distants Windows Vista et Windows XP, vos serveurs, postes de travail virtuels et ordinateurs clients doivent respecter la configuration système.

| | |
|--|---|
| Exigences logicielles VMware | <ul style="list-style-type: none"> ■ Vous devez disposer de serveurs et de postes de travail VMware View 4.6.1 ou version ultérieure. |
| Poste de travail distant | <ul style="list-style-type: none"> ■ Les postes de travail doivent exécuter les systèmes d'exploitation Windows Vista ou Windows XP 32 bits. ■ Les utilisateurs doivent lire leurs vidéos avec Windows Media Player 10 ou supérieur. |
| Ordinateur ou périphérique d'accès client | <ul style="list-style-type: none"> ■ Les postes de travail doivent exécuter les systèmes d'exploitation Windows Vista, Windows XP ou Windows XP Embedded 32 bits. ■ Windows Media Player 10 ou supérieur doit être installé sur les clients pour permettre la redirection vers le matériel local. |

- Le matériel d'affichage vidéo d'Horizon Client doit prendre en charge la superposition pour que MMR fonctionne correctement.

IMPORTANT Horizon Client 3.3 n'est pas pris en charge par les systèmes d'exploitation Windows XP et Windows Vista.

Formats multimédias pris en charge

La fonction MMR prend en charge les formats de fichier média que le système client prend en charge, car des décodeurs locaux doivent exister sur le client. Les formats de fichier incluent MPEG2-1, MPEG-2, MPEG-4 Part 2, WMV 7, 8 et 9; WMA, AVI, ACE, MP3 et WAV, entre autres.

REMARQUE Vous devez ajouter le port MMR en tant qu'exception à votre logiciel de pare-feu. Le port par défaut pour MMR est 9427.

Conditions d'utilisation de la redirection d'URL flash

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

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

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

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

- 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 Adobe Flash Player 10.1 ou version ultérieure pour Internet Explorer (qui utilise ActiveX).

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

Exigences pour l'utilisation de Microsoft Lync avec Horizon Client

Vous pouvez utiliser un client Microsoft Lync 2013 sur des postes de travail distants pour participer à des appels VoIP (Voice over IP) de communications unifiées et de conversation vidéo avec des périphériques audio et vidéo USB certifiés Lync. Il n'est plus nécessaire de disposer d'un téléphone IP dédié.

Cette architecture requiert l'installation d'un client Microsoft Lync 2013 sur le poste de travail distant et d'un plug-in VDI Microsoft Lync sur le point de terminaison du client. Les clients peuvent utiliser le client Microsoft Lync 2013 pour les fonctions de présence, de messagerie instantanée, de conférence Web et Microsoft Office.

À chaque appel VoIP ou de tchat vidéo Lync, le plug-in VDI Lync décharge tout le traitement multimédia du serveur de datacenter vers le point de terminaison du client, et code tout le multimédia en codecs audio et vidéo optimisés pour Lync. Cette architecture optimisée est hautement évolutive, entraîne une utilisation réduite de la bande passante réseau et fournit une livraison de données multimédia point à point avec la prise en charge de VoIP et de la vidéo en temps réel haute qualité. Pour plus d'informations, consultez le Livre blanc sur Horizon 6 et Microsoft Lync 2013, à l'adresse <http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-microsoft-lync-install-configure.pdf>.

REMARQUE L'enregistrement audio n'est pas encore pris en charge. Cette intégration est prise en charge uniquement avec le protocole d'affichage PCoIP.

Cette fonction a les exigences suivantes :

Système d'exploitation

- Système d'exploitation client : Windows 7 SP1 32 ou 64 bits ou Windows 8.x. Pour Horizon Client 3.5, vous pouvez également utiliser Windows 10.
- Le système d'exploitation de machine virtuelle (agent) dépend de la version de View Agent.

| Version | système d'exploitation client |
|-----------------------------|--|
| View Agent 6.2 ou supérieur | Windows 7 SP1 32 ou 64 bits, Windows 8.x, Windows 10 ou Windows Server 2008 R2 SP1 64 bits Pour les hôtes Microsoft RDS : Windows Server 2008 R2, Windows 2012 ou Windows 2012 R2 |
| View Agent 6.0 ou 6.1 | Windows 7 SP1 32 ou 64 bits, Windows 8.x ou Windows Server 2008 R2 SP1 64 bits |
| View Agent 5.3 | Windows 7 SP1 32 ou 64 bits |

Logiciel système client

- Version 32 bits du plug-in VDI Microsoft Lync

IMPORTANT La version 64 bits de Microsoft Office ne doit pas être installée sur la machine cliente. Le plug-in VDI Microsoft Lync 32 bits requis n'est pas compatible avec Microsoft Office 2013 64 bits.

- Le certificat de sécurité généré lors du déploiement de Microsoft Lync Server 2013 doit être importé dans le répertoire Autorités de certification racine approuvées.

Logiciel de poste de travail distant (agent)

- View Agent 5.3 ou supérieur
- Microsoft Lync 2013 Client
Avec View 5.3 ou un agent ultérieur, le niveau binaire de Lync 2013 Client ne doit pas nécessairement correspondre à celui du système d'exploitation de la machine virtuelle.
- Le certificat de sécurité généré lors du déploiement de Microsoft Lync Server 2013 doit être importé dans le répertoire Autorités de certification racine approuvées

Serveurs requis

- Un serveur exécutant le Serveur de connexion View 5.3 ou version ultérieure
- Un serveur exécutant Microsoft Lync Server 2013

- Une infrastructure vSphere pour héberger les machines virtuelles
Les hôtes de vCenter Server et ESXi doivent exécuter vSphere 5.0 ou supérieur.

Matériel

- Matériel prenant en charge tous les composants logiciels requis cités précédemment
- Point de terminaison client : CPU de 1,5 GHz ou plus et un minimum de 2 Go de RAM pour le plug-in Microsoft Lync 2013

REMARQUE Pour obtenir des informations de dépannage, reportez-vous aux articles de base de connaissances [VMware KB 2063769](#) et [VMware KB 2053732](#).

Exigences de l'authentification par carte à puce

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

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

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

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

View prend en charge les cartes à puce et les lecteurs de carte à puce qui utilisent un fournisseur PKCS#11 ou Microsoft CryptoAPI. Facultativement, vous pouvez installer la suite logicielle ActivIdentity ActivClient qui fournit des outils pour interagir avec des cartes à puce.

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

Pour installer des certificats sur une carte à puce, vous devez configurer un ordinateur pour qu'il agisse comme une station d'inscription. Cet ordinateur doit avoir l'autorité d'émettre des certificats de carte à puce pour les utilisateurs, et il doit être membre du domaine pour lequel vous émettez des certificats.

IMPORTANT Lorsque vous inscrivez une carte à puce, vous pouvez choisir la taille de clé du certificat résultant. Pour utiliser des cartes à puce avec des postes de travail locaux, vous devez sélectionner une clé de 1 024 bits ou de 2 048 bits au cours de l'inscription de carte à puce. Les certificats avec des clés de 512 bits ne sont pas pris en charge.

Le site Web Microsoft TechNet comporte des informations détaillées sur la planification et l'implémentation de l'authentification par carte à puce pour les systèmes Windows.

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

- Pour plus d'informations sur la configuration des serveurs View Server pour prendre en charge l'utilisation des cartes à puce, reportez-vous à la rubrique « Configurer l'authentification par carte à puce » dans le document *Administration de View*.

Tous les certificats d'autorité de certification applicables pour tous les certificats utilisateur approuvés doivent être ajoutés à un fichier de magasin d'approbations du serveur sur l'hôte du Serveur de connexion View ou sur l'hôte du serveur de sécurité. Ces certificats incluent des certificats racines et doivent inclure des certificats intermédiaires si le certificat de carte à puce de l'utilisateur a été délivré par une autorité de certification intermédiaire.

- Pour plus d'informations sur les tâches que vous pouvez effectuer dans Active Directory afin d'implémenter l'authentification par carte à puce, reportez-vous aux rubriques sur la préparation d'Active Directory pour l'authentification par carte à puce, dans le document *Installation de View*.

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

Certains systèmes d'exploitation invités Linux sont également pris en charge si vous possédez View Agent 6.1.1 ou version ultérieure et Horizon Client 3.4 ou version ultérieure. Pour plus d'informations sur la configuration système requise, la configuration des machines virtuelles Linux pour les utiliser dans Horizon 6 et obtenir la liste des fonctions prises en charge, consultez *Configuration des postes de travail Horizon 6 for Linux*, qui fait partie de la documentation d'Horizon 6, version 6.1.

Préparation du Serveur de connexion View pour Horizon Client

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

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

- Si vous prévoyez d'utiliser Access Point, qui est disponible avec Horizon 6 version 6.2 ou ultérieure, configurez le Serveur de connexion View pour qu'il fonctionne avec Access Point. Reportez-vous à *Déploiement et configuration d'un point d'accès*. Les dispositifs Access Point remplissent le même rôle que celui précédemment joué uniquement par des serveurs de sécurité View.
- Si vous utilisez un serveur de sécurité, assurez-vous de disposer des dernières versions de maintenance du Serveur de connexion View 5.3.x et du Serveur de sécurité View 5.3.x ou version ultérieure. Reportez-vous au document *Installation de View*.
- Si vous prévoyez d'utiliser une connexion tunnel sécurisée pour des périphériques client et si la connexion sécurisée est configurée avec un nom d'hôte DNS pour le Serveur de connexion 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 ou d'applications a été créé et que le compte d'utilisateur que vous souhaitez utiliser est autorisé à accéder au pool. Pour le Serveur de connexion View 5.3.x, consultez les rubriques sur la création de pools de postes de travail dans le document *Administration de View*. Pour le Serveur de connexion View 6.0 et versions antérieures, consultez les rubriques sur la création de pools de postes de travail et d'applications dans le document *Configuration de pools de postes de travail et d'applications pour View*.

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

Données Horizon Client collectées par VMware

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

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

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

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

| Description | Ce champ reste-t-il anonyme ? | Exemple |
|---|-------------------------------|--|
| Entreprise ayant produit l'application Horizon Client | Non | VMware |
| Nom du produit | Non | VMware Horizon Client |
| Version du produit client | Non | (Le format est <i>x.x.x-yyyyyy</i> , où <i>x.x.x</i> est le numéro de version du client et <i>yyyyyy</i> est le numéro de build.) |
| Architecture binaire du client | Non | Exemples : <ul style="list-style-type: none"> ■ i386 ■ x86_64 ■ arm |
| Nom du build du client | Non | Exemples : <ul style="list-style-type: none"> ■ VMware-Horizon-Client-Win32-Windows ■ VMware-Horizon-Client-Linux ■ VMware-Horizon-Client-iOS ■ VMware-Horizon-Client-Mac ■ VMware-Horizon-Client-Android ■ VMware-Horizon-Client-WinStore |
| Système d'exploitation hôte | Non | Exemples : <ul style="list-style-type: none"> ■ Windows 8.1 ■ Windows 7, 64 bits Service Pack 1 (Build 7601) ■ iPhone OS 5.1.1 (9B206) ■ Ubuntu 12.04.4 LTS ■ Mac OS X 10.8.5 (12F45) |

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

| Description | Ce champ reste-t-il anonyme ? | Exemple |
|---|-------------------------------|--|
| Noyau du système d'exploitation hôte | Non | Exemples : <ul style="list-style-type: none"> ■ 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 : <ul style="list-style-type: none"> ■ x86_64 ■ i386 ■ armv71 ■ ARM |
| Modèle du système hôte | Non | Exemples : <ul style="list-style-type: none"> ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision WorkStation T3400 (A04 03/21/2008) |
| Processeur du système hôte | Non | Exemples : <ul style="list-style-type: none"> ■ 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 : <ul style="list-style-type: none"> ■ 4096 ■ inconnu (pour Windows Store) |
| Nombre de périphériques USB connectés | Non | 2 (la redirection de périphériques USB est prise en charge uniquement pour les clients Linux, Windows et Mac OS X.) |
| Nombre maximal de connexions de périphériques USB simultanées | Non | 2 |
| ID de fournisseur de périphériques USB | Non | Exemples : <ul style="list-style-type: none"> ■ Kingston ■ NEC ■ Nokia ■ Wacom |
| ID de produit de périphérique USB | Non | Exemples : <ul style="list-style-type: none"> ■ DataTraveler ■ Gamepad ■ Disque de stockage ■ Souris sans fil |
| Famille de périphériques USB | Non | Exemples : <ul style="list-style-type: none"> ■ Sécurité ■ Périphérique d'interface humaine ■ Imagerie |
| Nombre d'utilisations du périphérique USB | Non | (Nombre de partages du périphérique) |

Installation d' Horizon Client pour Windows

2

Vous pouvez obtenir le programme d'installation d'Horizon Client pour Windows sur le site Web de VMware ou depuis une page d'accès Web fournie par le Serveur de connexion View. Vous pouvez définir différentes options de démarrage pour les utilisateurs finaux après l'installation d'Horizon Client.

Ce chapitre aborde les rubriques suivantes :

- « [Installer Horizon Client pour Windows](#) », page 21
- « [Activation du mode FIPS sur le système d'exploitation client Windows](#) », page 23
- « [Installation silencieuse d'Horizon Client](#) », page 24

Installer Horizon Client pour Windows

Les utilisateurs finaux utilisent Horizon Client pour se connecter à leurs postes de travail virtuels et à leurs applications distantes (hébergées) à partir d'un système client. Vous pouvez exécuter un fichier du programme d'installation Windows pour installer tous les composants d'Horizon Client.

Cette procédure décrit l'installation d'Horizon Client à l'aide d'un assistant d'installation interactive. Si vous préférez utiliser la fonction d'installation silencieuse en ligne de commande de MSI (Microsoft Windows Installer), reportez-vous à la section « [Installer Horizon Client en silence](#) », page 24.

REMARQUE Avec Horizon Client 3.0 ou version ultérieure, vous pouvez installer le logiciel client sur une machine virtuelle de poste de travail distant si ce poste de travail exécute View Agent 6.0 ou version ultérieure. Les entreprises peuvent utiliser cette stratégie, par exemple, si leurs utilisateurs finaux disposent de périphériques clients légers Windows et souhaitent accéder à des applications distantes à partir de ces périphériques.

Prérequis

- Vérifiez que le système client utilise un système d'exploitation pris en charge. Reportez-vous à la section « [Configuration système requise pour les clients Windows](#) », page 8.
- Vérifiez que vous disposez de l'URL d'accès à une page de téléchargement contenant le programme d'installation d'Horizon Client. Il peut s'agir de l'URL de la page de téléchargements de VMware à l'adresse <http://www.vmware.com/go/viewclients> ou de l'URL d'une instance du Serveur de connexion View.
- Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur le système client.
- Vérifiez que les contrôleurs de domaine disposent des derniers correctifs, d'un espace disque libre suffisant et peuvent communiquer entre eux. Si vous ne le faites pas, lorsque vous exécuterez le programme d'installation sur un système Windows 8.1, l'exécution du programme d'installation pourra être anormalement longue. Ce problème survient si le contrôleur de domaine de la machine ou un autre contrôleur de domaine de sa hiérarchie ne répond pas ou est inaccessible.

- Si vous prévoyez d'installer Horizon Client avec une cryptographie compatible FIPS, activez le mode FIPS sur le système d'exploitation Windows avant d'exécuter le programme d'installation du client. Reportez-vous à la section « [Activation du mode FIPS sur le système d'exploitation client Windows](#) », page 23.
- Conditions préalables pour la redirection USB :
 - Déterminez si, en mode FIPS, la personne qui utilise le périphérique client est autorisée à accéder à des périphériques USB connectés en local depuis un poste de travail virtuel. Si ce n'est pas le cas, vous pouvez désélectionner le composant **Redirection USB** que l'assistant présente ou installer le composant mais le désactiver à l'aide de GPO.

VMware vous recommande de toujours installer le composant **Redirection USB** et d'utiliser des GPO pour contrôler l'accès USB. Ainsi, si vous souhaitez activer ultérieurement la redirection USB pour un client, vous n'aurez pas à réinstaller Horizon Client. Pour en savoir plus, consultez la rubrique sur les paramètres du modèle d'administration pour la configuration d'Horizon Client.
 - Si vous prévoyez d'installer le composant **Redirection USB**, vérifiez que la fonction Mise à jour automatique Windows n'est pas désactivée sur l'ordinateur client.
- Déterminez si vous voulez utiliser la fonctionnalité qui permet à des utilisateurs finaux d'ouvrir une session sur Horizon Client et sur leur poste de travail virtuel en tant qu'utilisateur actuellement connecté. Les informations d'identification que l'utilisateur a saisies lors de l'ouverture de session sur le système client sont transmises à l'instance de Serveur de connexion View, puis au poste de travail distant. Certains systèmes d'exploitation client ne prennent pas cette fonction en charge.
- Si vous ne voulez pas que les utilisateurs finaux fournissent le nom de domaine complet (FQDN) de l'instance de Serveur de connexion View, déterminez le FQDN pour que vous puissiez le fournir lors de l'installation.

Procédure

- 1 Ouvrez une session sur le système client en tant qu'utilisateur avec des privilèges d'administrateur.
- 2 Sur le système client, accédez à l'URL de téléchargement du fichier du programme d'installation.

Sélectionnez le fichier du programme d'installation approprié, où *xxxxxx* est le numéro de build et *y.y.y* le numéro de version.

| Option | Action |
|---|--|
| Horizon Client sur des systèmes d'exploitation 64 bits | Sélectionnez VMware-Horizon-View-Client-x86_64-y.y.y-xxxxxx.exe, où <i>y.y.y</i> est le numéro de version et <i>xxxxxx</i> est le numéro de build. |
| Horizon Client sur des systèmes d'exploitation 32 bits | Sélectionnez VMware-Horizon-View-Client-x86-y.y.y-xxxxxx.exe, où <i>y.y.y</i> est le numéro de version et <i>xxxxxx</i> est le numéro de build. |

- 3 Pour démarrer le programme d'installation d'Horizon Client, double-cliquez sur le fichier du programme d'installation.

REMARQUE Horizon Client 3.3 et versions ultérieures ne sont pas pris en charge sur les systèmes d'exploitation Windows XP ou Windows Vista. Si vous tentez d'exécuter le programme d'installation sur un système d'exploitation non pris en charge, vous recevrez un message d'erreur.

- 4 Suivez les invites pour installer les composants de votre choix. Utilisez les instructions suivantes.

| Option | Description |
|---------------------|---|
| Protocole IP | Le programme d'installation de Horizon Client 3.3 ou version ultérieure vous invite à sélectionner un protocole réseau. Ne sélectionnez pas IPv6 , sauf si tous les composants de votre installation de View utilisent IPv6. Si vous sélectionnez IPv6 , plusieurs fonctionnalités seront indisponibles. Pour plus d'informations, reportez-vous au chapitre sur l'installation de View dans un environnement IPv6 dans le document <i>Installation de View</i> . |
| FIPS | Vous verrez une invite vous demandant si vous voulez installer le client avec la cryptographie compatible FIPS uniquement si vous avez déjà activé FIPS sur le système d'exploitation client, comme décrit dans les conditions préalables. Cette fonctionnalité est disponible avec Horizon Client 3.5 et versions ultérieures. |

Le service VMware Horizon Client est installé sur l'ordinateur client Windows.

Le nom de processus d'Horizon Client est `vmware-view`. Les noms de services des composants USB sont VMware USB Arbitration Service (`VMUSBArbService`) et VMware View USB (`vmware-view-usbd`).

Suivant

Démarrez Horizon Client et vérifiez que vous pouvez ouvrir une session sur l'application ou le poste de travail distant correct. Reportez-vous à la section « [Connexion à une application ou un poste de travail distant](#) », page 61.

Activation du mode FIPS sur le système d'exploitation client Windows

Vous devez activer le mode FIPS sur le système d'exploitation client avant d'exécuter le programme d'installation du client si vous prévoyez d'installer Horizon Client avec une cryptographie compatible FIPS.

Lorsque le mode FIPS (Federal Information Processing Standard) est activé sur le système d'exploitation client, les applications sont informées qu'elles ne doivent utiliser que des algorithmes cryptographiques compatibles avec FIPS-140 et conformes aux modes de fonctionnement approuvés par FIPS. Vous pouvez activer le mode FIPS en activant un paramètre de sécurité spécifique, dans la stratégie de sécurité locale ou dans le cadre de la stratégie de groupe, ou en modifiant une clé de registre Windows.

IMPORTANT L'installation d'Horizon Client avec une cryptographie compatible FIPS est une fonctionnalité d'Horizon Client 3.5 ou version ultérieure. Elle n'est prise en charge que pour les clients avec des systèmes d'exploitation Windows 7 SP1.

Pour plus d'informations sur la prise en charge de FIPS, disponible avec Horizon 6 version 6.2 ou version ultérieure, consultez le document *Installation de View*.

Définition de la propriété de configuration

Pour activer le mode FIPS sur le système d'exploitation client, vous pouvez utiliser un GPO Windows ou un paramètre de registre Windows pour l'ordinateur client.

- Pour utiliser le paramètre GPO, ouvrez l'éditeur de stratégie de groupe et accédez à :

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Activez le paramètre **Cryptographie système : utiliser des algorithmes compatibles FIPS pour le cryptage, le hachage et la signature**.

- Pour utiliser le registre Windows, accédez à la clé de registre suivante :

HKLM\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\Enabled

Pour activer le mode FIPS, réglez **Activé** sur 1.

Pour plus d'informations sur le mode FIPS, consultez <https://support.microsoft.com/en-us/kb/811833>.

IMPORTANT Si vous n'activez pas le mode FIPS avant d'exécuter le programme d'installation du client, vous ne voyez pas l'option pour utiliser la cryptographie compatible FIPS. Si vous installez Horizon Client sans cette option et que vous décidez ultérieurement d'utiliser cette option, vous devez désinstaller le client, activer le mode FIPS sur le système d'exploitation client et exécuter de nouveau le programme d'installation du client.

Installation silencieuse d' Horizon Client

Vous pouvez installer Horizon Client en silence en saisissant le nom de fichier du programme d'installation et les options d'installation dans la ligne de commande. Avec l'installation silencieuse, vous pouvez déployer efficacement des composants View dans une grande entreprise.

Installer Horizon Client en silence

Vous pouvez utiliser l'option d'installation silencieuse de Microsoft Windows Installer (MSI) pour installer Horizon Client sur plusieurs ordinateurs Windows. Dans une installation silencieuse, vous utilisez la ligne de commande et n'avez pas à répondre à des invites d'assistant.

Prérequis

- Vérifiez que le système client utilise un système d'exploitation pris en charge. Reportez-vous à la section « [Configuration système requise pour les clients Windows](#) », page 8.
- Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur le système client.
- Vérifiez que les contrôleurs de domaine disposent des derniers correctifs, d'un espace disque libre suffisant et peuvent communiquer entre eux. Si vous ne le faites pas, lorsque vous exécuterez le programme d'installation sur un système Windows 8.1, l'exécution du programme d'installation pourra être anormalement longue. Ce problème survient si le contrôleur de domaine de la machine ou un autre contrôleur de domaine de sa hiérarchie ne répond pas ou est inaccessible.
- Si vous prévoyez d'installer Horizon Client avec une cryptographie compatible FIPS, activez le mode FIPS sur le système d'exploitation Windows avant d'exécuter le programme d'installation du client. Reportez-vous à la section « [Activation du mode FIPS sur le système d'exploitation client Windows](#) », page 23.
- Déterminez si vous voulez utiliser la fonctionnalité qui permet à des utilisateurs finaux d'ouvrir une session sur Horizon Client et sur leur poste de travail virtuel en tant qu'utilisateur actuellement connecté. Les informations d'identification que l'utilisateur a saisies lors de l'ouverture de session sur le système client sont transmises à l'instance de Serveur de connexion View, puis au poste de travail distant. Certains systèmes d'exploitation client ne prennent pas cette fonction en charge.
- Familiarisez-vous avec les options de ligne de commande du programme d'installation MSI. Reportez-vous à la section « [Options de la ligne de commande Microsoft Windows Installer](#) », page 27.
- Familiarisez-vous avec les propriétés d'installation silencieuse (MSI) disponibles avec Horizon Client. Reportez-vous à la section « [Propriétés de l'installation silencieuse pour Horizon Client](#) », page 25.
- Déterminez si vous voulez autoriser les utilisateurs finaux à accéder à des périphériques USB connectés en local depuis leurs postes de travail virtuels. Si vous ne le voulez pas, définissez la propriété MSI, ADDLOCAL, sur la liste de fonctions d'intérêt et omettez la fonction USB. Pour plus d'informations, reportez-vous à « [Propriétés de l'installation silencieuse pour Horizon Client](#) », page 25.
- Si vous ne voulez pas que les utilisateurs finaux fournissent le nom de domaine complet (FQDN) de l'instance de Serveur de connexion View, déterminez le FQDN pour que vous puissiez le fournir lors de l'installation.

Procédure

- 1 Sur le système client, téléchargez le fichier du programme d'installation Horizon Client sur la page des produits VMware à l'adresse <http://www.vmware.com/go/viewclients>.

Sélectionnez le fichier du programme d'installation approprié, où *xxxxxx* est le numéro de build et *y.y.y* le numéro de version.

| Option | Action |
|---|--|
| Horizon Client sur des systèmes d'exploitation 64 bits | Sélectionnez VMware-Horizon-View-Client-x86_64-y.y.y-xxxxxx.exe, où <i>y.y.y</i> est le numéro de version et <i>xxxxxx</i> est le numéro de build. |
| Horizon Client sur des systèmes d'exploitation 32 bits | Sélectionnez VMware-Horizon-View-Client-x86-y.y.y-xxxxxx.exe, où <i>y.y.y</i> est le numéro de version et <i>xxxxxx</i> est le numéro de build. |

- 2 Ouvrez une invite de commande sur l'ordinateur client Windows.

- 3 Saisissez la commande d'installation sur une ligne.

Cet exemple installe Horizon Client en silence :

```
VMware-Horizon-View-Client-x86-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,USB,TSSO"
```

Vous pouvez également utiliser ADDLOCAL=ALL au lieu de ADDLOCAL=Core,USB,TSSO.

REMARQUE La fonction Core est obligatoire.

Suivant

Démarrez Horizon Client et vérifiez que vous pouvez ouvrir une session sur l'application ou le poste de travail distant correct. Reportez-vous à la section « [Connexion à une application ou un poste de travail distant](#) », page 61.

Propriétés de l'installation silencieuse pour Horizon Client

Vous pouvez inclure des propriétés spécifiques lorsque vous installez de façon silencieuse Horizon Client via la ligne de commande. Vous devez utiliser le format *PROPERTY=value* de manière que Microsoft Windows Installer (MSI) puisse interpréter les propriétés et les valeurs.

[Tableau 2-1](#) montre les propriétés de l'installation silencieuse d'Horizon Client que vous pouvez utiliser dans la ligne de commande.

Tableau 2-1. Propriétés MSI pour l'installation silencieuse d' Horizon Client

| Propriété MSI | Description | Valeur par défaut |
|-----------------------|---|--|
| INSTALLDIR | Chemin d'accès et dossier dans lequel le logiciel Horizon Client est installé. Par exemple : INSTALLDIR=""D:\abc\my folder"" Les guillemets délimitant le chemin permettent au programme d'installation MSI d'interpréter l'espace comme étant une partie valide du chemin. | %ProgramFiles %\VMware\VMware Horizon View Client |
| VDM_IP_PROTOCOL_USAGE | Spécifie la version IP (protocole réseau) que les composants View utilisent pour la communication. Les valeurs possibles sont IPv4 et IPv6 . | IPv4 |

Tableau 2-1. Propriétés MSI pour l'installation silencieuse d' Horizon Client (suite)

| Propriété MSI | Description | Valeur par défaut |
|--------------------|---|-------------------|
| VDM_SERVER | Nom de domaine complet (FQDN) de l'instance de Serveur de connexion View à laquelle les utilisateurs d'Horizon Client se connectent par défaut. Lorsque vous configurez cette propriété, les utilisateurs d'Horizon Client n'ont pas à fournir ce FQDN. Par exemple : VDM_SERVER=cs1.companydomain.com. Cette propriété MSI est facultative. | Aucune |
| DESKTOP_SHORTCUT | Configure une icône de raccourci de bureau pour Horizon Client. Le raccourci sera installé si la valeur est égale à 1. Le raccourci ne sera pas installé si la valeur est égale à 0. | 1 |
| STARTMENU_SHORTCUT | Configure un raccourci pour Horizon Client dans le menu Démarrer. Le raccourci sera installé si la valeur est égale à 1. Le raccourci ne sera pas installé si la valeur est égale à 0. | 1 |
| VDM_FIPS_ENABLED | (Horizon Client 3.5 ou version ultérieure) Spécifie s'il faut installer Horizon Client avec la cryptographie compatible FIPS. La valeur 1 installe le client avec la cryptographie compatible FIPS. La valeur 0 ne l'installe pas. REMARQUE Avant de définir cette option sur 1, vous devez activer le mode FIPS sur le système d'exploitation client Windows. Reportez-vous à la section « Activation du mode FIPS sur le système d'exploitation client Windows », page 23. | 0 |

Dans une commande d'installation silencieuse, vous pouvez utiliser la propriété MSI ADDLOCAL= pour spécifier des fonctionnalités à configurer par le programme d'installation d'Horizon Client. Chaque fonctionnalité de l'installation silencieuse correspond à une option d'installation que vous pouvez sélectionner au cours d'une installation interactive.

[Tableau 2-2](#) montre les fonctionnalités d'Horizon Client que vous pouvez entrer sur la ligne de commande et les options de l'installation interactive correspondantes.

Tableau 2-2. Fonctions de l'installation silencieuse d' Horizon Client et options de l'installation personnalisée interactive

| Fonction de l'installation silencieuse | Option de l'installation personnalisée dans une installation interactive |
|---|---|
| Core | aucune. |
| Si vous spécifiez des fonctionnalités individuelles avec la propriété MSI, ADDLOCAL=, vous devez inclure l'option Core . | Au cours d'une installation interactive, les fonctionnalités principales d'Horizon Client sont installées par défaut. |
| TSSO | Connexion en tant qu'utilisateur de domaine Windows actuellement connecté |
| USB | Redirection USB |

Options de la ligne de commande Microsoft Windows Installer

Pour installer Horizon Client en silence, vous devez utiliser des options et des propriétés de ligne de commande de MSI (Microsoft Windows Installer). Les programmes d'installation d'Horizon Client sont des programmes MSI et utilisent des fonctionnalités MSI standard. Vous pouvez également utiliser des options de ligne de commande MSI pour désinstaller Horizon Client en silence.

Pour plus d'informations sur MSI, rendez-vous sur le site Web de Microsoft. Pour plus d'informations sur les options de la ligne de commande MSI, rendez-vous sur le site Web de la bibliothèque MSDN (Microsoft Developer Network). Pour voir comment utiliser la ligne de commande MSI, vous pouvez ouvrir une invite de commande sur l'ordinateur client et saisir `msiexec /?`.

Pour exécuter le programme d'installation d'Horizon Client en silence, commencez par activer le mode silencieux sur le programme de démarrage qui extrait le programme d'installation dans un répertoire temporaire et démarre une installation interactive.

Le tableau suivant montre des options de ligne de commande qui contrôlent le programme de démarrage du programme d'installation.

Tableau 2-3. Options de ligne de commande pour le programme de démarrage

| Option | Description |
|--|---|
| <code>/s</code> | Désactive l'écran de démarrage et la boîte de dialogue d'extraction du programme de démarrage, qui empêche l'affichage de boîtes de dialogue interactives. Par exemple : <code>VMware-Horizon-View-Client-y.y.y-xxxxxx.exe /s</code> L'option <code>/s</code> est obligatoire pour que l'installation soit silencieuse. Dans ces exemples, <code>xxxxxx</code> correspond au numéro de build et <code>y.y.y</code> au numéro de version. |
| <code>/v "MSI_command_line_options"</code> | Demande au programme d'installation de transmettre à MSI la chaîne de caractères comprise entre guillemets, que vous avez entrée sur la ligne de commande comme un ensemble d'options à interpréter. Vous devez délimiter votre chaîne de caractères de la ligne de commande par des guillemets. Placez un guillemet après <code>/v</code> et à la fin de la ligne de commande. Par exemple : <code>VMware-Horizon-View-Client-y.y.y-xxxxxx.exe /s /v "command_line_options"</code> Pour demander au programme d'installation MSI d'interpréter une chaîne contenant des espaces, insérez deux jeux de guillemets doubles avant et après la chaîne. Par exemple, vous pouvez installer le client dans un nom de chemin d'installation contenant des espaces. Par exemple : <code>VMware--Horizon-View-Client-y.y.y-xxxxxx.exe /s /v "command_line_options INSTALLDIR=""d:\abc\my folder"""</code> Dans cet exemple, le programme d'installation MSI transmet le chemin du répertoire d'installation et n'essaie pas d'interpréter la chaîne comme deux options de ligne de commande. Notez le guillemet double final entourant toute la ligne de commande. L'option <code>/v "command_line_options"</code> est obligatoire pour exécuter une installation silencieuse. |

Le contrôle de la suite de l'installation silencieuse se fait en transmettant les options de la ligne de commande et les valeurs de propriété MSI au programme d'installation MSI, `msiexec.exe`. Le programme d'installation MSI inclut le code d'installation d'Horizon Client. Le programme d'installation utilise les valeurs et les options que vous saisissez dans la ligne de commande pour interpréter des choix d'installation et des options de configuration propres à Horizon Client.

Le tableau suivant montre les options de ligne de commande et les valeurs de propriété MSI transmises au programme d'installation MSI.

Tableau 2-4. Options de la ligne de commande et propriétés MSI

| Option ou propriété MSI | Description |
|----------------------------|--|
| /qn | <p>Demande au programme d'installation MSI de ne pas afficher les pages de l'assistant d'installation.</p> <p>Par exemple, vous voulez peut-être installer View Agent en silence et n'utiliser que des options et des fonctions d'installation par défaut :</p> <pre>VMware-Horizon-View-Client-y.y.y-xxxxxx.exe /s /v"/qn"</pre> <p>Dans ces exemples, <i>xxxxxx</i> correspond au numéro de build et <i>y.y.y</i> au numéro de version.</p> <p>Vous pouvez également utiliser l'option /qb pour afficher les pages de l'assistant d'installation dans une installation automatique non interactive. Pendant l'installation, les pages de l'assistant d'installation sont affichées, mais vous ne pouvez pas y répondre.</p> <p>L'option /qn ou /qb est obligatoire pour que l'installation soit silencieuse.</p> |
| INSTALLDIR | <p>(Facultatif) Spécifie un autre chemin d'installation pour le répertoire d'installation. Utilisez le format <i>INSTALLDIR=</i><i>path</i> pour spécifier un chemin d'installation. Vous pouvez ignorer cette propriété MSI si vous voulez installer le client dans le chemin par défaut.</p> |
| ADDLOCAL | <p>(Facultatif) Détermine les fonctionnalités propres au composant à installer. Dans une installation interactive, le programme d'installation affiche des options d'installation personnalisées à sélectionner. La propriété MSI, ADDLOCAL, vous permet de spécifier ces options d'installation sur la ligne de commande.</p> <p>Pour installer toutes les options d'installation personnalisées disponibles, saisissez ADDLOCAL=ALL.</p> <p>Par exemple : <code>VMware-Horizon-View-Client-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=ALL"</code></p> <p>Si vous n'utilisez pas la propriété MSI, ADDLOCAL, les options d'installation par défaut sont installées.</p> <p>Pour spécifier des options d'installation individuelles, saisissez une liste séparée par des virgules de noms d'option d'installation. Ne laissez pas d'espaces entre les noms. Utilisez le format <i>ADDLOCAL=</i><i>value,value,value</i>... .</p> <p>Par exemple, vous pouvez installer le client avec la fonctionnalité de redirection USB mais sans la fonctionnalité Se connecter en tant qu'utilisateur actuel :</p> <pre>VMware-Horizon-View-Client-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,USB"</pre> |
| LOGINASCURRENTUSER_DISPLAY | <p>(Facultatif) Détermine si la case à cocher Se connecter en tant qu'utilisateur actuel doit être visible dans la boîte de dialogue de connexion d'Horizon Client.</p> <p>Les valeurs valides sont 1 (activé) et 0 (désactivé). La valeur par défaut est 1, ce qui signifie que la case à cocher est visible et que les utilisateurs peuvent l'activer ou la désactiver et remplacer sa valeur par défaut. Lorsque la case est masquée, les utilisateurs ne peuvent pas remplacer sa valeur par défaut dans la boîte de dialogue de connexion d'Horizon Client.</p> |
| LOGINASCURRENTUSER_DEFAULT | <p>(Facultatif) Spécifie la valeur par défaut de la case à cocher Se connecter en tant qu'utilisateur actuel dans la boîte de dialogue de connexion d'Horizon Client. Les valeurs valides sont 1 (activé) et 0 (désactivé). Aucune valeur par défaut n'est définie, ce qui signifie que la case à cocher est désactivée et que les utilisateurs doivent fournir leur identité et leurs informations d'identification plusieurs fois avant de pouvoir accéder à un poste de travail distant.</p> <p>Lorsque la case Se connecter en tant qu'utilisateur actuel est cochée, l'identité et les informations d'identification que l'utilisateur a fournies lors de la connexion au système client sont transmises à l'instance du Serveur de connexion View, puis au poste de travail distant.</p> <p>Utilisez cette option avec l'option LOGINASCURRENTUSER_DISPLAY . Par exemple : <code>LOGINASCURRENTUSER_DISPLAY=1 LOGINASCURRENTUSER_DEFAULT=1</code></p> <p>Si un utilisateur exécute Horizon Client à partir de la ligne de commande et spécifie l'option <code>logInAsCurrentUser</code>, cette valeur remplace ce paramètre.</p> |

Tableau 2-4. Options de la ligne de commande et propriétés MSI (suite)

| Option ou propriété MSI | Description |
|-------------------------|---|
| REBOOT | (Facultatif) Vous pouvez utiliser l'option REBOOT=ReallySuppress pour supprimer tous les redémarrages et les invites de redémarrage. |
| /l*v <i>log_file</i> | <p>(Facultatif) Écrit les informations de journalisation dans le fichier journal spécifié. Par exemple : /l*v ""%TEMP%\vmmsi.log""</p> <p>Cet exemple génère un fichier journal détaillé semblable à celui généré lors d'une installation interactive.</p> <p>Vous pouvez utiliser cette option pour enregistrer des fonctions personnalisées qui s'appliquent uniquement à votre installation. Vous pouvez utiliser les informations enregistrées pour spécifier les fonctionnalités d'installation lors d'installations silencieuses ultérieures.</p> |

Exemple : Exemples d'installation

Dans les exemples suivants, *xxxxxx* correspond au numéro de build, *y.y.y* au numéro de version, *install_folder* au chemin du dossier d'installation et *view.mycompany.com* au nom d'une instance fictive du Serveur de connexion View.

Exemple d'installation par défaut :

```
VMware-Horizon-View-Client-x86_64-y.y.y-xxxxxx.exe /s /v"/qn REBOOT=ReallySuppress
INSTALLDIR=install_folder ADDLOCAL=ALL DESKTOP_SHORTCUT=1 STARTMENU_SHORTCUT=1
VDM_SERVER=view.mycompany.com /l*v "%TEMP%\log.txt""
```

Exemple d'installation et de configuration pour la fonctionnalité Se connecter en tant qu'utilisateur :

```
VMware-Horizon-View-Client-x86_64-y.y.y-xxxxxx.exe /s /v"/qn INSTALLDIR=install_folder
ADDLOCAL=Core,TSSO LOGINASCURRENTUSER_DISPLAY=1 LOGINASCURRENTUSER_DEFAULT=1 DESKTOP_SHORTCUT=1
STARTMENU_SHORTCUT=1 VDM_SERVER=view.mycompany.com /l*v "%TEMP%\log.txt""
```

Dans cet exemple, REBOOT=ReallySuppress est omis, car l'option TSSO (Connexion en tant qu'utilisateur de domaine Windows actuellement connecté) requiert un redémarrage.

Configuration d' Horizon Client pour les utilisateurs finaux

3

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

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

Tableau 3-1. 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 |
| 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 |
| 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 Client », page 32](#)
- [« Configuration de la vérification des certificats pour les utilisateurs finaux », page 37](#)
- [« Configuration des options TLS/SSL avancées », page 39](#)
- [« Utilisation du modèle de stratégie de groupe pour configurer VMware Horizon Client pour Windows », page 40](#)
- [« Exécution d'Horizon Client depuis la ligne de commande », page 56](#)
- [« Utilisation du Registre Windows pour configurer Horizon Client », page 59](#)

Utilisation d'URI pour configurer Horizon Client

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

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

- Adresse du Serveur de connexion View
- Numéro de port pour le Serveur de connexion View
- Nom d'utilisateur Active Directory
- Le nom d'utilisateur RADIUS ou RSA SecurID, s'il est différent du nom d'utilisateur Active Directory.
- Nom de domaine
- Nom affiché du poste de travail ou de l'application
- Taille de fenêtre
- Actions incluant la réinitialisation, la fermeture d'une session et le démarrage d'une session
- Protocole d'affichage
- Options pour la redirection des périphériques USB

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

REMARQUE Vous pouvez utiliser les URI pour lancer Horizon 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 ou l'application et, en option, une requête permettant de spécifier des actions de poste de travail ou d'application, ou des options de configuration.

Spécification d'URI

Utilisez la syntaxe suivante pour créer des URI permettant de lancer Horizon Client :

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

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

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

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

authority-part

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

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

`user1@server-address`

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 :

`server-address:port-number`

path-part

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

query-part

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

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

Requêtes prises en charge

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

action

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

| Valeur | Description |
|----------------------------|---|
| <code>browse</code> | Affiche une liste des postes de travail ou applications disponibles hébergées sur le serveur spécifié. Il ne vous est pas demandé de spécifier un poste de travail ou une application pour l'utilisation de cette action. |
| <code>start-session</code> | Lance le poste de travail ou l'application spécifiée. Si aucune requête d'action n'est fournie et que le nom du poste de travail ou de l'application est fourni, <code>start-session</code> est l'action par défaut. |

Tableau 3-2. Valeurs pouvant être utilisées avec la Requête d'action (suite)

| Valeur | Description |
|--------|--|
| reset | Éteint puis redémarre le poste de travail spécifié ou l'application distante. Les données non enregistrées sont perdues. La réinitialisation d'un poste de travail distant équivaut à appuyer sur le bouton Réinitialiser d'un ordinateur physique. Dans Horizon Client 3.0, si vous spécifiez une application, l'action sera ignorée. Dans Horizon Client 3.1, si vous spécifiez une application, l'utilisateur final est invité à confirmer la sortie de toutes les applications distantes. |
| logoff | Déconnecte l'utilisateur du système d'exploitation invité sur le poste de travail distant. Si vous spécifiez une application, l'action sera ignorée ou l'utilisateur final verra le message d'avertissement « Action d'URI non valide ». |

connectUSBOnInsert

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

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 un poste de travail distant. Pour utiliser cette requête, vous devez paramétrer la requête action sur **start-session** ou ne pas utiliser de requête action.

Tableau 3-3. 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. |
| windowSmall | Fenêtre de petite taille. |
| WxH | Personnalisez la résolution, spécifiez la largeur et la hauteur en pixels. Exemple de syntaxe : desktopLayout=1280x800 . |

desktopProtocol

Pour les postes de travail distants, les valeurs valides sont **RDP** et **PCoIP**. Par exemple, pour spécifier le protocole PCoIP, utilisez la syntaxe **desktopProtocol=PCoIP**. Pour les applications distantes, quel que soit le paramètre, les sessions d'application utilisent PCoIP.

domainName

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

| | |
|----------------------|--|
| filePath | <p>Spécifie le chemin d'accès au fichier sur le système local que vous voulez ouvrir avec l'application distante. Vous devez utiliser le chemin d'accès complet, y compris la lettre de lecteur. Utilisez l'encodage avec pourcentage pour les caractères suivants :</p> <ul style="list-style-type: none"> ■ Pour un deux-points (:), utilisez %3A ■ Pour une barre oblique inversée (\), utilisez %5C ■ Pour un espace (), utilisez %20 <p>Par exemple, pour représenter le chemin d'accès au fichier C:\test file.txt, utilisez C%3A%5Ctest%20file.txt.</p> |
| tokenUserName | <p>Spécifie le nom d'utilisateur RSA ou RADIUS. N'utilisez cette requête que si le nom d'utilisateur RSA ou RADIUS est différent du nom d'utilisateur Active Directory. Si vous ne spécifiez pas cette requête et que l'authentification RSA ou RADIUS est nécessaire, le nom d'utilisateur Windows est utilisé. La syntaxe se présente ainsi : tokenUserName=name.</p> |
| unattended | <p>Établit une connexion serveur avec un poste de travail distant en mode kiosque. Si vous utilisez cette requête, ne spécifiez pas d'informations utilisateur si vous avez généré le nom du compte à partir de l'adresse MAC du périphérique client. Cependant, si vous avez créé des noms de comptes personnalisés dans ADAM, par exemple des noms qui commencent par « custom- », vous devez spécifier les informations du compte.</p> |

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 Client est lancé 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.

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

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

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

REMARQUE Cette action n'est disponible que si l'administrateur View a activé cette fonction pour les utilisateurs finaux.

- 7 `vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session&connectUSBOnStartup=true`

Cet URI a le même effet que le premier exemple, et tous les périphériques USB connectés au système client sont redirigés vers le poste de travail distant.

- 8 `vmware-view://`

Horizon Client est lancé et l'utilisateur est dirigé vers la page pour entrer l'adresse d'une instance de 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>
```

Configuration de la vérification des certificats pour les utilisateurs finaux

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

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

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

Pour plus d'informations sur les types de vérifications effectuées, reportez-vous à la section « [Modes de vérification des certificats pour Horizon Client](#) », page 38.

Utilisez le fichier de modèle ADM de configuration de client (`vdm_client.adm`) pour définir le mode de vérification. Tous les fichiers ADM et ADMX qui fournissent les paramètres de stratégie de groupe sont disponibles dans un fichier .zip appelé `VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyy.zip`, où `x.x.x` est la version et `yyyyyy` est le numéro de build. Vous pouvez télécharger ce fichier GPO Bundle sur le site de téléchargement de VMware Horizon à l'adresse <http://www.vmware.com/go/downloadview>. Pour plus d'informations sur l'utilisation de ce modèle afin de contrôler les paramètres GPO, reportez-vous à la rubrique « [Utilisation du modèle de stratégie de groupe pour configurer VMware Horizon Client pour Windows](#) », page 40.

REMARQUE Vous pouvez également utiliser le fichier de modèle d'administration de configuration de client pour limiter l'utilisation de certains algorithmes et protocoles de chiffrement avant d'établir une connexion SSL chiffrée. Pour plus d'informations sur ce paramètre, reportez-vous à la rubrique « [Paramètres de sécurité des objets de stratégie de groupe \(GPO\) des clients](#) », page 42.

Si vous ne souhaitez pas configurer le paramètre de vérification des certificats en tant que stratégie de groupe, vous pouvez également activer la vérification des certificats en ajoutant le nom de valeur `CertCheckMode` à l'une des clés de registre suivantes sur l'ordinateur client :

- Pour Windows 32 bits : `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`
- Pour Windows 64 bits : `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`

Utilisez les valeurs suivantes dans la clé de registre :

- `0` implémente `Do not verify server identity certificates`.
- `1` implémente `Warn before connecting to untrusted servers`.
- `2` implémente `Never connect to untrusted servers`.

Si vous configurez le paramètre de stratégie de groupe et le paramètre `CertCheckMode` dans la clé de registre, le paramètre de stratégie de groupe est prioritaire sur la valeur de la clé de registre.

Modes de vérification des certificats pour Horizon Client

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

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

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

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

REMARQUE Pour obtenir des instructions sur la distribution d'un certificat racine auto-signé à tous les systèmes client Windows dans un domaine, reportez-vous à la rubrique intitulée « Ajouter le certificat racine aux autorités de certification racine approuvées » dans le document *Installation de View*.

Lorsque vous utilisez Horizon Client pour ouvrir une session sur un poste de travail, si votre administrateur l'a autorisé, vous pouvez cliquer sur **Configurer SSL** afin de définir le mode de vérification des certificats. Vous avez trois possibilités :

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

Si le mode de vérification des certificats est défini sur **Avertir**, vous pouvez toujours vous connecter à une instance du Serveur de connexion View qui utilise un certificat auto-signé.

Si un administrateur installe ultérieurement un certificat de sécurité à partir d'une autorité de certification de confiance, afin que toutes les vérifications de certificat aient lieu lorsque vous vous connectez, cette connexion approuvée est enregistrée pour ce serveur spécifique. À l'avenir, si ce serveur présente de nouveau un certificat auto-signé, la connexion échoue. Après qu'un serveur particulier présente un certificat entièrement vérifiable, il doit toujours faire ainsi.

IMPORTANT Si vous avez précédemment configuré les systèmes clients de votre société pour utiliser un chiffrement spécifique via GPO, en définissant par exemple les paramètres de stratégie de groupe SSL Cipher Suite Order, vous devez maintenant utiliser un paramètre de sécurité de stratégie de groupe Horizon Client inclus dans le fichier de modèle d'administration de View. Reportez-vous à

« Paramètres de sécurité des objets de stratégie de groupe (GPO) des clients », page 42. Vous pouvez également utiliser le paramètre de registre SSLCipherList sur le client. Reportez-vous à la section « Utilisation du Registre Windows pour configurer Horizon Client », page 59.

Configuration des options TLS/SSL avancées

Vous pouvez sélectionner les protocoles de sécurité et les algorithmes de chiffrement qui sont utilisés pour chiffrer les communications entre Horizon Client et Serveur de connexion View et View Agent dans le poste de travail distant.

Dans Horizon Client 3.1 et version ultérieure, ces options sont également utilisées pour chiffrer le canal USB (communication entre le démon du service USB et View Agent).

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

- Dans Horizon Client 3.5 et versions ultérieures, TLS v1.0, TLS v1.1 et TLS v1.2 sont activés par défaut. (SSL v2.0 et v3.0 sont désactivés.)
- Dans Horizon Client 3.3 et 3.4, TLS v1.0 et TLS v1.1 sont activés par défaut. (SSL v2.0, SSL v3.0 et TLS v1.2 sont désactivés.)
- Dans Horizon Client 3.2 et versions antérieures, SSL v3.0 est également activé par défaut. (SSL v2.0 et TLS v1.2 sont désactivés.)

REMARQUE Dans Horizon Client 3.1 et versions ultérieures, lorsque le démon du service USB se connecte à un poste de travail distant, il ajoute RC4 (:RC4-SHA: +RC4) à la fin de la chaîne de contrôle de chiffrement.

Vous devez modifier les protocoles de sécurité dans Horizon Client uniquement si votre serveur View Server ne prend pas en charge les paramètres actuels. Si vous configurez un protocole de sécurité pour Horizon Client qui n'est pas activé sur le serveur View Server auquel le client se connecte, une erreur TLS/SSL se produit et la connexion échoue.

IMPORTANT Si vous activez uniquement le protocole TLS v1.1 sur le client, vous devez vérifier que TLS v1.1 est également activé sur le poste de travail distant. Sinon, les périphériques USB ne peuvent pas être redirigés vers le poste de travail distant.

Sur le système client, vous pouvez utiliser un paramètre de stratégie de groupe ou un paramètre de Registre Windows pour modifier les chiffrements et protocoles par défaut. Pour plus d'informations sur l'utilisation d'un GPO, reportez-vous au paramètre nommé « Configure les protocoles et les algorithmes de chiffrement SSL », dans « Paramètres de sécurité des objets de stratégie de groupe (GPO) des clients », page 42. Pour plus d'informations sur l'utilisation du paramètre SSLCipherList dans le Registre Windows, reportez-vous à « Utilisation du Registre Windows pour configurer Horizon Client », page 59.

Utilisation du modèle de stratégie de groupe pour configurer VMware Horizon Client pour Windows

VMware Horizon Client inclut un fichier de modèle d'administration de stratégie de groupe permettant de configurer VMware Horizon Client. Vous pouvez optimiser et sécuriser les connexions des postes de travail distants en ajoutant les paramètres de stratégie de ce fichier de modèle d'administration à un objet de stratégie de groupe (GPO) nouveau ou existant dans Active Directory.

Le modèle de fichier d'administration d'View contient des stratégies de groupe Configuration d'ordinateur et Configuration d'utilisateur.

- Les stratégies Configuration d'ordinateur définissent des stratégies qui s'appliquent à Horizon Client, sans tenir compte de la personne qui exécute le client sur l'hôte.
- Les stratégies Configuration d'utilisateur définissent des stratégies Horizon Client qui s'appliquent à tous les utilisateurs qui exécutent Horizon Client, ainsi qu'aux paramètres de connexion RDP. Les stratégies Configuration d'utilisateur remplacent les stratégies Configuration d'ordinateur équivalentes.

View applique les stratégies au démarrage du poste de travail et lorsque les utilisateurs ouvrent une session.

Le fichier de modèle ADM de configuration de Horizon Client (`vdm_client.adm`) et tous les fichiers ADM et ADMX qui fournissent des paramètres de stratégie de groupe sont disponibles dans un fichier .zip nommé `VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyy.zip`, où `x.x.x` est la version et `yyyyyy` le numéro de build. Vous pouvez télécharger le fichier sur le site de téléchargement de VMware Horizon à l'adresse <http://www.vmware.com/go/downloadview>. Vous devez copier ce fichier sur votre serveur Active Directory et utiliser l'Éditeur de gestion des stratégies de groupes pour ajouter ce modèle d'administration. Pour obtenir des instructions, consultez la rubrique « Ajouter des modèles ADM View à un GPO » dans le document *Configuration de pools de postes de travail et d'applications dans View*.

Paramètres de définition de scripts des objets de stratégie de groupe (GPO) des clients

Vous pouvez définir des stratégies pour plusieurs paramètres identiques que vous avez utilisés pour exécuter VMware Horizon Client à partir de la ligne de commande, notamment la taille, le nom et le nom de domaine du poste de travail.

Le tableau suivant décrit les paramètres de définition de script du fichier de modèle d'administration pour la configuration de VMware Horizon Client. Le modèle fournit une version de Configuration d'ordinateur et de Configuration d'utilisateur de chaque paramètre de définition de script. Le paramètre de Configuration d'utilisateur remplace le paramètre de Configuration d'ordinateur équivalent.

Tableau 3-4. Modèle de configuration de VMware Horizon Client : définitions de script

| Paramètre | Description |
|---|--|
| Automatically connect if only one launch item is entitled | (Horizon Client 2.3 ou version ultérieure) Se connecte automatiquement au poste de travail si l'utilisateur n'est autorisé à en utiliser qu'un seul. Ce paramètre évite à l'utilisateur d'avoir à sélectionner le poste de travail dans une liste n'en contenant qu'un seul. |
| Connect all USB devices to the desktop on launch | Détermine si tous les périphériques USB disponibles sur le système client sont connectés au poste de travail lorsque ce dernier est lancé. |
| Connect all USB devices to the desktop when they are plugged in | Détermine si les périphériques USB sont connectés au poste de travail lorsqu'ils sont branchés sur le système client. |

Tableau 3-4. Modèle de configuration de VMware Horizon Client : définitions de script (suite)

| Paramètre | Description |
|---|---|
| DesktopLayout | <p>Spécifie la disposition de la fenêtre VMware Horizon Client visible par un utilisateur lorsqu'il se connecte à un poste de travail distant. Les différentes dispositions sont les suivantes :</p> <ul style="list-style-type: none"> ■ Full Screen ■ Multimonitor ■ Window – Large ■ Window – Small <p>Ce paramètre n'est disponible que lorsque le paramètre DesktopName to select setting est également défini.</p> |
| DesktopName to select | Spécifie le poste de travail par défaut proposé par VMware Horizon Client lors de la connexion. |
| Disable 3rd-party Terminal Services plugins | Détermine si VMware Horizon Client doit vérifier les plug-ins Services Terminal Server installés en tant que plug-ins RDP normaux. Si vous ne configurez pas ce paramètre, VMware Horizon Client vérifie les plug-ins tiers par défaut. Ce paramètre n'affecte pas les plug-ins propres à View, tels que la redirection USB. |
| Locked Guest Size | <p>(Horizon Client 3.1 ou version ultérieure) Spécifie la résolution de l'écran sur le poste de travail distant si l'affichage est utilisé sur un seul moniteur. Cela signifie que ce paramètre ne fonctionne pas si vous avez configuré l'affichage du poste de travail distant sur Tous les moniteurs. Après l'activation du paramètre, la fonctionnalité d'ajustement automatique du poste de travail distant est désactivée. La taille d'écran minimale est de 640 x 480. La taille d'écran maximale est de 4 096 x 4 096. Ce paramètre s'applique uniquement aux connexions PCoIP et ne s'applique pas aux connexions RDP.</p> <p>IMPORTANT Il est recommandé de ne pas définir une résolution plus élevée que la résolution maximale prise en charge pour le poste de travail distant, qui est définie dans View Administrator :</p> <ul style="list-style-type: none"> ■ Si 3D est activé, jusqu'à 2 moniteurs sont pris en charge à une résolution maximale de 1 920x1 200. ■ Si 3D n'est pas activé, jusqu'à 4 moniteurs sont pris en charge à une résolution maximale de 2 560 x 1 600. <p>En pratique, ce paramètre côté client sera ignoré s'il est défini à une résolution supérieure à celle possible, en fonction de la version du système d'exploitation, la capacité de vRAM et la profondeur des couleurs du poste de travail distant. Par exemple, si la résolution du poste de travail est définie sur 1 920x1 200 dans View Administrator, la résolution indiquée sur le client risque de ne pas être supérieure à 1 920x1 200, selon les possibilités du poste de travail distant.</p> |
| Logon DomainName | Spécifie le domaine NetBIOS utilisé par Horizon Client lors de la connexion. |
| Logon Password | Spécifie le mot de passe utilisé par Horizon Client lors de la connexion. Active Directory stocke ce mot de passe en texte brut. |
| Logon UserName | Spécifie le nom d'utilisateur utilisé par Horizon Client lors de la connexion. |

Tableau 3-4. Modèle de configuration de VMware Horizon Client : définitions de script (suite)

| Paramètre | Description |
|--|--|
| Server URL | Spécifie l'URL utilisée par Horizon Client lors de la connexion. Par exemple, <code>https://view1.example.com</code> . |
| Suppress error messages (when fully scripted only) | Détermine si les messages d'erreur d'Horizon Client doivent être masqués lors de la connexion. Ce paramètre ne s'applique que lorsque le processus d'ouverture de session est entièrement scripté, par exemple, lorsque toutes les informations d'ouverture de session requises sont préremplies par la règle. Si la connexion échoue en raison d'informations de connexion incorrectes, l'utilisateur n'est pas averti et le processus Horizon Client est interrompu. |

Paramètres de sécurité des objets de stratégie de groupe (GPO) des clients

Les paramètres de sécurité incluent des options concernant le certificat de sécurité, les informations d'identification de connexion et la fonctionnalité d'authentification unique.

Le tableau suivant décrit les paramètres de sécurité figurant dans le fichier de modèle d'administration pour la configuration d'Horizon Client. Ce tableau montre si les paramètres incluent à la fois les paramètres Computer Configuration (Configuration ordinateur) et User Configuration (Configuration utilisateur) ou uniquement les paramètres Computer Configuration (Configuration ordinateur). Pour les paramètres de sécurité qui incluent les deux types, le paramètre User Configuration (Configuration utilisateur) remplace le paramètre Computer Configuration (Configuration ordinateur) équivalent.

Tableau 3-5. Modèle de configuration d'Horizon Client : paramètres de sécurité

| Paramètre | Description |
|---|--|
| Allow command line credentials (Paramètre de Configuration d'ordinateur) | Détermine si les informations d'identification d'utilisateur peuvent être fournies avec des options de ligne de commande d'Horizon Client. Si ce paramètre est désactivé, les options <code>smartCardPIN</code> et <code>password</code> ne sont pas disponibles lorsque les utilisateurs exécutent Horizon Client à partir de la ligne de commande. Ce paramètre est activé par défaut. La valeur de Registre Windows équivalente est <code>AllowCmdLineCredentials</code> . |
| Servers Trusted For Delegation (Paramètre de Configuration d'ordinateur) | Spécifie les instances de Serveur de connexion View qui acceptent l'identité et les informations d'identification d'utilisateur qui sont transmises quand un utilisateur coche la case Log in as current user (Se connecter en tant qu'utilisateur actuel) . Si vous ne spécifiez aucune instance de Serveur de connexion View, toutes les instances de Serveur de connexion View acceptent ces informations. Pour ajouter une instance de Serveur de connexion View, utilisez l'un des formats suivants : <ul style="list-style-type: none"> ■ <code>domain\system\$</code> ■ <code>system\$@domain.com</code> ■ Nom principal de service (SPN) du service Serveur de connexion View. La valeur de Registre Windows équivalente est <code>BrokersTrustedForDelegation</code> . |

Tableau 3-5. Modèle de configuration d' Horizon Client : paramètres de sécurité (suite)

| Paramètre | Description |
|---|---|
| Certificate verification mode (Paramètre de Configuration d'ordinateur) | <p>Configure le niveau de la vérification de certificat exécutée par Horizon Client. Vous pouvez sélectionner l'un de ces modes :</p> <ul style="list-style-type: none"> ■ No Security. View n'effectue pas la vérification de certificat. ■ Warn But Allow. Lorsque les problèmes de certificat de serveur suivants se produisent, un avertissement s'affiche, mais l'utilisateur peut continuer à se connecter au Serveur de connexion View : <ul style="list-style-type: none"> ■ Un certificat auto-signé est fourni par View. Dans ce cas, cela est acceptable si le nom de certificat ne correspond pas au nom du Serveur de connexion View fourni par l'utilisateur dans Horizon Client. ■ Un certificat vérifiable qui a été configuré dans votre déploiement a expiré ou n'est pas encore valide. <p>Si une autre erreur de certificat se produit, View affiche une boîte de dialogue d'erreur et empêche l'utilisateur de se connecter au Serveur de connexion View.</p> <p>Warn But Allow est la valeur par défaut.</p> <ul style="list-style-type: none"> ■ Full Security. Si une erreur de type de certificat se produit, l'utilisateur ne peut pas se connecter au Serveur de connexion View. View affiche les erreurs de certificat à l'utilisateur. <p>Lorsque ce paramètre de stratégie de groupe est configuré, les utilisateurs peuvent voir le mode de vérification de certificat sélectionné dans Horizon Client, mais ils ne peuvent pas configurer le paramètre. La boîte de dialogue de configuration SSL informe les utilisateurs que l'administrateur a verrouillé le paramètre.</p> <p>Lorsque ce paramètre n'est pas configuré ou est désactivé, les utilisateurs d'Horizon Client peuvent sélectionner un mode de vérification de certificat.</p> <p>Pour autoriser un serveur View à vérifier les certificats fournis par Horizon Client, le client doit établir des connexions HTTPS avec l'hôte du Serveur de connexion View ou du serveur de sécurité. La vérification des certificats n'est pas prise en charge si vous déchargez SSL vers un serveur intermédiaire qui établit des connexions HTTP avec l'hôte de Serveur de connexion View ou du serveur de sécurité.</p> <p>Pour les clients Windows, si vous ne voulez pas configurer ce paramètre en tant que stratégie de groupe, vous pouvez également activer la vérification de certificat en ajoutant le nom de valeur CertCheckMode à l'une des clés de Registre suivantes sur l'ordinateur client :</p> <ul style="list-style-type: none"> ■ Pour Windows 32 bits : HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security ■ Pour Windows 64 bits : HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security <p>Utilisez les valeurs suivantes dans la clé de registre :</p> <ul style="list-style-type: none"> ■ 0 implémente No Security. ■ 1 implémente Warn But Allow. ■ 2 implémente Full Security. <p>Si vous configurez le paramètre de stratégie de groupe et le paramètre CertCheckMode dans la clé de Registre Windows, le paramètre de stratégie de groupe est prioritaire sur la valeur de la clé de registre.</p> |

Tableau 3-5. Modèle de configuration d' Horizon Client : paramètres de sécurité (suite)

| Paramètre | Description |
|--|--|
| Default value of the 'Log in as current user' checkbox (Paramètre de Configuration d'utilisateur et d'ordinateur) | <p>Spécifie la valeur par défaut de la case à cocher Se connecter en tant qu'utilisateur actuel dans la boîte de dialogue de connexion d'Horizon Client.</p> <p>Ce paramètre remplace la valeur par défaut spécifiée au cours de l'installation d'Horizon Client.</p> <p>Si un utilisateur exécute Horizon Client à partir de la ligne de commande et spécifie l'option <code>logInAsCurrentUser</code>, cette valeur remplace ce paramètre.</p> <p>Lorsque la case Se connecter en tant qu'utilisateur actuel est cochée, l'identité et les informations d'identification que l'utilisateur a fournies lors de la connexion au système client sont transmises à l'instance du Serveur de connexion View, puis au poste de travail distant. Lorsque la case n'est pas cochée, les utilisateurs doivent fournir leur identité et leurs informations d'identification plusieurs fois avant de pouvoir accéder à un poste de travail distant.</p> <p>Ce paramètre est désactivé par défaut.</p> <p>La valeur de Registre Windows équivalente est <code>LogInAsCurrentUser</code>.</p> |
| Display option to Log in as current user (Paramètre de Configuration d'utilisateur et d'ordinateur) | <p>Détermine si la case à cocher Se connecter en tant qu'utilisateur actuel doit être visible dans la boîte de dialogue de connexion d'Horizon Client.</p> <p>Lorsque la case est visible, les utilisateurs peuvent la cocher ou la décocher et remplacer sa valeur par défaut. Lorsque la case est masquée, les utilisateurs ne peuvent pas remplacer sa valeur par défaut dans la boîte de dialogue de connexion d'Horizon Client.</p> <p>Vous pouvez spécifier la valeur par défaut de la case Log in as current user (Se connecter en tant qu'utilisateur actuel) en utilisant le paramètre de règle <code>Default value of the 'Log in as current user' checkbox</code>.</p> <p>Ce paramètre est activé par défaut.</p> <p>La valeur de Registre Windows équivalente est <code>LogInAsCurrentUser_Display</code>.</p> |
| Enable jump list integration (Paramètre de Configuration d'ordinateur) | <p>Détermine si une liste de raccourcis doit s'afficher dans l'icône Horizon Client sur la barre des tâches des systèmes Windows 7 ou versions ultérieures. La liste des raccourcis permet aux utilisateurs de se connecter à des instances récentes du Serveur de connexion View et à des postes de travail récemment utilisés.</p> <p>Si Horizon Client est partagé, vous pouvez ne pas souhaiter que les utilisateurs voient les noms des postes de travail récemment utilisés. Vous pouvez désactiver la liste de raccourcis en désactivant ce paramètre.</p> <p>Ce paramètre est activé par défaut.</p> <p>La valeur de Registre Windows équivalente est <code>EnableJumplist</code>.</p> |
| Enable SSL encrypted framework channel (Paramètre de Configuration d'utilisateur et d'ordinateur) | <p>Détermine si SSL doit être activé pour les postes de travail View 5.0 et versions antérieures. Avant View 5.0, les données envoyées au poste de travail via le port TCP 32111 n'étaient pas chiffrées.</p> <ul style="list-style-type: none"> ■ Activer : active SSL, mais autorise le retour à la connexion non chiffrée précédente si le poste de travail distant ne prend pas en charge SSL. Par exemple, les postes de travail View 5.0 et versions antérieures ne prennent pas en charge SSL. Activer est le paramètre par défaut. ■ Désactiver : désactive SSL. Ce paramètre n'est pas recommandé, mais peut toutefois être utile pour le débogage ou si le canal n'est pas configuré en tunnel et peut par la suite faire l'objet d'une optimisation par un produit accélérateur WAN. ■ Appliquer : active SSL et refuse les connexions aux postes de travail qui ne prennent pas en charge SSL. <p>La valeur de Registre Windows équivalente est <code>EnableTicketSSLAuth</code>.</p> |

Tableau 3-5. Modèle de configuration d' Horizon Client : paramètres de sécurité (suite)

| Paramètre | Description |
|---|--|
| Configures SSL protocols and cryptographic algorithms (Paramètre de Configuration d'utilisateur et d'ordinateur) | <p>Configure la liste de chiffrements afin de limiter l'utilisation de certains protocoles et algorithmes de chiffrement avant l'établissement d'une connexion SSL chiffrée. La liste de chiffrements est composée d'une ou de plusieurs chaînes de chiffrement séparées par deux points.</p> <p>REMARQUE Toutes les chaînes de chiffrement sont sensibles à la casse.</p> <ul style="list-style-type: none"> ■ Si cette fonction est activée, la valeur par défaut d'Horizon Client 3.5 et versions ultérieures est TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH. ■ La valeur par défaut d'Horizon Client 3.3 et 3.4 est TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH. ■ La valeur dans Horizon Client 3.2 et versions antérieures est SSLv3:TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH. <p>Cela signifie que dans Horizon Client 3.5 et versions ultérieures, TLS v1.0, TLS v1.1 et TLS v1.2 sont activés. (SSL v2.0 et v3.0 sont désactivés.) Dans Horizon Client 3.3 et 3.4, TLS v1.0 et TLS v1.1 sont activés. (SSL v2.0, SSL v3.0 et TLS v1.2 sont désactivés.) Dans Horizon Client 3.2 et versions antérieures, SSL v3.0 est également activé. (SSL v2.0 et TLS v1.2 sont désactivés.)</p> <p>Les suites de chiffrement utilisent la spécification AES 128 ou 256 bits, suppriment les algorithmes DH anonymes, puis trient la liste de chiffrements actuels par longueur de clé de chiffrement.</p> <p>Lien de référence pour la configuration : http://www.openssl.org/docs/apps/ciphers.html.</p> <p>La valeur de Registre Windows équivalente est SSLCipherList.</p> |
| Enable Single Sign-On for smart card authentication (Paramètre de Configuration d'ordinateur) | <p>Détermine si l'authentification unique est activée pour l'authentification par carte à puce. Lorsque l'authentification unique est activée, Horizon Client stocke le code PIN de carte à puce chiffré dans la mémoire temporaire avant de l'envoyer au Serveur de connexion View. Lorsque l'authentification unique est désactivée, Horizon Client n'affiche pas de boîte de dialogue de code PIN personnalisé.</p> <p>La valeur de Registre Windows équivalente est EnableSmartCardSSO.</p> |
| Ignore bad SSL certificate date received from the server (Paramètre de Configuration d'ordinateur) | <p>(View 4.6 et versions antérieures uniquement) Détermine si les erreurs associées aux dates des certificats de serveur non valides doivent être ignorées. Ces erreurs se produisent quand un serveur envoie un certificat avec une date passée.</p> <p>La valeur de Registre Windows équivalente est IgnoreCertDateInvalid.</p> |
| Ignore certificate revocation problems (Paramètre de Configuration d'ordinateur) | <p>(View 4.6 et versions antérieures uniquement) Détermine si les erreurs associées à un certificat de serveur révoqué doivent être ignorées. Ces erreurs se produisent lorsque le serveur envoie un certificat qui a été révoqué et lorsque le client ne peut pas vérifier l'état de révocation d'un certificat.</p> <p>Ce paramètre est désactivé par défaut.</p> <p>La valeur de Registre Windows équivalente est IgnoreRevocation.</p> |
| Ignore incorrect SSL certificate common name (host name field) (Paramètre de Configuration d'ordinateur) | <p>(View 4.6 et versions antérieures uniquement) Détermine si les erreurs associées aux noms communs de certificats de serveur incorrects doivent être ignorées. Ces erreurs se produisent quand le nom commun sur le certificat ne correspond pas au nom d'hôte du serveur qui l'envoie.</p> <p>La valeur de Registre Windows équivalente est IgnoreCertCnInvalid.</p> |

Tableau 3-5. Modèle de configuration d' Horizon Client : paramètres de sécurité (suite)

| Paramètre | Description |
|--|--|
| Ignore incorrect usage problems (Paramètre de Configuration d'ordinateur) | (View 4.6 et versions antérieures uniquement) Détermine si les erreurs associées à une utilisation incorrecte d'un certificat de serveur doivent être ignorées. Ces erreurs se produisent lorsque le serveur envoie un certificat ayant un autre but que vérifier l'identité de l'expéditeur et crypter les communications du serveur. La valeur de Registre Windows équivalente est IgnoreWrongUsage. |
| Ignore unknown certificate authority problems (Paramètre de Configuration d'ordinateur) | (View 4.6 et versions antérieures uniquement) Détermine si les erreurs associées à une autorité de certification inconnue sur le certificat du serveur doivent être ignorées. Ces erreurs se produisent lorsque le serveur envoie un certificat signé par une autorité tierce non approuvée. La valeur de Registre Windows équivalente est IgnoreUnknownCa. |

Paramètres RDP des objets de stratégie de groupe (GPO) des clients

Lorsque vous utilisez le protocole d'affichage RDP de Microsoft, vous pouvez définir des stratégies de groupe pour des options telles que la redirection des périphériques audio, des imprimantes, des ports ou d'autres périphériques.

Le tableau suivant décrit les paramètres RDP (Remote Desktop Protocol) situés dans le fichier de modèle d'administration pour la configuration d'Horizon Client. Tous les paramètres RDP sont des paramètres de Configuration d'utilisateur.

Tableau 3-6. Horizon Client Modèle d'administration de configuration : paramètres RDP

| Paramètre | Description |
|---|---|
| Audio redirection | Détermine si les informations audio lues sur le poste de travail distant doivent être redirigées. Sélectionnez l'un des paramètres suivants : <ul style="list-style-type: none"> ■ Désactiver le son : le son est désactivé. ■ Lire sur la machine virtuelle (nécessaire pour la prise en charge d'USB VoIP) : les données audio sont lues sur le poste de travail distant. Ce paramètre requiert un périphérique audio USB partagé pour que le client reçoive le son. ■ Rediriger vers le client : les sons sont redirigés vers le client. Il s'agit du mode par défaut. Ce paramètre ne s'applique qu'à l'audio RDP. Les sons redirigés via MMR sont lus sur le client. |
| Enable audio capture redirection | Détermine si le périphérique d'entrée audio par défaut est redirigé du client vers la session distante. Lorsque ce paramètre est activé, le périphérique d'enregistrement audio sur le client s'affiche sur le poste de travail distant et peut enregistrer une entrée audio. Le paramètre par défaut est désactivé. |
| Bitmap cache file size in unit for number bpp bitmaps | Spécifie la taille du cache bitmap, en kilo-octets ou en méga-octets, à utiliser pour les paramètres de couleur bitmap d'un nombre de bits par pixel (bpp) spécifique. Des versions séparées de ce paramètre sont fournies pour les combinaisons unité/bpp suivantes : <ul style="list-style-type: none"> ■ Ko/8 bpp ■ Mo/8 bpp ■ Mo/16 bpp ■ Mo/24 bpp ■ Mo/32 bpp |
| Bitmap caching/cache persistence active | Détermine si la mise en cache permanente des bitmaps est utilisée (active). La mise en cache permanente des bitmaps peut améliorer les performances de votre ordinateur mais requiert plus d'espace disque. |

Tableau 3-6. Horizon Client Modèle d'administration de configuration : paramètres RDP (suite)

| Paramètre | Description |
|---------------------------|---|
| Color depth | <p>Spécifie l'intensité des couleurs du poste de travail distant. Sélectionnez l'un des paramètres disponibles :</p> <ul style="list-style-type: none"> ■ 8 bits ■ 15 bits ■ 16 bits ■ 24 bits ■ 32 bits <p>Pour les systèmes Windows XP 24 bits, vous devez activer la règle Limit Maximum Color Depth (Limiter le nombre maximal de couleurs) sous Configuration de l'ordinateur > Modèles d'administration > Composants Windows > Services Terminal Server et la définir sur 24 bits.</p> |
| Cursor shadow | Détermine si une ombre doit s'afficher sous le curseur sur le poste de travail distant. |
| Desktop background | Détermine si l'arrière-plan du poste de travail doit être visible lorsque des clients se connectent à un poste de travail distant. |
| Desktop composition | <p>(Windows Vista ou version ultérieure) Détermine si la composition du poste de travail doit être activée sur le poste de travail distant.</p> <p>Lorsque la composition de poste de travail est activée, les fenêtres individuelles ne se dessinent plus sur l'écran ou sur le périphérique d'affichage principal comme c'était le cas dans les précédentes versions de Microsoft Windows. Le dessin est redirigé vers des surfaces non affichées à l'écran, en mémoire vidéo, qui sont ensuite rendues sous la forme d'une image de poste de travail et représentées à l'écran.</p> |
| Enable compression | Détermine si les données RDP sont compressées. Ce paramètre est activé par défaut. |
| Enable RDP Auto-Reconnect | <p>Détermine si le composant client RDP doit tenter de se reconnecter à un poste de travail distant après un échec de connexion du protocole RDP. Ce paramètre n'a aucun effet si l'option Use secure tunnel connection to desktop (Utiliser une connexion par tunnel sécurisé vers le poste de travail) est activée dans View Administrator. Ce paramètre est désactivé par défaut.</p> <p>REMARQUE La reconnexion automatique RDP est prise en charge pour les postes de travail exécutant View Agent version 4.5 ou supérieure uniquement. Si un poste de travail possède une version antérieure de View Agent, certaines fonctions ne fonctionneront pas.</p> |
| Font smoothing | (Windows Vista ou version ultérieure) Détermine si l'anticrénelage doit s'appliquer aux polices sur le poste de travail distant. |
| Menu and window animation | Détermine si l'animation des menus et des fenêtres doit être activée lorsque des clients se connectent à un poste de travail distant. |
| Redirect clipboard | Détermine si les informations locales du Presse-papiers doivent être redirigées lorsque des clients se connectent au poste de travail distant. |
| Redirect drives | <p>Détermine si les lecteurs de disques locaux doivent être redirigés lorsque des clients se connectent au poste de travail distant. Par défaut, les lecteurs locaux sont redirigés.</p> <p>L'activation de ce paramètre, ou le laisser non configuré, permet de copier des données entre le lecteur redirigé sur le poste de travail distant et le lecteur sur l'ordinateur client. Désactivez ce paramètre si autoriser des données à passer du poste de travail distant à des ordinateurs clients d'utilisateurs représente un risque de sécurité potentiel dans votre déploiement. Une autre approche consiste à désactiver la redirection de dossier dans la machine virtuelle de poste de travail distant en activant le paramètre de stratégie de groupe de Microsoft Windows, Do not allow drive redirection.</p> <p>Le paramètre Redirect drives ne s'applique qu'à RDP.</p> |
| Redirect printers | Détermine si les imprimantes locales doivent être redirigées lorsque des clients se connectent au poste de travail distant. |

Tableau 3-6. Horizon Client Modèle d'administration de configuration : paramètres RDP (suite)

| Paramètre | Description |
|--|--|
| Redirect serial ports | Détermine si les ports COM locaux doivent être redirigés lorsque des clients se connectent au poste de travail distant. |
| Redirect smart cards | Détermine si les cartes à puce locales doivent être redirigées lorsque des clients se connectent au poste de travail distant. REMARQUE Ce paramètre s'applique aux connexions RDP et PCoIP. |
| Redirect supported plug-and-play devices | Détermine si les périphériques locaux de point de vente et Plug-and-Play doivent être redirigés lorsque des clients se connectent au poste de travail distant. Ce comportement est différent de la redirection gérée par le composant de redirection USB d'View Agent. |
| Shadow bitmaps | Détermine si les bitmaps sont ombrés. Ce paramètre n'a pas d'effet en plein écran. |
| Show contents of window while dragging | Détermine si le contenu des dossiers s'affiche lorsqu'un utilisateur les fait glisser vers un nouvel emplacement. |
| Themes | Détermine si des thèmes doivent s'afficher lorsque des clients se connectent à un poste de travail distant. |
| Windows key combination redirection | Détermine où les combinaisons de clés Windows sont appliquées. Ce paramètre vous permet d'envoyer des combinaisons de clés à la machine virtuelle distante ou d'appliquer des combinaisons de clés localement. Si ce paramètre n'est pas configuré, les combinaisons de clés sont appliquées localement. |

Paramètres généraux des objets de stratégie de groupe (GPO) de clients

Parmi les paramètres figurent les options de proxy, le transfert de fuseau horaire, l'accélération multimédia et d'autres paramètres d'affichage.

Paramètres généraux

Le tableau suivant décrit les paramètres généraux figurant dans le fichier de modèle d'administration pour la configuration d'Horizon Client. Les paramètres généraux incluent des paramètres de Configuration d'ordinateur et de Configuration d'utilisateur. Le paramètre de Configuration d'utilisateur remplace le paramètre de Configuration d'ordinateur équivalent.

Tableau 3-7. Modèle de configuration d' Horizon Client : paramètres généraux

| Paramètre | Description |
|--|--|
| Always on top (Paramètre de Configuration d'utilisateur) | Détermine si la fenêtre Horizon Client doit toujours rester au premier plan. L'activation de ce paramètre empêche la barre des tâches de Windows de s'afficher sur la fenêtre Horizon Client en plein écran. Ce paramètre est désactivé par défaut. |
| Default value of the "Hide the selector after launching an item" check box (Paramètre de Configuration d'utilisateur et d'ordinateur) | (Horizon Client 3.1 ou version ultérieure) Définit si la case Masquer le sélecteur après le lancement d'un élément est cochée par défaut. Ce paramètre est désactivé par défaut. |

Tableau 3-7. Modèle de configuration d' Horizon Client : paramètres généraux (suite)

| Paramètre | Description |
|---|---|
| Determines if the VMware View Client should use proxy.pac file (Paramètre de Configuration d'ordinateur) | (View 4.6 et versions antérieures uniquement) Détermine si Horizon Client doit utiliser un fichier de configuration automatique de proxy PAC (Proxy Auto Config). L'activation de ce paramètre force Horizon Client à utiliser un fichier PAC. Un fichier PAC (appelé communément <code>proxy.pac</code>) aide les navigateurs Web et d'autres agents d'utilisateur à trouver le serveur proxy approprié pour une demande particulière d'URL ou de site Web. Si vous activez ce paramètre sur une machine multicœur, l'application WinINet qu'Horizon Client utilise pour rechercher des informations de serveur proxy peut se bloquer. Désactivez ce paramètre si ce problème se produit sur votre machine. Ce paramètre est désactivé par défaut. REMARQUE Ce paramètre ne s'applique qu'aux connexions directes. Il n'affecte pas les connexions par tunnel. |
| Disable time zone forwarding (Paramètre de Configuration d'ordinateur) | Détermine si la synchronisation de fuseau horaire entre le poste de travail distant et le client connecté doit être désactivée. |
| Disable toast notifications (Paramètre de Configuration d'utilisateur et d'ordinateur) | Détermine s'il faut désactiver les notifications toast dans Horizon Client. Activez ce paramètre si vous ne voulez pas que l'utilisateur voie des notifications de toast dans le coin de l'écran. REMARQUE Si vous activez ce paramètre, l'utilisateur ne voit pas d'avertissement de 5 minutes lorsque la fonction Session Timeout (Délai d'expiration de la session) est active. |
| Don't check monitor alignment on spanning (Paramètre de Configuration d'utilisateur) | Par défaut, le poste de travail client ne s'étend pas sur plusieurs écrans si la combinaison de ces derniers ne forme pas un rectangle exact lorsqu'ils sont combinés. Activez ce paramètre pour remplacer la valeur par défaut. Ce paramètre est désactivé par défaut. |
| Enable multi-media acceleration (Paramètre de Configuration d'utilisateur) | Détermine si la redirection multimédia (MMR) est activée sur le client. MMR ne fonctionne pas correctement si le matériel d'affichage vidéo d' Horizon Client ne prend pas en charge la superposition. |
| Enable relative mouse (Paramètre de Configuration d'utilisateur et d'ordinateur) | (View 5.2 et versions ultérieures uniquement) Active la souris relative lors de l'utilisation du protocole d'affichage PCoIP. Le mode de souris relative améliore le comportement de la souris pour certaines applications graphiques et certains jeux. Si le poste de travail distant ne prend pas en charge la souris relative, ce paramètre ne sera pas utilisé. Ce paramètre est désactivé par défaut. |
| Enable the shade (Paramètre de Configuration d'utilisateur) | Détermine si la barre de menu ombre situé en haut de la fenêtre Horizon Client doit être visible. Ce paramètre est activé par défaut. REMARQUE La barre de menu ombre est désactivée par défaut pour le mode kiosque. |
| Tunnel proxy bypass address list (Paramètre de Configuration d'ordinateur) | Spécifie une liste d'adresses de tunnel. Le serveur proxy n'est pas utilisé pour ces adresses. Utilisez un point-virgule (;) pour séparer plusieurs entrées. |
| URL for View Client online help (Paramètre de Configuration d'ordinateur) | Spécifie une autre URL à partir de laquelle Horizon Client peut récupérer les pages d'aide. Ce paramètre est conçu pour être utilisé dans des environnements qui ne peuvent pas récupérer le système d'aide hébergé à distance car ils n'ont pas d'accès à Internet. |

Tableau 3-7. Modèle de configuration d' Horizon Client : paramètres généraux (suite)

| Paramètre | Description |
|---|--|
| Pin the shade (Paramètre de Configuration d'utilisateur) | Détermine si l'épingle de l'ombre située en haut de la fenêtre Horizon Client doit être activée, de sorte que le masquage automatique de la barre de menus ne se produit pas. Ce paramètre est sans effet si l'ombre est désactivée. Ce paramètre est activé par défaut. |
| Disable desktop disconnect messages (Paramètre de Configuration d'utilisateur et d'ordinateur) | Indique si les messages qui s'affichent généralement lors de la déconnexion du poste de travail doivent être désactivés. Ces messages s'affichent par défaut. |

Paramètres UBS des objets de stratégie de groupe (GPO) des clients

Vous pouvez définir des paramètres de stratégie USB pour View Agent et pour Horizon Client pour Windows. Lors de la connexion, Horizon Client télécharge les paramètres de stratégie USB à partir d'View Agent et les utilise avec ses propres paramètres de stratégie USB afin de décider des périphériques à rendre disponibles pour la redirection à partir de la machine hôte.

Le tableau suivant décrit chaque paramètre de fractionnement de périphérique USB composite situé dans le fichier de modèle d'administration pour la configuration d'Horizon Client. Les paramètres s'appliquent au niveau de l'ordinateur. Horizon Client lit de préférence les paramètres de l'objet de stratégie de groupe au niveau de l'ordinateur. Sinon, il lit ceux du registre dans HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB. Pour savoir comment View applique les stratégies de fractionnement de périphériques USB composites, reportez-vous aux rubriques concernant l'utilisation des stratégies pour contrôler la redirection USB dans le document *Configuration de pools de postes de travail et d'applications dans View*.

Tableau 3-8. Modèle de configuration d' Horizon Client : paramètres de fractionnement USB

| Paramètre | Propriétés |
|---|---|
| Autoriser le fractionnement automatique de périphérique | Autorise le fractionnement automatique de périphériques USB composites. La valeur par défaut est indéfinie, ce qui correspond à false . |
| Exclude Vid/Pid Device From Split | Exclut un périphérique USB composite spécifié par des ID de fournisseur et de produit du fractionnement. Le format du paramètre est <code>vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]...</code> Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (*) à la place de chiffres dans un ID. Par exemple : vid-0781_pid-55** La valeur par défaut n'est pas définie. |
| Split Vid/Pid Device | Traite les composants d'un périphérique USB composite spécifiés par des ID de fournisseur et de produit en tant que périphériques séparés. Le format du paramètre est <code>vid-xxxx_pid-yyy(exintf:zz[;exintf:ww])</code> Vous pouvez utiliser le mot-clé <code>exintf</code> pour exclure des composants de la redirection en spécifiant leur numéro d'interface. Vous devez spécifier les numéros d'ID au format hexadécimal et les numéros d'interface au format décimal en incluant les zéros à gauche. Vous pouvez utiliser le caractère générique (*) à la place de chiffres dans un ID. Par exemple : vid-0781_pid-554c(exintf:01;exintf:02) REMARQUE View n'inclut pas automatiquement les composants que vous n'avez pas explicitement exclus. Vous devez spécifier une règle de filtre telle que <code>Include Vid/Pid Device</code> pour inclure ces composants. La valeur par défaut n'est pas définie. |

Le tableau suivant décrit chaque paramètre de stratégie de filtrage des périphériques USB situé dans le fichier de modèle d'administration pour la configuration d'Horizon Client. Les paramètres s'appliquent au niveau de l'ordinateur. Horizon Client lit de préférence les paramètres de l'objet de stratégie de groupe au niveau de l'ordinateur. Sinon, il lit ceux du registre dans HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB. Pour savoir comment View applique les stratégies de fractionnement de périphériques USB composites, reportez-vous aux rubriques concernant la configuration des paramètres de stratégie de filtre pour la redirection USB dans le document *Configuration de pools de postes de travail et d'applications dans View*.

Tableau 3-9. Modèle de configuration d' Horizon Client : paramètres de filtrage USB

| Paramètre | Propriétés |
|--|---|
| Allow Audio Input Devices | Permet la redirection de périphériques d'entrée audio. La valeur par défaut est indéfinie, ce qui correspond à true . |
| Allow Audio Output Devices | Permet la redirection de périphériques de sortie audio. La valeur par défaut est indéfinie, ce qui correspond à false . |
| Allow HIDBootable | Permet la redirection de périphériques d'entrée autres que des claviers et des souris qui sont disponibles au démarrage (ou périphériques démarrables par HID). La valeur par défaut est indéfinie, ce qui correspond à true . |
| Autoriser le comportement du descripteur de périphérique à sécurité intégrée | Autorise la redirection des périphériques même si Horizon Client ne parvient pas à obtenir les descripteurs de configuration/périphérique. Pour autoriser un périphérique même si config/desc échoue, incluez-le dans les filtres d'inclusion tels que IncludeVidPid ou IncludePath. La valeur par défaut est indéfinie, ce qui correspond à false . |
| Autoriser d'autres périphériques d'entrée | Permet la redirection de périphériques d'entrée autres que des périphériques démarrables par HID ou des claviers avec périphériques de pointage intégrés. La valeur par défaut est indéfinie, ce qui correspond à true . |
| Allow Keyboard and Mouse Devices | Permet la redirection de claviers avec périphériques de pointage intégrés (souris, Trackball ou pavé tactile). La valeur par défaut est indéfinie, ce qui correspond à false . |
| Allow Smart Cards | Permet la redirection de périphériques à carte à puce. La valeur par défaut est indéfinie, ce qui correspond à false . |
| Allow Video Devices | Permet la redirection de périphériques vidéo. La valeur par défaut est indéfinie, ce qui correspond à true . |
| Désactiver la configuration à distance | Désactive l'utilisation de paramètres de View Agent lors de l'exécution du filtrage de périphérique USB. La valeur par défaut est indéfinie, ce qui correspond à false . |
| Exclude All Devices | Exclut tous les périphériques USB de la redirection. Si ce paramètre est défini sur true , vous pouvez utiliser d'autres paramètres de règle pour autoriser la redirection de périphériques spécifiques ou de familles de périphériques. Si ce paramètre est défini sur false , vous pouvez utiliser d'autres paramètres de règle pour empêcher la redirection de périphériques spécifiques ou de familles de périphériques. Si vous définissez la valeur de Exclude All Devices sur true sur View Agent, et si ce paramètre est transmis à Horizon Client, le paramètre de View Agent remplace celui d'Horizon Client. La valeur par défaut est indéfinie, ce qui correspond à false . |
| Exclude Device Family | Exclut des familles de périphériques de la redirection. Le format du paramètre est <i>family_name_1[:family_name_2]...</i> Par exemple : bluetooth;smart-card Si vous avez activé le fractionnement automatique de périphérique, View examine la famille de périphériques de chaque interface d'un périphérique USB composite afin de décider des interfaces à exclure. Si vous avez désactivé le fractionnement automatique de périphérique, View examine la famille de périphériques de l'ensemble du périphérique USB composite. La valeur par défaut n'est pas définie. |

Tableau 3-9. Modèle de configuration d' Horizon Client : paramètres de filtrage USB (suite)

| Paramètre | Propriétés |
|------------------------|--|
| Exclude Vid/Pid Device | <p>Exclut des périphériques avec des ID de fournisseur et de produit spécifiés de la redirection. Le format du paramètre est <code>vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]...</code></p> <p>Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (*) à la place de chiffres dans un ID.</p> <p>Par exemple : vid-0781_pid-****;vid-0561_pid-554c</p> <p>La valeur par défaut n'est pas définie.</p> |
| Exclude Path | <p>Exclut des périphériques dans des chemins de concentrateur ou de port spécifiés de la redirection. Le format du paramètre est <code>bus-x1[/y1].../port-z1[;bus-x2[/y2].../port-z2]...</code></p> <p>Vous devez spécifier des numéros de bus et de port au format hexadécimal. Vous ne pouvez pas utiliser le caractère générique dans les chemins.</p> <p>Par exemple : bus-1/2/3_port-02;bus-1/1/1/4_port-ff</p> <p>La valeur par défaut n'est pas définie.</p> |
| Include Device Family | <p>Inclut des familles de périphériques pouvant être redirigées. Le format du paramètre est <code>family_name_1[;family_name_2]...</code></p> <p>Par exemple : stockage</p> <p>La valeur par défaut n'est pas définie.</p> |
| Include Path | <p>Inclut des périphériques dans des chemins de concentrateur ou de port spécifiés pouvant être redirigés. Le format du paramètre est <code>bus-x1[/y1].../port-z1[;bus-x2[/y2].../port-z2]...</code></p> <p>Vous devez spécifier des numéros de bus et de port au format hexadécimal. Vous ne pouvez pas utiliser le caractère générique dans les chemins.</p> <p>Par exemple : bus-1/2_port-02;bus-1/7/1/4_port-0f</p> <p>La valeur par défaut n'est pas définie.</p> |
| Include Vid/Pid Device | <p>Inclut des périphériques avec des ID de fournisseur et de produit spécifiés pouvant être redirigés. Le format du paramètre est <code>vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]...</code></p> <p>Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (*) à la place de chiffres dans un ID.</p> <p>Par exemple : vid-0561_pid-554c</p> <p>La valeur par défaut n'est pas définie.</p> |

Paramètres de modèle d'administration pour les variables de session de client PCoIP de View

Le fichier de modèle d'administration pour les variables de session de client PCoIP de View (`pcoip.client.adm`) contient des paramètres de stratégie liés au protocole d'affichage PCoIP. Vous pouvez configurer les paramètres à des valeurs par défaut qui peuvent être remplacées par un administrateur, ou vous pouvez configurer les paramètres à des valeurs ne pouvant pas être remplacées.

Ce fichier ADM est disponible dans un fichier groupé .zip nommé `VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyy.zip`, que vous pouvez télécharger sur le site de téléchargement de VMware à l'adresse <https://my.vmware.com/web/vmware/downloads>. Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 6, qui inclut le fichier groupé .zip.

Tableau 3-10. Variables de la session de client PCoIP de View

| Paramètre | Description |
|--|---|
| Configure PCoIP client image cache size policy | <p>Contrôle la taille du cache d'images client PCoIP. Le client utilise une mise en cache d'images pour stocker des parties de l'affichage qui ont été précédemment transmises. La mise en cache d'images réduit la quantité de données qui sont retransmises.</p> <p>Ce paramètre ne s'applique qu'à des clients Windows et Linux lorsque Horizon Client, View Agent et Serveur de connexion View correspondent à la version View 5.0 ou version ultérieure.</p> <p>Lorsque ce paramètre n'est pas configuré ou qu'il est désactivé, PCoIP utilise une taille de cache d'images client par défaut de 250 Mo.</p> <p>Lorsque vous activez ce paramètre, vous pouvez configurer une taille de cache d'images client comprise entre 50 Mo minimum et 300 Mo maximum. La valeur par défaut est 250 Mo.</p> |
| Configure PCoIP event log verbosity | <p>Définit le niveau de détails du journal des événements PCoIP. Les valeurs sont comprises entre 0 (le moins de détails) et 3 (le plus de détails).</p> <p>Lorsque ce paramètre est activé, vous pouvez définir le niveau de détail entre 0 et 3. Lorsque le paramètre n'est pas configuré ou désactivé, le niveau de détail du journal des événements par défaut est 2.</p> <p>Lorsque ce paramètre est modifié lors d'une session PCoIP active, le nouveau paramètre prend effet immédiatement.</p> |
| Configure PCoIP session encryption algorithms | <p>Contrôle les algorithmes de cryptage annoncés par le point de terminaison PCoIP lors de la négociation de session.</p> <p>Cocher l'une des cases désactive l'algorithme de cryptage associé. Vous devez activer au moins un algorithme.</p> <p>Par défaut, les deux algorithmes Salsa20-256round12 et AES-128-GCM sont disponibles pour la négociation par ce point de terminaison.</p> <p>Ce paramètre s'applique à la fois à l'agent et au client. Les points de terminaison négocient l'algorithme de cryptage de session réel qui est utilisé. Si le mode approuvé FIPS140-2 est activé, la valeur Disable AES-128-GCM encryption (Désactiver le cryptage AES-128-GCM) est toujours remplacée pour que le cryptage AES-128-GCM soit activé. Notez que le mode FIPS n'est pas pris en charge avec Horizon Client 3.4.</p> <p>Si ce paramètre est désactivé ou qu'il n'est pas configuré, les deux algorithmes Salsa20-256round12 et AES-128-GCM sont disponibles pour la négociation par ce point de terminaison.</p> |
| Configure PCoIP virtual channels | <p>Spécifie les canaux virtuels qui peuvent et ne peuvent pas fonctionner sur des sessions PCoIP. Ce paramètre détermine également s'il est nécessaire de désactiver le traitement du presse-papier sur l'hôte PCoIP.</p> <p>Les canaux virtuels utilisés dans des sessions PCoIP doivent apparaître dans la liste d'autorisation des canaux virtuels. Les canaux virtuels qui apparaissent dans la liste des canaux virtuels interdits ne peuvent pas être utilisés dans des sessions PCoIP.</p> <p>Vous pouvez spécifier un maximum de 15 canaux virtuels à utiliser dans des sessions PCoIP.</p> <p>Séparez les noms de canal avec le caractère de barre verticale (). Par exemple, la chaîne d'autorisation des canaux virtuels pour autoriser les canaux virtuels mksvchan et vdp_rdpvcbridge est mksvchan vdp_rdpvcbridge.</p> <p>Si un nom de canal contient le caractère de barre verticale ou de barre oblique inverse (\), insérez un caractère de barre oblique inverse avant ce caractère. Par exemple, saisissez le nom de canal awk ward\channel comme suit : awk\ward\channel.</p> <p>Lorsque la liste des canaux virtuels autorisés est vide, tous les canaux virtuels sont interdits. Lorsque la liste des canaux virtuels interdits est vide, tous les canaux virtuels sont autorisés.</p> <p>Le paramètre des canaux virtuels s'applique à la fois à l'agent et au client. Les canaux virtuels doivent être activés à la fois sur l'agent et le client pour pouvoir être utilisés.</p> <p>Le paramètre des canaux virtuels fournit une case séparée qui vous permet de désactiver le traitement du presse-papier à distance sur l'hôte PCoIP. Cette valeur ne s'applique qu'à l'agent.</p> <p>Par défaut, tous les canaux virtuels sont activés, notamment le traitement du presse-papier.</p> |

Tableau 3-10. Variables de la session de client PCoIP de View (suite)

| Paramètre | Description |
|---|---|
| Configure the Client PCoIP UDP port | <p>Spécifie le port client UDP utilisé par les clients PCoIP logiciels. La valeur du port UDP spécifie le port UDP de base à utiliser. La valeur de plage du port UDP détermine le nombre de ports supplémentaires à essayer si le port de base n'est pas disponible.</p> <p>La plage s'étend du port de base à la somme du port de base et de la plage du port. Par exemple, si le port de base est 50002 et que la plage du port est 64, la plage s'étend de 50002 à 50066.</p> <p>Ce paramètre ne s'applique qu'au client.</p> <p>Par défaut, le port de base est 50002 et la plage du port est 64.</p> |
| Configure the maximum PCoIP session bandwidth | <p>Spécifie la bande passante maximale, en kilobits par seconde, dans une session PCoIP. La bande passante inclut la création d'images, le son, le canal virtuel, USB et le trafic PCoIP de contrôle.</p> <p>Définissez cette valeur sur la capacité globale du lien auquel votre point de terminaison est connecté, en tenant compte du nombre de sessions PCoIP simultanées prévues. Par exemple, avec une configuration VDI à un seul utilisateur (une session PCoIP unique) qui se connecte au moyen d'une connexion Internet 4 Mbits/s, définissez cette valeur sur 4 Mbit, ou 10 % de moins que cette valeur pour prévoir un autre trafic réseau. Lorsque vous prévoyez que plusieurs sessions PCoIP simultanées partageront un lien, comprenant plusieurs utilisateurs VDI ou une configuration RDS, vous pouvez régler ce paramètre en conséquence.</p> <p>Cependant, la diminution de cette valeur limitera la bande passante maximale de chaque session active.</p> <p>La définition de cette valeur empêche l'agent de transmettre un débit supérieur à la capacité de lien, ce qui pourrait entraîner une perte de paquets excessive et une mauvaise expérience utilisateur. Cette valeur est symétrique. Elle force le client et l'agent à utiliser la plus faible des deux valeurs qui sont définies côté client et agent. Par exemple, la définition d'une bande passante maximale de 4 Mbit/s force l'agent à transmettre à un débit plus faible, même si le paramètre est configuré sur le client.</p> <p>Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré sur un point de terminaison, le point de terminaison n'impose aucune contrainte de bande passante. Lorsque ce paramètre est configuré, le paramètre est utilisé comme la contrainte de bande passante maximale du point de terminaison en kilobits par seconde.</p> <p>La valeur par défaut lorsque ce paramètre n'est pas configuré est de 900000 kilobits par seconde.</p> <p>Ce paramètre s'applique à la fois à View Agent et au client. Si les deux points de terminaison ont des paramètres différents, la valeur la plus faible est utilisée.</p> |
| Configure the PCoIP transport header | <p>Configure l'en-tête de transport PCoIP et définit la priorité de la session de transport.</p> <p>L'en-tête de transport PCoIP est un en-tête 32 bits ajouté à tous les paquets UDP PCoIP (uniquement si l'en-tête de transport est activé et pris en charge des deux côtés). L'en-tête de transport PCoIP permet aux périphériques réseau de prendre de meilleures décisions concernant la hiérarchisation/qualité de service lors du traitement de la surcharge du réseau. L'en-tête de transport est activé par défaut.</p> <p>La priorité de session de transport détermine la priorité de session PCoIP signalée dans l'en-tête de transport PCoIP. Les périphériques réseau prennent de meilleures décisions concernant la hiérarchisation/qualité de service en fonction de la priorité de session de transport spécifiée.</p> <p>Lorsque le paramètre <code>Configure the PCoIP transport header</code> est activé, les priorités de session de transport suivantes sont disponibles :</p> <ul style="list-style-type: none"> ■ Haute ■ Moyenne (valeur par défaut) ■ Basse ■ Non définie <p>La valeur de priorité de session de transport est négociée par l'agent et le client PCoIP. Si l'agent PCoIP spécifie une valeur de priorité de session de transport, la session utilise la priorité de session spécifiée par l'agent. Si seul le client a spécifié une priorité de session de transport, la session utilise la priorité de session spécifiée par le client. Si ni l'agent ni le client n'a spécifié une priorité de session de transport, ou si Priorité non définie est spécifié, la session utilise la valeur par défaut, la priorité Moyenne.</p> |

Tableau 3-10. Variables de la session de client PCoIP de View (suite)

| Paramètre | Description |
|--|---|
| Enable the FIPS 140-2 approved mode of operation | <p>(Horizon Client 3.0 à 3.3 uniquement) Détermine s'il est nécessaire d'utiliser uniquement des algorithmes et des protocoles cryptographiques approuvés FIPS 140-2 pour établir une connexion PCoIP à distance. Activer ce paramètre remplace la désactivation du cryptage AES128-GCM.</p> <p>Ce paramètre s'applique à la fois à l'agent 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 cryptage disponibles pour la négociation de session.</p> <p>Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, le mode FIPS n'est pas utilisé.</p> <p>IMPORTANT Pour Horizon Client 3.5 et versions ultérieures, n'utilisez pas ce paramètre pour activer le mode FIPS. Au lieu de cela, vous activez le mode FIPS lorsque vous installez le client. Notez également que le mode FIPS n'est pas pris en charge avec Horizon Client 3.4.</p> |
| Enable/disable audio in the PCoIP session | <p>Détermine si le son est activé dans des sessions PCoIP. Le son doit être activé sur les deux points de terminaison. Lorsque ce paramètre est activé, le son PCoIP est autorisé. Lorsqu'il est désactivé, le son PCoIP est désactivé. Lorsque ce paramètre n'est pas configuré, le son est activé par défaut.</p> |
| Configure the PCoIP session bandwidth floor | <p>Spécifie une limite inférieure, en kilobits par seconde, pour la bande passante réservée par la session PCoIP.</p> <p>Ce paramètre configure le taux de transmission de bande passante minimum attendu pour le point de terminaison. Lorsque vous utilisez ce paramètre pour réserver de la bande passante pour un point de terminaison, l'utilisateur n'a pas à attendre que la bande passante soit disponible, ce qui améliore la réactivité de la session.</p> <p>Assurez-vous que vous ne sursouscrivez pas la bande passante totale réservée pour tous les points de terminaison. Assurez-vous que la somme des valeurs plancher de la bande passante pour toutes les connexions dans votre configuration ne dépasse pas la capacité du réseau.</p> <p>La valeur par défaut est 0, ce qui signifie qu'aucune bande passante minimale n'est réservée. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, aucune bande passante minimale n'est réservée.</p> <p>Ce paramètre s'applique à View Agent et au client, mais le paramètre n'affecte que le point de terminaison sur lequel il est configuré.</p> <p>Lorsque ce paramètre est modifié lors d'une session PCoIP active, la modification prend effet immédiatement.</p> |
| Configure the PCoIP session MTU | <p>Spécifie la taille de l'unité de transmission maximale (MTU) pour les paquets UDP d'une session PCoIP.</p> <p>La taille de la MTU inclut les en-têtes de paquet IP et UDP. Le protocole TCP utilise le mécanisme de découverte MTU standard pour définir la MTU et n'est pas affecté par ce paramètre.</p> <p>La taille de la MTU maximale est de 1 500 octets. La taille de la MTU minimale est de 500 octets. La valeur par défaut est de 1 300 octets.</p> <p>En général, vous n'avez pas à modifier la taille de la MTU. Modifiez cette valeur si vous avez une configuration de réseau inhabituelle qui provoque une fragmentation de paquets PCoIP.</p> <p>Ce paramètre s'applique à la fois à View Agent et au client. Si les deux points de terminaison ont des paramètres de taille de MTU différents, la valeur la plus faible est utilisée.</p> <p>Si ce paramètre est désactivé ou qu'il n'est pas configuré, le client utilise la valeur par défaut dans la négociation avec View Agent.</p> |

Exécution d' Horizon Client depuis la ligne de commande

Vous pouvez exécuter Horizon Client pour Windows à partir de la ligne de commande ou via des scripts. Vous pouvez en avoir besoin pour implémenter une application kiosque qui accordent aux utilisateurs finaux l'autorisation d'accès à des applications poste de travail.

Utilisez la commande `vmware-view.exe` pour exécuter Horizon Client pour Windows à partir de la ligne de commande. Vous pouvez ajouter des options à la commande pour modifier le comportement d' Horizon Client.

Utilisation des commandes d' Horizon Client

La syntaxe de la commande `vmware-view` contrôle le fonctionnement d'Horizon Client.

Utilisez la forme suivante de la commande `vmware-view` dans une invite de commande Windows.

```
vmware-view [command_line_option [argument]] ...
```

Le chemin d'accès par défaut au fichier exécutable de la commande `vmware-view` varie en fonction de votre système.

- Sur des systèmes 32 bits, le chemin est `C:\Program Files\VMware\VMware Horizon View Client\`.
- Sur des systèmes 64 bits, le chemin est `C:\Program Files (x86)\VMware\VMware Horizon View Client\`.

Pour votre convenance, ajoutez ce chemin à votre variable d'environnement `PATH`.

Le tableau suivant présente les options de ligne de commande que vous pouvez utiliser avec la commande `vmware-view`.

Tableau 3-11. Options de ligne de commande d' Horizon Client

| Option | Description | | | | | | | | |
|---|---|-------------------|---------------------|---------------------|--------------------------|--------------------|--------------|--------------------|--------------|
| <code>/?</code> | Affiche la liste d'options de commande. | | | | | | | | |
| <code>-appName application_name</code> | Spécifie le nom de l'application comme il apparaît dans la fenêtre de sélection des postes de travail et des applications. Il s'agit du nom affiché spécifié pour le pool d'applications dans l'assistant de création de pool. | | | | | | | | |
| <code>-connectUSBOnStartup</code> | Lorsqu'elle est définie sur <code>true</code> , redirige tous les périphériques USB vers le poste de travail qui sont actuellement connectés à l'hôte. Cette option est implicitement définie si vous spécifiez l'option <code>-unattended</code> . L'option par défaut est <code>false</code> . | | | | | | | | |
| <code>-connectUSBOnInsert</code> | Lorsqu'elle est définie sur <code>true</code> , connecte un périphérique USB au poste de travail de premier plan, lorsque vous branchez le périphérique. Cette option est implicitement définie si vous spécifiez l'option <code>-unattended</code> . L'option par défaut est <code>false</code> . | | | | | | | | |
| <code>-desktopLayout window_size</code> | Spécifie l'affichage de la fenêtre pour le poste de travail : <table border="0"> <tr> <td>fullscreen</td><td>Full screen display</td></tr> <tr> <td>multimonitor</td><td>Multiple-monitor display</td></tr> <tr> <td>windowLarge</td><td>Large window</td></tr> <tr> <td>windowSmall</td><td>Small window</td></tr> </table> | fullscreen | Full screen display | multimonitor | Multiple-monitor display | windowLarge | Large window | windowSmall | Small window |
| fullscreen | Full screen display | | | | | | | | |
| multimonitor | Multiple-monitor display | | | | | | | | |
| windowLarge | Large window | | | | | | | | |
| windowSmall | Small window | | | | | | | | |
| <code>-desktopName desktop_name</code> | Spécifie le nom du poste de travail comme il apparaît dans la fenêtre de sélection des postes de travail et des applications. Il s'agit du nom affiché spécifié pour le pool dans l'assistant de création de pool. IMPORTANT Ne spécifiez pas cette option pour les clients en mode kiosque. Cette option n'a aucun effet lorsque le poste de travail s'exécute en mode kiosque. Pour le mode kiosque, la connexion est établie au premier poste de travail dans la liste des postes de travail octroyés. | | | | | | | | |

Tableau 3-11. Options de ligne de commande d' Horizon Client (suite)

| Option | Description |
|--|--|
| <code>-desktopProtocol protocol</code> | Spécifie le protocole du poste de travail à utiliser comme il apparaît dans la fenêtre de sélection des postes de travail et des applications. Le protocole peut être PCOIP ou RDP. |
| <code>-domainName domain_name</code> | Spécifie le domaine NETBIOS que l'utilisateur final utilise pour ouvrir une session d'Horizon Client. Utilisez par exemple <code>monentreprise</code> plutôt que <code>monentreprise.com</code> . |
| <code>-file file_path</code> | Spécifie le chemin d'un fichier de configuration qui contient des options et des arguments de commande supplémentaires. Reportez-vous à la section « Consulter le fichier de configuration Horizon Client », page 58. |
| <code>-h</code> | Affiche les options de l'aide. |
| <code>-hideClientAfterLaunchSession</code> | (Disponible pour Horizon Client 3.1 et version ultérieure) Lorsque cette option est définie sur <code>true</code> , la fenêtre de sélection des applications et des postes de travail distants est masquée après le lancement d'une session distante. |
| <code>-languageId Locale_ID</code> | Assure la localisation de différentes langues dans Horizon Client. Si une bibliothèque de ressources est disponible, spécifiez l'ID de paramètre local (LCID) à utiliser. Pour l'anglais US, saisissez la valeur 0x409. |
| <code>-logInAsCurrentUser</code> | Lorsqu'elle est définie sur <code>true</code> , utilise les informations d'identification que l'utilisateur final fournit lors de l'ouverture de session sur le système client pour ouvrir une session sur l'instance de Serveur de connexion View, puis sur le poste de travail View. L'option par défaut est <code>false</code> . |
| <code>-nonInteractive</code> | Supprime des zones de messages d'erreur lors du démarrage d' Horizon Client à partir d'un script. Cette option est implicitement définie si vous spécifiez l'option <code>-unattended</code> . |
| <code>-noVMwareAddins</code> | Empêche le chargement de canaux virtuels spécifiques de VMware tels que l'impression virtuelle. |
| <code>-password password</code> | Spécifie le mot de passe que l'utilisateur final utilise pour ouvrir une session d'Horizon Client. Vous n'avez pas à spécifier cette option pour des clients en mode kiosque si vous générez le mot de passe automatiquement. |
| <code>-printEnvironmentInfo</code> | Affiche l'adresse IP, l'adresse MAC et le nom de machine du périphérique client. |
| <code>-serverURL connection_server</code> | Spécifie l'URL, l'adresse IP ou le FQDN de l'instance de Serveur de connexion View. |
| <code>-singleAutoConnect</code> | Indique que si l'utilisateur n'est autorisé à accéder qu'à une seule application ou un seul poste de travail, lorsque celui-ci s'authentifie auprès du serveur, l'application ou le poste de travail se connecte automatiquement et l'utilisateur voit sa session s'ouvrir. Ce paramètre évite à l'utilisateur d'avoir à sélectionner l'application ou le poste de travail dans une liste contenant un seul élément. |
| <code>-smartCardPIN PIN</code> | Spécifie le code PIN lorsqu'un utilisateur final insère une carte à puce pour ouvrir une session. |
| <code>-standalone</code> | <p>Pris en charge pour des fins de compatibilité descendante. Il s'agit du comportement par défaut de ce client. Il n'est pas nécessaire de spécifier <code>-standalone</code>. Lance une deuxième instance d'Horizon Client qui peut se connecter au même ou à un autre Serveur de connexion View.</p> <p>Pour plusieurs connexions de postes de travail au même ou à un différent serveur, l'utilisation du tunnel sécurisé est prise en charge.</p> <p>REMARQUE La seconde connexion de poste de travail peut ne pas avoir accès au matériel local, tel que des périphériques USB, des cartes à puce, des imprimantes et plusieurs écrans.</p> |

Tableau 3-11. Options de ligne de commande d' Horizon Client (suite)

| Option | Description |
|----------------------------------|---|
| <code>-unattended</code> | <p>Exécute Horizon Client dans un mode non interactif approprié aux clients en mode Kiosque. Vous devez également spécifier :</p> <ul style="list-style-type: none"> ■ Le nom de compte du client, si vous n'avez pas généré le nom de compte à partir de l'adresse MAC du périphérique client. Le nom doit commencer par la chaîne de caractères « custom- » ou par un autre préfixe que vous avez configuré dans ADAM. ■ Le mot de passe du client, si vous n'avez pas généré un mot de passe automatiquement lorsque vous avez configuré le compte pour le client. <p>L'option <code>-unattended</code> définit implicitement les options <code>-nonInteractive</code>, <code>-connectUSBOnStartup</code>, <code>-connectUSBOnInsert</code> et <code>-desktopLayout multimonitor</code>.</p> |
| <code>-userName user_name</code> | <p>Spécifie le nom de compte que l'utilisateur final utilise pour ouvrir une session d'Horizon Client. Vous n'avez pas à spécifier cette option pour les clients en mode kiosque si vous générez le nom de compte à partir de l'adresse MAC du périphérique client.</p> |

Les options que vous spécifiez sur la ligne de commande ou dans le fichier de configuration sont prioritaires par rapport aux règles système générales que vous avez définies, qui en retour remplacent les règles utilisateur.

Vous pouvez spécifier toutes les options par des stratégies de groupe Active Directory, à l'exception de `-file`, `-languageId`, `-printEnvironmentInfo`, `-smartCardPIN` et `-unattended`.

Consulter le fichier de configuration Horizon Client

Vous pouvez consulter les options de ligne de commande pour Horizon Client dans un fichier de configuration.

Vous pouvez spécifier le chemin du fichier de configuration comme argument de l'option `-filefile_path` de la commande `vmware-view`. Commande `vmware-view`. Le fichier doit être un fichier texte Unicode (UTF-16) ou ASCII.

Exemple : Exemple de fichier de configuration pour une application non interactive

L'exemple suivant montre le contenu d'un fichier de configuration pour une application non interactive.

```
-serverURL https://view.yourcompany.com
-username autouser
-password auto123
-domainName companydomain
-desktopName autodesktop
-nonInteractive
```

Exemple : Exemple de fichier de configuration pour un client en mode kiosque

L'exemple suivant montre un client en mode kiosque dont le nom compte est basé sur son adresse MAC. Le client a un mot de passe généré automatiquement.

```
-serverURL 145.124.24.100
-unattended
```

Utilisation du Registre Windows pour configurer Horizon Client

Vous pouvez définir des paramètres par défaut pour Horizon Client dans le Registre Windows plutôt que de les spécifier sur la ligne de commande. Les entrées de stratégie ont priorité sur les paramètres de Registre Windows et les paramètres de ligne de commande ont priorité sur les entrées de stratégie.

Tableau 3-12 présente les paramètres de registre pour la connexion à Horizon Client. Ces paramètres se trouvent sous HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDM\Client\ dans le registre. Cet emplacement est propre à l'utilisateur, alors que les paramètres HKEY_LOCAL_MACHINE décrits dans le tableau suivant sont définis au niveau de l'ordinateur et sont communs à tous les utilisateurs locaux et de domaine qui, dans un environnement de domaine Windows, ont l'autorisation de se connecter à l'ordinateur.

Tableau 3-12. Paramètres de registre Horizon Client pour les informations d'identification

| Paramètre de registre | Description |
|-----------------------|---|
| Mot de passe | Spécifie le mot de passe par défaut. |
| Nom d'utilisateur | Spécifie le nom d'utilisateur par défaut. |

Tableau 3-13 présente les paramètres de registre pour la connexion à Horizon Client qui n'incluent pas d'informations d'identification de connexion. L'emplacement de ces paramètres dépend du type de système utilisé :

- Pour Windows 32 bits : HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\
- Pour Windows 64 bits : HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\

Tableau 3-13. Paramètres de registre d' Horizon Client

| Paramètre de registre | Description |
|-----------------------|---|
| DomainName | Spécifie le nom de domaine NETBIOS par défaut. Utilisez par exemple <code>monentreprise</code> plutôt que <code>monentreprise.com</code> . |
| EnableShade | Indique si la barre de menus (ombre) en haut de la fenêtre Horizon Client doit être activée. Elle l'est par défaut sauf pour les clients en mode kiosque. La valeur false désactive la barre de menus. REMARQUE Ce paramètre s'applique uniquement lorsque la disposition d'affichage est définie sur Tous les moniteurs ou Plein écran . |
| ServerURL | Spécifie l'instance du Serveur de connexion View par défaut par son URL, son adresse IP ou son FQDN. |
| EnableSoftKeypad | (Horizon Client 3.3 et versions ultérieures) Si cette valeur est définie sur true et qu'une fenêtre Horizon Client est activée, les événements du clavier physique, du clavier à l'écran, de la souris et du pavé d'écriture sont envoyés vers l'application ou le poste de travail distant, même si la souris ou le clavier à l'écran ne figure pas dans la fenêtre Horizon Client. La valeur par défaut est false . |

Le tableau suivant présente les paramètres de sécurité que vous pouvez ajouter. L'emplacement de ces paramètres dépend du type de système utilisé :

- Pour Windows 32 bits : HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security
- Pour Windows 64 bits : HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security

Tableau 3-14. Paramètres de sécurité

| Paramètre de registre | Description et valeurs valides |
|-----------------------|---|
| CertCheckMode | <p>Spécifie le mode de vérification de certificat.</p> <ul style="list-style-type: none"> ■ 0 implémente Do not verify server identity certificates. ■ 1 implémente Warn before connecting to untrusted servers. ■ 2 implémente Never connect to untrusted servers. |
| SSLCipherList | <p>Configure la liste de chiffrements afin de limiter l'utilisation de certains protocoles et algorithmes de chiffrement avant l'établissement d'une connexion SSL chiffrée. La liste de chiffrements est composée d'une ou de plusieurs chaînes de chiffrement séparées par deux points.</p> <p>REMARQUE Toutes les chaînes de chiffrement sont sensibles à la casse.</p> <ul style="list-style-type: none"> ■ Si cette fonction est activée, la valeur par défaut d'Horizon Client 3.5 et versions ultérieures est TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:EC DH+AES:RSA+AES:@STRENGTH. ■ La valeur par défaut d'Horizon Client 3.3 et 3.4 est TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH. ■ La valeur dans Horizon Client 3.2 et versions antérieures est SSLv3:TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH. <p>Cela signifie que dans Horizon Client 3.5 et versions ultérieures, TLS v1.0, TLS v1.1 et TLS v1.2 sont activés. (SSL v2.0 et v3.0 sont désactivés.) Dans Horizon Client 3.3 et 3.4, TLS v1.0 et TLS v1.1 sont activés. (SSL v2.0, SSL v3.0 et TLS v1.2 sont désactivés.) Dans Horizon Client 3.2 et versions antérieures, SSL v3.0 est également activé. (SSL v2.0 et TLS v1.2 sont désactivés.)</p> <p>Les suites de chiffrement utilisent la spécification AES 128 ou 256 bits, suppriment les algorithmes DH anonymes, puis trient la liste de chiffrements actuels par longueur de clé de chiffrement.</p> <p>Lien de référence pour la configuration : http://www.openssl.org/docs/apps/ciphers.html .</p> |

Gestion des connexions aux applications et postes de travail distants

4

Horizon 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 ou d'utiliser des applications distantes. À des fins de dépannage, il vous permet également de réinitialiser les applications et postes de travail distants.

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

Ce chapitre aborde les rubriques suivantes :

- [« Connexion à une application ou un poste de travail distant », page 61](#)
- [« Conseils pour l'utilisation de la fenêtre de sélection des postes de travail et des applications », page 64](#)
- [« Partager l'accès aux dossiers et lecteurs locaux », page 65](#)
- [« Masquer la fenêtre VMware Horizon Client », page 67](#)
- [« Reconnexion à un poste de travail ou à une application », page 67](#)
- [« Créer un raccourci de poste de travail ou d'application sur votre poste de travail client ou menu Démarrer », page 68](#)
- [« Basculer entre des postes de travail ou des applications », page 69](#)
- [« Fermer une session ou se déconnecter », page 70](#)

Connexion à une application ou un poste de travail distant

Après avoir ouvert une session sur un Serveur de connexion View, vous pouvez vous connecter aux applications et aux postes de travail distants que vous êtes autorisé à utiliser.

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

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

Prérequis

- Obtenez les informations d'identification dont vous avez besoin pour ouvrir une session, telles que le nom d'utilisateur et le mot de passe, le nom d'utilisateur et le code secret RSA SecurID, le nom d'utilisateur et le code secret pour l'authentification ou le numéro d'identification personnel (PIN) de carte à puce.

- Obtenez le nom de domaine NETBIOS pour ouvrir une session. Utilisez par exemple `monentreprise` plutôt que `monentreprise.com`.
- Effectuez les tâches administratives décrites dans « [Préparation du Serveur de connexion View pour Horizon Client](#) », page 18.
- Si vous vous trouvez à l'extérieur du réseau d'entreprise et si vous n'utilisez pas de serveur de sécurité pour accéder au poste de travail distant, vérifiez que votre périphérique client est configuré pour utiliser une connexion VPN et activez cette connexion.

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

- Vérifiez que vous disposez du nom de domaine complet (FQDN) du serveur qui fournit l'accès à l'application ou au poste de travail distant. Notez que les traits de soulignement (_) ne sont pas pris en charge dans les noms de serveur. Vous avez également besoin du numéro de port si le port n'est pas 443.
- Si vous prévoyez d'utiliser le protocole d'affichage RDP pour vous connecter à un poste de travail distant, vérifiez que le paramètre de stratégie de groupe AllowDirectRDP de View Agent est activé.
- Si votre administrateur l'a autorisé, vous pouvez configurer le mode de vérification des certificats pour le certificat SSL présenté par Serveur de connexion View. Pour savoir quel mode utiliser, reportez-vous à la section « [Modes de vérification des certificats pour Horizon Client](#) », page 38.

Procédure

- 1 Double-cliquez sur le raccourci de bureau **VMware Horizon Client** ou cliquez sur **Démarrer > Programmes > VMware > VMware Horizon Client**.
- 2 (Facultatif) Pour définir le mode de vérification des certificats, cliquez sur le bouton **Options** situé dans la barre de menus et sélectionnez **Configurer SSL**.
Vous pouvez configurer cette option uniquement si votre administrateur l'a autorisé.
- 3 (Facultatif) Pour vous connecter en tant qu'utilisateur de domaine Windows actuellement connecté, cliquez sur le bouton **Options** dans la barre de menus et sélectionnez **Se connecter en tant qu'utilisateur actuel**.
Cette option est disponible si le module **Se connecter en tant qu'utilisateur actuel** est installé sur votre système client et si votre administrateur a activé le paramétrage global pour cette fonction. Certaines sociétés choisissent de ne pas l'activer.
- 4 Double-cliquez sur le bouton **+ Ajouter un serveur** si aucun serveur n'a encore été ajouté ou cliquez sur le bouton **+ Nouveau serveur** dans la barre de menus, et entrez le nom du Serveur de connexion View ou d'un serveur de sécurité, puis cliquez sur **Connecter**.

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

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

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

- 5 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**.

- 6 Saisissez les informations d'identification d'un utilisateur autorisé à utiliser au moins un pool de postes de travail ou d'applications, sélectionnez le domaine et cliquez sur **Ouvrir une session**.

Si vous saisissez le nom d'utilisateur à l'aide du format **user@domain**, le nom est traité comme un nom d'utilisateur principal (UPN) à cause du signe @, et le menu déroulant du domaine est désactivé.

Pour plus d'informations sur la création de pools de postes de travail et les autorisations utilisateur correspondantes, consultez le document *Configuration de pools de postes de travail et d'applications dans View*.

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

| Option | Description |
|-----------------------------------|---|
| Protocole d'affichage | Si votre administrateur l'a activée, vous pouvez utiliser la liste Connecter Via pour choisir entre les protocoles d'affichage PCoIP et Microsoft RDP. PCoIP fournit une expérience PC optimisée pour délivrer des images, du contenu audio et vidéo sur le réseau local ou sur le réseau WAN. |
| Disposition de l'affichage | Utilisez la liste Affichage pour sélectionner une taille de fenêtre ou pour utiliser plusieurs écrans. |

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

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

- 9 Pour vous connecter à une application ou un poste de travail distant, double-cliquez sur son icône ou cliquez avec le bouton droit de la souris sur l'icône et sélectionnez **Lancer** dans le menu contextuel.

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

Une fois que vous êtes connecté, la fenêtre de l'application ou du poste de travail distant s'ouvre. Si vous êtes autorisé à accéder à plusieurs postes de travail ou applications, la fenêtre de sélection des postes de travail et des applications reste également ouverte de manière que vous puissiez vous connecter à plusieurs éléments en même temps.

Si vous disposez d'Horizon Client 3.4 ou d'une version ultérieure, la boîte de dialogue Partage peut apparaître. Dans la boîte de dialogue Partage, vous pouvez autoriser ou refuser l'accès aux fichiers situés sur votre système local. Pour plus d'informations, reportez-vous à la section « [Partager l'accès aux dossiers et lecteurs locaux](#) », page 65.

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

- Déterminez si le Serveur de connexion View est configuré pour ne pas utiliser SSL. Le logiciel client nécessite des connexions SSL. Vérifiez si le paramètre général dans View Administrator de la case **Use SSL for client connections (Utiliser SSL pour les connexions client)** est désélectionné. Si c'est le cas, vous devez cocher la case pour que SSL soit utilisé ou configurer votre environnement de sorte que les clients puissent se connecter à un équilibreur de charge activé pour HTTPS ou à un autre périphérique intermédiaire configuré pour établir une connexion HTTP vers Serveur de connexion View.

- Vérifiez que le certificat de sécurité pour le Serveur de connexion View fonctionne correctement. Si ce n'est pas le cas, dans View Administrator, vous pouvez également voir que View Agent sur des postes de travail n'est pas accessible. Il s'agit de symptômes de problèmes de connexion supplémentaires causés par des problèmes de certificat.
- Vérifiez que les balises définies sur l'instance de Serveur de connexion View autorisent les connexions depuis cet utilisateur. Reportez-vous au document *Administration de View*.
- Vérifiez que l'utilisateur est autorisé à accéder à ce poste de travail ou à cette application. Reportez-vous au document *Configuration de pools de postes de travail et d'applications dans View*.
- Si vous utilisez le protocole d'affichage RDP pour vous connecter à un poste de travail distant, vérifiez que le système client distant autorise les connexions à des postes de travail distants.

Suivant

Configurez les options de démarrage. Si vous ne voulez pas que les utilisateurs finaux fournissent le nom d'hôte de Serveur de connexion View ou si vous voulez configurer d'autres options de démarrage, utilisez une option de ligne de commande pour créer un raccourci de bureau. Reportez-vous à la section « [Exécution d'Horizon Client depuis la ligne de commande](#) », page 56.

Conseils pour l'utilisation de la fenêtre de sélection des postes de travail et des applications

Pour simplifier votre travail, vous pouvez réorganiser et réduire le nombre d'icônes dans l'écran de sélection des postes de travail et des applications d'Horizon Client.

Une fois que vous vous êtes authentifié et connecté à un serveur particulier, une fenêtre s'affiche incluant des icônes pour toutes les applications et tous les postes de travail distants que vous avez le droit d'utiliser. Essayez les suggestions suivantes pour lancer rapidement vos applications et postes de travail distants les plus fréquemment employés :

- Tapez rapidement les premières lettres du nom. Par exemple, si vous avez des icônes pour Paint, PowerPoint et Publisher, vous pouvez taper rapidement **pa** pour sélectionner l'application Paint.
Si plusieurs éléments correspondent aux lettres tapées, vous pouvez appuyer sur F4 pour accéder au prochain élément correspondant. Lorsque vous atteignez le dernier élément, vous pouvez appuyer sur F4 pour revenir au premier élément correspondant.
- Pour marquer une icône comme favori, cliquez avec le bouton droit sur l'icône et sélectionnez **Marquer comme favori** dans le menu contextuel. Après la sélection de favoris, cliquez sur le bouton **Afficher la vue Favoris** (icône étoile) pour supprimer toutes les icônes qui ne sont pas des favoris.
- Dans la vue Favoris, sélectionnez une icône et faites-la glisser pour changer l'ordre des icônes. Lorsque vous n'êtes pas dans la vue Favoris, par défaut les icônes de postes de travail s'affichent en premier, par ordre alphabétique, suivies des icônes d'applications, également présentées par ordre alphabétique. Mais vous pouvez faire glisser des icônes pour les repositionner dans la vue Favoris.
L'ordre des icônes est enregistré sur le serveur que vous utilisez, lorsque vous vous déconnectez du serveur ou lorsque vous lancez une application ou un poste de travail. Si vous ne vous déconnectez pas manuellement du serveur ou ne lancez pas d'élément, vos modifications ne seront pas enregistrées.
- Créez un raccourci pour accéder à l'application ou au poste de travail distant depuis votre poste de travail local sans devoir utiliser la fenêtre de sélection. Cliquez avec le bouton droit sur l'icône et sélectionnez **Créer un raccourci** dans le menu contextuel.

- Cliquez avec le bouton droit sur l'icône de l'application ou du poste de travail distant et sélectionnez **Ajouter au menu Démarrer** dans le menu contextuel afin que vous puissiez accéder à l'application ou au poste de travail distant à partir de votre menu Démarrer local et ainsi éviter la fenêtre de sélection.

REMARQUE Si vous utilisez un système client Windows 7 ou version ultérieure, après la connexion à un serveur, un poste de travail ou une application, vous pouvez ouvrir Horizon Client et cliquer avec le bouton droit sur l'icône Horizon Client dans la barre des tâches Windows pour sélectionner ce serveur, cette application ou ce poste de travail récemment utilisé. La liste peut comporter jusqu'à 10 éléments. Pour supprimer un élément, cliquez avec le bouton droit sur celui-ci et sélectionnez **Supprimer de cette liste**.

Si vous cliquez avec le bouton droit sur l'icône Horizon Client dans la barre des tâches et ne voyez pas une liste de raccourcis, cliquez avec le bouton droit sur la barre des tâches, sélectionnez **Propriétés**, puis cliquez sur l'onglet **Menu Démarrer**. Dans la section Confidentialité, cochez la case **Stocker et afficher les fichiers récemment ouverts dans le menu Démarrer et la barre des tâches**, puis cliquez sur **OK**.

Partager l'accès aux dossiers et lecteurs locaux

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

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

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

Avec Horizon Client 3.5 et versions ultérieures, vous pouvez également activer la fonction permettant d'ouvrir des fichiers locaux avec des applications distantes directement depuis le système de fichiers local. Lorsque vous cliquez avec le bouton droit sur un fichier local, le menu **Ouvrir avec** répertorie également les applications distantes disponibles. Vous pouvez également définir les fichiers pour qu'ils s'ouvrent automatiquement avec des applications distantes lorsque vous double-cliquez dessus. Lorsque vous activez cette fonction, tous les fichiers sur votre système de fichiers local avec certaines extensions de fichier sont enregistrés avec le serveur View Server sur lequel vous avez ouvert une session. Par exemple, si Microsoft Word est l'une des applications distantes disponibles depuis le serveur View Server, vous pouvez cliquer avec le bouton droit sur un fichier .docx sur votre système de fichiers local et ouvrir le fichier avec l'application MS Word distante. Cette fonction requiert également des serveurs et des agents Horizon 6.2.

Prérequis

Pour partager des dossiers et des lecteurs avec une application ou un poste de travail distant, vous devez disposer d'Horizon Client 3.4 ou version ultérieure, et votre administrateur View doit avoir activé la fonction de redirection de lecteur client pour l'application ou le poste de travail distant.

Pour utiliser la fonction de redirection de lecteur client, vous devez installer View Agent 6.1.1 ou version ultérieure. L'option **Redirection du lecteur client** de View Agent doit être activée. Pour plus d'informations, reportez-vous au document *Configuration de pools de postes de travail et d'applications dans View*.

Procédure

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

| Option | Description |
|--|---|
| Dans la fenêtre de sélection des postes de travail et applications | Cliquez avec le bouton droit sur l'icône d'un poste de travail ou d'une application, sélectionnez Paramètres et sélectionnez Partage dans le volet de gauche de la fenêtre qui s'affiche. |
| Dans la boîte de dialogue Partage qui s'affiche lors de la connexion à un poste de travail ou une application | Cliquez sur le lien Paramètres > Partage de la boîte de dialogue. |
| À partir de l'OS du poste de travail | Sélectionnez Options > Partager les dossiers dans la barre de menus. |

- 2 Configurez les paramètres de la redirection de lecteur client.

| Option | Action |
|---|--|
| Partager un dossier ou un lecteur spécifique avec des applications et des postes de travail distants | <p>Cliquez sur le bouton Ajouter, recherchez et sélectionnez le dossier ou le lecteur à partager, puis cliquez sur OK.</p> <p>REMARQUE Il n'est pas possible de partager un dossier sur un périphérique USB si le périphérique est déjà connecté à une application ou un poste de travail distant à l'aide de la fonction de redirection USB.</p> <p>De plus, n'activez pas la fonction de redirection USB qui connecte automatiquement les périphériques USB au démarrage ou lorsque le périphérique est inséré. Si vous l'activez, la prochaine fois que vous démarrez Horizon Client ou que vous branchez le périphérique USB, le périphérique sera connecté à l'aide de la fonction de redirection USB plutôt qu'à la fonction de redirection de lecteur client.</p> |
| Arrêter le partage d'un dossier ou d'un lecteur spécifique | Sélectionnez le dossier ou le lecteur dans la liste des dossiers et cliquez sur le bouton Supprimer . |
| Autoriser les applications et les postes de travail distants à accéder à des fichiers de votre répertoire d'utilisateurs local | Cochez la case Partager vos fichiers locaux nom-utilisateur . |
| Activer la fonction permettant d'ouvrir un fichier local avec une application distante depuis le système de fichiers local | <p>Cochez la case Ouvrir des fichiers locaux dans des applications hébergées. Avec cette option, vous pouvez cliquer avec le bouton droit sur un fichier dans votre système de fichiers local et choisir d'ouvrir le fichier avec une application distante.</p> <p>Vous pouvez également modifier les propriétés du fichier pour que tous les fichiers avec cette extension soient ouverts avec l'application distante par défaut, comme lorsque vous double-cliquez sur le fichier. Par exemple, vous pouvez cliquer avec le bouton droit sur un fichier, sélectionner Propriétés et cliquer sur Modifier afin de sélectionner l'application distante pour ouvrir les fichiers de ce type.</p> <p>Cette fonction requiert Horizon Client 3.5. Votre administrateur peut désactiver cette fonction.</p> |
| Ne pas afficher la boîte de dialogue Partage lorsque vous vous connectez à une application ou à un poste de travail distant | <p>Cochez la case Ne pas afficher la boîte de dialogue lors de la connexion à un poste de travail ou à une application.</p> <p>Si cette case n'est pas cochée, la boîte de dialogue Partage s'affiche lorsque vous vous connectez pour la première fois à un poste de travail ou à une application après une connexion à un serveur. Par exemple, si vous ouvrez une session sur un serveur avant de vous connecter à un poste de travail, la boîte de dialogue Partage s'affiche. Si vous vous connectez ensuite à une autre application ou un autre poste de travail, cette boîte de dialogue ne s'affiche plus. Pour afficher de nouveau cette boîte de dialogue, vous devez vous déconnecter du serveur puis rouvrir une session.</p> |

Suivant

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

- Depuis un poste de travail Windows distant, ouvrez l'explorateur Windows, cliquez sur **Ordinateur** et consultez la section **Autres**.
- Depuis une application distante, si applicable, sélectionnez **Fichier > Ouvrir** ou **Fichier > Enregistrer sous** et naviguez vers le dossier ou le lecteur qui s'affiche dans le système de fichiers comme lecteur réseau utilisant le format de nom *nom-dossier sur NOM-DE-LA-MACHINE*.

Masquer la fenêtre VMware Horizon Client

Vous pouvez masquer la fenêtre VMware Horizon Client après avoir lancé une application ou un poste de travail distant.

Dans Horizon Client 3.1 ou version ultérieure, vous pouvez masquer la fenêtre VMware Horizon Client après avoir lancé une application ou un poste de travail distant. Vous pouvez également définir une préférence afin de toujours masquer la fenêtre VMware Horizon Client après le lancement d'une application ou d'un poste de travail distant.

REMARQUE Les administrateurs peuvent utiliser un paramètre de stratégie de groupe pour indiquer si la fenêtre doit toujours être masquée après le lancement d'une application ou d'un poste de travail distant.

Pour plus d'informations, reportez-vous à la section « [Paramètres généraux des objets de stratégie de groupe \(GPO\) de clients](#) », page 48.

Procédure

- Pour masquer la fenêtre VMware Horizon Client après avoir lancé une application ou un poste de travail distant, cliquez sur le bouton **Fermer** dans le coin de la fenêtre VMware Horizon Client.
- Pour définir une préférence prévoyant de toujours masquer la fenêtre VMware Horizon Client après le lancement d'une application ou d'un poste de travail distant, avant de vous connecter à un serveur View Server, cliquez sur le bouton **Options** dans la barre de menus et sélectionnez **Masquer le sélecteur après le lancement d'un élément**.
- Pour afficher la fenêtre VMware Horizon Client après qu'elle a été masquée, cliquez avec le bouton droit sur l'icône VMware Horizon Client dans la barre d'état système, puis sélectionnez **Afficher VMware Horizon Client** ou, si vous avez ouvert une session sur un poste de travail distant, cliquez sur le bouton **Options** dans la barre de menus, puis sélectionnez **Passer à un autre ordinateur de bureau**.

Reconnexion à un poste de travail ou à une application

Pour des raisons de sécurité, les administrateurs définissent des délais d'attente qui vous déconnectent d'un serveur après un certain nombre d'heures et qui verrouillent une application distante après un certain nombre de minutes d'inactivité.

Avec la fonctionnalité d'applications distantes de View 6.0, si vous n'avez pas utilisé une application distante pendant un certain temps, vous recevez une invite d'avertissement 30 secondes avant le verrouillage automatique de l'application. Si vous ne répondez pas, l'application est verrouillée. Par défaut, l'expiration du délai d'attente survient après 15 minutes d'inactivité, mais votre administrateur peut modifier cette période.

Par exemple, si vous vous éloignez de votre ordinateur alors qu'une ou plusieurs applications sont ouvertes, leurs fenêtres risquent de ne plus être ouvertes lors de votre retour une heure plus tard. Vous verrez peut-être plutôt une boîte de dialogue vous invitant à cliquer sur le bouton **OK** pour que les fenêtres d'application s'affichent de nouveau.

Le délai d'attente du serveur est généralement configuré à un certain nombre d'heures d'inactivité. Par défaut, si Horizon Client est ouvert et connecté à un serveur particulier pendant plus de 10 heures, vous devrez vous reconnecter. Ce délai d'attente s'applique que vous soyez connecté à une application distante ou à un poste de travail distant.

Pour configurer ces paramètres de délai d'attente dans View Administrator, accédez à **Paramètres globaux** et modifiez les paramètres généraux.

Créer un raccourci de poste de travail ou d'application sur votre poste de travail client ou menu Démarrer

Vous pouvez créer un raccourci pour une application ou un poste de travail distant. Le raccourci s'affiche sur votre poste de travail client, tout comme les raccourcis d'applications localement installées. Vous pouvez également créer un élément de menu Démarrer qui s'affiche dans la liste Programmes.

Procédure

- 1 Démarrez Horizon Client et connectez-vous au serveur.
- 2 Dans la fenêtre de sélection des postes de travail et des applications, cliquez avec le bouton droit sur une application ou un poste de travail, puis sélectionnez **Créer un raccourci** ou **Ajouter au menu Démarrer** dans le menu contextuel qui s'affiche.

Selon la commande que vous avez sélectionnée, un élément de raccourci est créé sur votre poste de travail client ou dans le menu Démarrer de votre système client.

Suivant

Vous pouvez renommer, supprimer ou exécuter toute action sur ce raccourci que vous pouvez effectuer sur les raccourcis des applications localement installées. Lorsque vous utilisez le raccourci, si vous n'êtes pas déjà connecté au serveur, un message vous invite à vous connecter avant que la fenêtre d'application ou de poste de travail distant ne s'ouvre.

Basculer entre des postes de travail ou des applications

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

Procédure

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

| Option | Action |
|---|--|
| Choisir une autre application ou un autre poste de travail sur le même serveur | <p>Effectuez l'une des opérations suivantes :</p> <ul style="list-style-type: none"> ■ Si vous êtes actuellement connecté à un poste de travail distant, sélectionnez Options > Changer de poste de travail dans la barre de menus d'Horizon Client, puis sélectionnez un poste de travail ou une application à lancer. ■ Vous êtes actuellement connecté à une application distante, cliquez avec le bouton droit sur l'icône VMware Horizon Client dans la barre d'état système et sélectionnez Afficher VMware Horizon Client pour afficher la fenêtre de sélection des postes de travail et des applications, puis double-cliquez sur l'icône de l'autre poste de travail ou application. ■ Dans la fenêtre de sélection des postes de travail et applications, double-cliquez sur l'icône de l'autre poste de travail ou application. Ce poste de travail ou cette application s'ouvre dans une nouvelle fenêtre de manière à pouvoir disposer de plusieurs fenêtres ouvertes et à basculer entre elles. |
| Choisir une application ou un poste de travail sur un serveur différent | <p>Effectuez l'une des opérations suivantes :</p> <ul style="list-style-type: none"> ■ Si vous souhaitez maintenir l'application ou le poste de travail actuel ouvert et vous connecter également à une application ou un poste de travail distant sur un autre serveur, démarrez une nouvelle instance d'Horizon Client et connectez-vous à l'autre poste de travail ou application. ■ Si vous souhaitez fermer le poste de travail actuel et vous connecter à un poste de travail sur un autre serveur, accédez à la fenêtre de sélection de postes de travail, cliquez sur l'icône Se déconnecter dans l'angle supérieur gauche de la fenêtre, puis confirmez que vous souhaitez fermer votre session sur ce poste de travail. Vous serez déconnecté du serveur actuel et de toutes les sessions de poste de travail ouvertes. Vous pouvez ensuite vous connecter à un autre serveur. |

Fermer une session ou se déconnecter

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

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

REMARQUE La combinaison de touches Windows Ctrl+Alt+Suppr n'est pas prise en charge sur les postes de travail distants. Pour utiliser l'équivalent de la combinaison de touches Ctrl+Alt+Del, cliquez sur le bouton **Envoyer Ctrl+Alt+Delete** dans la barre de menus.

Dans la plupart des cas, vous pouvez également appuyer sur Ctrl+Alt+Inser. Toutefois, sur les postes de travail Windows 8.1, cette combinaison ne fonctionne pas si vous utilisez le protocole d'affichage Microsoft RDP.

Procédure

- Se déconnecter d'un poste de travail distant sans fermer la session.

| Option | Action |
|---|--|
| Dans la fenêtre du poste de travail distant | <p>Effectuez l'une des opérations suivantes :</p> <ul style="list-style-type: none"> ■ Cliquez sur le bouton Fermer dans le coin de la fenêtre du poste de travail. ■ Sélectionnez Options > Se déconnecter dans la barre de menus de la fenêtre du poste de travail. |
| Depuis la fenêtre de sélection des postes de travail et applications | <p>La fenêtre de sélection des postes de travail et applications est ouverte si vous êtes autorisé à avoir plusieurs postes de travail et applications sur le serveur. Effectuez l'une des opérations suivantes :</p> <ul style="list-style-type: none"> ■ Dans le coin supérieur gauche de la fenêtre de sélection de postes de travail, cliquez sur l'icône Se déconnecter de ce serveur, puis cliquez sur Oui dans la zone d'avertissement. ■ Si vous disposez d'Horizon Client 3.0, vous pouvez cliquer sur le bouton Fermer dans le coin de la fenêtre de sélection de postes de travail, puis cliquer sur Oui dans la zone d'avertissement. <p>Si vous disposez d'Horizon Client 3.1 ou d'une version ultérieure, un clic sur le bouton Fermer ferme uniquement la fenêtre de sélection de postes de travail.</p> |

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

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

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

- Se déconnecter d'une application distante.

| Option | Action |
|--|--|
| Se déconnecter de l'application mais pas du serveur | Quittez l'application de la façon habituelle, par exemple en cliquant sur le bouton Fermer dans le coin de la fenêtre d'application. |
| Se déconnecter de l'application et du serveur | Effectuez l'une des opérations suivantes : <ul style="list-style-type: none"> ■ Dans le coin supérieur gauche de la fenêtre de sélection d'applications, cliquez sur l'icône Se déconnecter de ce serveur, puis cliquez sur Oui dans la zone d'avertissement. ■ Cliquez avec le bouton droit sur l'icône Horizon Client dans la barre d'état système et sélectionnez Quitter. |
| Fermer la fenêtre de sélection d'applications mais laisser l'application en cours d'exécution | Si vous disposez d'Horizon Client 3.1 ou version ultérieure, un clic sur le bouton Fermer ferme uniquement la fenêtre de sélection d'applications. Si vous disposez d'Horizon Client 3.0, la fermeture de cette fenêtre vous déconnecte également de l'application. |

- Fermez la session lorsqu'aucun poste de travail distant n'est ouvert.

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

- Démarrez Horizon Client, connectez-vous au Serveur de connexion View qui fournit l'accès au poste de travail distant et entrez vos informations d'identification d'authentification.
- Cliquez avec le bouton droit sur l'icône du poste de travail et sélectionnez **Fermer la session**.

Travail dans une application ou un poste de travail distant

5

View fournit l'environnement de poste de travail ou d'application familier et personnalisé que tous les utilisateurs finaux attendent. Les utilisateurs finaux peuvent accéder à des périphériques USB et autres connectés à leur ordinateur local, envoyer des documents à une imprimante pouvant être détectée par leur ordinateur local, s'authentifier avec des cartes à puce et utiliser plusieurs écrans.

Ce chapitre aborde les rubriques suivantes :

- [« Matrice de prise en charge des fonctionnalités pour les clients Windows », page 73](#)
- [« Internationalisation », page 76](#)
- [« Activation de la prise en charge des claviers à l'écran », page 78](#)
- [« Utilisation de plusieurs moniteurs », page 78](#)
- [« Connecter des périphériques USB », page 80](#)
- [« Utilisation de la fonctionnalité Audio/Vidéo en temps réel pour webcams et microphones », page 84](#)
- [« Utilisation de scanners », page 87](#)
- [« Utilisation de la redirection de port série », page 88](#)
- [« Copier-coller du texte et des images », page 89](#)
- [« Utilisation des applications distantes », page 90](#)
- [« Impression à partir d'une application ou d'un poste de travail distant », page 90](#)
- [« Contrôler l'affichage d'Adobe Flash », page 92](#)
- [« Utilisation de la fonction de souris relative pour des applications de CAO et 3D », page 93](#)
- [« Raccourcis clavier », page 94](#)

Matrice de prise en charge des fonctionnalités pour les clients Windows

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

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

Tableau 5-1. Fonctionnalités de poste de travail distant prises en charge sur les systèmes Horizon Client sur Windows

| Fonction | Poste de travail Windows XP (View Agent 6.0.2 et versions antérieures) | Poste de travail Windows Vista (View Agent 6.0.2 et versions antérieures) | Poste de travail Windows 7 | Poste de travail Windows 8 .x | Poste de travail Windows 10 | Poste de travail Windows Server 2008/2012 R2 |
|--|---|--|-----------------------------------|--------------------------------------|------------------------------------|---|
| redirection USB | Limité | Limité | X | X | X | X |
| Redirection de lecteur client | | | X | X | X | X |
| Audio/Vidéo en temps réel (RTAV) | Limité | Limité | X | X | X | X |
| Redirection de scanner | | Limité | X | X | X | X |
| Redirection de port série | | | X | X | X | X |
| Protocole d'affichage RDP | Limité | Limité | X | X | X | X |
| Protocole d'affichage PCoIP | Limité | Limité | X | X | X | X |
| Gestion de persona | Limité | Limité | X | X | | |
| Wyse MMR | Limité | Limité | | | | |
| Redirection multimédia (MMR) Windows Media | | | X | X | | |
| Impression basée sur l'emplacement | Limité | Limité | X | X | X | X |
| Impression virtuelle | Limité | Limité | X | X | X | X |
| Cartes à puce | Limité | Limité | X | X | X | X |
| RSA SecurID ou RADIUS | Limité | Limité | X | X | X | X |
| Authentification unique | Limité | Limité | X | X | X | X |
| Plusieurs écrans | Limité | Limité | X | X | X | X |

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

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

Pour plus d'informations sur les éditions de chaque système d'exploitation client et les service packs pris en charge, consultez « [Configuration système requise pour les clients Windows](#) », page 8.

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

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

REMARQUE Le tableau suivant contient des lignes uniquement pour les fonctionnalités prises en charge.

Tableau 5-2. Fonctionnalités prises en charge par les hôtes RDS avec View Agent 6.0.x ou version ultérieure installée

| Fonction | Hôte Windows Server 2008 R2 RDS sur une machine physique | Hôte Windows Server 2008 R2 RDS sur une machine virtuelle | Hôte Windows Server 2012 RDS sur une machine physique | Hôte Windows Server 2012 RDS sur une machine virtuelle |
|--|--|---|---|--|
| RSA SecurID ou RADIUS | X | X | X | X |
| Carte à puce | View Agent 6.1 et versions ultérieures | View Agent 6.1 et versions ultérieures | View Agent 6.1 et versions ultérieures | View Agent 6.1 et versions ultérieures |
| Authentification unique | X | X | X | X |
| Protocole d'affichage RDP (pour les clients de poste de travail) | X | X | X | X |
| Protocole d'affichage PCoIP | X | X | X | X |
| Protocole Blast (pour HTML Access) | | View Agent 6.0.2 et versions ultérieures | | View Agent 6.0.2 et versions ultérieures |
| Redirection multimédia (MMR) Windows Media | View Agent 6.1.1 et versions ultérieures | View Agent 6.1.1 et versions ultérieures | View Agent 6.1.1 et versions ultérieures | View Agent 6.1.1 et versions ultérieures |
| Redirection USB (périphériques de stockage USB uniquement) | | | View Agent 6.1 et versions ultérieures | View Agent 6.1 et versions ultérieures |
| Redirection de lecteur client | View Agent 6.1.1 et versions ultérieures | View Agent 6.1.1 et versions ultérieures | View Agent 6.1.1 et versions ultérieures | View Agent 6.1.1 et versions ultérieures |
| Impression virtuelle (pour clients de poste de travail) | | View Agent 6.0.1 et versions ultérieures | | View Agent 6.0.1 et versions ultérieures |
| Impression basée sur l'emplacement | | View Agent 6.0.1 et versions ultérieures | | View Agent 6.0.1 et versions ultérieures |
| Plusieurs moniteurs (pour clients de poste de travail) | X | X | X | X |
| Unity Touch (pour clients mobiles) | X | X | X | X |

REMARQUE Les fonctions de carte à puce et redirection USB requièrent également Horizon Client 3.3 ou version ultérieure. La fonction Redirection multimédia Windows Media requiert Horizon Client 3.2 ou version ultérieure.

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

Limitations de certaines fonctionnalités

Les restrictions suivantes s'appliquent aux fonctionnalités prises en charge sur les clients Windows.

Tableau 5-3. Configuration requise pour des fonctionnalités spécifiques

| Fonction | Configuration requise |
|--|--|
| Redirection multimédia (MMR) Windows Media | Requiert View Agent 6.0.2 ou version ultérieure et Horizon Client 3.2 ou version ultérieure. Pour utiliser la fonctionnalité MMR Windows Media avec des postes de travail RDS, vous devez posséder View Agent 6.1.1 ou version ultérieure. |
| Redirection de port série | Requiert View Agent 6.1.1 ou version ultérieure et Horizon Client 3.4 ou version ultérieure. Pour Windows 10, requiert Horizon Client 3.5 ou version ultérieure et View Agent 6.2 ou version ultérieure. |
| Impression virtuelle et impression basée sur l'emplacement pour les postes de travail Windows Server 2008 R2, les postes de travail RDS (sur hôtes RDS de machine virtuelle) et les applications distantes | Requiert Horizon Client 3.1 ou version ultérieure et serveurs Horizon 6.0.1 avec View ou version ultérieure. |
| Redirection de scanner | Requiert View Agent 6.0.2 ou version ultérieure et Horizon Client 3.2 ou version ultérieure. Nécessite le protocole d'affichage PCoIP. Pour Windows 10, requiert Horizon Client 3.5 ou version ultérieure et View Agent 6.2 ou version ultérieure. |
| Redirection de lecteur client | Pour les postes de travail de machine virtuelle mono-utilisateur et basés sur des sessions sur les hôtes RDS, requiert Horizon Client 3.5 et versions ultérieures et View Agent 6.1.1 et versions ultérieures. |

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

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

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

Fonctions prises en charge pour les postes de travail Linux

Certains systèmes d'exploitation invités Linux sont pris en charge si vous possédez View Agent 6.1.1 ou version ultérieure et Horizon Client 3.4 pour Windows. Pour voir une liste des systèmes d'exploitation Linux pris en charge et des informations sur les fonctions prises en charge, consultez *Configuration des postes de travail Horizon 6 for Linux*, qui fait partie de la documentation d'Horizon 6, version 6.1.

Internationalisation

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

Utilisation d'un IME (éditeur de méthode d'entrée) local

Lors de l'utilisation de claviers et de paramètres régionaux non anglais, vous pouvez utiliser un IME (éditeur de méthode d'entrée) installé sur votre système local pour envoyer des caractères non anglais à une application hébergée distante.

Vous pouvez aussi utiliser des touches de raccourci et les icônes de la zone de notification (barre d'état système) de votre système local pour changer d'IME. Aucun IME ne doit être installé sur l'hôte RDS distant.

Cette fonction est prise en charge par Horizon Client 3.2 et version ultérieure.

Lorsque cette fonction est activée, l'IME local est utilisé. Si un IME est installé et configuré sur l'hôte RDS sur lequel l'application distante est installée, cet IME distant est ignoré.

Par défaut, la fonctionnalité est désactivée. Chaque fois que vous activez ou désactivez la fonction dans le paramètre, vous devez vous déconnecter du serveur et vous connecter à nouveau pour que le changement puisse prendre effet.

Prérequis

- Vérifiez qu'au moins un IME est installé sur le système client.
- Assurez-vous que la langue d'entrée sur votre système client local correspond à la langue utilisée dans votre IME.

La langue d'entrée sur l'hôte RDS n'est pas applicable.

- Vérifiez que vous utilisez Horizon Client 3.2 ou version ultérieure.
- Vérifiez que View Agent 6.0.2 est installé sur le poste de travail distant.

Procédure

- 1 Dans la fenêtre de sélection de l'application et du poste de travail de Horizon Client, cliquez avec le bouton droit sur une application distante et sélectionnez **Paramètres**.
- 2 Dans le volet des applications distantes qui apparaît, cochez la case **Étendre l'IME local aux applications hébergées** et cliquez sur **OK**.
- 3 Redémarrez la session à l'aide de l'une des méthodes suivantes :

| Option | Description |
|---------------------------------------|--|
| Se déconnecter du serveur | Déconnectez-vous du serveur, puis connectez-vous à nouveau au serveur et à l'application. Vous pouvez reprendre vos applications ; de la même manière que les postes de travail distants, elles ont été déconnectées, mais pas fermées. |
| Réinitialiser les applications | Cliquez avec le bouton droit sur une icône de l'application distante, sélectionnez Paramètres et cliquez sur Réinitialiser . Lorsque vous utilisez cette option, si des postes de travail distants sont ouverts, ils ne sont pas déconnectés. Cependant, toutes les applications distantes sont fermées et doivent être redémarrées. |

Le paramètre prend effet uniquement après le redémarrage de la session. Le paramètre s'applique à toutes les applications hébergées distantes sur le serveur.

- 4 Utilisez l'IME local comme vous le feriez avec des applications installées localement.

La langue et une icône correspondant à l'IME s'affichent dans la zone de notification (barre d'état système) de votre système client local. Vous pouvez utiliser des touches de raccourci pour changer de langue ou d'IME. Les combinaisons de touches qui permettent d'accomplir certaines actions (comme Ctrl+X pour couper le texte et Alt+Flèche droite pour passer d'un onglet à un autre) continueront à fonctionner.

REMARQUE Sur les systèmes Windows 7 et 8.x, vous pouvez spécifier des touches de raccourci pour les IME en utilisant la boîte de dialogue Services de texte et langues d'entrée (disponible en accédant à **Panneau de configuration > Région et langue > onglet Claviers et langues > bouton Modifier les claviers > Services de texte et langues d'entrée > onglet Paramètres de touches avancés**).

Activation de la prise en charge des claviers à l'écran

Vous pouvez configurer votre système client de sorte que si une fenêtre Horizon Client est activée, les événements du clavier physique, du clavier à l'écran, de la souris et du pavé d'écriture soient envoyés vers l'application ou le poste de travail distant, même si la souris ou le clavier à l'écran ne figure pas dans la fenêtre Horizon Client.

Cette fonctionnalité, disponible avec Horizon Client 3.3 et versions ultérieures, est particulièrement utile si vous utilisez une tablette Windows x86 telle que Windows Surface Pro. Pour utiliser cette fonctionnalité, vous devez définir la clé de Registre Windows EnableSoftKeypad sur true. L'emplacement de cette clé dépend du type de système utilisé :

- Pour Windows 32 bits : HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\
- Pour Windows 64 bits : HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\

Utilisation de plusieurs moniteurs

Quel que soit le protocole d'affichage, vous pouvez utiliser plusieurs moniteurs avec un poste de travail distant.

Si vous utilisez le mode d'affichage Tous les moniteurs et que vous cliquez sur le bouton Réduire, lorsque vous agrandissez la fenêtre, celle-ci repasse en mode Tous les moniteurs. De la même façon, si vous utilisez le mode Plein écran et que vous réduisez la fenêtre, lorsque vous agrandissez la fenêtre, celle-ci repasse en mode Plein écran sur un écran.

Dans la fenêtre de sélection des postes de travail et applications d'Horizon Client, vous pouvez cliquer avec le bouton droit sur l'icône d'un poste de travail et sélectionner **Afficher** pour choisir si la fenêtre du poste de travail utilise un ou plusieurs écrans.

Utilisation de tous les écrans pour Horizon Client

Lorsque vous configurez Horizon Client pour qu'il utilise tous les moniteurs, si vous agrandissez la fenêtre d'une application, la fenêtre passe en plein écran sur le seul moniteur qui la contient.

Horizon Client prend en charge les configurations de moniteur suivantes :

- Si vous utilisez 2 moniteurs, il n'est pas nécessaire que les moniteurs soient dans le même mode. Par exemple, si vous utilisez un ordinateur portable connecté à un moniteur externe, le moniteur externe peut être en mode portrait ou en mode paysage.
- Si vous 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 et si la hauteur totale est inférieure à 4 096 pixels.

- Pour utiliser la fonction de rendu 3D, vous devez utiliser le protocole d'affichage PCoIP. Vous pouvez utiliser 2 moniteurs maximum, avec une résolution maximale de 1 920 x 1 200. Pour une résolution de 4K (3 840 x 2 160), un seul moniteur est pris en charge.
- Avec Horizon Client 3.4 ou version antérieure et PCoIP, vous pouvez utiliser jusqu'à 4 moniteurs pour afficher un poste de travail distant, avec une résolution maximale de 2 560 x 1 600 si vous disposez de suffisamment de RAM vidéo.
- Avec Horizon Client 3.5 et PCoIP, la résolution d'écran de poste de travail distant de 4K (3 840 x 2 160) est prise en charge. Le nombre d'écrans 4K pris en charge dépend de la version matérielle de la machine virtuelle de poste de travail et de la version de Windows.

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

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

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

- Si vous disposez de Microsoft RDP 7, vous pouvez utiliser un maximum de 16 moniteurs pour afficher un poste de travail distant.
- Si vous utilisez le protocole d'affichage Microsoft RDP, Connexion Bureau à distance Microsoft (RDC) 6.0 ou version ultérieure doit être installé sur le poste de travail distant.

Utilisation d'un écran dans une configuration à plusieurs écrans

Si vous disposez de plusieurs écrans mais que vous voulez qu'Horizon Client utilise uniquement l'un d'entre eux, après l'installation du client, vous pouvez choisir qu'une fenêtre de poste de travail se lance dans un mode qui n'est pas Tous les moniteurs. Par défaut, la fenêtre est lancée sur l'écran principal.

Avec Horizon Client 3.4 ou version ultérieure, vous pouvez faire glisser la fenêtre du poste de travail vers un écran secondaire et, lors du prochain lancement du poste de travail, la fenêtre du poste de travail sera affichée sur cet écran. Cette préférence de mémorisation du dernier écran utilisé présente les limites suivantes :

- Pour le mode d'affichage, vous devez choisir de lancer la fenêtre dans l'un des modes fenêtrés (Grande, Petite ou Personnalisé) plutôt qu'en mode Plein écran ou Tous les moniteurs.
- Vous devez utiliser le protocole d'affichage PCoIP.
- La fenêtre est lancée et centrée dans le moniteur et utilise la taille de fenêtre que vous avez sélectionnée pour le mode d'affichage, pas une taille que vous pouvez avoir créée en faisant glisser la fenêtre pour la redimensionner.
- Cette préférence n'est pas prise en charge pour les applications distantes (hébergées).

Cette préférence est mémorisée pour chaque poste de travail.

Modifier le mode d'affichage lorsque la fenêtre d'un poste de travail est ouverte

Si vous possédez Horizon Client 3.4 ou version ultérieure, vous pouvez changer de mode d'affichage (passer du mode Tous les moniteurs au mode Plein écran par exemple) sans être obligé de vous déconnecter du poste de travail.

Cette fonction de modification du mode d'affichage alors que la fenêtre du poste de travail est ouverte est prise en charge uniquement pour les fenêtres de poste de travail, pas pour les applications distantes (hébergées).

Prérequis

- Vous devez posséder Horizon Client 3.4 ou version ultérieure. Avec Horizon Client 3.3 et versions antérieures, si vous voulez modifier les modes d'affichage, vous devez vous déconnecter du poste de travail distant puis sélectionner le nouveau mode d'affichage avant de vous reconnecter.
- Vous devez utiliser le protocole d'affichage PCoIP.

Procédure

- 1 Sur le système client, dans la zone de notification (barre d'état système), cliquez avec le bouton droit sur l'icône **Horizon Client** et sélectionnez l'option pour ouvrir la fenêtre Paramètres.

REMARQUE Vous pouvez également ouvrir la fenêtre Paramètres depuis la fenêtre de sélection des applications et des postes de travail.

- 2 Sélectionnez le poste de travail et sélectionnez une option d'affichage.

Connecter des périphériques USB

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

Lorsque vous utilisez cette fonctionnalité, la plupart des périphériques USB connectés au système client local deviennent disponibles dans un menu d'Horizon Client. Vous utilisez le menu pour connecter et déconnecter les périphériques.

REMARQUE Dans Horizon Client 3.3 ou version ultérieure et View Agent 6.1 ou version ultérieure, vous pouvez aussi rediriger des lecteurs USB et des disques durs connectés localement pour les utiliser dans les postes de travail et les applications RDS. Les autres types de périphériques USB, notamment d'autres types de périphériques de stockage tels que les lecteurs de stockage de sécurité et les CD-ROM USB, ne sont pas pris en charge dans les postes de travail et les applications RDS.

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

- Lorsque vous accédez à un périphérique USB à partir d'un menu d'Horizon Client et que vous utilisez le périphérique dans un poste de travail distant, vous ne pouvez pas accéder au périphérique sur l'ordinateur local.
- Les périphériques USB qui ne sont pas affichés dans le menu, mais qui sont disponibles dans un poste de travail distant, incluent des périphériques d'interface humaine, tels que des claviers et des dispositifs de pointage. Le poste de travail distant et l'ordinateur local utilisent ces périphériques en même temps. L'interaction avec ces périphériques peut parfois être lente à cause de la latence du réseau.
- Des lecteurs de disques USB de taille importante peuvent nécessiter plusieurs minutes avant d'apparaître sur le poste de travail.

- Certains périphériques USB requièrent des pilotes spécifiques. Si un pilote requis n'est pas déjà installé sur un poste de travail distant, vous pouvez être invité à l'installer lorsque vous connectez le périphérique USB au poste de travail distant.
- Si vous prévoyez d'ajouter des périphériques USB qui utilisent des pilotes MTP, tels que des smartphones et des tablettes Samsung fonctionnant sous Android, vous devez configurer Horizon Client afin qu'il connecte automatiquement des périphériques USB à votre poste de travail distant. Dans le cas contraire, si vous tentez de rediriger manuellement le périphérique USB à l'aide d'un élément de menu, le périphérique ne sera pas redirigé, sauf si vous le débranchez avant de le brancher de nouveau.
- VMware ne recommande pas la connexion à des scanners à l'aide du menu **Connecter un périphérique USB**. Pour utiliser un scanner physique, utilisez la fonctionnalité de redirection de scanner. Cette fonctionnalité est disponible pour Horizon Client 3.2 ou version ultérieure utilisé avec View Agent 6.0.2 ou version ultérieure. Reportez-vous à la section « [Utilisation de scanners](#) », page 87.
- Les webcams ne sont pas prises en charge pour la redirection USB via le menu **Connecter le périphérique USB**. Pour utiliser une webcam ou un périphérique d'entrée audio, vous devez utiliser la fonctionnalité Audio/Vidéo en temps réel. Cette fonctionnalité est disponible quand elle est utilisée avec View 5.2 Feature Pack 2 ou version ultérieure. Reportez-vous à la section « [Utilisation de la fonctionnalité Audio/Vidéo en temps réel pour webcams et microphones](#) », page 84.
- La redirection de périphériques audio USB dépend de l'état du réseau et n'est pas fiable. Certains périphériques requièrent un débit de données élevé même lorsqu'ils sont inactifs. Si vous disposez de la fonctionnalité Audio/Vidéo en temps réel intégrée à View 5.2 Feature Pack 2 ou version ultérieure, les périphériques d'entrée/sortie audio fonctionneront correctement et vous n'aurez pas besoin d'utiliser la redirection USB pour ces périphériques.

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

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

IMPORTANT Cette procédure explique comment utiliser un élément de menu VMware Horizon Client afin de configurer la connexion automatique de périphériques USB à un poste de travail distant. Vous pouvez également configurer la connexion automatique en utilisant l'interface de ligne de commande Horizon Client ou en créant une stratégie de groupe.

Pour plus d'informations sur l'interface de ligne de commande, consultez « [Exécution d'Horizon Client depuis la ligne de commande](#) », page 56. Pour plus d'informations sur la création de stratégies de groupe, reportez-vous au document *Configuration des pools de postes de travail et d'applications dans View*.

Prérequis

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

Cette tâche inclut l'installation du composant **Redirection USB** de View Agent, et peut inclure la configuration de stratégies de groupe concernant la redirection USB. Pour plus d'informations, consultez le document *Administration de View* si vous utilisez un Serveur de connexion View et Agent 5.3.x. Consultez *Configuration des pools de postes de travail et d'applications dans View* si vous utilisez un Serveur de connexion View et Agent 6.0 ou version ultérieure.

- Lors de l'installation d'Horizon Client, le composant **Redirection USB** doit avoir été installé. Si vous n'avez pas inclus ce composant dans l'installation, désinstallez le client et exécutez de nouveau le programme d'installation pour inclure le composant **Redirection USB**.

Procédure

- Connectez manuellement le périphérique USB à un poste de travail distant.
 - a Connectez le périphérique USB au système client local.
 - b Dans la barre de menus VMware Horizon Client, cliquez sur **Connecter le périphérique USB**.
 - c Sélectionnez un périphérique USB.

Le périphérique est redirigé manuellement du système local vers le poste de travail distant.

- Connectez le périphérique USB à une application hébergée distante.
 - a Dans la fenêtre de sélection des postes de travail et des applications, lancez l'application distante.
Le nom de l'application est celui que votre administrateur a configuré pour l'application.
 - b Dans la fenêtre de sélection des postes de travail et des applications, cliquez avec le bouton droit sur l'icône de l'application et sélectionnez **Paramètres**.
 - c Dans le volet de gauche, sélectionnez **Périphériques USB**.
 - d Dans le volet de droite, sélectionnez le périphérique USB et cliquez sur **Connecter**.
 - e Sélectionnez l'application et cliquez sur **OK**.

REMARQUE Le nom de l'application dans la liste est issu de l'application elle-même et peut ne pas correspondre au nom de l'application configuré par votre administrateur tel qu'il doit apparaître dans la fenêtre de sélection des postes de travail et des applications.

Vous pouvez à présent utiliser le périphérique USB avec l'application distante. À la fermeture de l'application, le périphérique USB n'est pas libéré immédiatement.

- f Après avoir utilisé l'application, pour libérer le périphérique USB afin de pouvoir y accéder à partir de votre système local, dans la fenêtre de sélection des postes de travail et des applications, ouvrez la fenêtre Paramètres, sélectionnez **Périphériques USB**, puis **Déconnecter**.
- Configurez Horizon Client afin de connecter automatiquement des périphériques USB au poste de travail distant lorsque vous les branchez au système local.
Utilisez la fonction de connexion automatique si vous prévoyez de connecter des périphériques qui utilisent des pilotes MTP, tels que les smartphones et tablettes Samsung fonctionnant sous Android.
 - a Avant de brancher le périphérique USB, démarrez Horizon Client et connectez-vous à un poste de travail distant.
 - b Dans la barre de menus VMware Horizon Client, sélectionnez **Connecter le périphérique USB > Connexion automatique de périphériques USB à l'insertion**.
 - c Branchez le périphérique USB.

Les périphériques USB que vous connectez à votre système local après le démarrage d'Horizon Client sont redirigés vers le poste de travail distant.
 - Configurez Horizon Client afin de connecter automatiquement des périphériques USB au poste de travail distant au démarrage d'Horizon Client.
 - a Dans la barre de menus VMware Horizon Client, sélectionnez **Connecter le périphérique USB > Connexion automatique de périphériques USB au démarrage**.
 - b Branchez le périphérique USB et redémarrez Horizon Client.

Les périphériques USB connectés au système local au démarrage d'Horizon Client sont redirigés vers le poste de travail distant.

Le périphérique USB apparaît dans le poste de travail. Cela peut prendre jusqu'à 20 secondes. Lorsque vous connectez le périphérique au poste de travail pour la première fois, il peut vous être demandé d'installer des pilotes.

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

Suivant

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

Configurer les clients pour qu'ils se reconnectent lors du redémarrage de périphériques USB

Si vous ne configurez pas Horizon Client pour qu'il connecte automatiquement les périphériques USB à votre poste de travail View, vous pouvez toujours configurer Horizon Client pour qu'il se reconnecte à des périphériques spécifiques qui redémarrent de façon occasionnelle. Sinon, lorsqu'un périphérique redémarre pendant une mise à niveau, il se connecte au système local plutôt qu'au poste de travail View.

Si vous prévoyez d'ajouter un périphérique USB, tel qu'un smartphone ou une tablette, qui est automatiquement redémarré durant les mises à niveau du système d'exploitation, vous pouvez paramétrer Horizon Client pour qu'il reconnecte automatiquement ce périphérique spécifique au poste de travail View. Pour effectuer cette tâche, modifiez un fichier de configuration sur le client.

Si vous utilisez l'option **Connexion automatique à l'insertion** d'Horizon Client, tous les périphériques que vous branchez sur le système client sont redirigés vers le poste de travail View. Si vous ne souhaitez pas que tous les périphériques soient connectés, suivez la procédure suivante pour configurer Horizon Client, de sorte que seuls certains périphériques USB soient reconnectés automatiquement.

Prérequis

Déterminez le format hexadécimal de l'ID du fournisseur (VID) et l'ID du produit (PID) du périphérique. Pour plus d'instructions, consultez l'article VMware KB sur <http://kb.vmware.com/kb/1011600>.

Procédure

- 1 Utilisez un éditeur de texte pour ouvrir le fichier `config.ini` sur le client.

| Version du SE | Chemin du fichier |
|------------------|---|
| Windows 7 ou 8.x | C:\ProgramData\VMware\VMware USB Arbitration Service\config.ini |
| Windows XP | C:\Documents and Settings\All Users\Application Data\VMware\VMware USB Arbitration Service\config.ini |

- 2 Configurez la propriété `slow-reconnect` pour le ou les périphérique(s) spécifique(s).

```
usb.quirks.device0 = "<varname
id="VARNAME_E03132EDFEFB4D1C84C723B04ED10CBC">vid</varname>:<varname
id="VARNAME_538902E793F746A2902743ACB4A490F1">pid</varname> slow-reconnect"
```

Ici, *vid:pid* représente l'ID du fournisseur et l'ID du produit, au format hexadécimal, pour le périphérique. Par exemple, les lignes suivantes paramètrent cette propriété pour deux périphériques USB :

```
usb.quirks.device0 = "0x0529:0x0001 slow-reconnect"
usb.quirks.device1 = "0x0601:0x0009 slow-reconnect"
```

Spécifiez les propriétés du périphérique `usb.quirks.deviceN` dans l'ordre, en commençant par 0. Par exemple, si la ligne `usb.quirks.device0` est suivie par une ligne avec `usb.quirks.device2` plutôt que `usb.quirks.device1`, seule la première ligne est lue.

Lorsque des périphériques tels que des smart phones et des tablettes subissent une mise à niveau de leur système d'exploitation ou de leur micrologiciel, la mise à niveau réussira, puisque le périphérique va redémarrer puis se connecter au poste de travail View qui le gère.

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

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

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

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

Conditions d'utilisation de votre Webcam

Vous pouvez utiliser sur votre poste de travail une webcam intégrée ou connectée à votre ordinateur local si un administrateur View a configuré la fonctionnalité Audio/vidéo en temps réel et si le protocole d'affichage 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, ne la connectez pas via le menu **Connecter un périphérique USB** d'Horizon Client. L'utilisation de redirection de périphériques USB dégrade les performances des conversations vidéo.

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

Sélectionner une webcam préférée sur un système client Windows

Avec la fonctionnalité Audio-vidéo en temps réel, une seule des webcams de votre système client est utilisée sur votre poste de travail View. Vous pouvez définir une valeur de clé de registre pour spécifier la webcam préférée.

La webcam préférée est utilisée sur le poste de travail distant si elle est disponible. Sinon, une autre webcam est utilisée.

Prérequis

- Assurez-vous qu'une webcam USB est installée et opérationnelle sur votre système client.
- Assurez-vous que vous utilisez le protocole d'affichage PCoIP pour votre poste de travail distant.

Procédure

- 1 Connectez la webcam que vous souhaitez utiliser.
- 2 Démarrez un appel, puis arrêtez l'appel.
Ce processus crée un fichier journal.
- 3 Ouvrez le fichier journal de débogage avec un éditeur de texte.

| Système d'exploitation | Emplacement du fichier journal |
|-------------------------------|--|
| Windows XP | C:\Documents and Settings\username\Local Settings\Application Data\VMware\VDM\Logs\debug-20YY-MM-DD-XXXXXX.txt |
| Windows 7 ou Windows 8 | C:\Users\%username%\AppData\Local\VMware\VDM\Logs\debug-20YY-MM-DD-XXXXXX.txt |

Le format du fichier journal est debug-20AA-MM-JJ-XXXXXX.txt, où 20 AA est l'année, MM le mois, JJ le jour et XXXXXX est un nombre.

- 4 Recherchez [ViewMMDevRedir] VideoInputBase::LogDevEnum dans le fichier journal pour trouver les entrées du fichier journal qui fait référence aux webcams connectées.

Voici un extrait du fichier journal identifiant la webcam Microsoft LifeCam HD-5000 :

```
[ViewMMDevRedir] VideoInputBase::LogDevEnum - 2 Device(s) found
```

```
[ViewMMDevRedir] VideoInputBase::LogDevEnum - Index=0 Name=Integrated Webcam
UserId=vid_1bcf&pid_2b83&mi_00#7&1b2e878b&0&0000 SystemId=\\?\usb#vid_1bcf&pid_2b83&mi_00#
```

```
[ViewMMDevRedir] VideoInputBase::LogDevEnum - Index=1 Name=Microsoft LifeCam HD-5000
UserId=vid_045e&pid_076d&mi_00#8&11811f49&0&0000 SystemId=\\?\usb#vid_045e&pid_076d&mi_00#
```

- 5 Copiez l'identificateur utilisateur de la webcam préférée.
Par exemple, copiez vid_045e&pid_076d&mi_00#8&11811f49&0&0000 pour définir Microsoft LifeCam HD-5000 comme webcam par défaut.
- 6 Lancez l'éditeur du registre (regedit.exe) et accédez à HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\RTAV.
- 7 Collez la partie de l'identificateur de la chaîne de caractères dans la valeur **srcWCamId**.
Par exemple, collez vid_045e&pid_076d&mi_00#8&11811f49&0&0000 dans **srcWCamId**.
- 8 Enregistrez vos modifications et quittez le registre.
- 9 Démarrez un nouvel appel.

Sélectionner un microphone par défaut sur un système client Windows

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

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

IMPORTANT Si vous utilisez un microphone USB, ne le connectez pas via le menu **Connecter un périphérique USB** d'Horizon Client. L'utilisation de redirection de périphériques USB dégrade les performances de la fonctionnalité Audio/Vidéo en temps réel.

Prérequis

- Assurez-vous que vous disposez d'un microphone USB ou un autre type 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 Si vous êtes en cours d'un appel, arrêtez l'appel.
- 2 Cliquez avec le bouton droit sur l'icône haut-parleur dans votre barre d'état système et sélectionnez **Périphériques d'enregistrement**.
Vous pouvez également ouvrir le Contrôle du son à partir de du Panneau de configuration et cliquer sur l'onglet **Enregistrement**.
- 3 Dans l'onglet **Enregistrement** de la boîte de dialogue Son, cliquez avec le bouton droit sur le microphone que vous préférez utiliser.
- 4 Sélectionnez **Définir comme périphérique par défaut** et cliquez sur **OK**.
- 5 Démarrez un nouvel appel à partir de votre poste de travail View.

Utilisation de scanners

Avec Horizon Client 3.2 et versions ultérieures, vous pouvez scanner des informations vers vos postes de travail à distance et applications distantes avec des scanners connectés à votre système client local. Cette fonctionnalité redirige les données d'analyse en utilisant une quantité de bande passante beaucoup plus faible que celle utilisée par la redirection USB.


La redirection de scanner prend en charge les périphériques d'analyse standard qui sont compatibles avec les formats TWAIN et WIA (Windows Image Acquisition). Bien que les pilotes du périphérique d'analyse doivent être installés sur le système client, vous n'avez pas besoin d'installer les pilotes du périphérique d'analyse sur le système d'exploitation du poste de travail distant sur lequel View Agent est installé.

Si un administrateur View a configuré la fonction de redirection de scanner et si vous utilisez le protocole d'affichage PCoIP, un scanner connecté à votre système local peut être utilisé dans une application ou un poste de travail distant.

IMPORTANT Si vous utilisez un scanner, ne le connectez pas via le menu **Connecter un périphérique USB** dans Horizon Client. En effet, cette opération achemine le périphérique via la redirection USB, si bien que les performances seront inutilisables.

Lorsque les données d'analyse sont redirigées vers une application ou un poste de travail distant, vous ne pouvez pas accéder au scanner sur l'ordinateur local. Inversement, lorsqu'un scanner est utilisé sur l'ordinateur local, vous ne pouvez pas y accéder via l'application ou le poste de travail distant.

Conseils pour l'utilisation de la fonctionnalité de redirection de scanner

- Cliquez sur l'icône de scanner () dans la barre d'état système ou la zone de notification du poste de travail distant pour sélectionner un scanner non par défaut ou pour modifier des paramètres de configuration. Sur les applications RDS, l'icône de la barre système est redirigée vers l'ordinateur client local.

Vous n'avez pas à utiliser le menu qui apparaît lorsque vous cliquez sur cette icône. La fonctionnalité de redirection de scanner fonctionne sans autre configuration. Le menu de l'icône vous permet de configurer des options telles que le périphérique à utiliser, lorsque plusieurs périphériques sont connectés à l'ordinateur client.

REMARQUE Si le menu qui apparaît ne répertorie aucun scanner, cela signifie que le scanner connecté à l'ordinateur client est incompatible. Si l'icône de scanner est absente, cela signifie que la fonctionnalité de redirection de scanner est désactivée ou qu'elle n'est pas installée sur le poste de travail distant. En outre, cette icône n'apparaît pas sur les systèmes client Mac ou Linux, car la fonctionnalité n'est pas prise en charge sur ces systèmes.

- Cliquez sur l'option **Préférences** dans le menu pour sélectionner les options de contrôle de la compression d'image, masquer les webcams du menu de redirection de scanner et déterminer comment sélectionner le scanner par défaut.

Vous pouvez sélectionner l'option permettant de masquer les webcams si vous prévoyez d'utiliser la fonctionnalité d'Audio/Vidéo en temps réel pour rediriger les webcams (recommandé par VMware). Utilisez la redirection de scanner avec les webcams pour vous prendre en photo et scanner le cliché.

REMARQUE Si vous configurez la redirection de scanner pour qu'elle utilise un scanner spécifique et que le scanner n'est pas disponible, la redirection de scanner ne fonctionnera pas.

- Bien que la plupart des scanners TWAIN affichent la boîte de dialogue des paramètres du scanner par défaut, ce n'est pas le cas de certains. Pour ceux qui n'affichent pas les options de paramètres, vous pouvez utiliser l'option **Préférences** dans le menu de l'icône du scanner et sélectionner l'option **Toujours afficher la boîte de dialogue des paramètres du scanner**.

- La numérisation d'une image trop grande ou à une résolution trop élevée peut ne pas fonctionner. Dans ce cas, il se peut que l'indicateur de progression de la numérisation soit figé, ou que l'application de scanner se ferme de façon inattendue. Si vous réduisez le poste de travail View, un message d'erreur peut apparaître sur votre système client, vous avertissant que la résolution est trop élevée. Pour résoudre ce problème, réduisez la résolution ou recadrez l'image à une taille inférieure et numérisez-la à nouveau.

Utilisation de la redirection de port série


Avec cette fonction, les utilisateurs peuvent rediriger des ports série (COM) connectés en local, tels que des ports RS232 intégrés ou des adaptateurs USB-série. Les périphériques, comme les imprimantes, les lecteurs de code-barres et autres périphériques série, peuvent être connectés à ces ports et utilisés sur les postes de travail distants.

Si un administrateur View a configuré la fonction de redirection de port série, et si vous utilisez Horizon Client 3.4 ou version ultérieure et le protocole d'affichage PCoIP, la redirection de port série fonctionne sur votre poste de travail distant sans configuration supplémentaire. Par exemple, COM1 sur le système client local est redirigé en tant que COM1 sur le poste de travail distant. COM2 est redirigé en tant que COM2, sauf si le port COM est déjà utilisé. Si c'est le cas, le port COM est mappé pour éviter les conflits. Par exemple, si COM1 et COM2 existent déjà sur le poste de travail distant, COM1 sur le client est mappé vers COM3 par défaut.

Bien que des pilotes de périphérique doivent être installés sur le système client, vous n'avez pas besoin d'installer les pilotes de périphérique sur le système d'exploitation du poste de travail distant sur lequel View Agent est installé. Par exemple, si vous utilisez un adaptateur USB-série qui requiert des pilotes de périphérique spécifiques pour fonctionner sur votre système client local, vous devez installer ces pilotes uniquement sur le système client.

IMPORTANT Si vous utilisez un périphérique qui se branche sur un adaptateur USB-série, ne connectez pas le périphérique depuis le menu **Connecter le périphérique USB** dans Horizon Client. En effet, cette opération achemine le périphérique via la redirection USB, et ignore la fonctionnalité de redirection de port série.

Conseils pour l'utilisation de la fonctionnalité de redirection de port série

- Cliquez sur l'icône de port série () dans la barre d'état système ou la zone de notification du poste de travail distant pour connecter, déconnecter et personnaliser les ports COM mappés.

Lorsque vous cliquez sur l'icône de port série, le menu contextuel **Redirection série COM pour VMware Horizon** s'affiche.

REMARQUE Si les éléments du menu contextuel sont grisés, cela signifie que l'administrateur a verrouillé la configuration. Notez aussi que l'icône s'affiche uniquement si vous utilisez les versions requises de View Agent et d'Horizon Client pour Windows, et vous devez vous connecter sur PCoIP. L'icône ne s'affiche pas si vous vous connectez à un poste de travail distant depuis un Mac, Linux ou un client mobile.

- Dans le menu contextuel, les éléments de port sont répertoriés au format suivant, par exemple : **COM1 mappé vers COM3**. Le premier port, qui est COM1 dans cet exemple, est le port physique ou l'adaptateur USB-série utilisé sur le système client local. Le deuxième port, qui est COM3 dans cet exemple, est le port utilisé dans le poste de travail virtuel.
- Cliquez avec le bouton droit sur un port COM pour sélectionner la commande **Propriétés du port**. Dans la boîte de dialogue Propriétés COM, vous pouvez configurer un port afin qu'il se connecte automatiquement lorsqu'une session de poste de travail distant est démarrée, ou ignorer DSR (c'est-à-dire le signal data-set-ready), ce qui est requis pour certains modems et autres périphériques.

Vous pouvez également modifier le numéro de port utilisé sur le poste de travail distant. Par exemple, si le port COM1 sur le client est mappé vers COM3 sur le poste de travail distant, mais que l'application que vous utilisez requiert COM1, vous pouvez modifier le numéro de port sur COM1. Si COM1 existe déjà sur le poste de travail distant, vous pouvez voir **COM1 (chevauché)**. Vous pouvez toujours utiliser ce port chevauché. Le poste de travail distant peut recevoir des données série via le port depuis l'hôte ESXi et depuis le système client.

- Assurez-vous de vous connecter à un port COM mappé avant d'essayer de lancer une application qui requiert un accès à ce port. Par exemple, cliquez avec le bouton droit sur un port COM et sélectionnez **Connecter** pour utiliser le port sur le poste de travail distant. Lorsque vous lancez l'application, elle ouvre le port série.

Lorsqu'un port COM redirigé est ouvert et utilisé sur un poste de travail distant, vous ne pouvez pas accéder au port sur l'ordinateur local. Inversement, lorsqu'un port COM est utilisé sur l'ordinateur local, vous ne pouvez pas y accéder sur le poste de travail distant.

- Sur le poste de travail distant, vous pouvez utiliser l'onglet **Paramètres du port** du Gestionnaire de périphériques Windows pour définir le débit en bauds par défaut d'un port COM particulier. Veillez à utiliser les mêmes paramètres dans le Gestionnaire de périphériques Windows sur votre système client. Notez que les paramètres de cet onglet sont utilisés uniquement si l'application ne spécifie pas les paramètres du port.
- Avant de pouvoir vous déconnecter du port COM, vous devez fermer le port dans l'application ou fermer l'application. Vous pouvez ensuite sélectionner la commande **Déconnecter** pour vous déconnecter et rendre le port COM physique disponible pour utilisation sur l'ordinateur client.

Copier-coller du texte et des images

Par défaut, vous pouvez copier-coller du texte à partir de votre système client vers une application ou un poste de travail distant. Si votre administrateur active la fonctionnalité, vous pouvez également copier-coller le texte à partir d'une application ou d'un poste de travail distant vers votre système client ou entre deux applications ou postes de travail distants. Certaines restrictions s'appliquent.

Si vous utilisez le protocole d'affichage PCoIP et un poste de travail distant View 5.x ou version ultérieure, votre administrateur View peut définir cette fonctionnalité afin que les opérations de copier-coller soient autorisées uniquement à partir de votre système client vers un poste de travail distant, uniquement à partir d'un poste de travail distant vers votre système client, pour les deux, ou pour aucun des deux. Si vous utilisez une application distante View 6.0 avec View, les mêmes règles s'appliquent.

Les administrateurs configurent la fonctionnalité de copier-coller à l'aide d'objets de stratégie de groupe (GPO) qui appartiennent à View Agent dans des applications ou postes de travail distants. Pour plus d'informations, consultez la rubrique concernant les variables de session générale View PCoIP dont le paramètre appelé **Configurer la redirection du presse-papiers** dans le document *Configuration de pools de postes de travail et d'applications pour View*, dans le chapitre abordant les stratégies de configuration.

Les formats de fichiers supportés comprennent le texte, les images et les fichiers RTF (Rich Text Format). Le presse-papier peut stocker 1 Mo de données pour des opérations de copie-coller. Si vous copiez du texte formaté, certaines de ces données comprennent du texte et certaines comprennent des informations concernant le formatage. Par exemple, il est possible qu'un document de 800 Ko puisse utiliser plus de 1 Mo de données lorsque celui-ci est copié puisque plus de 200 Ko de données RTF peuvent être stockées dans le presse-papier.

Si vous copiez un volume considérable de texte formaté ou du texte et une image, il est possible que certaines sections de ce texte ou son ensemble apparaisse(nt) sans formatage ou image lorsque vous essayez de le ou les coller. La raison en est que les trois types de données sont parfois stockés séparément. Par exemple, les images peuvent être stockées en tant qu'images ou en tant que données RTF, selon le type de document à partir duquel vous copiez les données.

Si le texte et les données RTF prennent moins de 1 Mo réunis, le texte formaté est collé. Il arrive souvent que les données RTF ne peuvent être tronquées. Ainsi, si le texte et le formatage prennent plus de 1 Mo, les données RTF sont ignorées et le texte brut est collé.

Si vous ne pouvez pas coller l'ensemble du texte formaté et les images que vous avez sélectionnées en une seule opération, il se peut que vous deviez copier et coller de plus petits volumes en plusieurs opérations.

Vous ne pouvez pas copier et coller des fichiers entre un poste de travail distant et le système de fichiers sur l'ordinateur client.

Utilisation des applications distantes

Les applications distantes ont l'aspect des applications installées sur votre PC ou ordinateur portable client.

- Vous pouvez réduire et agrandir une application distante via l'application. Lorsqu'une application distante est réduite, elle s'affiche dans la barre des tâches de votre système client. Vous pouvez également réduire et agrandir l'application distante en cliquant sur son icône dans la barre des tâches.
- Vous pouvez quitter une application distante dans l'application ou en cliquant avec le bouton droit sur son icône dans la barre des tâches.
- Vous pouvez appuyer sur Alt+Tab pour basculer entre des applications distantes ouvertes.
- Dans Horizon Client 3.1 et version ultérieure, si une application distante crée un élément de barre d'état système Windows, cet élément s'affiche également dans la barre d'état système sur votre ordinateur client Windows. Par défaut, les icônes de la barre d'état système sont uniquement visibles pour afficher des notifications, mais vous pouvez personnaliser ce comportement comme pour des applications installées en mode natif.

REMARQUE Si vous ouvrez le Panneau de configuration pour personnaliser les icônes de la zone de notification, les noms des icônes des applications distantes sont répertoriés sous la forme VMware Horizon Client - *application name*.

Enregistrement de documents dans une application distante

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

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

Impression à partir d'une application ou d'un poste de travail distant

À partir d'un poste de travail distant, vous pouvez imprimer vers une imprimante virtuelle ou vers une imprimante USB connectée à votre ordinateur client. L'impression virtuelle et l'impression USB fonctionnent en même temps sans problème.

Pour utiliser la fonction d'impression virtuelle avec les types d'applications et postes de travail distants suivants, Horizon Client 3.1 ou version ultérieure doit être installée :

- Postes de travail distants exécutant un système d'exploitation Windows Server
- Postes de travail basés sur des sessions (sur les hôtes RDS de machine virtuelle)
- Applications hébergées distantes

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

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

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

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

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

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

- La fonction Windows pour imprimer vers un fichier.

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

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

Prérequis

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

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, reportez-vous au document *Administration de View* si vous utilisez un Serveur de connexion View et View Agent 5.x ou version antérieure. Reportez-vous à *Configuration des pools de postes de travail et d'applications dans View* si vous utilisez Serveur de connexion View et View Agent 6.0 ou version ultérieure.

Procédure

- 1 Dans le poste de travail distant Windows 7 ou Windows 8.x, cliquez sur **Démarrer > Périphériques et imprimantes**.
- 2 Dans la fenêtre Périphériques et imprimantes, cliquez avec le bouton droit sur l'imprimante par défaut, sélectionnez **Propriétés de l'imprimante** dans le menu contextuel et choisissez l'imprimante.

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

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

- 5 Dans la boîte de dialogue Options d'impression, sélectionnez les différents onglets et précisez les paramètres à utiliser.
Pour les paramètres avancés **Mise en page**, VMware recommande de conserver ceux par défaut.
- 6 Cliquez sur **OK**.
- 7 Pour utiliser des formulaires papier personnalisés, définissez les formulaires sur le client.
 - a Accédez à **Panneau de configuration > Matériel et audio > Périphériques et imprimantes**.
 - b Sélectionnez l'imprimante, puis cliquez sur **Propriétés du serveur d'impression** en haut de l'écran.
 - c Dans l'onglet **Formulaires**, spécifiez les paramètres, puis cliquez sur **Enregistrer le formulaire**.
 Ce formulaire est désormais disponible dans votre poste de travail distant.

Utilisation d'imprimantes USB

Dans un environnement View, les imprimantes virtuelles et celles qui utilisent la fonction de redirection USB peuvent fonctionner ensemble sans conflit.

Une imprimante USB est une imprimante qui est connectée à un port USB du système client local. Pour envoyer des travaux d'impression vers une imprimante USB, vous pouvez utiliser la fonction de redirection USB ou d'impression virtuelle. L'impression USB peut parfois être plus rapide que l'impression virtuelle selon les conditions du réseau.

- Vous pouvez utiliser la redirection USB pour connecter une imprimante USB à un port USB virtuel d'un poste de travail distant tant que les pilotes nécessaires sont installés sur ce dernier.

Si vous utilisez cette fonction de redirection, l'imprimante n'est plus logiquement connectée au port USB physique du client. L'imprimante USB n'apparaît pas dans la liste des imprimantes locales de la machine cliente locale. Cela signifie également que vous pouvez imprimer sur l'imprimante USB à partir du poste de travail distant, mais pas à partir de la machine client locale.

Dans le poste de travail distant, les imprimantes USB redirigées apparaissent sous la forme `<printer_name>`.

Pour plus d'informations sur la connexion d'imprimante USB, reportez-vous à « [Connecter des périphériques USB](#) », page 80.

- Sur certains clients, vous pouvez également utiliser la fonction d'impression virtuelle pour envoyer des travaux d'impression vers une imprimante USB. Si vous utilisez la fonction d'impression virtuelle, vous pouvez imprimer sur une imprimante USB à partir du poste de travail distant et du client local, et vous n'avez pas besoin d'installer des pilotes d'impression sur le poste de travail distant.

Contrôler l'affichage d'Adobe Flash

L'administrateur View peut configurer le niveau d'affichage du contenu Adobe Flash sur votre poste de travail View de manière à économiser les ressources informatiques. Dans certains cas, ces paramètres peuvent entraîner une faible qualité de lecture. En déplaçant le pointeur de la souris dans le contenu Adobe Flash, vous pouvez remplacer les paramètres Adobe Flash spécifiés par votre administrateur View.

Le contrôle d'affichage Adobe Flash est disponible pour les sessions Internet Explorer sur Windows uniquement, et pour les versions 9 et 10 d'Adobe Flash uniquement. Pour contrôler la qualité d'affichage d'Adobe Flash, vous ne devez pas exécuter ce dernier en mode plein écran.

Procédure

- 1 À partir d'Internet Explorer sur le poste de travail View, accédez au contenu Adobe Flash pertinent et lancez-le si nécessaire.

Selon la façon dont votre administrateur View a configuré les paramètres Adobe Flash, vous remarquerez peut-être que des trames sont supprimées ou que la qualité de lecture est médiocre.

- 2 Déplacez le pointeur de la souris dans le contenu Adobe Flash pendant sa lecture.

La qualité d'affichage est améliorée tant que le curseur reste dans le contenu Adobe Flash.

- 3 Pour conserver l'amélioration de la qualité, double-cliquez dans le contenu Adobe Flash.

Utilisation de la fonction de souris relative pour des applications de CAO et 3D

Si vous utilisez le protocole d'affichage PCoIP avec des applications de CAO ou 3D dans un poste de travail View 5.2 ou version ultérieure, les performances de la souris s'améliorent lorsque vous activez la fonction de souris relative.

Dans la plupart des cas, si vous utilisez des applications ne nécessitant pas le rendu 3D, Horizon Client transmet des informations sur les mouvements du pointeur de la souris à l'aide des coordonnées absolues. À l'aide des coordonnées absolues, le client convertit les mouvements de la souris localement, ce qui améliore les performances, en particulier si vous vous trouvez à l'extérieur du réseau d'entreprise.

Pour les tâches nécessitant l'utilisation d'applications gourmandes en ressources graphiques, telles qu'AutoCAD, ou pour jouer à des jeux vidéo 3D, vous pouvez améliorer les performances de la souris en activant la fonction de souris relative, qui utilise les coordonnées relatives plutôt que les coordonnées absolues. Pour utiliser cette fonctionnalité, sélectionnez **Options > Activer la souris relative** dans la barre de menus d'Horizon Client.

REMARQUE Si vous utilisez Horizon Client en mode fenêtré, plutôt qu'en mode Plein écran, et que la fonctionnalité de souris relative est activée, il est possible que vous ne puissiez pas déplacer le pointeur de la souris dans les options de menu Horizon Client ou déplacer le pointeur en dehors de la fenêtre Horizon Client. Pour résoudre cette situation, appuyez sur Ctrl+Alt.

Lorsque la fonction de souris relative est activée, les performances peuvent être lentes si vous vous trouvez à l'extérieur du réseau d'entreprise, sur un WAN.

IMPORTANT Cette fonction requiert un poste de travail View 5.2 ou version ultérieure et vous devez activer le rendu 3D pour le pool de postes de travail. Pour plus d'informations sur les paramètres de pool et les options disponibles pour le rendu 3D, reportez-vous au document *Administration de View* si vous utilisez un Serveur de connexion View et View Agent 5.x ou une version antérieure. Reportez-vous à *Configuration des pools de postes de travail et d'applications dans View* si vous utilisez un Serveur de connexion View et View Agent 6.0 ou version ultérieure.

Raccourcis clavier

Avec Horizon Client 3.1 et version ultérieure, vous pouvez utiliser des raccourcis clavier pour des commandes de menu et des actions courantes.

Raccourcis qui fonctionnent dans Horizon Client de la même manière que dans toutes les applications

Tableau 5-4. Raccourcis clavier courants

| Action | Touche ou combinaison de touches |
|--|--|
| Cliquez sur le bouton mis en surbrillance dans une boîte de dialogue. | Appuyez sur Entrée. |
| Appelez le menu contextuel. | Appuyez sur Maj+F10. |
| Cliquez sur le bouton Annuler dans une boîte de dialogue. | Appuyez sur Échap. |
| Naviguez entre les éléments de la fenêtre de la sélection de serveurs, ou dans la fenêtre de sélection de postes de travail et d'applications. | Utilisez une touche fléchée pour vous déplacer dans la direction de la flèche. Appuyez sur Tabulation pour vous déplacer vers la droite. Appuyez sur Maj+Tabulation pour vous déplacer vers la gauche. |
| Supprimez un élément de la fenêtre de sélection de serveurs, ou de la fenêtre de sélection de postes de travail et d'applications. | Appuyez sur Supprimer. |
| Dans Windows 8.x, naviguez entre l'écran d'accueil et l'écran du bureau | Appuyez sur la touche Windows. |

Raccourcis de la fenêtre d' Horizon Client (liste de sélection de serveurs)

Tableau 5-5. Combinaisons de touches spécifiques de la fenêtre dans laquelle vous spécifiez à quel serveur vous souhaitez vous connecter

| Commande de menu ou action | Combinaison de touches |
|--|------------------------|
| Ouvrir le système d'aide dans une fenêtre de navigateur | Alt+O+A, Ctrl+A |
| Commande Nouveau serveur | Alt+N |
| Afficher la fenêtre Informations de support | Alt+O+I |
| Afficher la fenêtre À propos d'Horizon Client | Alt+O+V |
| Commande Configurer SSL | Alt+O+O |
| Commande Masquer le sélecteur après le lancement d'un élément | Alt+O+M |

Raccourcis du sélecteur d'applications et de postes de travail distants

Tableau 5-6. Touches et combinaisons de touches à utiliser dans la fenêtre de sélection de postes de travail et d'applications

| Commande de menu ou action | Combinaison de touches |
|---|------------------------|
| Ouvrir le système d'aide dans une fenêtre de navigateur | Alt+O+A, Ctrl+A |
| Afficher le menu Options | Alt+O |
| Afficher la fenêtre Informations de support | Alt+O+I |
| Afficher la fenêtre À propos d'Horizon Client | Alt+O+V |
| Se déconnecter du poste de travail distant | Maj+F10+S |

Tableau 5-6. Touches et combinaisons de touches à utiliser dans la fenêtre de sélection de postes de travail et d'applications (suite)

| Commande de menu ou action | Combinaison de touches |
|---|------------------------|
| Se déconnecter et fermer la session du serveur | Alt+D |
| Basculer entre Afficher les favoris et Tout afficher | Alt+F |
| Pendant l'affichage des favoris, après la saisie des premiers caractères du nom de l'application ou du poste de travail, accéder à l'élément suivant correspondant à la recherche | F4 |
| Pendant l'affichage des favoris, accéder à l'élément précédent correspondant à la recherche | Maj+F4 |
| Marquer comme favori ou supprimer une désignation de favori | Maj+F10+F |
| Afficher le menu Paramètres | Alt+S, ou Maj+F10+P |
| Lancer l'élément sélectionné | Entrée ou Maj+F10+L |
| Épingler un raccourci pour l'application ou le poste de travail distant dans le menu Démarrer du système client (pour Windows 7 et version antérieure) ou dans l'écran d'accueil (pour Windows 8.x) | Maj+F10+J |
| Afficher le menu contextuel Paramètres d'affichage pour le poste de travail distant sélectionné | Maj+F10+A |
| Utiliser le protocole d'affichage PCoIP pour se connecter au poste de travail distant sélectionné | Maj+F10+O |
| Utiliser le protocole d'affichage RDP pour se connecter au poste de travail distant sélectionné | Maj+F10+M |
| Créer un raccourci de poste de travail pour l'élément sélectionné | Maj+F10+C |
| Ajouter l'élément sélectionné à votre menu Démarrer ou votre écran d'accueil | Maj+F10+J |
| Réinitialiser le poste de travail sélectionné (si votre administrateur vous permet de réinitialiser) | Maj+F10+R |
| Actualiser la liste de postes de travail et d'applications | F5 |

Raccourcis de la fenêtre Bureau (avec une session PCoIP)

Ces raccourcis fonctionnent si vous appuyez d'abord sur Ctrl+Alt ou cliquez sur la barre de menu d'Horizon Client, plutôt qu'à l'intérieur du système d'exploitation du poste de travail distant, avant d'appuyer sur les touches.

Tableau 5-7. Combinaisons de touches pour les sessions PCoIP

| Commande de menu ou action | Combinaison de touches |
|--|------------------------|
| Relâcher le curseur de la souris afin qu'il ne soit plus à l'intérieur du système d'exploitation du poste de travail distant | Ctrl+Alt |
| Afficher le menu Options | Alt+O |
| Afficher la fenêtre Informations de support | Alt+O+I |
| Afficher la fenêtre À propos d'Horizon Client | Alt+O+V |
| Commande Passer à un autre ordinateur de bureau | Alt+O+P |
| Commande Connexion auto à cet ordinateur de bureau | Alt+O+N |
| Commande Activer la souris relative | Alt+O+T |

Tableau 5-7. Combinaisons de touches pour les sessions PCoIP (suite)

| Commande de menu ou action | Combinaison de touches |
|--|-------------------------------|
| Commande Envoyer Ctrl+Alt+Suppr | Alt+O+C |
| Commande Déconnecter | Alt+O+D |
| Commande Déconnecter et fermer la session | Alt+O+F |
| Commande Connecter un périphérique USB | Alt+U |

Résolution des problèmes d'Horizon Client

6

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

Ce chapitre aborde les rubriques suivantes :

- [« Que faire si Horizon Client se ferme de façon inattendue », page 97](#)
- [« Réinitialiser une application ou un poste de travail distant », page 97](#)
- [« Désinstallation d'Horizon Client », page 98](#)

Que faire si Horizon Client se ferme de façon inattendue

Il arrive que Horizon Client se ferme sans que vous l'ayez demandé.

Problème

Il arrive que Horizon Client se ferme de façon inattendue. En fonction de la configuration de votre View Connection Server, il est possible qu'un message tel que `Aucune connexion sécurisée vers le View Connection Server` s'affiche. Dans certains cas, aucun message ne s'affiche.

Cause

Ce problème survient lorsque la connexion au View Connection Server est perdue.

Solution

- ◆ Redémarrez Horizon Client. Vous devriez pouvoir vous connecter dès la prochaine exécution du View Connection Server. Si les problèmes de connexion persistent, contactez votre administrateur View.

Réinitialiser une application ou un poste de travail distant

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

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

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

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

Procédure

- 1 Pour réinitialiser un poste de travail distant, utilisez la commande **Réinitialiser le poste de travail**.

| Option | Action |
|---|---|
| À partir de l'OS du poste de travail | Sélectionnez Options > Réinitialiser le poste de travail dans la barre de menu. |
| Dans la fenêtre de sélection des postes de travail et applications | Cliquez avec le bouton droit sur l'icône du poste de travail et sélectionnez Réinitialiser le poste de travail . |

- 2 Pour réinitialiser vos applications, utilisez le bouton **Réinitialiser** dans la fenêtre de sélection des postes de travail et applications.
 - a Cliquez sur le bouton **Paramètres** (icône engrenage) dans la barre de menus.
 - b Sélectionnez **Applications** dans le volet de gauche, cliquez sur le bouton **Réinitialiser** dans le volet de droite, puis cliquez sur **OK**.

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

Suivant

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

Désinstallation d' Horizon Client

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

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

Par exemple, utilisez l'applet **Ajouter ou supprimer des programmes**, disponible dans votre système d'exploitation Windows pour supprimer l'application VMware Horizon Client.

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

Reportez-vous à la section [Chapitre 2, « Installation d'Horizon Client pour Windows »](#), page 21.

Index

A

Adobe Media Server **15**
applications 3D **93**
applications de CAO **93**
applications distantes **90**
Audio/Vidéo en temps réel, configuration système **10**
authentification par carte à puce, configuration **17**

B

basculer entre postes de travail **69**

C

certificats, ignorer des problèmes **37, 38**
certificats SSL, vérification **37**
claviers, à l'écran **78**
claviers à l'écran **78**
collage texte et images **89**
commande de menu Envoyer Ctrl+Alt+Del **70**
commande vmware-view
 fichier de configuration **58**
 syntaxe **56**
communications unifiées **15**
conditions préalables pour les périphériques client **18**
configuration matérielle requise
 authentification par carte à puce **17**
 pour systèmes Windows **8**
configuration système, pour Windows **8**
connexion automatique de périphériques USB **80**
connexions de serveur **61**
contrôle, affichage vidéo Adobe Flash **92**
copie texte et images **89**
Ctrl+Alt+Delete **70**

D

déconnexion d'un poste de travail distant **70**
délais d'attente **67**
désinstallation d'Horizon Client **98**
diffusion multimédia **12**
diffusion multimédia (MMR) **12**
disposition écran **61**
domain **61**

E

enregistrement de documents dans une application distante **90**
exemples d'URI **35**
exigences logicielles client **7**

F

favoris **64**
fenêtre de sélection des postes de travail et des applications **64**
fermer une session **70**
fichier vdm_client.adm de définition des objets de stratégie de groupe **40**
Fichiers de modèle d'administration (ADM), Composants View **40**
fonction d'impression virtuelle **73, 91**
formats de fichier média, pris en charge **12**

H

Horizon Client
 configuration **31**
 dépannage **97**
 fichier de configuration **58**
 s'exécutant à partir de la ligne de commande **56**
 se déconnecter d'un poste de travail **70**
 se ferme de façon inattendue **97**

I

icônes dans la fenêtre de sélection des postes de travail et des applications **64**
images, copie **89**
IME (éditeur de méthode d'entrée) **77**
imprimantes, configuration **91**
Imprimantes USB **90, 92**
imprimantes virtuelles **90**
imprimer à partir d'un poste de travail **90**
installation silencieuse, View Client **24**

M

masquer la fenêtre Horizon Client **67**
matrice de prise en charge des fonctions **73**
microphone **86**
Microsoft RDP **73, 78**

Microsoft Windows Installer
 options de ligne de commande pour
 l'installation silencieuse **27**
 propriétés pour View Client **25**
 mode d'affichage des écrans **80**
 mode FIPS **23**
 modes de vérification des certificats **37**

O

objets de stratégie de groupe côté client **40**
 options
 disposition écran **61**
 protocole d'affichage **61**
 options d'affichage, poste de travail **61**
 options SSL **39**
 ordinateurs Windows, installation de View
 Client **21**
 ouvrir session, Serveur de connexion View **61**

P

paramètres de GPO, général **48**
 paramètres de sécurité des objets de stratégie
 de groupe (GPO) **42**
 paramètres de ThinPrint **91**
 paramètres RPD, GPO **46**
 paramètres USB, GPO **50**
 partage de dossiers **65**
 partage de fichiers et de dossiers du système
 client **65**
 PCoIP **73**
 périphériques, connexion USB **80, 83**
 périphériques USB
 définition des stratégies de groupe pour **40**
 utilisation avec des postes de travail View **73**
 plusieurs moniteurs **78**
 ports COM, redirection série **11, 88**
 poste de travail
 basculer **69**
 fermer une session sur **70**
 options d'affichage **61**
 protocole d'affichage **61**
 réinitialiser **97**
 se connecter à **61**
 préférences, poste de travail **61**
 prise en charge de Microsoft Lync **15**
 prise en charge du client léger **73**
 profils virtuels **73**
 programme d'amélioration du produit, données
 de pool de postes de travail **19**
 programme d'installation client **21**
 protocole d'affichage, poste de travail **61**
 protocoles d'affichage
 Microsoft RDP **73**
 View PCoIP **73**

R

raccourcis, pour des applications et des postes
 de travail distants **68**
 raccourcis clavier **94**
 Redirection d'URL Flash, configuration
 système **15**
 redirection de lecteur client **65**
 redirection de port série **11, 88**
 redirection de scanner **10, 87**
 registre
 paramètres équivalant à des commandes de
 ligne de commande **59**
 paramètres pour View Client **59**
 réinitialiser le poste de travail **97**

S

scanners TWAIN **10, 87**
 scanners WIA **10, 87**
 se connecter
 à un poste de travail **61**
 au Serveur de connexion View **61**
 périphériques USB **80, 83**
 Serveur de connexion View, se connecter à **61**
 serveurs de sécurité **18**
 souris relative **93**
 stratégies de groupe **40**
 Syntaxe d'URI pour Horizon Clients **32**
 systèmes d'exploitation, pris en charge sur View
 Agent **18**

T

texte, copie **89**
 touches de raccourcis **94**

U

URI (Identifiants uniformes de ressource) **32**

V

variables de session de client PCoIP **52**
 vérification des certificats de serveur **37**
 vidéo Adobe Flash, contrôle **92**
 View Agent, exigences d'installation **18**
 View Client
 configuration système requise pour
 Windows **8**
 installation en silence sur un PC ou un
 ordinateur portable Windows **24**
 installation sur un PC ou un ordinateur
 portable Windows **21**
 paramètres de registre **59**
 propriétés de l'installation silencieuse **25**
 syntaxe de commande **56**
 VoIP (voice over IP) **15**

W

webcam **84, 85**

Windows, installation de View Client sur **8**

Wyse MMR **73**

