Utilisation de VMware Horizon Client pour Windows

VMware Horizon Client for Windows 4.5

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-002510-00

vmware®

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

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

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

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

docfeedback@vmware.com

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

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

Table des matières

Utilisation de VMware Horizon Client pour 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'Horizon 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. Assurez-vous que vos paramètres Internet Explorer sont exacts et que vous pouvez accéder à l'URL du Serveur de connexion via Internet Explorer.

Ce chapitre aborde les rubriques suivantes :

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

Tous les périphériques Windows x86-64 ou x86

Mémoire

Au moins 1 Go de RAM

Systèmes d'exploitation

Les systèmes d'exploitation suivants sont pris en charge :

OS	Version	Service Pack ou option de service	Éditions prises en charge
Windows 10	32 ou 64 bits	Current Branch (CB) version 1703 (Creators Update) Current Branch (CB) version 1607 (Anniversary Update) Current Branch for Business (CBB) version 1607 (Anniversary Update) Long-Term Servicing Branch (LTSB) version 1607 (Anniversary Update)	Home, Pro, Enterprise et IoT Core
Windows 8 ou 8.1	32 ou 64 bits	Aucun ou Update 2	Pro , Enterprise et Industry Embedded
Windows 7	32 ou 64 bits	SP1	Home, Enterprise, Professional et Ultimate
Windows Server 2008 R2	64 bits	Dernière mise à jour	Standard
Windows Server 2012 R2	64 bits	Dernière mise à jour	Standard

Windows Server 2008 R2 et Windows Server 2012 R2 sont pris en charge pour exécuter Horizon Client en mode imbriqué. Pour plus d'informations, reportez-vous à la section « Fonctionnalités prises en charge en mode imbriqué », page 91.

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

Dernière version de maintenance de View 6.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 Unified Access Gateway pour que les systèmes clients ne nécessitent pas de connexion VPN.

Remarque Les clients peuvent également se connecter au dispositif Unified Access Gateway, qui est disponible avec Horizon 6 version 6.2 et versions ultérieures.

Protocoles d'affichage

VMware Blast, PCoIP et RDP

Exigences matérielles pour PCoIP et VMware Blast

- 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 :

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

  Comme indicateur rapide, vous pouvez utiliser les calculs suivants :

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

Exigences matérielles pour RDP

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

Exigences logicielles pour RDP

- Pour Windows 7, utilisez RDP 7.1 ou 8.0. Windows 7 comprend RDP 7. 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 l'agent configure la règle de pare-feu locale pour les connexions RDP entrantes afin qu'elle corresponde au port RDP actuel du système d'exploitation hôte, qui est en général le port 3389. Si vous modifiez le numéro du port RDP, vous devez modifier les règles de pare-feu associées.

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

Configuration requise pour les graphiques et la vidéo

- Carte graphique prenant en charge Direct3D 11 Video.
- Pilotes vidéo et de cartes graphiques les plus récents.
- Pour Windows 7 SP1, installez la mise à jour de plate-forme pour Windows 7 SP1 et Windows Server 2008 R2 SP1. Pour plus d'informations, accédez à https://support.microsoft.com/fr-fr/kb/2670838.

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, votre déploiement d'Horizon doit satisfaire certaines exigences matérielles et logicielles.

Postes de travail distants

View Agent 5.2 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure, doit être installé sur les postes de travail. S'agissant des postes de travail View Agent 5.2, la version correspondante de Remote Experience Agent doit également être installée sur les postes de travail. Par exemple, si View Agent 5.2 est installé, vous devez également installer Remote Experience Agent à partir de View 5.2 Feature Pack 2. Consultez le document *Installation et administration de View Feature Pack*. Si vous disposez de View Agent 6.0 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure, aucun Feature Pack n'est requis. Pour utiliser la fonctionnalité Audio/Vidéo en temps réel avec des applications et des postes de travail publiés, vous devez disposer d'Horizon Agent 7.0.2 ou version ultérieure.

Ordinateur Horizon Client ou périphérique d'accès client

- L'Audio/Vidéo en temps réel est pris en charge 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 10.
- Les pilotes des webcams et des périphériques audio doivent être installés, et la webcam ainsi que le périphérique audio doivent être opérationnels sur l'ordinateur client. Pour utiliser l'Audio/Vidéo en temps réel, vous n'avez pas à installer les pilotes des périphériques sur le système d'exploitation du poste de travail où l'agent est installé.

Protocoles d'affichage

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

Configuration système requise pour la redirection de scanner

Vous pouvez analyser des informations vers vos postes de travail distants 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.

Postes de travail distants

Les postes de travail distants requièrent l'installation de View Agent 6.0.2 ou version ultérieure, ou Horizon Agent 7.0 ou 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 de poste de travail Windows et invités Windows Server, l'option de configuration de redirection de scanner d'Horizon 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, ainsi que sur la configuration de la redirection de scanner dans les applications et les postes de travail distants, consultez « Configuration de redirection de scanner » dans *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Ordinateur Horizon Client ou périphérique d'accès client

- La redirection de scanner est prise en charge sous Windows 7, Windows 8/8.1 et Windows 10.
- 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 l'agent est installé.

Norme de scanner

TWAIN ou WIA

Protocoles d'affichage

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

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

Configuration système requise pour 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 d'Horizon doit répondre à certaines exigences matérielles et logicielles.

Postes de travail distants

Les postes de travail distants requièrent l'installation de View Agent 6.1.1 ou version ultérieure, ou d'Horizon Agent 7.0 ou 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 à session unique :

- 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
- Windows Server 2016 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 sur lequel l'agent est installé.

Remarque Pour plus d'informations sur la configuration de la redirection de port série sur les postes de travail distants, consultez « Configuration de la redirection de port série » dans *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Ordinateur Horizon Client ou périphérique d'accès client

- La redirection de port série est prise en charge sur les systèmes clients Windows 7, Windows 8.x et Windows 10.
- 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 de périphérique sur le système d'exploitation du poste de travail à distance sur lequel l'agent est installé.

Protocoles d'affichage

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

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

Configuration système requise pour la redirection multimédia (MMR)

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

Postes de travail distants

- View Agent 6.0.2 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure, doit être installé sur les postes de travail mono-utilisateur.
- View Agent 6.1.1 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure, doit être installé sur l'hôte RDS des postes de travail basés sur des sessions.
- Pour plus d'informations sur les exigences de système d'exploitation, les exigences logicielles et les paramètres de configuration de l'application ou du poste de travail distant, consultez les rubriques sur la Redirection multimédia Windows Media dans *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Ordinateur Horizon Client ou périphérique d'accès client

Windows 7 32 ou 64 bits, Windows 8.x ou Windows 10.

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.

Configuration système requise pour la redirection Flash

Avec la redirection Flash, si vous utilisez Internet Explorer 9, 10 ou 11, le contenu Flash est envoyé au système client. Le système client effectue la lecture du contenu multimédia, ce qui réduit la charge sur l'hôte ESXi.

Poste de travail distant	■ Horizon Agent 7.0 ou version ultérieure doit être installé sur un poste de travail distant mono-utilisateur (VDI), avec l'option de redirection Flash. L'option de redirection Flash n'est pas sélectionnée par défaut. Consultez les rubriques sur l'installation d'Horizon Agent dans le document *Configuration des postes de travail virtuels dans Horizon 7*. ■ Les paramètres de stratégie de groupe appropriés doivent être configurés. Consultez les rubriques sur la configuration de la redirection Flash dans le document *Configuration des postes de travail virtuels dans Horizon 7*. ■ La redirection Flash est prise en charge sur les postes de travail distants mono-utilisateur Windows 7, Windows 8, Windows 8.1 et Windows 10. ■ Internet Explorer 9, 10 ou 11 doit être installé avec le plug-in Flash ActiveX correspondant. ■ Après l'installation, le composant complémentaire VMware View FlashMMR Server doit être activé dans Internet Explorer.
Ordinateur Horizon Client ou périphérique d'accès client	■ La redirection Flash est prise en charge sur Windows 7, Windows 8, Windows 8.1 et Windows 10. ■ Le plug-in Flash ActiveX doit être installé et activé
Protocole d'affichage de la session distante	VMware Blast, PCoIP

Conditions d'utilisation de la redirection d'URL flash

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

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

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

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

- 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, consultez la documentation d'Horizon.

Configuration système requise pour 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, Windows 8.x ou Windows 10.

- Le système d'exploitation de machine virtuelle (agent) dépend de la version de l'agent.

Version	système d'exploitation client
View Agent 6.2 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure	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 Server 2012 ou Windows Server 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 version ultérieure, ou Horizon Agent 7.0 ou version ultérieure
- 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 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.

Configuration requise pour l'utilisation de la redirection de contenu URL

Avec la fonctionnalité de redirection de contenu URL, le contenu URL peut être redirigé à partir de la machine cliente vers une application ou un poste de travail distant (redirection client vers agent), ou à partir d'une application ou d'un poste de travail distant vers la machine cliente (redirection agent vers client).

Par exemple, il vous suffit de cliquer sur un lien de l'application Microsoft Word native sur le client pour que le lien s'ouvre dans l'application Internet Explorer distante. Vous pouvez également cliquer sur un lien dans l'application Internet Explorer distante : le lien s'ouvre alors dans un navigateur natif sur la machine cliente. Vous pouvez configurer un nombre quelconque de protocoles pour la redirection, notamment HTTP, mailto et callto.

Internet Explorer 9, 10 et 11 sont les navigateurs pris en charge dans lesquels vous pouvez taper ou cliquer sur une URL pour qu'elle soit redirigée.

Remarque Cette fonction n'est pas opérationnelle pour les liens sur lesquels vous cliquez dans des applications universelles Windows 10, y compris le navigateur Microsoft Edge.

Pour utiliser la redirection client vers agent, vous devez activer la redirection de contenu URL lorsque vous installez Horizon Client. Vous devez installer Horizon Client à partir de la ligne de commande pour activer la redirection de contenu URL. Pour plus d'informations, consultez « Installation d'Horizon Client à partir de la ligne de commande », page 30.

Pour utiliser la redirection agent vers client, un administrateur d'Horizon doit activer la redirection de contenu URL lors de l'installation d'Horizon Agent. Pour plus d'informations, reportez-vous aux documents *Configuration des postes de travail virtuels dans Horizon 7* ou *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

Un administrateur Horizon doit également configurer des paramètres qui spécifient comment Horizon Client redirige le contenu URL à partir du système client vers une application ou un poste de travail distant, ou comment Horizon Agent redirige le contenu URL à partir d'une application ou d'un poste de travail distant vers la machine cliente. Pour plus d'informations sur la configuration, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Configuration requise pour l'utilisation de Skype Entreprise avec Horizon Client

Vous pouvez exécuter Skype Entreprise sur un poste de travail virtuel sans affecter l'infrastructure virtuelle et sans entraîner de surcharge du réseau. Tous les processus multimédias ont lieu sur la machine cliente Windows, plutôt que sur le poste de travail virtuel, au cours des appels audio et vidéo de Skype.

Pour utiliser cette fonctionnalité, vous devez installer le pack de virtualisation pour Skype Entreprise sur la machine cliente lors de l'installation d'Horizon Client pour Windows. Pour plus d'informations, consultez Chapitre 2, « Installation d'Horizon Client pour Windows », page 27.

Un administrateur Horizon doit également installer le pack de virtualisation VMware pour Skype Entreprise sur le poste de travail virtuel lors de l'installation d'Horizon Agent. Pour plus d'informations, consultez le document *Configuration des postes de travail virtuels dans Horizon 7*.

Pour connaître l'ensemble de la configuration requise, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

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.

Horizon 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'Horizon doivent également respecter certaines exigences de configuration pour prendre en charge les cartes à puce :

- Pour plus d'informations sur la configuration du Serveur de connexion pour la prise en charge des cartes à puce, consultez le document*Administration de View*.

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

- Pour plus d'informations sur les tâches que vous pouvez effectuer dans Active Directory afin d'implémenter l'authentification par carte à puce, consultez le document *Administration de View*.

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

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

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

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

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

Exigences de l'authentification de périphérique

Vous pouvez configurer une authentification de certificat pour les périphériques client.

Cette fonctionnalité a les exigences suivantes :

- Unified Access Gateway 2.6 ou version ultérieure.
- Horizon 7 version 7.0 ou version ultérieure.
- Un certificat installé sur le périphérique client qui sera accepté par Unified Access Gateway.

Systèmes d'exploitation de poste de travail pris en charge

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

Pour obtenir une liste des systèmes d'exploitation invités Windows pris en charge, consultez le document *Installation de View*.

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

Préparation du Serveur de connexion pour Horizon Client

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

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

- Si vous prévoyez d'utiliser Unified Access Gateway, configurez le Serveur de connexion pour qu'il fonctionne avec Unified Access Gateway. Reportez-vous au document *Déploiement et configuration d'Unified Access Gateway*. Les dispositifs Unified Access Gateway remplissent le même rôle que celui précédemment joué uniquement par des serveurs de sécurité.

- Si vous utilisez un serveur de sécurité, assurez-vous de disposer des dernières versions de maintenance du Serveur de connexion 5.3.x et du Serveur de sécurité 5.3.x ou versions ultérieures. Pour plus d'informations, reportez-vous au document *Installation de View*.
- Si vous prévoyez d'utiliser une connexion tunnel sécurisée pour des périphériques client et si la connexion sécurisée est configurée avec un nom d'hôte DNS pour le Serveur de connexion ou un serveur de sécurité, vérifiez que le périphérique client peut résoudre ce nom DNS.

  Pour activer ou désactiver le tunnel sécurisé, dans Horizon Administrator, accédez à la boîte de dialogue Modifier les paramètres du Serveur de connexion Horizon et cochez la case **Utiliser une connexion par tunnel sécurisé 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 plus d'informations, reportez-vous au document *Configuration des postes de travail virtuels dans Horizon 7* ou *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

  Important Si les utilisateurs finaux disposent d'un écran haute résolution et prévoient d'utiliser le paramètre client Mode haute résolution lors de l'affichage de leur poste de travail distant en mode plein écran, vous devez allouer suffisamment de mémoire VRAM pour chaque poste de travail distant Windows 7 ou version ultérieure. La quantité de mémoire vRAM requise dépend du nombre de moniteurs configurés pour les utilisateurs finaux et de la résolution d'affichage. Pour estimer la quantité de vRAM requise, consultez le document *Planification de l'architecture de View*.
- Pour pouvoir utiliser une authentification à deux facteurs, telle que l'authentification RSA SecurID ou RADIUS, avec Horizon Client, vous devez activer cette fonctionnalité sur le Serveur de connexion. Pour plus d'informations, consultez les rubriques concernant l'authentification à deux facteurs dans le document *Administration de View*.
- Pour masquer les informations de sécurité dans Horizon Client, notamment les informations d'URL de serveur et le menu déroulant **Domaine**, activez les paramètres **Masquer les informations de serveur dans l'interface utilisateur client** et **Masquer la liste de domaines dans l'interface utilisateur client** dans Horizon Administrator. Ces paramètres globaux sont disponibles dans Horizon 7 versions 7.1 et ultérieures. Pour plus d'informations sur la configuration des paramètres globaux, consultez le document *Administration de View*.

  Pour s'authentifier lorsque le menu déroulant **Domaine** est masqué, les utilisateurs doivent fournir des informations sur le domaine en entrant leur nom d'utilisateur au format ***domaine**nomutilisateur*** ou ***utilisateur*nom@*domaine*** dans la zone de texte **Nom d'utilisateur**.

  Important Si vous activez les paramètres **Masquer les informations de serveur dans l'interface utilisateur client** et **Masquer la liste de domaines dans l'interface utilisateur client** et sélectionnez l'authentification à deux facteurs (RSA SecureID ou RADIUS) pour l'instance du Serveur de connexion, n'appliquez pas la correspondance des noms d'utilisateur Windows. L'application de la correspondance des noms d'utilisateur Windows empêchera les utilisateurs d'entrer des informations sur le domaine dans la zone de texte Nom d'utilisateur et la connexion échouera toujours. Pour plus d'informations, consultez les rubriques concernant l'authentification à deux facteurs dans le document *Administration de View*.
- Pour permettre aux utilisateurs d'accéder aux applications publiées dans Horizon Client sans avoir à s'authentifier, vous devez activer cette fonctionnalité dans le Serveur de connexion. Pour plus d'informations, consultez les rubriques concernant l'accès sans authentification dans le document *Administration de View*.

Effacement du dernier nom d'utilisateur utilisé pour se connecter à un serveur

Lorsque des utilisateurs se connectent à une instance du Serveur de connexion pour laquelle le paramètre global **Masquer la liste de domaines dans l'interface utilisateur client** est activé, le menu déroulant **Domaine** est masqué dans Horizon Client et les utilisateurs fournissent des informations sur le domaine dans la zone de texte **Nom d'utilisateur** d'Horizon Client. Par exemple, les utilisateurs doivent entrer leur nom d'utilisateur au format ***domaine**nomutilisateur*** ou ***nomutilisateur@domaine***.

Dans un système client Windows, une clé de registre détermine si le dernier nom d'utilisateur est enregistré et affiché dans la zone de texte **Nom d'utilisateur** la prochaine fois qu'un utilisateur se connecte au serveur. Pour éviter d'afficher le dernier nom d'utilisateur dans la zone de texte **Nom d'utilisateur** et ainsi dévoiler des informations sur le domaine, vous devez définir la valeur de la clé de registre `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\dontdisplaylastusername` sur 1 dans le système client Windows.

Pour plus d'informations sur le masquage des informations de sécurité dans Horizon Client, notamment le menu déroulant **Domaine** et les informations sur l'URL de serveur, consultez les rubriques sur les paramètres généraux dans le document *Administration de View*.

Configurer des options VMware Blast

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

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

Vous ne pouvez pas modifier l'option de condition réseau après vous être connecté à un serveur. Vous pouvez configurer le décodage H.264 avant ou après vous être connecté à un serveur.

Prérequis

Cette fonctionnalité requiert Horizon Agent 7.0 ou version ultérieure.

Procédure

1 Cliquez sur le bouton **Options** dans la barre de menus et sélectionnez **Configurer VMware Blast**.

  Si vous êtes connecté à un serveur, vous pouvez cliquer sur l'icône **Paramètres** (engrenage) et sélectionner **VMware Blast**. Vous ne pouvez pas modifier l'option de condition réseau après vous être connecté à un serveur.

2 Configurez les options de décodage et de condition réseau.

Option	Action
H.264	Configurez cette option, avant ou après la connexion au Serveur de connexion, pour autoriser le décodage H.264 dans Horizon Client. Lorsque cette option est sélectionnée (paramètre par défaut), Horizon Client utilise le décodage H.264 si l'agent prend en charge le codage logiciel ou matériel H.264. Si l'agent ne prend pas en charge le codage logiciel ou matériel H.264, Horizon Client utilise le décodage JPG/PNG. Désélectionnez cette option pour utiliser le décodage JPG/PNG.
Sélectionnez votre condition réseau pour une expérience optimale	Vous ne pouvez configurer cette option qu'avant la connexion au Serveur de connexion. Sélectionnez l'une des options de condition réseau suivantes : ■ **Excellent** : Horizon Client utilise uniquement la mise en réseau TCP. Cette option est idéale pour un environnement LAN. ■ **Classique (par défaut)** : Horizon Client fonctionne en mode mixte. En mode mixte, Horizon Client utilise la mise en réseau TCP lors de la connexion au serveur et utilise BEAT (Blast Extreme Adaptive Transport) si l'agent et Blast Security Gateway (si activé) prennent en charge la connectivité BEAT. Cette option est le paramètre par défaut. ■ **Faible** : Horizon Client n'utilise la mise en réseau BEAT que si le serveur tunnel BEAT est activé sur le serveur ; sinon il passe en mode mixte. **Remarque** Dans Horizon 7 versions 7.1 et antérieures, les instances du Serveur de connexion et du serveur de sécurité ne prennent pas en charge le serveur tunnel BEAT. Unified Access Gateway 2.9 et les versions ultérieures prennent en charge le serveur tunnel BEAT. Blast Security Gateway pour les instances du Serveur de connexion et du serveur de sécurité ne prend pas en charge la mise en réseau BEAT.

3 Cliquez sur **OK** pour enregistrer vos modifications.

Les modifications de H.264 seront appliquées la prochaine fois qu'un utilisateur se connectera à une application ou un poste de travail distant et qu'il sélectionnera le protocole d'affichage VMware Blast. Vos modifications n'ont pas d'incidence sur les sessions VMware Blast existantes.

Utilisation des paramètres proxy d'Internet Explorer

Horizon Client utilise automatiquement des paramètres proxy configurés dans Internet Explorer.

Contournement des paramètres proxy

Horizon Client utilise les paramètres de contournement de proxy d'Internet Explorer pour contourner les connexions HTTPS vers un hôte du Serveur de connexion, un serveur de sécurité ou un dispositif Unified Access Gateway.

Si le tunnel sécurisé est activé sur l'hôte du Serveur de connexion, le serveur de sécurité ou le dispositif Unified Access Gateway, vous devez utiliser le paramètre de stratégie de groupe `Liste d'adresses de contournement de proxy par tunnel` dans le fichier de modèle d'administration ADM ou ADMX de configuration d'Horizon Client afin de spécifier une liste d'adresses pour contourner la connexion par tunnel. Le serveur proxy n'est pas utilisé pour ces adresses. Utilisez un point-virgule (;) pour séparer plusieurs entrées. Ce paramètre de stratégie de groupe crée la clé de registre suivante :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\VMware, Inc.\VMware VDM\Client\TunnelProxyBypass
```

Vous ne pouvez pas utiliser ce paramètre de stratégie de groupe pour les connexions directes. Si l'application du paramètre de stratégie de groupe ne fonctionne pas comme prévu, essayez de contourner le proxy pour les adresses locales. Pour plus d'informations, consultez https://blogs.msdn.microsoft.com/askie/2015/10/12/how-to-configure-proxy-settings-for-ie10-and-ie11-as-iem-is-not-available/.

Basculement de proxy

Horizon Client prend en charge le basculement de proxy avec le paramètre **Utiliser un script de configuration automatique** sous **Configuration automatique** dans **Options Internet > Connexions > Paramètres de réseau local** dans Internet Explorer. Pour utiliser ce paramètre, vous devez créer un script de configuration automatique qui renvoie plusieurs serveurs proxy.

Données Horizon Client collectées par VMware

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

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

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

L'administrateur qui installe le Serveur de connexion peut choisir de participer au programme d'amélioration du produit VMware lors de l'exécution de l'assistant d'installation du Serveur de connexion, ou un administrateur peut définir une option dans Horizon 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 *x.x.x-yyyyyy*, où *x.x.x* est le numéro de version du client et *yyyyyy* est le numéro de build.)
Architecture binaire du client	Non	Exemples : ■ i386 ■ x86_64 ■ arm
Nom du build du client	Non	Exemples : ■ VMware-Horizon-Client-Win32-Windows ■ VMware-Horizon-Client-Linux ■ VMware-Horizon-Client-iOS ■ VMware-Horizon-Client-Mac ■ VMware-Horizon-Client-Android ■ VMware-Horizon-Client-WinStore

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

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

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

Description	Ce champ reste-t-il anonyme ?	Exemple
Famille de périphériques USB	Non	Exemples : ■ 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. Vous pouvez définir différentes options de démarrage pour les utilisateurs finaux après l'installation d'Horizon Client.

Ce chapitre aborde les rubriques suivantes :

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

Si vous prévoyez d'installer Horizon Client avec un chiffrement compatible FIPS (Federal Information Processing Standard), vous devez activer le mode FIPS sur le système d'exploitation client avant d'exécuter le programme d'installation d'Horizon Client.

Lorsque le mode FIPS est activé dans le système d'exploitation client, les applications n'utilisent que des algorithmes de chiffrement compatibles avec FIPS-140 et conformes aux modes d'opération 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 un chiffrement compatible FIPS est prise en charge uniquement pour les systèmes clients disposant des systèmes d'exploitation Windows 7 SP1 ou version ultérieure.

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 FIPS

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

- Pour utiliser le paramètre de stratégie de groupe, ouvrez l'éditeur de stratégie de groupe, accédez à `Configuration ordinateur\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Options de sécurité` et activez le paramètre **Chiffrement système : utilisez des algorithmes compatibles FIPS pour le chiffrement, le hachage et la signature**.

- Pour utiliser le registre Windows, accédez à `HKLM\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\Enabled` et définissez **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 d'Horizon Client, l'option du programme d'installation pour utiliser le chiffrement compatible FIPS ne s'affiche pas lors d'une installation personnalisée. Le chiffrement compatible FIPS n'est pas activé lors d'une installation classique. Si vous installez Horizon Client sans l'option de chiffrement compatible FIPS et que vous décidez ultérieurement d'utiliser l'option, vous devez désinstaller le client, activer le mode FIPS sur le système d'exploitation client et exécuter de nouveau le programme d'installation d'Horizon Client.

Installer Horizon Client pour Windows

Les utilisateurs finaux ouvrent Horizon Client pour se connecter à leurs applications et à leurs postes de travail distants 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 comment installer Horizon Client à l'aide d'un assistant d'installation interactive. Pour installer Horizon Client à partir de la ligne de commande, reportez-vous à la section « Installation d'Horizon Client à partir de la ligne de commande », page 30. Pour installer la fonctionnalité Redirection de contenu URL, vous devez exécuter le programme d'installation à partir de la ligne de commande.

Remarque Vous pouvez installer Horizon Client sur une machine virtuelle de poste de travail distant si ce poste de travail exécute View Agent 6.0 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure. Les entreprises peuvent utiliser cette stratégie d'installation si leurs utilisateurs finaux accèdent à des applications distantes à partir de périphériques de client léger Windows.

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 10.
- 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.
- 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 un chiffrement compatible FIPS, activez le mode FIPS sur le système d'exploitation client avant d'exécuter le programme d'installation d'Horizon Client. Reportez-vous à la section « Activation du mode FIPS sur le système d'exploitation client Windows », page 27.
- Si vous prévoyez d'installer le composant **Redirection USB**, procédez comme suit :
  - Déterminez si la personne qui utilise le périphérique client est autorisée à accéder à des périphériques USB connectés en local depuis un poste de travail distant. Si l'accès n'est pas autorisé, n'installez pas le composant **Redirection USB** ou bien installez le composant et désactivez-le en utilisant un paramètre de stratégie de groupe. Si vous utilisez une stratégie de groupe pour désactiver la redirection USB, vous n'avez pas besoin de réinstaller Horizon Client si vous décidez ultérieurement d'activer la redirection USB pour un client. Pour plus d'informations, reportez-vous à la section « Paramètres de définition de scripts des objets de stratégie de groupe (GPO) des clients », page 48.

  - Vérifiez que la fonctionnalité Mise à jour automatique Windows n'est pas désactivée sur l'ordinateur client.
- Décidez s'il convient ou non d'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 du Serveur de connexion, 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 du Serveur de connexion, déterminez le FQDN pour que vous puissiez le fournir lors de l'installation.

Procédure

1 Connectez-vous au système client comme administrateur.

2 Accédez à la page de produit VMware à l'adresse http://www.vmware.com/go/viewclients.

3 Téléchargez le fichier du programme d'installation, par exemple, `VMware-Horizon-Client-y.y.y-xxxxxx.exe`.

xxxxxx correspond au numéro de build et *y.y.y* au numéro de version.

4 Double-cliquez sur le fichier du programme d'installation pour commencer l'installation.

5 Sélectionnez le type d'installation et suivez les invites.

Option	Action
Installation classique	Cliquez sur **Accepter et installer**. Le programme d'installation installe les fonctionnalités Redirection USB et Se connecter en tant qu'utilisateur actuel.
Installation personnalisée	Cliquez sur **Personnaliser l'installation** et sélectionnez les fonctions à installer. Vous devez sélectionner cette option pour effectuer les tâches suivantes : spécifier un emplacement d'installation différent de celui par défaut, utiliser le protocole Internet IPv6, configurer une instance du Serveur de connexion par défaut, configurer le comportement de connexion par défaut, activer le chiffrement compatible FIPS, installer le composant Core Remote Experience 32 bits sur une machine 64 bits ou installer le pack de virtualisation VMware pour Skype Entreprise. Les options d'installation personnalisée du chiffrement compatible FIPS sont disponibles dans le programme d'installation uniquement si le mode FIPS est activé sur le système d'exploitation client. Suivez ces instructions lors de la sélection des fonctions personnalisées : ■ Ne sélectionnez pas l'option **IPv6**, sauf si tous les composants de votre environnement Horizon utilisent le protocole IPv6 Internet. Certaines fonctionnalités ne sont pas disponibles dans un environnement IPv6. Pour plus d'informations, reportez-vous au document *Installation de View*. ■ Sélectionnez la fonctionnalité **Core Remote Experience 32 bits sur une machine 64 bits** si la machine cliente 64 bits ne dispose pas d'un plug-in 64 bits pour le produit. Vous ne pouvez pas installer le pack de virtualisation pour Skype Entreprise si vous sélectionnez cette fonctionnalité.

Certaines fonctionnalités vous obligent à redémarrer le système client.

Le programme d'installation installe certains services Windows, notamment VMware Horizon Client (`horizon_client_service`) et VMware USB Arbitration Service (`VMUSBArbService`).

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 75.

Installation d' Horizon Client à partir de la ligne de commande

Vous pouvez installer Horizon Client en saisissant le nom de fichier du programme d'installation, les commandes d'installation et les propriétés d'installation dans la ligne de commande.

Lorsque vous installez Horizon Client à partir de la ligne de commande, vous pouvez effectuer une installation silencieuse. L'installation silencieuse vous permet de déployer efficacement Horizon Client dans une entreprise de grande taille.

Commandes d'installation d' Horizon Client

Lorsque vous installez Horizon Client à partir de la ligne de commande, vous pouvez spécifier certaines commandes d'installation.

Le tableau suivant décrit les commandes d'installation d'Horizon Client.

Tableau 2-1. Commandes d'installation d' Horizon Client

vdmadmin	Description
`/?` ou `/help`	Répertorie les propriétés et les commandes d'installation d'Horizon Client.
`/silent`	Installe Horizon Client en mode silencieux. Vous n'avez pas besoin de répondre aux invites de l'Assistant.
`/install`	Installe Horizon Client de manière interactive. Vous devez répondre aux invites de l'Assistant.
`/uninstall`	Désinstalle Horizon Client.
`/repair`	Répare Horizon Client.
`/norestart`	Supprime tous les redémarrages et les invites de redémarrage au cours du processus d'installation.
`/x /extract`	Extrait les modules du programme d'installation dans le répertoire `TEMP %`.

Propriétés d'installation d' Horizon Client

Lorsque vous installez Horizon Clientà partir de la ligne de commande, vous pouvez spécifier certaines propriétés d'installation.

Le tableau suivant décrit les propriétés d'installation d'Horizon Client.

Tableau 2-2. Propriétés d'installation d' Horizon Client

Propriété	Description	Valeur par défaut
`INSTALLDIR`	Chemin d'accès et dossier dans lequel Horizon Client est installé. Par exemple : `INSTALLDIR=""D:\abc\my folder""` Les guillemets délimitant le chemin permettent au programme d'installation 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 Horizon Client utilisent pour la communication. Les valeurs possibles sont IPv4 et IPv6.	IPv4

Tableau 2-2. Propriétés d'installation d' Horizon Client (suite)

Propriété	Description	Valeur par défaut
VDM_FIPS_ENABLED	Spécifie s'il faut installer Horizon Client avec la cryptographie compatible FIPS. La valeur 1 installe Horizon Client avec un chiffrement compatible FIPS. La valeur 0 installe Horizon Client sans chiffrement compatible FIPS. **Remarque** Avant de définir cette propriété 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 27.	0
VDM_SERVER	Nom de domaine complet (FQDN) de l'instance du Serveur de connexion à laquelle les utilisateurs d'Horizon Client se connectent par défaut. Par exemple : `VDM_Server=cs1.companydomain.com` Lorsque vous configurez cette propriété, les utilisateurs d'Horizon Client n'ont pas à fournir ce nom de domaine complet (FQDN).	aucune
LOGINASCURRENTUSER_DISPLAY	Détermine si **Se connecter en tant qu'utilisateur actuel** s'affiche dans le menu **Options** de la barre de menus Horizon Client. Les valeurs valides sont 1 (activé) ou 0 (désactivé).	1
LOGINASCURRENTUSER_DEFAULT	Détermine si **Se connecter en tant qu'utilisateur actuel** est sélectionné par défaut dans le menu **Options** de la barre de menus Horizon Client. Les valeurs valides sont 1 (activé) et 0 (désactivé). Lorsque l'option Se connecter en tant qu'utilisateur actuel est le comportement de connexion par défaut, 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, puis au poste de travail distant. Lorsque l'option Se connecter en tant qu'utilisateur actuel n'est pas le comportement de connexion par défaut, les utilisateurs doivent fournir leur identité et leurs informations d'identification plusieurs fois avant de pouvoir accéder à une application ou un poste de travail distant.	0

Tableau 2-2. Propriétés d'installation d' Horizon Client (suite)

Propriété	Description	Valeur par défaut
ADDLOCAL	Spécifie les fonctionnalités à installer dans une installation silencieuse. Les valeurs valides sont les suivantes : ■ ALL : installe toutes les fonctionnalités disponibles, à l'exception de Redirection de contenu URL. ■ TSSO : installe la fonctionnalité Se connecter en tant qu'utilisateur actuel. ■ USB : installe la fonctionnalité Redirection USB. Pour spécifier des fonctionnalités individuelles, entrez une liste de noms de fonctionnalités séparés par des virgules. Ne laissez pas d'espaces entre les noms. Par exemple, pour installer Horizon Client avec la fonctionnalité Redirection USB, mais sans la fonctionnalité Se connecter en tant qu'utilisateur actuel, tapez la commande suivante : `VMware-Horizon-Client-y.y.y-xxxxxx.exe /silent ADDLOCAL=USB`	aucune
INSTALL_32BITRMKS	Sur une machine cliente 64 bits, spécifie s'il convient d'installer le composant Core Remote Experience 32 bits. La valeur 1 installe le composant Core Remote Experience 32 bits. La valeur 0 installe le composant Core Remote Experience 64 bits. Installez le composant Core Remote Experience 32 bits si la machine cliente 64 bits ne dispose pas d'un plug-in 64 bits pour le produit. Cette propriété n'est pas valide sur une machine cliente 32 bits.	0
INSTALL_SFB	Spécifie s'il faut installer le pack de virtualisation VMware pour Skype Entreprise. La fonctionnalité sera installée si la valeur est égale à 1. La fonctionnalité ne sera pas installée si la valeur est égale à 0. Cette fonctionnalité n'est pas compatible avec le composant Core Remote Experience 32 bits (INSTALL_32BITRMKS=1).	0
URL_FILTERING_ENABLED	Spécifie s'il faut installer la fonctionnalité de redirection de contenu URL. La fonctionnalité sera installée si la valeur est égale à 1. La fonctionnalité ne sera pas installée si la valeur est égale à 0. Lorsque vous affectez 1 à cette propriété dans une installation interactive, la case à cocher **Redirection de contenu URL** s'affiche sous Fonctionnalités supplémentaires dans la boîte de dialogue d'installation personnalisée et est sélectionnée par défaut. La case à cocher ne s'affiche pas, sauf si vous affectez 1 à cette propriété. **Remarque** La propriété ADDLOCAL=ALL n'inclut pas la fonctionnalité Redirection de contenu URL.	0

Installation d' Horizon Client à partir de la ligne de commande

Vous pouvez installer Horizon Client à partir de la ligne de commande en tapant le nom de fichier du programme d'installation et en spécifiant des propriétés et des commandes d'installation. Vous pouvez installer Horizon Clienten mode silencieux à partir de la ligne de commande.

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 10.
- 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 un chiffrement compatible FIPS, activez le mode FIPS sur le système d'exploitation client avant d'exécuter le programme d'installation d'Horizon Client. Reportez-vous à la section « Activation du mode FIPS sur le système d'exploitation client Windows », page 27.
- Décidez s'il convient ou non d'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 du Serveur de connexion, puis au poste de travail distant. Certains systèmes d'exploitation client ne prennent pas cette fonction en charge.
- Familiarisez-vous avec les commandes d'installation d'Horizon Client. Reportez-vous à la section « Commandes d'installation d'Horizon Client », page 30.
- Familiarisez-vous avec les propriétés d'installation d'Horizon Client. Reportez-vous à la section « Propriétés d'installation d'Horizon Client », page 30.
- Déterminez si vous voulez autoriser les utilisateurs finaux à accéder à des périphériques USB connectés en local à partir de leurs postes de travail distants. Si ce n'est pas le cas, définissez la propriété d'installation `ADDLOCAL` sur la liste des fonctionnalités et omettez la fonctionnalité USB. Pour plus d'informations, reportez-vous à la section « Propriétés d'installation d'Horizon Client », page 30.
- Si vous ne voulez pas que les utilisateurs finaux fournissent le nom de domaine complet (FQDN) de l'instance du Serveur de connexion, déterminez le FQDN pour que vous puissiez le fournir lors de l'installation.

Procédure

1. Connectez-vous au système client comme administrateur.
2. Accédez à la page de produit VMware à l'adresse http://www.vmware.com/go/viewclients.
3. Téléchargez le fichier du programme d'installation d'Horizon Client, par exemple, `VMware-Horizon-Client-y.y.y-xxxxxx.exe`.

   xxxxxx correspond au numéro de build et *y.y.y* au numéro de version.
4. Ouvrez une invite de commande sur l'ordinateur client Windows.
5. Tapez le nom de fichier du programme d'installation, les commandes d'installation et les propriétés d'installation sur une seule ligne.

   `VMware-Horizon-Client-y.y.y-xxxxxx.exe [commands] [properties]`

Le programme d'installation installe Horizon Client selon les commandes d'installation et les propriétés que vous spécifiez. Si vous spécifiez la commande d'installation `/silent`, les invites de l'Assistant ne s'affichent pas.

Le programme d'installation installe certains services Windows, notamment VMware Horizon Client (`horizon_client_service`) et VMware USB Arbitration Service (`VMUSBArbService`).

Exemple : Commandes d'installation

La commande suivante installe Horizon Client de manière interactive et active la fonctionnalité Redirection de contenu URL.

```
VMware-Horizon-Client-y.y.y-xxxxxx.exe URL_FILTERING_ENABLED=1
```

La commande suivante installe Horizon Client en mode silencieux et supprime tous les redémarrages et les invites de redémarrage au cours du processus d'installation.

```
VMware-Horizon-Client-y.y.y-xxxxxx.exe /silent /norestart
```

Suivant

Si vous avez activé la fonctionnalité Redirection de contenu URL lorsque vous avez installé Horizon Client, vérifiez que la fonctionnalité est installée. Reportez-vous à la section « Vérifiez l'installation de Redirection de contenu URL », page 34.

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 75.

Vérifiez l'installation de Redirection de contenu URL

Si vous avez activé la fonctionnalité Redirection de contenu URL lorsque vous avez installé Horizon Client, vérifiez que la fonctionnalité a été installée.

Prérequis

Spécifiez la propriété d'installation `URL_FILTERING_ENABLED=1` lorsque vous installez Horizon Client. Reportez-vous à la section « Installation d'Horizon Client à partir de la ligne de commande », page 30.

Procédure

1. Connectez-vous à la machine cliente.
2. Accédez au répertoire `%PROGRAMFILES%\VMware\VMware Horizon View Client\` et vérifiez que les fichiers `vmware-url-protocole-lancement-helper.exe` et `vmware-url-filtrage-plugin.dll` sont installés dans ce répertoire.
3. Vérifiez que le composant complémentaire Plug-in de filtrage d'URL de VMware Horizon View est installé et activé dans Internet Explorer sur la machine cliente.

Mettre à niveau Horizon Client en ligne

Vous pouvez mettre à niveau Horizon Client en ligne si la fonctionnalité de mise à niveau en ligne est activée. Cette fonctionnalité est désactivée par défaut.

Vous pouvez activer cette fonctionnalité en modifiant les paramètres de stratégie de groupe `Enable Horizon Client online update` et `URL for Horizon Client online update`. Pour plus d'informations, reportez-vous à la section « Paramètres généraux des objets de stratégie de groupe (GPO) de clients », page 58.

Prérequis

- Enregistrez votre travail avant d'effectuer la mise à jour d'Horizon Client. La mise à jour peut initier un redémarrage système.
- Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur le système client.

Procédure

1 Connectez-vous en tant qu'administrateur.

2 Dans Horizon Client, cliquez sur **Mises à jour du logiciel** sur l'un des deux écrans.

Écran Horizon Client	Action
Avant de vous connecter à un Serveur de connexion	Cliquez sur **Options > Mises à jour du logiciel**.
Après vous être connecté à un Serveur de connexion	Cliquez sur **Aide > Mises à jour du logiciel**

3 Cliquez sur **Rechercher les mises à jour**.

4 Cliquez sur **Télécharger et installer**.

Configuration d'Horizon Client pour les utilisateurs finaux 3

La configuration d'Horizon Client pour les utilisateurs finaux peut impliquer la configuration d'URI pour démarrer Horizon Client, la configuration du mode de vérification des certificats, la définition d'options TLS/SSL avancées et l'utilisation de fichiers de modèle ADMX de stratégie de groupe pour configurer des paramètres personnalisés.

Ce chapitre aborde les rubriques suivantes :

Paramètres de configuration communs

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

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

Tableau 3-1. Paramètres de configuration communs

Paramètre	Mécanismes de configuration
Adresse du Serveur de connexion	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

Tableau 3-1. Paramètres de configuration communs (suite)

Paramètre	Mécanismes de configuration
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

Utilisation d'URI pour configurer Horizon Client

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

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

- Adresse du Serveur de connexion
- Numéro de port du Serveur de connexion
- Nom d'utilisateur Active Directory
- Nom 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 déconnexion 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 démarrer Horizon Client uniquement si le logiciel client est déjà installé sur des ordinateurs clients.

Syntaxe pour la création d'URI vmware-view

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

Spécification d'URI

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

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

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

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

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

authority-part

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

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

`user1@`*`server-address`*

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

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

`server-address``:`*`port-number`*

path-part

Spécifie le poste de travail ou l'application. Utilise le nom d'affichage du poste de travail ou de l'application. Ce nom est celui spécifié dans Horizon 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
`browse`	Affiche une liste des postes de travail et applications disponibles hébergés sur le serveur spécifié. Il ne vous est pas demandé de spécifier un poste de travail ou une application pour l'utilisation de cette action.
`start-session`	Ouvre l'application ou le poste de travail spécifié. Si aucune requête d'action n'est fournie et que le nom du poste de travail ou de l'application est fourni, `start-session` est l'action par défaut.

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.
`restart`	Éteint puis redémarre le poste de travail spécifié. Le redémarrage d'un poste de travail distant équivaut à la commande de redémarrage du système d'exploitation Windows. En général, le système d'exploitation invite l'utilisateur à enregistrer toutes les données non enregistrées avant de redémarrer.
`logoff`	Déconnecte l'utilisateur du système d'exploitation invité sur le poste de travail distant. Si vous spécifiez une application, l'action est ignorée ou l'utilisateur final voit le message d'avertissement « Action d'URI non valide ».

args

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

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

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

appProtocol

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

connectUSBOnInsert

Connecte un périphérique USB au poste de travail virtuel 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 **`true`** et **`false`**. Exemple de syntaxe : **`connectUSBOnInsert=true`**.

connectUSBOnStartup

Redirige tous les périphériques USB actuellement connectés au système client vers le poste de travail. 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 **`true`** et **`false`**. Exemple de syntaxe : **`connectUSBOnStartup=true`**.

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 de la valeur par défaut.
`multimonitor`	Tous les moniteurs affichent leur contenu en plein écran.
`windowLarge`	Fenêtre de grande taille.
`windowSmall`	Fenêtre de petite taille.
*W*x*H*	Personnalisez la résolution, spécifiez la largeur et la hauteur en pixels. Exemple de syntaxe : **`desktopLayout=1280x800`**.

desktopProtocol

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

domainName

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

filePath

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 :

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

Par exemple, pour représenter le chemin d'accès au fichier `C:\test file.txt`, utilisez **`C%3A%5Ctest%20file.txt`**.

tokenUserName

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`***.

unattended

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.

useExisting

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

unauthenticatedAccessEnabled	Si cette option est définie sur **`true`**, la fonctionnalité Accès non authentifié est activée par défaut. L'option **Se connecter de manière anonyme à l'aide de l'accès non authentifié** est affichée dans l'interface utilisateur et sélectionnée. Si cette option est définie sur **`false`**, la fonctionnalité Accès non authentifié est désactivée. L'option **Se connecter de manière anonyme à l'aide de l'accès non authentifié** est masquée et désactivée. Lorsque cette option est définie sur **""**, la fonctionnalité Accès non authentifié est désactivée et le paramètre **Se connecter de manière anonyme à l'aide de l'accès non authentifié** n'apparaît pas sur l'interface utilisateur et est désactivé. Exemple de syntaxe : **`unauthenticatedAccessEnabled=true`**.
unauthenticatedAccessAccount	Définit le compte à utiliser si la fonctionnalité Accès non authentifié est activée. Si la fonctionnalité Accès non authentifié est désactivée, cette requête est ignorée. Exemple de syntaxe utilisant le compte d'utilisateur **`anonymous1`** : **`unauthenticatedAccessAccount=anonymous1`**.

Exemples d'URI de vmware-view

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

Exemples de syntaxe URI

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

Horizon Client démarre et se connecte au serveur `view.mycompany.com`. La boîte de dialogue de connexion invite l'utilisateur à fournir un nom d'utilisateur, un nom de domaine et un mot de passe. Après l'ouverture de session, Horizon Client affiche une boîte de dialogue qui invite l'utilisateur à confirmer l'opération de réinitialisation pour Poste de travail principal.

Remarque Cette action est uniquement disponible si un administrateur Horizon a activé la fonctionnalité de réinitialisation de poste de travail pour le poste de travail.

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

Horizon Client démarre et se connecte au serveur `view.mycompany.com`. La boîte de dialogue de connexion invite l'utilisateur à fournir un nom d'utilisateur, un nom de domaine et un mot de passe. Après l'ouverture de session, Horizon Client affiche une boîte de dialogue qui invite l'utilisateur à confirmer l'opération de redémarrage du poste de travail principal.

Remarque Cette action est uniquement disponible si un administrateur Horizon a activé la fonctionnalité de redémarrage de poste de travail pour le poste de travail.

9 `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.

10 `vmware-view://`

Cet URI démarre Horizon Client s'il n'est pas en cours d'exécution, ou fait passer Horizon Client au premier plan s'il est en cours d'exécution.

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

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

Vous pouvez également taper cette commande dans l'invite de ligne de commande de Windows à l'aide de la syntaxe suivante :

```
vmware-view.exe --serverURL 10.10.10.10 --appName "My Notepad++" --args "\"my new.txt\""
```

Dans cet exemple, les guillemets sont échappés avec les caractères `\"`.

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

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

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

13 `vmware-view://view.mycompany.com/Notepad?unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous1`

Horizon Client démarre et se connecte au serveur `view.mycompany.com` en utilisant le compte d'utilisateur **`anonymous1`**. L'application Notepad est lancée sans inviter l'utilisateur à fournir ses informations d'identification.

Exemples de code HTML

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

```
<html>
<body>

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

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

</body>
</html>
```

Configuration de la vérification des certificats pour les utilisateurs finaux

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

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

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

Pour plus d'informations sur les types de vérifications effectuées, reportez-vous à la section « Définition du mode de vérification de certificats pour Horizon Client », page 45.

Utilisez le fichier de modèle d'administration ADMX de configuration d'Horizon Client (`vdm_client.admx`) pour définir le mode de vérification. Tous les fichiers ADMX qui fournissent les paramètres de stratégie de groupe sont disponibles dans un fichier `.zip` nommé `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, où *x.x.x* est la version et *yyyyyyy* 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 48.

Remarque Vous pouvez également utiliser le fichier de modèle ADMX de configuration d'Horizon 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 51.

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.

Remarque Dans une version ultérieure, il se peut que la configuration de ce paramètre à l'aide du registre Windows ne soit plus prise en charge. Vous devez utiliser un paramètre GPO.

Définition du mode de vérification de certificats pour Horizon Client

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

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

- Le certificat a-t-il 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 plus d'informations sur la distribution d'un certificat racine auto-signé à tous les systèmes clients Windows dans un domaine, consultez « 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 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 qu'aucune vérification des certificats n'a lieu.

Si le mode de vérification des certificats est défini sur **Avertir**, vous pouvez toujours vous connecter à une instance du Serveur de connexion 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 ADMX. Reportez-vous à la section « Paramètres de sécurité des objets de stratégie de groupe (GPO) des clients », page 51. 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 73.

Configuration des options TLS/SSL avancées

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

Ces options de sécurité sont également utilisées pour chiffrer le canal USB.

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

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

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

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

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

Sur le système client, vous pouvez utiliser 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 51. 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 73.

Configurer le comportement de reconnexion d'applications

Lorsque vous vous déconnectez d'un serveur, des applications en cours peuvent rester ouvertes. Vous pouvez configurer comment les applications en cours se comportent lorsque vous vous reconnectez au serveur.

Un administrateur Horizon peut désactiver les paramètres de comportement de reconnexion d'applications dans Horizon Client à partir de la ligne de commande ou en définissant un paramètre de stratégie de groupe. Le paramètre de stratégie de groupe est prioritaire sur le paramètre de ligne de commande. Pour plus d'informations, consultez l'option `–appSessionReconnectionBehavior` dans « Utilisation des commandes d'Horizon Client », page 68 ou le paramètre de stratégie de groupe **Comportement de reprise d'une session d'application déconnectée** dans « Paramètres de définition de scripts des objets de stratégie de groupe (GPO) des clients », page 48.

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 Applications distantes qui s'affiche, sélectionnez un paramètre de comportement de reconnexion d'applications.

Option	Description
Demander la reconnexion pour ouvrir des applications	Horizon Client vous informe qu'une ou plusieurs applications distantes sont en cours d'exécution lorsque vous vous reconnectez au serveur. Vous pouvez cliquer sur **Se reconnecter aux applications** pour rouvrir les fenêtres des applications ou sur **Pas maintenant** pour ne pas les rouvrir.
Se reconnecter automatiquement pour ouvrir des applications	Les fenêtres des applications en cours se rouvrent automatiquement lorsque vous vous reconnectez au serveur.
Ne pas demander la reconnexion et ne pas se reconnecter automatiquement	Horizon Client ne vous invite pas à rouvrir les applications en cours et les fenêtres des applications en cours ne se rouvrent pas lorsque vous vous reconnectez au serveur.

3 Cliquez sur **OK** pour enregistrer vos modifications.

Le paramètre s'applique lors de votre prochaine connexion au serveur.

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

VMware Horizon Client inclut un fichier de modèle d'administration ADMX de stratégie de groupe que vous pouvez utiliser pour 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 ADMX à un objet de stratégie de groupe (GPO) nouveau ou existant dans Active Directory.

Le fichier de modèle 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.

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

Le fichier de modèle d'administration ADMX de configuration d'Horizon Client (`vdm_client.admx`) ainsi que tous les fichiers ADMX qui fournissent des paramètres de stratégie de groupe sont disponibles dans un fichier `.zip` nommé `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, où *x.x.x* est la version et *yyyyyyy* le numéro de build. Vous pouvez télécharger les fichiers sur le site de téléchargement de VMware Horizon à l'adresse http://www.vmware.com/go/downloadview. Vous devez copier ces fichiers sur votre serveur Active Directory et utiliser l'Éditeur de gestion des stratégies de groupes pour ajouter les modèles d'administration. Pour obtenir des instructions, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

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 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 ADMX de configuration de VMware Horizon Client. Le fichier de 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. Les paramètres se trouvent dans le dossier **Configuration de VMware Horizon Client > Définitions de script** dans l'Éditeur de gestion de stratégie de groupe.

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

Paramètre	Description
`Automatically connect if only one launch item is entitled`	Se connecte automatiquement au poste de travail s'il est le seul autorisé pour l'utilisateur. 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. **Remarque** Ce paramètre ne s'applique pas aux applications publiées.
`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. **Remarque** Ce paramètre ne s'applique pas aux applications publiées.

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

Paramètre	Description
`DesktopLayout`	Spécifie la disposition de la fenêtre Horizon Client visible par un utilisateur lorsqu'il se connecte à un poste de travail distant. Les différentes dispositions sont les suivantes : ■ `Full Screen` ■ `Multimonitor` ■ `Window – Large` ■ `Window – Small` Ce paramètre n'est disponible que lorsque le paramètre `DesktopName to select setting` est également défini.
`DesktopName to select`	Spécifie le poste de travail par défaut proposé par Horizon Client lors de la connexion.
`Disable 3rd-party Terminal Services plugins`	Détermine si 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,Horizon Client vérifie les plug-ins tiers par défaut. Ce paramètre n'affecte pas les plug-ins spécifiques d'Horizon, comme la redirection USB.
`Locked Guest Size`	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. **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 Horizon Administrator : ■ 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. 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 1 920 x 1 200 dans Horizon Administrator, la résolution indiquée sur le client risque de ne pas être supérieure à 1 920 x 1 200, selon les possibilités du poste de travail distant.
`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. Pour une sécurité améliorée, il est recommandé de ne pas spécifier ce paramètre. Les utilisateurs peuvent entrer le mot de passe de façon interactive.
`Logon UserName`	Spécifie le mot de passe utilisé par Horizon Client lors de la connexion. Active Directory stocke ce mot de passe en texte brut.
`Server URL`	Spécifie l'URL utilisée par Horizon Client lors de la connexion. Par exemple, `https://view1.example.com`.

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

Paramètre	Description
`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.
`Disconnected application session resumption behavior`	Détermine comment les applications en cours se comportent lorsque des utilisateurs se reconnectent à un serveur. Les choix sont les suivants : ■ Demander la reconnexion pour ouvrir des applications ■ Se reconnecter automatiquement pour ouvrir des applications ■ Ne pas demander et ne pas se reconnecter automatiquement Lorsque ce paramètre est activé, les utilisateurs finaux ne peuvent pas configurer le comportement de reconnexion d'applications sur la page Paramètres dans Horizon Client. Lorsque ce paramètre est désactivé, les utilisateurs finaux peuvent configurer le comportement de reconnexion d'applications dans Horizon Client. Ce paramètre est désactivé par défaut.
`Enable Unauthenticated Access to the server`	Détermine si des utilisateurs doivent entrer des informations d'identification pour accéder à leurs applications lorsqu'ils utilisent Horizon Client. Lorsque ce paramètre est activé, le paramètre **Se connecter de manière anonyme à l'aide de l'accès non authentifié** dans Horizon Client est affiché, désactivé et sélectionné. Le client peut revenir à une autre méthode d'authentification si l'accès non authentifié n'est pas disponible. Lorsque ce paramètre est désactivé, les utilisateurs doivent toujours entrer leurs informations d'identification pour se connecter et accéder à leurs applications. Le paramètre **Se connecter de manière anonyme à l'aide de l'accès non authentifié** dans Horizon Client est masqué et désélectionné. Lorsque ce paramètre n'est pas configuré (par défaut), les utilisateurs peuvent activer l'accès non authentifié dans Horizon Client. Le paramètre **Se connecter de manière anonyme à l'aide de l'accès non authentifié** est affiché, activé et désélectionné.
`Account to use for Unauthenticated Access`	Spécifie le compte d'utilisateur Accès non authentifié qu'Horizon Client utilise pour se connecter de manière anonyme au serveur si le paramètre de stratégie de groupe `Enable Unauthenticated Access to the server` est activé ou si un utilisateur active l'accès non authentifié en sélectionnant **Se connecter de manière anonyme à l'aide de l'accès non authentifié** dans Horizon Client. Si l'accès non authentifié n'est pas utilisé pour une connexion spécifique à un serveur, ce paramètre est ignoré. Lorsque ce paramètre n'est pas configuré, les utilisateurs peuvent choisir un compte. Ce paramètre n'est pas configuré par défaut.

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 ADMX de configuration d'Horizon Client. Ce tableau montre si les paramètres incluent à la fois les paramètres Configuration ordinateur et Configuration utilisateur, ou uniquement les paramètres 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. Ces paramètres se trouvent dans le dossier **Configuration de VMware Horizon Client > Paramètres de sécurité** de l'Éditeur de gestion de stratégie de groupe.

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

Paramètre	Ordinateur	Utilisateur	Description
`Allow command line credentials`	X		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 `smartCardPIN` et `password` 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 `AllowCmdLineCredentials`.
`Servers Trusted For Delegation`	X		Spécifie les instances du Serveur de connexion qui acceptent l'identité de l'utilisateur et les informations d'identification qui sont transmises lorsqu'un utilisateur sélectionne **Se connecter en tant qu'utilisateur actuel** dans le menu **Options** de la barre de menus Horizon Client. Si vous ne spécifiez aucune instance de Serveur de connexion, toutes les instances de Serveur de connexion acceptent ces informations. Pour ajouter une instance de Serveur de connexion, utilisez l'un des formats suivants : ■ **`domain\system$`** ■ **`system$@domain.com`** ■ Nom principal de service (SPN) du service Serveur de connexion. La valeur de Registre Windows équivalente est `BrokersTrustedForDelegation`.

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

Paramètre	Ordinateur	Utilisateur	Description
`Certificate verification mode`	X		Configure le niveau de la vérification de certificat exécutée par Horizon Client. Vous pouvez sélectionner l'un de ces modes : ■ `No Security`. Horizon n'effectue pas la vérification de certificat. ■ `Warn But Allow`. Un certificat auto-signé est fourni par Horizon. Dans ce cas, il est acceptable si son nom ne correspond pas à celui du Serveur de connexion fourni par l'utilisateur dans Horizon Client. Si une autre condition d'erreur de certificat se produit, Horizon affiche une boîte de dialogue d'erreur et empêche l'utilisateur de se connecter au Serveur de connexion. `Warn But Allow` est la valeur par défaut. ■ `Full Security`. Si une erreur de type de certificat se produit, l'utilisateur ne peut pas se connecter au Serveur de connexion. Horizon affiche des erreurs de certificat à l'utilisateur. 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. Lorsque ce paramètre n'est pas configuré ou est désactivé, les utilisateurs d'Horizon Client peuvent sélectionner un mode de vérification de certificat. Pour autoriser un serveur à vérifier les certificats fournis par Horizon Client, le client doit établir des connexions HTTPS avec l'hôte du Serveur de connexion 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 du Serveur de connexion ou du serveur de sécurité. Si vous ne souhaitez 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 : ■ 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 `No Security`. ■ **`1`** implémente `Warn But Allow`. ■ **`2`** implémente `Full Security`. 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. **Remarque** Dans une version ultérieure, il se peut que la configuration de ce paramètre à l'aide du registre Windows ne soit plus prise en charge. Vous devez utiliser un paramètre GPO.

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

Paramètre	Ordinateur	Utilisateur	Description
`Default value of the 'Log in as current user' checkbox`	X	X	Spécifie la valeur par défaut de **Se connecter en tant qu'utilisateur actuel** dans le menu **Options** de la barre de menus Horizon Client. Ce paramètre remplace la valeur par défaut spécifiée au cours de l'installation d'Horizon Client. Si un utilisateur exécute Horizon Client à partir de la ligne de commande et spécifie l'option `logInAsCurrentUser`, cette valeur remplace ce paramètre. Lorsque l'option **Se connecter en tant qu'utilisateur actuel** est sélectionnée dans le menu **Options**, 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, puis à l'application ou au poste de travail distant. Lorsque l'option **Se connecter en tant qu'utilisateur actuel** est désélectionnée, les utilisateurs doivent fournir leur identité et leurs informations d'identification plusieurs fois avant de pouvoir accéder à une application ou un poste de travail distant. Ce paramètre est désactivé par défaut. La valeur de Registre Windows équivalente est `LogInAsCurrentUser`.
`Display option to Log in as current user`	X	X	Détermine si **Se connecter en tant qu'utilisateur actuel** est visible dans le menu **Options** de la barre de menus Horizon Client. Lorsque l'option **Se connecter en tant qu'utilisateur actuel** est visible, les utilisateurs peuvent sélectionner ou désélectionner cette option et remplacer sa valeur par défaut. Lorsque l'option **Se connecter en tant qu'utilisateur actuel** est masquée, les utilisateurs ne peuvent pas remplacer sa valeur par défaut dans le menu **Options** d'Horizon Client. Vous pouvez spécifier la valeur par défaut de **Se connecter en tant qu'utilisateur actuel** en utilisant le paramètre de stratégie `Default value of the 'Log in as current user' checkbox`. Ce paramètre est activé par défaut. La valeur de Registre Windows équivalente est `LogInAsCurrentUser_Display`.
`Enable jump list integration`	X		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 de raccourcis permet aux utilisateurs de se connecter à des instances du Serveur de connexion et des postes de travail récents. 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. Ce paramètre est activé par défaut. La valeur de Registre Windows équivalente est `EnableJumplist`.

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

Paramètre	Ordinateur	Utilisateur	Description
`Enable SSL encrypted framework channel`	X	X	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. ■ **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. La valeur de Registre Windows équivalente est `EnableTicketSSLAuth`.
`Configures SSL protocols and cryptographic algorithms`	X	X	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. **Remarque** La chaîne de chiffrement est sensible à la casse. La chaîne de chiffrement par défaut est **TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES**. Cela signifie que TLS v1, TLS v1.1 et TLS v1.2 sont activés. (SSL v2.0 et v3.0 sont supprimés.) 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. Lien de référence pour la configuration : http://www.openssl.org/docs/apps/ciphers.html . La valeur de Registre Windows équivalente est `SSLCipherList`.
`Enable Single Sign-On for smart card authentication`	X		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. Lorsque l'authentification unique (Single Sign-On) est désactivée, Horizon Client n'affiche pas de boîte de dialogue de code PIN personnalisée. La valeur de Registre Windows équivalente est `EnableSmartCardSSO`.

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

Paramètre	Ordinateur	Utilisateur	Description
`Ignore certificate revocation problems`	X	X	Détermine si les erreurs associées à un certificat de serveur révoqué sont ignorées. Ces erreurs se produisent lorsque le certificat que le serveur envoie a été révoqué ou que le client ne peut pas vérifier l'état de révocation du certificat. Ce paramètre est désactivé par défaut.
`Unlock remote sessions when the client machine is unlocked`	X	X	Détermine si la fonctionnalité Déverrouillage récursif est activée. Cette fonctionnalité déverrouille toutes les sessions distantes après que la machine cliente a été déverrouillée. Cette fonctionnalité s'applique uniquement après qu'un utilisateur s'est connecté au serveur en tant qu'utilisateur actuel. Ce paramètre est activé par défaut.

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 ADMX de configuration d'Horizon Client. Tous les paramètres RDP sont des paramètres de Configuration d'utilisateur. Les paramètres se trouvent dans le dossier **Configuration de VMware Horizon Client > Paramètres RDP** dans l'Éditeur de gestion de stratégie de groupe.

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 : ■ **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 mégaoctets, 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 : ■ Mo/8 bpp ■ Mo/16 bpp ■ Mo/24 bpp ■ Mo/32 bpp

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

Paramètre	Description
`In-memory bitmap cache size in KB for 8bpp bitmaps`	Spécifie la taille, en kilo-octets, du cache d'images bitmap de la RAM à utiliser pour le paramètre de couleur à 8 bits par pixel. Si ScaleBitmapCachesByBPP a la valeur true (par défaut), cette taille de cache est multipliée par le nombre d'octets par pixel pour déterminer la taille réelle du cache de la RAM. Lorsque ce paramètre est activé, entrez une taille en kilo-octets.
`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.
`Color depth`	Spécifie l'intensité des couleurs du poste de travail distant. Sélectionnez l'un des paramètres disponibles : ■ 8 bits ■ 15 bits ■ 16 bits ■ 24 bits ■ 32 bits 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.
`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`	(Windows Vista ou version ultérieure) Détermine si la composition du poste de travail doit être activée sur le poste de travail distant. 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.
`Enable compression`	Détermine si les données RDP sont compressées. Ce paramètre est activé par défaut.
`Enable RDP Auto-Reconnect`	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 **Utiliser une connexion par tunnel sécurisé vers le poste de travail** est activée dans Horizon Administrator. Ce paramètre est désactivé par défaut.
`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.

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

Paramètre	Description
`Redirect drives`	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. 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`. Le paramètre `Redirect drives` ne s'applique qu'à RDP.
`Redirect printers`	Détermine si les imprimantes locales doivent être redirigées lorsque des clients se connectent au poste de travail distant.
`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 de l'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.
`Enable Credential Security Service Provider`	Spécifie si la connexion Bureau à distance doit utiliser l'authentification au niveau du réseau (NLA). Sous Windows Vista, les connexions de poste de travail à distance requièrent la NLA par défaut. Si le système d'exploitation invité nécessite l'authentification au niveau du réseau pour les connexions de poste de travail distant, vous devez activer ce paramètre de sorte qu'Horizon Client soit en mesure de se connecter au poste de travail distant. En plus d'activer ce paramètre, vous devez également vérifier que les conditions suivantes sont satisfaites : ■ Le client et le système d'exploitation client prennent en charge la NLA. ■ Les connexions client directes sont activées pour l'instance du Serveur de connexion. Les connexions par tunnel ne sont pas prises en charge avec la NLA.

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 ADMX de 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. Les paramètres se trouvent dans le dossier **Configuration de VMware Horizon Client** de l'Éditeur de gestion de stratégie de groupe.

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

Paramètre	Ordinateur	Utilisateur	Description
`Always on top`		X	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`	X	X	Définit si la case **Masquer le sélecteur après le lancement d'un élément** est cochée par défaut. Ce paramètre est désactivé par défaut.
`Disable time zone forwarding`	X		Détermine si la synchronisation de fuseau horaire entre le poste de travail distant et le client connecté doit être désactivée.
`Disable toast notifications`	X	X	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.
`Disallow passing through client information in a nested session`	X		Spécifie s'il faut empêcher Horizon Client de transférer les informations du client dans une session imbriquée. Lorsqu'il est activé, si Horizon Client est en cours d'exécution dans une session Horizon, il enverra les informations physiques réelles du client au lieu des informations du périphérique de machine virtuelle. Ce paramètre s'applique aux informations du client suivantes : domaine et nom du périphérique, type de client, adresse IP et adresse MAC. Ce paramètre est désactivé par défaut, ce qui signifie que le transfert d'informations du client dans une session imbriquée est autorisé.
`Don't check monitor alignment on spanning`		X	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`		X	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.

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

Paramètre	Ordinateur	Utilisateur	Description
`Enable relative mouse`	X	X	(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`		X	Détermine si le 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.
`Enable Horizon Client online update`	X		Active la fonctionnalité de mise à niveau en ligne. Ce paramètre est désactivé par défaut.
`Tunnel proxy bypass address list`	X		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 Horizon Client online help`	X		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.
`Pin the shade`		X	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`	X	X	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.
`Disable sharing files and folders`		X	Spécifie si la fonctionnalité de redirection du lecteur client est disponible dans Horizon Client. Lorsque ce paramètre est défini sur Activé, toute la fonctionnalité de redirection du lecteur client est désactivée dans Horizon Client, notamment la capacité d'ouvrir des fichiers locaux avec des applications distantes. De plus, les éléments suivants sont masqués dans l'interface utilisateur d'Horizon Client : ■ Partage de volet dans la boîte de dialogue Paramètres ■ Élément **Partager les dossiers** dans le menu **Option** dans un poste de travail distant ■ Élément **Partage** pour Horizon Client dans la barre d'état système ■ Boîte de dialogue Partage qui s'affiche la première fois que vous vous connectez à une application ou un poste de travail distant après vous être connecté à un serveur Lorsque ce paramètre est défini sur Désactivé, la fonctionnalité de redirection du lecteur client est entièrement opérationnelle. Si ce paramètre n'est pas configuré, la valeur par défaut est Désactivé. Ce paramètre n'est pas configuré par défaut.
`Always hide the remote floating language (IME) bar for Hosted Apps`	X	X	Force la barre de langue flottante à disparaître pour les sessions d'application. Lorsque ce paramètre est activé, la barre de langue flottante n'est jamais affichée dans une session d'application distante, que la fonctionnalité IME local soit activée ou non. Lorsque ce paramètre est désactivé, la barre de langue flottante n'est affichée que si la fonctionnalité IME local est désactivée. Ce paramètre est désactivé par défaut.

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

Paramètre	Ordinateur	Utilisateur	Description
`Put icon cache in user's Local profile folder`	X		Spécifie si Horizon Client place ses fichiers de cache des icônes dans le dossier `Local` de l'utilisateur plutôt que dans le dossier `Itinérance` utilisé précédemment. Lorsque ce paramètre est défini sur Activé, Horizon Client place ses fichiers de cache des icônes dans le dossier `Local` de l'utilisateur. Lorsque vous démarrez Horizon Client pour la première fois, il déplace ses fichiers de cache existants du dossier `Itinérance` vers le dossier `Local` et place les nouveaux fichiers de cache dans le dossier `Local`. L'activation de cette stratégie peut permettre d'améliorer le temps de réponse d'applications distantes lorsque des profils d'itinérance sont utilisés pour empêcher la synchronisation des fichiers de cache. Si ce paramètre n'est pas configuré, la valeur par défaut est Désactivé. Ce paramètre n'est pas configuré par défaut.
`Disable opening local files in hosted applications`		X	Spécifie si Horizon Client enregistre des gestionnaires locaux pour les extensions de fichier que les applications hébergées prennent en charge. Lorsque ce paramètre est défini sur Activé, Horizon Client n'enregistre aucun gestionnaire d'extension de fichier et n'autorise pas l'utilisateur à remplacer le paramètre. Lorsque ce paramètre est défini sur Désactivé, Horizon Client enregistre toujours les gestionnaires d'extension de fichier. Par défaut, les gestionnaires d'extension de fichier sont enregistrés, mais les utilisateurs peuvent désactiver la fonctionnalité dans l'interface utilisateur d'Horizon Client en utilisant le paramètre **Activer la fonction permettant d'ouvrir un fichier local avec une application distante depuis le système de fichiers local** sur le volet Partage dans la boîte de dialogue Paramètres. Pour plus d'informations, reportez-vous à la section « Partager l'accès aux dossiers et lecteurs locaux », page 81. Si ce paramètre n'est pas configuré, la valeur par défaut est Désactivé. Ce paramètre n'est pas configuré par défaut.
`Redirect smart card readers in Local Mode`	X		Le mode local n'est pas pris en charge dans cette version.
`Delay the start of replications when starting Horizon Client with Local Mode`	X		Le mode local n'est pas pris en charge dans cette version.
`Default Exit Behavior For Local Mode Desktops`		X	Le mode local n'est pas pris en charge dans cette version.

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

Vous pouvez définir des paramètres de stratégie USB pour l'agent et pour Horizon Client pour Windows. Lors de la connexion, Horizon Client télécharge les paramètres de stratégie USB depuis l'agent et les utilise avec les paramètres de stratégie USB d'Horizon Client, afin de décider des périphériques qu'il va rendre disponibles pour la redirection depuis la machine hôte.

Le tableau suivant décrit chaque paramètre de stratégie pour le fractionnement de périphériques USB composite situé dans le fichier de modèle d'administration ADMX de 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`. Les paramètres se trouvent dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'Éditeur de gestion de stratégie de groupe.

Pour voir une description de la façon dont Horizon applique les stratégies pour le fractionnement de périphériques USB composites, consultez les rubriques sur l'utilisation de stratégies pour contrôler la redirection USB dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

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

Paramètre	Propriétés
`Allow Auto Device Splitting`	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 `vid-`*xxx1*`_pid-`*yyy2*`[;vid-`*xxx2*`_pid-`*yyy2*`]…` Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (**`*`**) à la place de chiffres dans un ID. Par exemple : **`vid-0781_pid-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 `vid-`*xxxx*`_pid-`*yyyy*`(exintf:`*zz*`[;exintf:`*ww*` ])` Vous pouvez utiliser le mot-clé **`exintf`** pour exclure des composants de la redirection en spécifiant leur numéro d'interface. Vous devez spécifier les numéros d'ID au format hexadécimal et les numéros d'interface au format décimal en incluant les zéros à gauche. Vous pouvez utiliser le caractère générique (**`*`**) à la place de chiffres dans un ID. Par exemple : **`vid-0781_pid-554c(exintf:01;exintf:02)`** **Remarque** Horizon n'inclut pas automatiquement les composants que vous n'avez pas explicitement exclus. Vous devez spécifier une règle de filtre telle que `Include Vid/Pid Device` pour inclure ces composants. La valeur par défaut n'est pas définie.

Le tableau suivant décrit chaque paramètre de stratégie de filtrage des périphériques USB situé dans le fichier de modèle ADMX de 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 voir une description de la façon dont Horizon applique les stratégies pour le filtrage de périphériques USB, consultez les rubriques sur la configuration de paramètres de stratégie de filtre pour la redirection USB dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

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`**. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'Éditeur de gestion de stratégie de groupe.
`Allow Audio Output Devices`	Permet la redirection de périphériques de sortie audio. La valeur par défaut est indéfinie, ce qui correspond à **`false`**. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'Éditeur de gestion de stratégie de groupe.
`Allow HID-Bootable`	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`**. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'Éditeur de gestion de stratégie de groupe.
`Allow Device Descriptor Failsafe Behavior`	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`**. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB > Paramètres non configurables par Agent** de l'Éditeur de gestion de stratégie de groupe.
`Allow Other Input Devices`	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`**. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'Éditeur de gestion de stratégie de groupe.
`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`**. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'Éditeur de gestion de stratégie de groupe.
`Allow Smart Cards`	Permet la redirection de périphériques à carte à puce. La valeur par défaut est indéfinie, ce qui correspond à **`false`**. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'Éditeur de gestion de stratégie de groupe.
`Allow Video Devices`	Permet la redirection de périphériques vidéo. La valeur par défaut est indéfinie, ce qui correspond à **`true`**. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'Éditeur de gestion de stratégie de groupe.
`Disable Remote Configuration`	Désactive l'utilisation des paramètres de l'agent lors de l'exécution du filtrage des périphériques USB. La valeur par défaut est indéfinie, ce qui correspond à **`false`**. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB > Paramètres non configurables par Agent** de l'Éditeur de gestion de stratégie de groupe.

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

Paramètre	Propriétés
`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 l'agent, et si ce paramètre est transmis à Horizon Client, le paramètre de l'agent remplace celui d'Horizon Client. La valeur par défaut est indéfinie, ce qui correspond à **`false`**. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'Éditeur de gestion de stratégie de groupe.
`Exclude Device Family`	Exclut des familles de périphériques de la redirection. Le format du paramètre est *family_name_1*[`;`*family_name_2*]… Par exemple : **`bluetooth;smart-card`** Si vous avez activé le fractionnement automatique de périphérique, Horizon examine la famille de périphériques de chaque interface d'un périphérique USB composite pour décider quelles interfaces doivent être exclues. Si vous avez désactivé le fractionnement automatique de périphérique, Horizon examine la famille de périphérique de l'ensemble du périphérique USB composite. La valeur par défaut n'est pas définie. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'Éditeur de gestion de stratégie de groupe.
`Exclude Vid/Pid Device`	Exclut des périphériques avec des ID de fournisseur et de produit spécifiés de la redirection. Le format du paramètre est `vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]… Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (**`*`**) à la place de chiffres dans un ID. Par exemple : **`vid-0781_pid-****;vid-0561_pid-554c`** La valeur par défaut n'est pas définie. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'Éditeur de gestion de stratégie de groupe.
`Exclude Path`	Exclut des périphériques dans des chemins de concentrateur ou de port spécifiés de la redirection. Le format du paramètre est `bus-`*x1*[*/y1*]`.../port-`*z1*[`;bus-`*x2*[*/y2*]`.../port-`*z2*] … Vous devez spécifier des numéros de bus et de port au format hexadécimal. Vous ne pouvez pas utiliser le caractère générique dans les chemins. Par exemple : **`bus-1/2/3_port-02;bus-1/1/1/4_port-ff`** La valeur par défaut n'est pas définie. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB > Paramètres non configurables par Agent** de l'Éditeur de gestion de stratégie de groupe.
`Include Device Family`	Inclut des familles de périphériques pouvant être redirigées. Le format du paramètre est *family_name_1*[`;`*family_name_2*]… Par exemple : **`storage`** La valeur par défaut n'est pas définie. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'Éditeur de gestion de stratégie de groupe.

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

Paramètre	Propriétés
`Include Path`	Inclut des périphériques dans des chemins de concentrateur ou de port spécifiés pouvant être redirigés. Le format du paramètre est `bus-`*x1*`[/`*y1*`]…/port-`*z1*`[;bus-`*x2*`[/`*y2*`]…/port-`*z2*`]…` Vous devez spécifier des numéros de bus et de port au format hexadécimal. Vous ne pouvez pas utiliser le caractère générique dans les chemins. Par exemple : **`bus-1/2_port-02;bus-1/7/1/4_port-0f`** La valeur par défaut n'est pas définie. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB > Paramètres non configurables par Agent** de l'Éditeur de gestion de stratégie de groupe.
`Include Vid/Pid Device`	Inclut des périphériques avec des ID de fournisseur et de produit spécifiés pouvant être redirigés. Le format du paramètre est `vid-`*xxx1*`_pid-`*yyy2*`[;vid-`*xxx2*`_pid-`*yyy2*`]…` Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (`*`) à la place de chiffres dans un ID. Par exemple : **`vid-0561_pid-554c`** La valeur par défaut n'est pas définie. Ce paramètre se trouve dans le dossier **Configuration de VMware Horizon Client > Afficher la configuration USB** de l'Éditeur de gestion de stratégie de groupe.

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

Le fichier de modèle d'administration ADMX pour les variables de session de client PCoIP (`pcoip.client.admx`) contient des paramètres de stratégie liés au protocole d'affichage PCoIP. Vous pouvez configurer les paramètres avec les valeurs par défaut de l'ordinateur qui peuvent être remplacées par un administrateur. Vous pouvez aussi configurer les paramètres utilisateur avec des valeurs ne pouvant pas être remplacées. Les paramètres qui peuvent être remplacés se trouvent dans le dossier des **Variables de session de client PCoIP > Valeurs par défaut remplaçables par l'administrateur** de l'Éditeur de gestion de stratégie de groupe. Les paramètres qui ne peuvent pas être remplacés se trouvent dans le dossier **Variables de session de client PCoIP > Valeurs par défaut remplaçables par l'administrateur** de l'Éditeur de gestion de stratégie de groupe.

Les fichiers ADMX sont disponibles dans un fichier groupé `.zip` nommé `VMware-Horizon-Extras-Bundle-`*x.x.x-yyyyyyy*`.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 7, qui inclut le fichier groupé `.zip`.

Tableau 3-10. Variables de session de client PCoIP

Paramètre	Description
`Configure PCoIP client image cache size policy`	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. 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. 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.
`Configure PCoIP event log verbosity`	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). 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. Lorsque ce paramètre est modifié lors d'une session PCoIP active, le nouveau paramètre prend effet immédiatement.

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

Paramètre	Description
`Configure PCoIP session encryption algorithms`	Contrôle les algorithmes de cryptage annoncés par le point de terminaison PCoIP lors de la négociation de session. Cocher l'une des cases désactive l'algorithme de cryptage associé. Vous devez activer au moins un algorithme. 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 **Désactiver le chiffrement AES-128-GCM** sera remplacée si les chiffrements AES-128-GCM et AES-256-GCM sont désactivés. Si le paramètre `Configure SSL Connections` est désactivé ou n'est pas configuré, les deux algorithmes Salsa20-256round12 et AES-128-GCM sont disponibles pour la négociation par ce point de terminaison. Les algorithmes de chiffrement pris en charge, par ordre de préférence, sont SALSA20/12-256, AES-GCM-128 et AES-GCM-256. Par défaut, tous les algorithmes de chiffrement pris en charge sont disponibles à la négociation à partir de ce point de terminaison.
`Configure PCoIP virtual channels`	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. 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. Vous pouvez spécifier un maximum de 15 canaux virtuels à utiliser dans des sessions PCoIP. 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`**. 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`**. 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. 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. 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. Par défaut, tous les canaux virtuels sont activés, notamment le traitement du presse-papier.
`Configure the Client PCoIP UDP port`	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. 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. Ce paramètre ne s'applique qu'au client. Par défaut, le port de base est 50002 et la plage du port est 64.

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

Paramètre	Description
`Configure the maximum PCoIP session bandwidth`	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. 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. Cependant, la diminution de cette valeur limitera la bande passante maximale de chaque session active. 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. 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. La valeur par défaut lorsque ce paramètre n'est pas configuré est de 900000 kilobits par seconde. Ce paramètre s'applique à la fois à l'agent et au client. Si les deux points de terminaison ont des paramètres différents, la valeur la plus faible est utilisée.
`Configure the PCoIP transport header`	Configure l'en-tête de transport PCoIP et définit la priorité de la session de transport. 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. 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. Lorsque le paramètre `Configure the PCoIP transport header` est activé, les priorités de session de transport suivantes sont disponibles : ■ **Haute** ■ **Moyenne** (valeur par défaut) ■ **Basse** ■ **Non définie** 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**.
`Enable/disable audio in the PCoIP session`	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.

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

Paramètre	Description
`Configure the PCoIP session bandwidth floor`	Spécifie une limite inférieure, en kilobits par seconde, pour la bande passante réservée par la session PCoIP. 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. 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. 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. Ce paramètre s'applique à l'agent et au client, mais le paramètre n'affecte que le point de terminaison sur lequel il est configuré. Lorsque ce paramètre est modifié lors d'une session PCoIP active, la modification prend effet immédiatement.
`Configure the PCoIP session MTU`	Spécifie la taille de l'unité de transmission maximale (MTU) pour les paquets UDP d'une session PCoIP. 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. 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. 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. Ce paramètre s'applique à la fois à l'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. Si ce paramètre est désactivé ou qu'il n'est pas configuré, le client utilise la valeur par défaut dans la négociation avec l'agent.
`Configure SSL connections to satisfy Security Tools`	Spécifie comment les connexions de négociation de session SSL sont établies. Pour satisfaire les outils de sécurité, tels que les scanners de ports, activez ce paramètre et procédez comme suit : 1 Stockez le certificat de l'autorité de certification ayant signé un certificat du serveur afin qu'il soit utilisé avec PCoIP dans le magasin de certificats racines approuvés. 2 Configurez l'agent afin qu'il charge des certificats uniquement à partir du magasin de certificats. Si le magasin personnel de la machine locale est utilisé, laissez le nom du magasin de certificats de l'autorité de certification avec la valeur « ROOT », sauf si un emplacement de magasin différent a été utilisé dans l'étape 1. Si ce paramètre est désactivé ou n'a pas été configuré, la suite de chiffrement AES-128 n'est pas disponible. Le point de terminaison utilise alors les certificats de l'autorité de certification du magasin MY du compte de la machine et les certificats de l'autorité de certification du magasin ROOT.
`Configure SSL protocols`	Configure le protocole OpenSSL pour limiter l'utilisation de certains protocoles avant l'établissement d'une connexion SSL chiffrée. La liste de protocoles est composée d'une ou de plusieurs chaînes de protocole OpenSSL séparées par des caractères deux-points. Toutes les chaînes de chiffrement sont insensibles à la casse. La valeur par défaut est : `TLS1.1:TLS1.2`. Cela signifie que TLS v1.1 et TLS v1.2 sont activés et que SSL v2.0, SSL v3.0 et TLS v1.0 sont désactivés. Si ce paramètre est défini dans le client et l'agent, la règle de négociation du protocole OpenSSL est suivie.

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

Paramètre	Description
`Configure PCoIP event log cleanup by time in days`	Active la configuration du nettoyage du journal des événements PCoIP par durée en jours. Lorsque ce paramètre est configuré, il contrôle le nettoyage des fichiers journaux en fonction de la durée en jours. Par exemple, pour une valeur de *n* différente de zéro, les fichiers journaux antérieurs à *n* jours sont supprimés en mode silencieux. La valeur 0 indique qu'aucun nettoyage de fichier en fonction de la durée n'est effectué. Lorsque cette stratégie est désactivée ou qu'elle n'a pas été configurée, la valeur par défaut du nettoyage du journal des événements en fonction de la durée en jours est de 7. Le nettoyage du fichier journal s'effectue une seule fois au démarrage d'une session. Toute modification apportée au paramètre n'est appliquée qu'à l'ouverture de la prochaine session.
`Configure PCoIP event log cleanup by size in MB`	Active la configuration du nettoyage du journal des événements PCoIP par taille en Mo. Lorsque ce paramètre est configuré, il contrôle le nettoyage des fichiers journaux en fonction de la taille en Mo. Par exemple, pour une valeur de *m* différente de zéro, les fichiers journaux dont la taille est plus importante que *m* Mo sont supprimés en mode silencieux. La valeur 0 indique qu'aucun nettoyage de fichier en fonction de la taille n'est effectué. Lorsque cette stratégie est désactivée ou qu'elle n'a pas été configurée, la valeur par défaut du nettoyage du journal des événements en fonction de la taille en Mo est de 100.

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` à partir d'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
`/?`	Affiche la liste d'options de commande.
`-appName` *application_name*	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.
`-appProtocol` *protocol*	Spécifie le protocole d'affichage de l'application distante à utiliser, si disponible. Le protocole d'affichage peut être Blast ou PCoIP.

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

Option	Description
argument `-appSessionReconnectionBehavior`	Spécifie le paramètre de comportement de reconnexion d'applications. ■ `always` implémente **Se reconnecter automatiquement pour ouvrir des applications** ■ `never` implémente **Ne pas demander la reconnexion et ne pas se reconnecter automatiquement** ■ `ask` implémente **Demander la reconnexion pour ouvrir des applications** Lorsque vous utilisez cette option, les paramètres de reconnexion d'application sont désactivés sur la page Paramètres dans Horizon Client.
argument `-args`	Spécifie des arguments de ligne de commande à ajouter au lancement d'applications distantes. Par exemple : `vmware-view.exe --serverURL 10.10.10.10 --appName "My Notepad++" --args "\"my new.txt\""`
`-connectUSBOnStartup`	Lorsqu'elle est définie sur `true`, 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 `-unattended`. L'option par défaut est `false`.
`-connectUSBOnInsert`	Lorsqu'elle est définie sur `true`, 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 `-unattended`. L'option par défaut est `false`.
`-desktopLayout` *window_size*	Spécifie l'affichage de la fenêtre pour le poste de travail : **`fullscreen`** Affichage en plein écran. **`multimonitor`** Affichage sur plusieurs moniteurs. **`windowLarge`** Fenêtre de grande taille. **`windowSmall`** Fenêtre de petite taille. **`length X width`** Taille personnalisée. Par exemple : 800 x 600
`-desktopName` *desktop_name*	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.
`-desktopProtocol` *protocol*	Spécifie le protocole d'affichage à utiliser comme il apparaît dans la fenêtre de sélection des postes de travail et applications. Le protocole d'affichage peut être Blast, PCoIP ou RDP.
`-domainName` *domain_name*	Spécifie le domaine NETBIOS que l'utilisateur final utilise pour ouvrir une session d'Horizon Client. Utilisez par exemple `monentreprise` plutôt que `monentreprise.com`.
`-file` *file_path*	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 72.
`-h`	Affiche les options de l'aide.
`-hideClientAfterLaunchSession`	Lorsque cette option est définie sur `true`, cela masque la fenêtre de sélection des applications et des postes de travail distants ainsi que le menu **Afficher VMware Horizon Client** après le lancement d'une session distante. Lorsque cette option est définie sur `false`, cela affiche la fenêtre de sélection des applications et des postes de travail distants ainsi que le menu **Afficher VMware Horizon Client** après le lancement d'une session distante. L'option par défaut est `true`.

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

Option	Description
`–languageId` *Locale_ID*	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.

`–listMonitors`	Répertorie les valeurs d'index et les informations de disposition de l'affichage des moniteurs connectés. Par exemple :
	`1: (0, 0, 1920, 1200)`
	`2: (1920, 0, 3840, 1200)`
	`3: (–900, –410, 0, 1190)`
	Vous pouvez utiliser les valeurs d'index dans l'option `–monitors`.

`–logInAsCurrentUser`	Lorsqu'elle est définie sur `true`, 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 du Serveur de connexion, puis sur le poste de travail distant. L'option par défaut est `false`.
`–monitors "`*n*`[,`*n*`,`*n*`,`*n*`]"`	Spécifie les moniteurs à utiliser dans une configuration à plusieurs moniteurs, où *n* est la valeur d'index d'un moniteur. Vous pouvez utiliser l'option `–listMonitors` pour déterminer les valeurs d'index des moniteurs connectés. Vous pouvez spécifier jusqu'à quatre valeurs d'index, séparées par des virgules. Par exemple : **`–monitors "1,2"`** Cette option n'a pas d'effet tant que `–desktopLayout` n'est pas défini sur `multimonitor`.
`–nonInteractive`	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 `–unattended`.
`–noVMwareAddins`	Empêche le chargement de canaux virtuels spécifiques de VMware tels que l'impression virtuelle.
`–password` *password*	Spécifie le mot de passe que l'utilisateur final utilise pour ouvrir une session d'Horizon Client. La console de commande ou tout outil de script traite le mot de passe en texte brut. Vous n'avez pas à spécifier cette option pour des clients en mode kiosque si vous générez le mot de passe automatiquement. Pour une sécurité améliorée, il est recommandé de ne pas spécifier cette option. Les utilisateurs peuvent entrer le mot de passe de façon interactive.
`–printEnvironmentInfo`	Affiche l'adresse IP, l'adresse MAC et le nom de machine du périphérique client.
`–serverURL` *connection_server*	Spécifie l'URL, l'adresse IP ou le FQDN de l'instance du Serveur de connexion.
`–shutdown`	Arrête tous les postes de travail et applications ainsi que les composants d'interface utilisateur pertinents.
`–singleAutoConnect`	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.
`–smartCardPIN` *PIN*	Spécifie le code PIN lorsqu'un utilisateur final insère une carte à puce pour ouvrir une session.
`–usernameHint` *user_name*	Spécifie le nom de compte à utiliser comme aide-mémoire du nom d'utilisateur.

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

Option	Description
`–standalone`	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 `–standalone`. Lance une deuxième instance d'Horizon Client qui peut se connecter à la même ou à une autre instance du Serveur de connexion. Pour plusieurs connexions de postes de travail au même ou à un différent serveur, l'utilisation du tunnel sécurisé est prise en charge. **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.
`–supportText` *file_name*	Spécifie le chemin d'accès complet d'un fichier texte. Le contenu du fichier est affiché dans la boîte de dialogue Informations de support.
`–unattended`	Exécute Horizon Client dans un mode non interactif approprié aux clients en mode Kiosque. Vous devez également spécifier : ■ 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. L'option `–unattended` définit implicitement les options `–nonInteractive`, `–connectUSBOnStartup`, `–connectUSBOnInsert` et `–desktopLayout multimonitor`.
`–unauthenticatedAccessAccount`	Spécifie un compte d'utilisateur Accès non authentifié à utiliser pour se connecter de manière anonyme au serveur lorsque l'accès non authentifié est activé. Si l'accès non authentifié n'est pas activé, cette option est ignorée. Par exemple : `vmware–view.exe –serverURL ag–broker.agwork.com –unauthenticatedAccessEnabled true –unauthenticatedAccessAccount anonymous1`
`–unauthenticatedAccessEnabled`	Spécifie le comportement de l'accès non authentifié : ■ `true` active l'accès non authentifié. Le client peut revenir à une autre méthode d'authentification si l'accès non authentifié n'est pas disponible. Le paramètre **Se connecter de manière anonyme à l'aide de l'accès non authentifié** est affiché, désactivé et sélectionné dans Horizon Client. ■ `false` nécessite la saisie de vos informations d'identification pour vous connecter à vos applications et y accéder. Le paramètre **Se connecter de manière anonyme à l'aide de l'accès non authentifié** est masqué et désélectionné dans Horizon Client. Si vous ne spécifiez pas cette option, vous pouvez activer l'accès non authentifié dans Horizon Client. Le paramètre **Se connecter de manière anonyme à l'aide de l'accès non authentifié** est affiché, activé et désélectionné.

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

Option	Description

`–useExisting`	Vous permet de lancer plusieurs applications et postes de travail distants à partir d'une seule session Horizon Client.
	Lorsque vous spécifiez cette option, Horizon Client détermine si une session avec les mêmes nom d'utilisateur, domaine et URL de serveur existe déjà et, si c'est le cas, réutilise cette session au lieu d'en créer une.
	Par exemple, dans la commande suivante, user-1 lance l'application Calculatrice et une session est créée.
	`vmware–view.exe –userName user–1 –password secret –domainName domain –appName Calculator –serverURL view.mycompany.com –useExisting`
	Dans la commande suivante, user1 lance l'application Paint avec les mêmes nom d'utilisateur, domaine et URL de serveur, et la même session est utilisée.
	`vmware–view.exe –userName user–1 –password secret –domainName domain –appName Paint –serverURL view.mycompany.com –useExisting`

`–userName` *user_name*	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.

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

Remarque Les paramètres de stratégie de groupe prévalent sur ceux spécifiés dans la ligne de commande.

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 `–file`*file_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 paramètres de stratégie de groupe prévalent sur les paramètres de registre Windows, et les paramètres de registre Windows prévalent sur la ligne de commande.

Remarque Dans une version ultérieure, il se peut que les paramètres de registre Windows décrits dans cette section ne soient plus pris en charge. Vous devez utiliser les paramètres GPO.

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 `monentreprise` plutôt que `monentreprise.com`.
`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 par défaut par son URL, son adresse IP ou son FQDN.
`EnableSoftKeypad`	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`	Spécifie le mode de vérification de certificat. ■ **`0`** implémente `Do not verify server identity certificates`. ■ **`1`** implémente `Warn before connecting to untrusted servers`. ■ **`2`** implémente `Never connect to untrusted servers`.
`SSLCipherList`	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. **Remarque** Toutes les chaînes de chiffrement sont sensibles à la casse. La chaîne de chiffrement par défaut est **TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH +AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES**. Cela signifie que TLSv.1, TLSv1.1 et TLSv1.2 sont activés. (SSL v2.0 et v3.0 sont supprimés.) 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. Lien de référence pour la configuration : http://www.openssl.org/docs/apps/ciphers.html .

Gestion des connexions aux applications et postes de travail distants

4

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

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

Ce chapitre aborde les rubriques suivantes :

Connexion à une application ou un poste de travail distant

Après avoir ouvert une session sur un serveur, 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 devrez peut-être 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 6.0 ou version ultérieure.

La fonctionnalité **Se connecter en tant qu'utilisateur actuel** est disponible même si Horizon Client est installé sur un poste de travail distant.

Prérequis

- Procurez-vous les informations d'identification de connexion, telles que le nom d'utilisateur et le mot de passe, le nom d'utilisateur et le code secret RSA SecurID, le nom d'utilisateur et le code secret pour l'authentification RADIUS ou le numéro d'identification personnel (PIN) de carte à puce.
- Obtenez le nom de domaine NETBIOS pour ouvrir une session. Utilisez par exemple `monentreprise` plutôt que `monentreprise.com`.
- Effectuez les tâches administratives décrites dans « Préparation du Serveur de connexion pour Horizon Client », page 20.
- Si vous vous trouvez à l'extérieur du réseau d'entreprise et si vous n'utilisez pas de serveur de sécurité pour accéder à l'application ou au poste de travail distant, vérifiez que votre périphérique client est configuré pour utiliser une connexion VPN et activez cette connexion.

  Important Dans la plupart des cas, utilisez un serveur de sécurité plutôt qu'un VPN.

- Vérifiez que vous disposez du nom de domaine complet (FQDN) du serveur qui fournit l'accès à l'application ou au poste de travail distant. Les traits de soulignement (_) ne sont pas pris en charge dans les noms de serveur. Si le port n'est pas le port 443, vous avez également besoin du numéro de port.
- Si vous prévoyez d'utiliser le protocole d'affichage RDP pour vous connecter à un poste de travail distant, vérifiez que le paramètre de stratégie de groupe AllowDirectRDP de l'agent est activé.
- Si votre administrateur l'a autorisé, configurez le mode de vérification des certificats pour le certificat SSL présenté par le Serveur de connexion. Pour savoir quel mode utiliser, reportez-vous à la section « Définition du mode de vérification de certificats pour Horizon Client », page 45.

Procédure

1. Si une connexion VPN est requise, activez le VPN.
2. Double-cliquez sur le raccourci de bureau de **VMware Horizon Client** ou cliquez sur **Démarrer > Programmes > VMware Horizon Client**.
3. (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 ce paramètre uniquement si votre administrateur l'a autorisé.
4. (Facultatif) Pour vous connecter en tant qu'utilisateur de domaine Windows actuellement connecté, cliquez sur le bouton **Options** sur la barre de menus et sélectionnez **Se connecter en tant qu'utilisateur actuel**.

   Ce paramètre est disponible si la fonctionnalité **Se connecter en tant qu'utilisateur actuel** est installée sur votre système client.

5 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 ou d'un serveur de sécurité, puis cliquez sur **Connecter**.

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

Il est possible qu'un message de confirmation s'affiche avant l'affichage de la boîte de dialogue Connexion.

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

---

6 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**.

7 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 entrez le nom d'utilisateur au format **`nomutilisateur@domaine`**, le nom est traité comme un nom d'utilisateur principal (UPN) à cause du signe @ et le menu déroulant **Domaine** est désactivé.

Si le menu déroulant **Domaine** est masqué, vous devez entrer le nom d'utilisateur sous la forme ***`nomutilisateur@domaine`*** ou ***`domaine\nomutilisateur`***.

8 (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 la fenêtre.

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

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

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

10 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 publié qui est hébergé sur un hôte RDS Microsoft et si le poste de travail est déjà configuré pour utiliser un autre protocole d'affichage, vous ne pouvez pas vous connecter immédiatement. Vous êtes invité à utiliser le protocole actuellement configuré ou à demander au système de fermer votre session sur le 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.

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 81.

Si l'authentification sur le serveur 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 est configuré pour ne pas utiliser SSL. Le logiciel client nécessite des connexions SSL. Vérifiez si le paramètre général dans Horizon Administrator de la case **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 équilibrage de charge activé pour HTTPS ou à un autre périphérique intermédiaire configuré pour établir une connexion HTTP vers le Serveur de connexion.
- Vérifiez que le certificat de sécurité pour le Serveur de connexion fonctionne correctement. Si ce n'est pas le cas, dans Horizon Administrator, vous pouvez également voir que l'agent sur des postes de travail n'est pas accessible. Ces symptômes indiquent qu'il existe d'autres problèmes de connexion causés par des problèmes de certificat.
- Vérifiez que les balises définies sur l'instance du Serveur de connexion 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 des postes de travail virtuels dans Horizon 7* ou *Configuration d'applications et de postes de travail publiés dans Horizon 7*.
- 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 paramètres de démarrage. Si vous ne voulez pas que les utilisateurs finaux fournissent le nom d'hôte de l'instance du Serveur de connexion ou si vous voulez configurer d'autres paramètres 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 68.

Utiliser l'accès non authentifié pour se connecter à des applications distantes

Un administrateur peut utiliser la fonctionnalité Accès non authentifié pour créer des utilisateurs avec un accès non authentifié et autoriser ces utilisateurs à accéder à des applications distantes sur une instance du Serveur de connexion. Les utilisateurs avec un accès non authentifié peuvent se connecter au serveur de façon anonyme pour se connecter à leurs applications distantes.

Par défaut, les utilisateurs sélectionnent le paramètre **Se connecter de manière anonyme à l'aide de l'accès non authentifié** du menu **Options** et sélectionnent un compte d'utilisateur pour se connecter de manière anonyme. Un administrateur peut configurer les paramètres de stratégie de groupe de manière à présélectionner le paramètre **Se connecter de manière anonyme à l'aide de l'accès non authentifié** et permettre aux utilisateurs de se connecter à l'aide d'un compte d'utilisateur Accès non authentifié spécifique.

Prérequis

- Effectuez les tâches administratives décrites dans « Préparation du Serveur de connexion pour Horizon Client », page 20.

- Configurez des utilisateurs avec un accès non authentifié sur l'instance du Serveur de connexion. Pour plus d'informations, consultez « Fournir un accès non authentifié pour des applications publiées » dans le document *Administration de View*.
- Si vous êtes à l'extérieur du réseau d'entreprise, vérifiez que votre périphérique client est configuré pour utiliser une connexion VPN et activez cette connexion.
- Vérifiez que vous disposez du nom de domaine complet (FQDN) du serveur qui fournit l'accès à l'application distante. Les traits de soulignement (_) ne sont pas pris en charge dans les noms de serveur. Si le port n'est pas le port 443, vous avez également besoin du numéro de port.
- Si votre administrateur l'a autorisé, configurez le mode de vérification des certificats pour le certificat SSL présenté par le Serveur de connexion. Pour savoir quel mode utiliser, reportez-vous à la section « Définition du mode de vérification de certificats pour Horizon Client », page 45.
- (Facultatif) Configurez les paramètres de stratégie de groupe **Compte à utiliser pour l'accès non authentifié** et **Se connecter de manière anonyme à l'aide de l'accès non authentifié** pour modifier le comportement de l'accès non authentifié par défaut. Pour plus d'informations, consultez « Paramètres de définition de scripts des objets de stratégie de groupe (GPO) des clients », page 48.

Procédure

1 Si une connexion VPN est requise, activez le VPN.

2 Double-cliquez sur le raccourci de bureau de **VMware Horizon Client** ou cliquez sur **Démarrer > Programmes > VMware Horizon Client**.

3 Si votre administrateur vous le demande, cliquez sur le bouton **Options** dans la barre de menus et sélectionnez **Se connecter de manière anonyme à l'aide de l'accès non authentifié**.

En fonction de la configuration de votre système client, ce paramètre peut être déjà sélectionné.

4 (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 ce paramètre uniquement si votre administrateur l'a autorisé.

5 Connectez-vous au serveur sur lequel vous disposez d'un accès non authentifié à des applications distantes.

Option	Action
Se connecter à un nouveau serveur	Double-cliquez sur le bouton **+ Ajouter un serveur** ou cliquez sur le bouton **+ Nouveau serveur** dans la barre de menus, entrez le nom du serveur et cliquez sur **Se connecter**.
Se connecter à un serveur existant	Double-cliquez sur l'icône du serveur dans la fenêtre d'accueil d'Horizon Client.

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

Il est possible qu'un message de confirmation s'affiche avant l'affichage de la boîte de dialogue Connexion.

6 Lorsque la boîte de dialogue Connexion s'affiche, sélectionnez un compte d'utilisateur dans le menu déroulant **Compte d'utilisateur**, si nécessaire.

Si un seul compte d'utilisateur est disponible, le menu déroulant est désactivé et le compte d'utilisateur est déjà sélectionné.

7 (Facultatif) Si la case **Toujours utiliser ce compte** est disponible, cochez-la pour contourner la boîte de dialogue Connexion lors de votre prochaine connexion au serveur.

Pour décocher ce paramètre avant votre prochaine connexion au serveur, cliquez avec le bouton droit sur l'icône de serveur sur la fenêtre d'accueil d'Horizon Client et sélectionnez **Oublier le compte d'accès non authentifié enregistré**.

8 Cliquez sur **Connexion** pour vous connecter au serveur.

La fenêtre de sélection des applications s'affiche.

9 Pour démarrer l'application, double-cliquez sur une icône de l'application.

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.

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

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

Vous pouvez également activer la fonctionnalité 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 sur lequel vous avez ouvert une session. Par exemple, si Microsoft Word est l'une des applications distantes disponibles depuis le serveur, 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 fonctionnalité requiert des serveurs et des agents Horizon 6.2.

Un administrateur peut masquer la fonctionnalité de redirection du lecteur client dans Horizon Client en activant un paramètre de stratégie de groupe. Pour plus d'informations, consultez **Désactiver le partage de fichiers et de dossiers** dans Tableau 3-7.

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

Prérequis

Pour partager des dossiers et des lecteurs avec une application ou un poste de travail distant, vous devez activer la fonctionnalité de redirection de lecteur client. Cette tâche inclut l'installation de View Agent 6.1.1 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure, et l'activation de l'option de l'agent **Redirection du lecteur client**. Elle peut également inclure la configuration de stratégies pour contrôler le comportement de la redirection de lecteur client. Pour plus d'informations, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

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	Cliquez sur le bouton **Ajouter**, recherchez et sélectionnez le dossier ou le lecteur à partager, puis cliquez sur **OK**. **Remarque** Il n'est pas possible de partager un dossier sur un périphérique USB si le périphérique est déjà connecté à une application ou un poste de travail distant à l'aide de la fonction de redirection USB. 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'avec la fonction de redirection de lecteur client.
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***.
Partager des périphériques de stockage USB avec des applications et des postes de travail distants	Cochez la case **Autoriser l'accès au stockage amovible**. La fonction de redirection de lecteur client partage automatiquement tous les périphériques de stockage USB insérés dans votre système client et tous les lecteurs externes connectés via FireWire et Thunderbolt. Il n'est pas nécessaire de sélectionner un périphérique spécifique à partager. **Remarque** Les périphériques de stockage USB déjà connectés à une application ou un poste de travail distant avec la fonction de redirection USB ne sont pas partagés. Si cette case est décochée, vous pouvez utiliser la fonction de redirection USB pour connecter des périphériques de stockage USB à des applications et des postes de travail distants.

Option	Action
Activer la fonction permettant d'ouvrir un fichier local avec une application distante depuis le système de fichiers local	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. 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. Votre administrateur peut désactiver cette fonctionnalité.
Ne pas afficher la boîte de dialogue Partage lorsque vous vous connectez à une application ou à un poste de travail distant	Cochez la case **Ne pas afficher la boîte de dialogue lors de la connexion à un poste de travail ou à une application**. Si cette case n'est pas cochée, la boîte de dialogue Partage s'affiche lorsque vous vous connectez pour la première fois à un poste de travail ou à une application après une connexion à un serveur. Par exemple, si vous ouvrez une session sur un serveur avant de vous connecter à un poste de travail, la boîte de dialogue Partage s'affiche. Si vous vous connectez ensuite à une autre application ou un autre poste de travail, cette boîte de dialogue ne s'affiche plus. Pour afficher de nouveau cette boîte de dialogue, vous devez vous déconnecter du serveur puis rouvrir une session.

Suivant

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

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

Masquer la fenêtre VMware Horizon Client

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

Vous pouvez également définir une préférence qui masque toujours la fenêtre VMware Horizon Client après l'ouverture 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 l'ouverture 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 58.

Procédure

- Pour masquer la fenêtre VMware Horizon Client après avoir ouvert 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 qui masque toujours la fenêtre VMware Horizon Client après l'ouverture d'une application ou d'un poste de travail distant, avant de vous connecter à un serveur, 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'expiration, dans Horizon Administrator, accédez à **Paramètres généraux** 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	Effectuez l'une des opérations suivantes : ■ 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	Effectuez l'une des opérations suivantes : ■ Si vous souhaitez maintenir l'application ou le poste de travail actuel ouvert et vous connecter également à une application ou un poste de travail distant sur un autre serveur, démarrez une nouvelle instance d'Horizon Client et connectez-vous à l'autre poste de travail ou application. ■ Si vous souhaitez fermer le poste de travail actuel et vous connecter à un poste de travail sur un autre serveur, accédez à la fenêtre de sélection de postes de travail, cliquez sur l'icône **Se déconnecter** dans l'angle supérieur gauche de la fenêtre, puis confirmez que vous souhaitez fermer votre session sur ce poste de travail. Vous serez déconnecté du serveur actuel et de toutes les sessions 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.

Procédure

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

Option	Action
Dans la fenêtre du poste de travail distant	effectuez l'une des opérations suivantes : ■ 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	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. Dans le coin supérieur gauche de la fenêtre de sélection de postes de travail, cliquez sur l'icône **Se déconnecter de ce serveur**, puis sur **Oui** dans la zone d'avertissement.

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

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

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

- 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 : ■ 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	Cliquer sur le bouton **Fermer** ne ferme que la fenêtre de sélection des applications.

- 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.

  a Démarrez Horizon Client, connectez-vous au serveur qui fournit l'accès au poste de travail distant et entrez vos informations d'identification d'authentification.

  b 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

Horizon 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

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 1 0	Poste de travail Windows Server 2008/20 12 R2 ou Windows Server 2016
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 VMware Blast			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	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, ou Horizon Agent 7.0 ou version ultérieure. Les postes de travail Windows Server 2012 R2 requièrent View Agent 6.1 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure.

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

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 10.

Fonctionnalités prises en charge pour les postes de travail publiés sur les hôtes RDS

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

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

Tableau 5-2. Fonctionnalités prises en charge par les hôtes RDS avec View Agent 6.0.x ou version ultérieure, ou Horizon Agent 7.0.x ou version ultérieure, installé

Fonction	Hôte RDS Windows Server 2008 R2	Hôte RDS Windows Server 2012	Hôte RDS Windows Server 2016
RSA SecurID ou RADIUS	X	X	Horizon Agent 7.0.2 et versions ultérieures
Carte à puce	View Agent 6.1 et versions ultérieures	View Agent 6.1 et versions ultérieures	Horizon Agent 7.0.2 et versions ultérieures
Authentification unique	X	X	Horizon Agent 7.0.2 et versions ultérieures
Protocole d'affichage RDP (pour les clients de poste de travail)	X	X	Horizon Agent 7.0.2 et versions ultérieures
Protocole d'affichage PCoIP	X	X	Horizon Agent 7.0.2 et versions ultérieures
Protocole d'affichage VMware Blast	Horizon Agent 7.0 et version ultérieure	Horizon Agent 7.0 et version ultérieure	Horizon Agent 7.0.2 et versions ultérieures
HTML Access	View Agent 6.0.2 et versions ultérieures (machine virtuelle uniquement)	View Agent 6.0.2 et versions ultérieures (machine virtuelle uniquement)	Horizon Agent 7.0.2 et versions ultérieures
Redirection multimédia (MMR) Windows Media	View Agent 6.1.1 et versions ultérieures	View Agent 6.1.1 et versions ultérieures	Horizon Agent 7.0.2 et versions ultérieures
Redirection USB (périphériques de stockage USB uniquement)		View Agent 6.1 et versions ultérieures	Horizon Agent 7.0.2 et versions ultérieures
Redirection de lecteur client	View Agent 6.1.1 et versions ultérieures	View Agent 6.1.1 et versions ultérieures	Horizon Agent 7.0.2 et versions ultérieures
Impression virtuelle (pour clients de poste de travail)	View Agent 6.0.1 et versions ultérieures (machine virtuelle uniquement)	View Agent 6.0.1 et versions ultérieures (machine virtuelle uniquement)	Horizon Agent 7.0.2 et versions ultérieures (machine virtuelle uniquement)
Redirection de scanner	View Agent 6.0.2 et versions ultérieures	View Agent 6.0.2 et versions ultérieures	Horizon Agent 7.0.2 et versions ultérieures
Impression basée sur l'emplacement	View Agent 6.0.1 et versions ultérieures (machine virtuelle uniquement)	View Agent 6.0.1 et versions ultérieures (machine virtuelle uniquement)	Horizon Agent 7.0.2 et versions ultérieures (machine virtuelle uniquement)

Tableau 5-2. Fonctionnalités prises en charge par les hôtes RDS avec View Agent 6.0.x ou version ultérieure, ou Horizon Agent 7.0.x ou version ultérieure, installé (suite)

Fonction	Hôte RDS Windows Server 2008 R2	Hôte RDS Windows Server 2012	Hôte RDS Windows Server 2016
Plusieurs moniteurs (pour clients de poste de travail)	X	X	Horizon Agent 7.0.2 et versions ultérieures
Unity Touch (pour les clients Chrome OS et mobiles)	X	X	Horizon Agent 7.0.2 et versions ultérieures
Audio/Vidéo en temps réel (RTAV)	Horizon Agent 7.0.2 et versions ultérieures	Horizon Agent 7.0.2 et versions ultérieures	Horizon Agent 7.0.3 et versions ultérieures

Pour plus d'informations sur les éditions de chaque système d'exploitation invité et les service packs pris en charge, consultez le document *Installation de View*.

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. Pour utiliser la fonctionnalité MMR Windows Media avec des postes de travail RDS, vous devez posséder View Agent 6.1.1 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure. Si vous utilisez le protocole d'affichage VMware Blast, vous devez posséder Horizon Agent 7.0 ou version ultérieure.
Redirection de port série	Requiert View Agent 6.1.1 ou version ultérieure. Pour Windows 10, requiert View Agent 6.2 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure. Si vous utilisez le protocole d'affichage VMware Blast, vous devez posséder Horizon Agent 7.0 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 6.0.1 avec View ou version ultérieure. Si vous utilisez le protocole d'affichage VMware Blast pour cette fonctionnalité, vous devez posséder Horizon Agent 7.0 ou version ultérieure.

Tableau 5-3. Configuration requise pour des fonctionnalités spécifiques (suite)

Fonction	Configuration requise
Redirection de scanner	Requiert View Agent 6.0.2 ou version ultérieure. Nécessite le protocole d'affichage PCoIP. Pour Windows 10, requiert View Agent 6.2 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure. Si vous utilisez le protocole d'affichage VMware Blast, vous devez posséder Horizon Agent 7.0 ou version ultérieure.
Redirection de lecteur client	Pour les postes de travail de machine virtuelle mono-utilisateur et les postes de travail publiés sur les hôtes RDS, requiert View Agent 6.1.1 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure. Si vous utilisez le protocole d'affichage VMware Blast, vous devez posséder Horizon Agent 7.0 ou version ultérieure.

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

Vous ne pouvez utiliser des applications distantes que si vous êtes connecté à un Serveur de connexion 6.0 ou version ultérieure. Pour plus d'informations sur les systèmes d'exploitation pris en charge par l'hôte RDS qui fournit des applications et des postes de travail publiés, consultez le document *Installation de View*.

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, ou Horizon Agent 7.0 ou version ultérieure. Pour obtenir une liste des systèmes d'exploitation Linux pris en charge ainsi que des informations sur les fonctionnalités prises en charge, consultez *Configuration des postes de travail Horizon 6 for Linux* ou *Configuration des postes de travail virtuels dans Horizon 7*.

Fonctionnalités prises en charge en mode imbriqué

Le mode imbriqué est parfois utilisé pour les clients zéro ou les clients légers pour que, quand l'utilisateur final se connecte au client zéro, Horizon Client démarre automatiquement et connecte l'utilisateur à un poste de travail distant. Sur ce poste de travail distant, l'utilisateur lance des applications hébergées.

Dans cette configuration, le poste de travail distant est un poste de travail de machine virtuelle mono-utilisateur ou un poste de travail fourni par un hôte RDS. Dans les deux cas, pour fournir des applications hébergées, le logiciel Horizon Client doit être installé sur le poste de travail distant. Cette configuration est appelée mode imbriqué, car le client se connecte à un poste de travail sur lequel le client est également installé.

Les systèmes d'exploitation suivants sont pris en charge lors de l'exécution d'Horizon Client en mode imbriqué.

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows 7 Enterprise SP1
- Windows 10 Enterprise, version 1607

Les fonctionnalités suivantes sont prises en charge lorsqu'un utilisateur utilise Horizon Client en mode imbriqué.

- Protocoles d'affichage VMware Blast, PCoIP et RDP
- Impression basée sur l'emplacement
- Impression virtuelle
- Authentification unique (sans carte à puce)
- Redirection du Presse-papiers
- redirection de contenu URL
- Se connecter en tant qu'utilisateur actuel

Internationalisation

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

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.

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 View Agent 6.0.2, ou Horizon Agent 7.0 ou version ultérieure, 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 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\`

Redimensionnement de la fenêtre du poste de travail distant

Si vous faites glisser un coin de la fenêtre du poste de travail distant pour la redimensionner, une info-bulle affiche la résolution de l'écran dans le coin inférieur droit de la fenêtre.

Si vous utilisez le protocole d'affichage VMware Blast ou PCoIP, l'info-bulle change pour afficher des résolutions d'écran différentes lorsque vous modifiez la taille de la fenêtre du poste de travail. Ces informations sont utiles si vous devez redimensionner le poste de travail distant à une résolution spécifique.

Vous ne pouvez pas modifier la résolution de la fenêtre du poste de travail distant si un administrateur a verrouillé la taille de l'invité ou si vous utilisez le protocole d'affichage RDP. Dans ces cas-là, l'info-bulle de résolution indique la résolution initiale.

Écrans et résolution d'écran

Vous pouvez étendre un poste de travail distant sur plusieurs moniteurs. Si vous disposez d'un moniteur haute résolution, vous pouvez afficher l'application ou le poste de travail distant en pleine résolution.

Le mode d'affichage Tous les moniteurs affiche une fenêtre de poste de travail distant sur plusieurs moniteurs. La fenêtre de poste de travail distant s'affiche sur tous les moniteurs par défaut. Vous pouvez utiliser la fonctionnalité de plusieurs moniteurs sélective pour afficher une fenêtre de poste de travail distant sur un sous-ensemble de vos moniteurs.

Si vous utilisez le mode 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.

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.

Configurations à plusieurs moniteurs prises en charge

Horizon Client prend en charge les configurations à plusieurs moniteurs suivantes :

- Si vous utilisez deux moniteurs, il n'est pas nécessaire qu'ils 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.
- Les moniteurs peuvent être placés côte à côte, associés deux par deux ou empilés verticalement, seulement si vous utilisez deux moniteurs et si la hauteur totale est inférieure à 4 096 pixels.
- Pour utiliser la fonctionnalité de plusieurs moniteurs sélective, vous devez utiliser le protocole d'affichage VMware Blast ou PCoIP. Pour plus d'informations, reportez-vous à la section « Sélectionner des moniteurs spécifiques dans une configuration à plusieurs moniteurs », page 95.
- Pour utiliser la fonction de rendu 3D, vous devez utiliser le protocole d'affichage VMware Blast ou PCoIP. Vous pouvez utiliser deux 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.
- Si vous utilisez des pools de postes de travail de clone instantané, vous pouvez utiliser jusqu'à deux moniteurs pour afficher un poste de travail distant, avec une résolution maximale de 2 560 x 1 600.
- Avec le protocole d'affichage VMware Blast ou PCoIP, la résolution d'écran de poste de travail distant de 4K (3 840 x 2 160) est prise en charge. Le nombre d'écrans 4K pris en charge dépend de la version matérielle de la machine virtuelle de poste de travail et de la version de Windows.

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

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

Remarque Lorsque la résolution d'écran de poste de travail distant est définie sur 3 840 x 2 160 (4K), les éléments sur l'écran peuvent sembler plus petits, et il peut vous être impossible d'utiliser la boîte de dialogue Résolution d'écran sur le poste de travail distant pour agrandir le texte et les autres éléments. Dans ce scénario, vous pouvez définir le DPI de la machine cliente sur le paramètre approprié et activer la fonctionnalité de synchronisation DPI afin de rediriger le paramètre DPI de la machine cliente vers le poste de travail distant.

- 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.

Sélectionner des moniteurs spécifiques dans une configuration à plusieurs moniteurs

Vous pouvez utiliser la fonctionnalité de plusieurs moniteurs sélective pour sélectionner les moniteurs sur lesquels afficher une fenêtre de poste de travail distant. Par exemple, si vous disposez de trois moniteurs, vous pouvez spécifier que la fenêtre de poste de travail distant n'apparaît que sur deux de ces moniteurs. Par défaut, une fenêtre de poste de travail distant apparaît sur tous les moniteurs dans une configuration à plusieurs moniteurs.

Vous pouvez sélectionner jusqu'à quatre moniteurs adjacents. Les moniteurs peuvent être placés les uns à côté des autres, empilés deux par deux ou empilés à la verticale. Deux moniteurs au maximum peuvent être empilés à la verticale.

Cette fonctionnalité n'est pas prise en charge pour les applications distantes.

Procédure

1. Démarrez Horizon Client et connectez-vous à un serveur.
2. Dans la fenêtre de sélection des postes de travail et des applications, cliquez avec le bouton droit sur le poste de travail distant et sélectionnez **Paramètres**.
3. Sélectionnez **PCoIP** ou **VMware Blast** dans le menu déroulant **Se connecter via**.
4. Sélectionnez **Tous les moniteurs** dans le menu déroulant **Affichage**.

   Des miniatures des moniteurs actuellement connectés à votre système client s'affichent sous Paramètres d'affichage. La topologie d'affichage correspond aux paramètres d'affichage sur votre système client.
5. Cliquez sur une miniature pour sélectionner ou désélectionner un moniteur sur lequel afficher la fenêtre de poste de travail distant.

   Lorsque vous sélectionnez un moniteur, sa miniature devient verte. Un message d'avertissement s'affiche si vous enfreignez une règle de sélection d'affichage.
6. Cliquez sur **Appliquer** pour enregistrer vos modifications.
7. Cliquez sur **OK** pour fermer la boîte de dialogue.
8. Connectez-vous au poste de travail distant.

   Vos modifications s'appliquent immédiatement lorsque vous vous connectez au poste de travail distant. Vos modifications sont enregistrées dans le fichier de préférences d'Horizon Client du poste de travail distant une fois que vous fermez Horizon Client.

Utiliser un moniteur dans une configuration à plusieurs moniteurs

Si vous disposez de plusieurs moniteurs, mais que vous voulez qu'une fenêtre de poste de travail distant n'apparaisse que sur un seul moniteur, vous pouvez configurer la fenêtre de poste de travail distant pour qu'elle s'ouvre sur un seul moniteur.

Cette préférence n'est pas prise en charge pour les applications distantes.

Procédure

1 Démarrez Horizon Client et connectez-vous à un serveur.

2 Dans la fenêtre de sélection des postes de travail et des applications, cliquez avec le bouton droit sur le poste de travail distant et sélectionnez **Paramètres**.

3 Sélectionnez **PCoIP** ou **VMware Blast** dans le menu déroulant **Se connecter via**.

4 Dans le menu **Affichage**, sélectionnez **Fenêtre - Grande**, **Fenêtre - Petite** ou **Personnalisé**.

Si vous sélectionnez **Personnalisé**, vous pouvez sélectionner une taille de fenêtre spécifique.

5 Cliquez sur **Appliquer** pour enregistrer vos modifications.

Vos modifications s'appliquent immédiatement lorsque vous cliquez sur **Appliquer**.

6 Cliquez sur **OK** pour fermer la boîte de dialogue.

Par défaut, la fenêtre de poste de travail distant s'ouvre sur le moniteur principal. Vous pouvez faire glisser la fenêtre de poste de travail distant vers un écran secondaire et, lors de la prochaine ouverture du poste de travail distant, la fenêtre de poste de travail distant s'affichera sur ce moniteur. La fenêtre est ouverte 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.

Utiliser la mise à l'échelle de l'affichage

En général, un utilisateur dont la vue est faible ou qui dispose d'un écran avec une résolution élevée, tel qu'un moniteur 4K, active la mise à l'échelle en définissant le paramètre DPI (points par pouce) sur plus de 100 % sur la machine cliente. Avec la fonctionnalité de mise à l'échelle de l'affichage, l'application ou le poste de travail distant prend en charge le paramètre de mise à l'échelle de la machine cliente et l'application ou le poste de travail distant s'affiche en taille normale plutôt qu'en taille très réduite.

Horizon Client enregistre le paramètre de mise à l'échelle de l'affichage pour chaque poste de travail distant séparément. Le paramètre de mise à l'échelle de l'affichage s'applique à toutes les applications distantes qui sont disponibles pour l'utilisateur actuellement connecté. Le paramètre de mise à l'échelle de l'affichage apparaît même si le paramètre DPI est de 100 % sur la machine cliente.

Un administrateur peut masquer le paramètre de mise à l'échelle de l'affichage en activant le paramètre de stratégie de groupe **Locked Guest Size** d'Horizon Client. L'activation du paramètre de stratégie de groupe **Locked Guest Size** ne désactive pas la fonctionnalité de synchronisation DPI. Pour désactiver la fonctionnalité de synchronisation DPI, un administrateur doit désactiver le paramètre de stratégie de groupe **Synchronisation DPI**. Pour plus d'informations, reportez-vous à la section « Utilisation de la synchronisation DPI », page 97.

Dans une configuration à plusieurs moniteurs, l'utilisation de la mise à l'échelle de l'affichage n'affecte pas les résolutions maximales ni le nombre de moniteurs pris en charge par Horizon Client. Lorsque la mise à l'échelle de l'affichage est autorisée et effective, elle est basée sur le paramètre DPI du moniteur principal.

Cette procédure décrit comment activer la fonctionnalité de mise à l'échelle de l'affichage avant de vous connecter à une application ou un poste de travail distant. Vous pouvez activer la fonctionnalité de mise à l'échelle de l'affichage une fois que vous êtes connecté à un poste de travail distant en sélectionnant **Options > Autoriser la mise à l'échelle de l'affichage**.

Procédure

1 Démarrez Horizon Client et connectez-vous à un serveur.

2 Dans la fenêtre de sélection des postes de travail et des applications, cliquez avec le bouton droit sur l'application ou le poste de travail distant et sélectionnez **Paramètres**.

3 Cochez la case **Autoriser la mise à l'échelle de l'affichage**.

4 Cliquez sur **Appliquer** pour enregistrer vos modifications.

5 Cliquez sur **OK** pour fermer la boîte de dialogue.

Utilisation de la synchronisation DPI

La fonctionnalité de synchronisation DPI garantit que le paramètre DPI du poste de travail distant correspond à celui de la machine cliente pour les nouvelles sessions distantes. Lorsque vous démarrez une nouvelle session, Horizon Agent définit une valeur DPI dans le poste de travail distant qui correspond à la valeur DPI de la machine cliente.

La fonctionnalité de synchronisation DPI ne peut pas modifier le paramètre DPI des sessions distantes actives. Si vous vous reconnectez à une session distante existante, la fonctionnalité de mise à l'échelle de l'affichage met à l'échelle l'application ou le poste de travail distant de façon appropriée.

La fonctionnalité de synchronisation DPI est activée par défaut. Un administrateur peut désactiver la fonctionnalité de synchronisation DPI en désactivant le paramètre de stratégie de groupe **Synchronisation DPI** d'Horizon Agent. Vous devez vous déconnecter puis vous reconnecter pour que la modification de configuration prenne effet. Pour plus d'informations, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Lorsque la fonctionnalité de synchronisation DPI et la fonctionnalité de mise à l'échelle de l'affichage sont toutes deux activées, une seule fonctionnalité prend effet. La mise à l'échelle de l'affichage n'a lieu que lorsque la synchronisation DPI n'a pas encore pris effet (c'est-à-dire avant que le paramètre DPI sur le poste de travail distant corresponde au paramètre DPI sur la machine cliente) et la mise à l'échelle de l'affichage cesse de fonctionner une fois que les paramètres DPI correspondent.

Pour les postes de travail de machine virtuelle à session unique, la fonctionnalité de synchronisation DPI est prise en charge sur les systèmes d'exploitation invités suivants :

- 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
- Windows Server 2016 configuré en tant que poste de travail

Pour les applications et les postes de travail publiés, la fonctionnalité de synchronisation DPI est prise en charge sur les hôtes RDS suivants :

- Windows Server 2012 R2
- Windows Server 2016

La fonctionnalité de synchronisation DPI requiert Horizon Agent 7.0.2 ou version ultérieure et Horizon Client 4.2 ou version ultérieure.

Remarque La fonctionnalité de synchronisation DPI n'est pas disponible si vous utilisez Horizon Client 4.2 avec Horizon Agent 7.0 ou 7.0.1, ou Horizon Client 4.0 ou 4.1 avec Horizon Agent 7.0.2 ou version ultérieure. Seule la fonctionnalité de mise à l'échelle de l'affichage est disponible dans ces scénarios.

Voici des conseils sur l'utilisation de la fonctionnalité de synchronisation DPI :

- Si vous modifiez le paramètre DPI sur la machine cliente, vous devez vous déconnecter puis vous reconnecter pour qu'Horizon Client prenne connaissance du nouveau paramètre DPI sur la machine cliente. Cette exigence s'applique même si la machine cliente exécute Windows 10.
- Si vous démarrez une session distante sur une machine cliente avec un paramètre DPI supérieur à 100 %, et que vous utilisez la même session sur une autre machine cliente avec un paramètre DPI différent supérieur à 100 %, vous devez vous déconnecter puis vous reconnecter sur la deuxième machine cliente pour que la synchronisation DPI fonctionne sur la deuxième machine cliente.
- Même si les machines Windows 10 et Windows 8.x prennent en charge différents paramètres DPI sur différents moniteurs, la fonctionnalité de synchronisation DPI n'utilise que la valeur DPI définie sur le moniteur principal de la machine cliente. Tous les moniteurs dans le poste de travail distant utilisent également le même paramètre DPI que le moniteur principal de la machine cliente. Horizon Client ne prend pas en charge différents paramètres DPI dans différents moniteurs.
- Si un administrateur modifie la valeur du paramètre de stratégie de groupe **Synchronisation DPI** pour Horizon Agent, vous devez vous déconnecter puis vous reconnecter pour que le nouveau paramètre prenne effet.
- Lorsque vous connectez un ordinateur portable prenant en charge différents paramètres DPI sur différents moniteurs à un moniteur externe, et que vous définissez le moniteur externe comme moniteur principal, Windows change automatiquement le moniteur principal et le paramètre DPI du moniteur principal chaque fois que vous détachez ou rattachez le moniteur externe. Dans ce cas, vous devez vous déconnecter puis vous reconnecter sur le système client pour qu'Horizon Client sache que le moniteur principal a changé, et vous devez vous déconnecter puis vous reconnecter sur l'application ou le poste de travail distant pour que les paramètres DPI correspondent entre le système client et l'application ou le poste de travail distant.
- Pour les machines clientes Windows 10, cliquez avec le bouton droit sur votre poste de travail, sélectionnez **Paramètres d'affichage > Paramètres d'affichage avancés > Dimensionnement avancé du texte et des autres éléments**, cliquez sur le lien **définir un niveau de mise à l'échelle personnalisé**, puis déconnectez-vous et reconnectez-vous pour que le nouveau paramètre DPI prenne effet.

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

Vous pouvez changer de mode d'affichage (passer du mode Tous les moniteurs au mode Plein écran, par exemple) sans devoir vous déconnecter d'un poste de travail distant.

Cette fonctionnalité n'est pas prise en charge pour les applications distantes.

Prérequis

Vérifiez que vous utilisez le protocole d'affichage VMware Blast ou 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 distant 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 View Agent 6.1 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure, vous pouvez également rediriger des lecteurs USB et des disques durs connectés localement pour les utiliser dans des postes de travail et des applications publiés sur des hôtes 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 publiés. Avec Horizon Agent 7.0.2 ou version ultérieure, les applications et les postes de travail publiés peuvent prendre en charge des périphériques USB plus génériques, tels que les tablettes de signature TOPAZ ou Wacom, ainsi que la pédale de contrôle de dictaphone Olympus. Les autres types de périphériques USB, tels que les périphériques de stockage et les lecteurs CD-ROM USB, ne sont pas pris en charge dans les postes de travail et les applications publiés.

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'attacher des périphériques USB qui utilisent des pilotes MTP, tels que des smartphones et des tablettes Samsung fonctionnant sous Android, configurez 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 n'est pas redirigé, sauf si vous le débranchez avant de le brancher de nouveau.
- Ne vous connectez pas 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 utilisé avec View Agent 6.0.2 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure. Reportez-vous à la section « Utilisation de scanners », page 110.
- 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 103.

- 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 fonctionnent correctement et vous n'avez 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 perd la connectivité réseau. Si vous redirigez un périphérique à écran tactile, le poste de travail distant reçoit 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.

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 68. Pour plus d'informations sur la création de stratégies de groupe, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Prérequis

- Pour utiliser des périphériques USB avec un poste de travail distant, un administrateur Horizon doit activer la fonctionnalité USB pour le poste de travail distant.

  Cette tâche inclut l'installation du composant **Redirection USB** de l'agent, et peut inclure la configuration de stratégies concernant la redirection USB. Pour plus d'informations, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

- 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, ouvrez 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, rouvrez 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. Un périphérique USB peut prendre jusqu'à 20 secondes pour s'afficher sur le poste de travail. 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 fonctionnalités de poste de travail distant dans Horizon 7*.

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 distant, 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 distant.

Si vous prévoyez d'attacher 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 ce périphérique spécifique au poste de travail distant. Pour effectuer cette tâche, modifiez un fichier de configuration sur le client.

Si vous utilisez l'option **Connexion automatique lors de l'insertion** d'Horizon Client, tous les périphériques que vous branchez sur le système client sont redirigés vers le poste de travail distant. 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, 8.x ou Windows 10	`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 = "vid:pid 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 smartphones et des tablettes, subissent une mise à niveau de leur système d'exploitation ou de leur microprogramme, la mise à niveau réussira, puisque le périphérique va redémarrer puis se connecter au poste de travail distant 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 fonctionnalité Audio/Vidéo en temps réel, de la résolution et de la fréquence d'images sur un poste de travail distant, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*. 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 Horizon a configuré la fonctionnalité Audio/vidéo en temps réel et si le protocole d'affichage VMware Blast ou PCoIP est utilisé. Vous pouvez utiliser la webcam dans les applications de conférences telles que Skype, Webex ou Google Hangouts.

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

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

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

Important Si vous utilisez une webcam USB, 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 ou un microphone préféré sur un système client Windows

Avec la fonctionnalité Audio/Vidéo en temps réel, un seul des microphones ou des webcams de votre système client est utilisé sur votre application ou poste de travail distant. Pour spécifier quel microphone ou webcam est préféré, vous pouvez configurer les paramètres de l'Audio/Vidéo en temps réel dans Horizon Client.

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

Avec la fonctionnalité Audio/Vidéo en temps réel, les périphériques vidéo, 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.

Remarque Si vous utilisez une webcam ou un microphone USB, ne le connectez pas via le menu **Connecter un périphérique USB** d'Horizon Client. En effet, cette opération achemine le périphérique via la redirection USB et il ne peut donc pas utiliser la fonctionnalité Audio/Vidéo en temps réel.

Prérequis

- Assurez-vous que vous disposez d'une webcam USB ou d'un microphone USB ou autre installé et opérationnel sur votre système client.
- Vérifiez que vous utilisez le protocole d'affichage VMware Blast ou PCoIP pour votre application ou poste de travail distant.
- Connectez-vous à un serveur.

Procédure

1 Ouvrez la boîte de dialogue Paramètres et sélectionnez **Audio/Vidéo en temps réel** dans le volet de gauche.

   Vous pouvez ouvrir la boîte de dialogue Paramètres en cliquant sur l'icône **Paramètres** (engrenage) dans le coin supérieur droit de l'écran du poste de travail et de l'application ou en cliquant avec le bouton droit de la souris sur l'icône d'un poste de travail ou d'une application et en sélectionnant **Paramètres**.

2 Sélectionnez la webcam préférée dans le menu déroulant **Webcam préférée** et le microphone préféré dans le menu déroulant **Microphone préféré**.

   Les menus déroulants indiquent les webcams et les microphones disponibles sur le système client.

3 Cliquez sur **OK** ou **Appliquer** pour enregistrer vos modifications.

Lors du prochain démarrage d'une application ou d'un poste de travail distant, le microphone et la webcam préférés que vous avez sélectionnés seront redirigés vers l'application ou le poste de travail distant.

Copier et 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 un administrateur Horizon active la fonctionnalité, vous pouvez également copier et coller du 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.

Les formats de fichiers supportés comprennent le texte, les images et les fichiers RTF (Rich Text Format). Certaines restrictions s'appliquent.

Si vous utilisez le protocole d'affichage VMware Blast ou PCoIP, un administrateur Horizon peut définir cette fonctionnalité pour que les opérations Copier et Coller soient autorisées uniquement depuis votre système client vers une application ou un poste de travail distant ou uniquement depuis une application ou un poste de travail distant vers votre système client, ou les deux, ou aucun.

Les administrateurs Horizon configurent la capacité de copier et coller en configurant des paramètres de stratégie de groupe qui dépendent d'Horizon Agent. Selon la version d'Horizon Server et d'Horizon Agent utilisée, les administrateurs peuvent également avoir la possibilité d'utiliser des stratégies de groupe pour limiter les formats de Presse-papiers lors des opérations Copier et Coller, ou d'utiliser des stratégies de carte à puce pour contrôler le comportement copier-coller sur les postes de travail distants. Pour plus d'informations, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Dans Horizon 7 version 7.0 et antérieures et Horizon Client 4.0 et versions antérieures, le Presse-papiers peut contenir 1 Mo de données pour les opérations copier-coller. Dans la version 7.0.1 et les versions ultérieures d'Horizon 7 et dans la version 4.1 et les versions ultérieures d'Horizon Client, la taille de mémoire du Presse-papiers est configurable pour le serveur et pour le client. Lorsqu'une session PCoIP ou VMware Blast est établie, le serveur envoie la taille de la mémoire de son Presse-papiers au client. La taille de mémoire effective du Presse-papiers est la plus petite des valeurs de taille de mémoire du Presse-papiers du serveur et du client.

Si vous copiez du texte formaté, certaines de ces données comprennent du texte et certaines comprennent des informations concernant le formatage. Si vous copiez un volume considérable de texte formaté ou du texte avec une image, il est possible que seule une partie du texte, ou sa totalité, s'affiche, mais sans formatage ou image lorsque vous essayez de le coller. Cela est dû au fait 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 la taille maximale du Presse-papiers, 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 la taille maximale du Presse-papiers, les données RTF sont ignorées et le texte brut est collé.

Si vous ne parvenez pas à coller l'ensemble du texte formaté et les images que vous avez sélectionnées en une seule fois, effectuez l'opération en plusieurs fois en copiant et collant de plus petits volumes.

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

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

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

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

Pour définir la taille de la mémoire du Presse-papiers, modifiez la valeur du registre Windows `HKLM\Software\VMware, Inc.\VMware VDPService\Plugins\MKSVchan\ClientClipboardSize`. Le type de valeur est REG_DWORD. La valeur est spécifiée en Ko. Si vous spécifiez 0 ou si vous ne spécifiez aucune valeur, la taille par défaut de la mémoire du Presse-papiers du client est de 8 192 Ko (8 Mo).

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

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.

- 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 au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

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.

Vous pouvez utiliser la fonctionnalité d'impression virtuelle avec les types suivants d'applications et de postes de travail distants :

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

Pour utiliser l'impression virtuelle, l'administrateur Horizon doit activer la fonctionnalité d'impression virtuelle pour le poste de travail distant. Cette tâche inclut l'activation de l'option d'installation **Impression virtuelle** dans le programme d'installation de l'agent, et peut inclure la configuration de stratégies concernant le comportement de l'impression virtuelle. Pour plus d'informations, reportez-vous au document *Configuration des postes de travail virtuels dans Horizon 7* ou *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

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 publiés sur des hôtes RDS si View Agent 6.2 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure, est installé. Si View Agent 6.1 ou version antérieure est installé sur le poste de travail distant, les imprimantes virtuelles apparaissent sous la forme *<printer_name>#:<number>*.
3. Dans la fenêtre Propriétés de l'imprimante, cliquez sur l'onglet **Installation du périphérique** et spécifiez les paramètres à utiliser.

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

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

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

6 Cliquez sur **OK**.

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 Horizon, les imprimantes virtuelles et les imprimantes USB redirigées peuvent fonctionner en même temps sans problème.

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 99.

- 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 Horizon peut paramétrer le contenu Adobe Flash pour qu'il s'affiche sur votre poste de travail distant à un niveau conçu pour conserver les ressources informatiques. Dans certains cas, ces paramètres peuvent se traduire par une mauvaise qualité de lecture. En déplaçant le pointeur de la souris sur le contenu Adobe Flash, vous pouvez remplacer les paramètres d'Adobe Flash que votre administrateur Horizon spécifie.

Le contrôle de l'affichage Adobe Flash est disponible pour des sessions Internet Explorer uniquement sous Windows, et pour Adobe Flash versions 9 et 10 uniquement. Pour contrôler la qualité d'affichage Adobe Flash, Adobe Flash ne doit pas être exécuté en mode Plein écran.

Procédure

1 Dans Internet Explorer, dans le poste de travail distant, accédez au contenu Adobe Flash de votre choix et démarrez-le si nécessaire.

En fonction de la façon dont votre administrateur Horizon a paramétré Adobe Flash, des cadres peuvent ne pas s'afficher, ou la qualité de lecture peut être mauvaise.

2 Déplacez le pointeur de la souris sur le contenu Adobe Flash pendant la lecture.

La qualité d'affichage est meilleure tant que le curseur reste sur le contenu Adobe Flash.

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

Cliquer sur des liens URL qui s'ouvrent à l'extérieur d' Horizon Client

Un administrateur peut configurer des liens URL sur lesquels vous cliquez dans une application ou un poste de travail distant et qui s'ouvrent dans le navigateur par défaut sur votre système client. Il peut s'agir d'un lien vers une page Web, un numéro de téléphone, une adresse e-mail ou un autre type de lien. Cette fonction est appelée Redirection de contenu URL.

Un administrateur peut également configurer des liens URL sur lesquels vous cliquez dans un navigateur ou une application sur votre système client et qui s'ouvrent dans une application ou un poste de travail distant. Dans ce scénario, si Horizon Client n'est pas déjà ouvert, il démarre et vous invite à vous connecter.

Un administrateur peut configurer la fonctionnalité de redirection de contenu URL pour des raisons de sécurité. Par exemple, si vous vous trouvez sur le réseau d'entreprise et que vous cliquez sur un lien qui pointe vers une URL en dehors du réseau, il est plus sûr d'ouvrir le lien dans une application distante. Un administrateur peut configurer l'application qui ouvre le lien.

La première fois que vous démarrez Horizon Client et que vous vous connectez à un serveur sur lequel la fonctionnalité Redirection de contenu URL est configurée, Horizon Client vous invite à ouvrir l'application VMware Horizon URL Filter lorsque vous cliquez sur un lien de redirection. Cliquez sur **Ouvrir** pour autoriser la redirection de contenu URL.

Selon la configuration de la fonctionnalité Redirection de contenu URL, Horizon Client peut afficher un message d'alerte vous demandant de remplacer votre navigateur Web par défaut par VMware Horizon URL Filter. Si vous voyez cette invite, cliquez sur le bouton **Utiliser « VMware Horizon URL Filter »** pour autoriser VMware Horizon URL Filter comme navigateur par défaut. Cette invite ne s'affiche qu'une seule fois, sauf si vous modifiez votre navigateur par défaut après avoir cliqué sur **Utiliser « VMware Horizon URL Filter »**.

Horizon Client peut également afficher un message d'alerte vous demandant de sélectionner une application lorsque vous cliquez sur une URL. Si vous voyez cette invite, vous pouvez cliquer sur **Choisir une application** pour rechercher une application sur votre système client ou cliquer sur **Rechercher dans l'App Store** pour rechercher et installer une nouvelle application. Si vous cliquez sur **Annuler**, l'URL ne s'ouvre pas.

Chaque entreprise configure ses propres stratégies de redirection d'URL. Si vous avez des questions sur le comportement de la fonctionnalité Redirection de contenu URL dans votre entreprise, contactez votre administrateur système.

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

Si vous utilisez le protocole d'affichage Blast Extreme ou 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 sur les options disponibles pour le rendu 3D, consultez le document *Configuration des postes de travail virtuels dans Horizon 7* ou *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

Utilisation de scanners

Vous pouvez analyser des informations vers vos postes de travail distants 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 l'agent est installé.

Si un administrateur Horizon a configuré la fonctionnalité de redirection de scanner et si vous utilisez le protocole d'affichage Blast Extreme ou 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 distant, 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 Horizon a configuré la fonctionnalité de redirection de port série, et si vous utilisez le protocole d'affichage VMware Blast Extreme ou 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 l'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 l'agent et d'Horizon Client pour Windows, et vous devez vous connecter sur Blast Extreme ou 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 déconnecter le port COM, vous devez le fermer 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.
- Si vous configurez un port série pour qu'il se connecte automatiquement, que vous lancez une application qui ouvre le port série, puis déconnectez et reconnectez la session de poste de travail, la fonctionnalité de connexion automatique n'est pas opérationnelle. Vous ne pouvez pas non plus vous connecter à l'aide de l'option de menu de l'icône de la barre d'état système du port série. Dans la plupart des cas, l'application ne peut plus utiliser le port série. Ce comportement est normal. Vous devez fermer l'application, déconnecter la session de poste de travail et la reconnecter pour résoudre le problème.

Raccourcis clavier

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+P
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+P
Afficher la fenêtre À propos d'Horizon Client	Alt+O+V
Se déconnecter du poste de travail distant	Maj+F10+S
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 de poste de travail (avec une session PCoIP ou VMware Blast Extreme)

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 et VMware Blast

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
Appeler la boîte de dialogue Partager les dossiers	Alt+O+F
Basculer **Activer la mise à l'échelle de l'affichage**	Alt+O+N
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
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

Dépannage de Horizon Client 6

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

Ce chapitre aborde les rubriques suivantes :

Problèmes avec la saisie au clavier

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

Problème

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

Cause

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

Solution

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

Connexion à un serveur en mode Workspace ONE

Si vous ne pouvez pas vous connecter à un serveur directement via Horizon Client, ou si vos droits de poste de travail et d'application ne sont pas visibles dans Horizon Client, le mode Workspace ONE est peut-être activé sur le serveur.

Problème

- Lorsque vous tentez de vous connecter au serveur directement via Horizon Client, Horizon Client vous redirige vers le portail Workspace ONE.
- Lorsque vous ouvrez un poste de travail ou une application via un raccourci ou un URI, ou lorsque vous ouvrez un fichier local via l'association de fichier, la demande vous redirige vers le portail Workspace ONE pour l'authentification.
- Lorsque vous ouvrez un poste de travail ou une application via Workspace ONE et qu'Horizon Client démarre, vous ne pouvez pas voir ou ouvrir d'autres applications ou postes de travail autorisés dans Horizon Client.

Cause

À partir d'Horizon 7 version 7.2, un administrateur peut activer le mode Workspace ONE sur une instance du Serveur de connexion. Ce comportement est normal lorsque le mode Workspace ONE est activé sur une instance du Serveur de connexion.

Solution

Utilisez Workspace ONE pour vous connecter à un serveur compatible avec Workspace ONE et accéder à vos applications et postes de travail distants.

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

Cause

Ce problème survient lorsque la connexion au Serveur de connexion est perdue.

Solution

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

Redémarrer un poste de travail distant

Vous devrez peut-être redémarrer un poste de travail distant si le système d'exploitation du poste de travail cesse de répondre. Le redémarrage d'un poste de travail distant équivaut à la commande de redémarrage du système d'exploitation Windows. En général, le système d'exploitation de poste de travail vous invite à enregistrer toutes les données non enregistrées avant de redémarrer.

Vous pouvez redémarrer un poste de travail distant uniquement si un administrateur Horizon a activé la fonctionnalité de redémarrage de poste de travail pour le poste de travail.

Pour plus d'informations sur l'activation de la fonctionnalité de redémarrage de poste de travail, consultez le document *Configuration des postes de travail virtuels dans Horizon 7* ou *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

Procédure

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

Option	Action
À partir de l'OS du poste de travail	Sélectionnez **Options > Redémarrer le poste de travail** dans la barre de menus.
Depuis la fenêtre de sélection des postes de travail	Cliquez avec le bouton droit sur l'icône du poste de travail et sélectionnez **Redémarrer le poste de travail**.

Horizon Client vous invite à confirmer l'action de redémarrage.

Le système d'exploitation sur le poste de travail distant redémarre et Horizon Client se déconnecte et ferme la session sur le poste de travail.

Suivant

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

Si le redémarrage du poste de travail distant ne résout pas le problème, vous devrez peut-être réinitialiser le poste de travail distant. Reportez-vous à la section « Réinitialiser un poste de travail distant ou des applications distantes », page 119.

Réinitialiser un poste de travail distant ou des applications distantes

Vous devez peut-être réinitialiser un poste de travail distant si le système d'exploitation du poste de travail cesse de répondre et que le redémarrage du poste de travail distant ne résout pas le problème. La réinitialisation des applications distantes ferme toutes les applications ouvertes.

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 sont fermés sans être enregistrés.

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

Vous pouvez réinitialiser un poste de travail distant uniquement si un administrateur Horizon a activé la fonctionnalité de réinitialisation de poste de travail pour le poste de travail.

Pour plus d'informations sur l'activation de la fonctionnalité de réinitialisation de poste de travail, consultez le document *Configuration des postes de travail virtuels dans Horizon 7* ou *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

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 des applications distantes, 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**.

Lorsque vous réinitialisez un poste de travail distant, le système d'exploitation sur le poste de travail distant redémarre et Horizon Client se déconnecte et ferme la session sur le poste de travail. Lorsque vous réinitialisez des applications distantes, les applications se ferment.

Suivant

Il convient d'observer un temps d'attente suffisant pour le démarrage du système avant de tenter de se reconnecter à l'application ou au poste de travail distant.

Réparer Horizon Client pour Windows

Vous pouvez parfois résoudre des problèmes liés à Horizon Client en réparant l'application Horizon Client.

Prérequis

Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur le système client.

Procédure

- Pour réparer Horizon Client de manière interactive, double-cliquez sur le programme d'installation d'Horizon Client ou exécutez le programme d'installation d'Horizon Client avec la commande d'installation `/repair` à partir de la ligne de commande, et cliquez sur **Réparer**.
- Pour réparer Horizon Client en mode silencieux, exécutez le programme d'installation d'Horizon Client avec les commandes d'installation `/silent` et `/repair` à partir de la ligne de commande.

  Par exemple : `VMware-Horizon-Client-y.y.y-xxxxxx.exe /silent /repair`

Désinstaller Horizon Client pour Windows

Vous pouvez avoir à désinstaller et réinstaller Horizon Client si la réparation d'Horizon Client ne résout pas le problème.

Cette procédure montre comment désinstaller Horizon Client si vous disposez du programme d'installation d'Horizon Client. Si vous ne disposez pas du programme d'installation d'Horizon Client, vous pouvez désinstaller Horizon Client de la même manière que vous désinstallez d'autres applications sur votre système Windows. Par exemple, vous pouvez utiliser la fonction Ajout/Suppression de programmes du système d'exploitation Windows pour désinstaller Horizon Client.

Prérequis

Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur le système client.

Procédure

- Pour désinstaller Horizon Client de manière interactive, double-cliquez sur le programme d'installation d'Horizon Client ou exécutez le programme d'installation d'Horizon Client avec la commande d'installation `/uninstall` à partir de la ligne de commande, et cliquez sur **Supprimer**.
- Pour désinstaller Horizon Client en mode silencieux, exécutez le programme d'installation d'Horizon Client avec les commandes d'installation `/silent` et `/uninstall` à partir de la ligne de commande.

  Par exemple : `VMware-Horizon-Client-y.y.y-xxxxxx.exe /silent /uninstall`

Suivant

Réinstallez Horizon Client. Reportez-vous à la section Chapitre 2, « Installation d'Horizon Client pour Windows », page 27.

Index

U

V

W