Configuration des fonctionnalités de poste de travail distant dans Horizon 7

VMware Horizon 7 7.2

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-002454-00-00

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

Configuration des fonctionnalités de poste de travail distant dans Horizon 7

1

Configuration des fonctionnalités de poste de travail distant dans Horizon 7 décrit comment configurer des fonctionnalités de poste de travail distant qui sont installées avec Horizon Agent sur des postes de travail de machine virtuelle ou sur un hôte RDS. Vous pouvez également configurer des stratégies pour contrôler le comportement des pools de postes de travail et d'applications, des machines et des utilisateurs.

Public cible

Ces informations sont destinées à toute personne souhaitant configurer des fonctionnalités de poste de travail distant ou des stratégies sur des postes de travail de machine virtuelle ou des hôtes RDS. Les informations sont destinées aux administrateurs système Windows qui connaissent bien le fonctionnement des centres de données et de la technologie des machines virtuelles.

Configuration des fonctionnalités de poste de travail distant

2

Certaines fonctionnalités de poste de travail distant qui sont installées avec Horizon Agent peuvent être mises à jour dans des versions Feature Pack Update ainsi que dans des versions principales d'Horizon 7. Vous pouvez configurer ces fonctionnalités afin d'améliorer l'expérience de vos utilisateurs finaux sur les postes de travail distants.

Parmi ces fonctionnalités, citons notamment HTML Access, Unity Touch, la redirection d'URL Flash, l'Audio/Vidéo en temps réel, la redirection multimédia (MMR) Windows Media, la redirection USB, la redirection de scanner et la redirection de port série.

Pour plus d'informations sur HTML Access, reportez-vous au document *Utilisation de HTML Access*, disponible dans la page Web de documentation de VMware Horizon Client.

Pour plus d'informations sur la Redirection USB, reportez-vous à Chapitre 4, « Utilisation de périphériques USB avec des applications et postes de travail distants », page 77.

Ce chapitre aborde les rubriques suivantes :

Configuration d'Unity Touch

Avec Unity Touch, les utilisateurs de tablettes et de smartphones peuvent facilement parcourir, rechercher et ouvrir des applications et des fichiers Windows, choisir des applications et des fichiers préférés et passer d'une application en cours d'exécution à une autre, le tout sans utiliser le menu Démarrer ou la barre des tâches. Vous pouvez configurer une liste par défaut d'applications favorites qui s'affichent dans la barre latérale Unity Touch.

Vous pouvez désactiver ou activer la fonctionnalité Unity Touch après son installation en configurant le paramètre de stratégie de groupe **Activer Unity Touch**.

Les documents de VMware Horizon Client pour les périphériques iOS et Android offrent plus d'informations sur les fonctions destinées aux utilisateurs d'Unity Touch.

Configuration système requise pour Unity Touch

Le logiciel Horizon Client et les périphériques mobiles sur lesquels vous installez Horizon Client doivent respecter certaines exigences de version pour prendre en charge Unity Touch.

Poste de travail Horizon 7

Pour prendre en charge Unity Touch, les logiciels suivants doivent être installés sur la machine virtuelle accédée par l'utilisateur :

- Vous pouvez installer la fonctionnalité Unity Touch en installant View Agent 6.0 ou version ultérieure. Reportez-vous à la section « Installer View Agent sur une machine virtuelle » dans le document *Configuration des postes de travail virtuels dans Horizon 7*.
- Systèmes d'exploitation : Windows 7 (32 ou 64 bits), Windows 8 (32 ou 64 bits), Windows 8.1 (32 ou 64 bits), Windows Server 2008 R2 ou Windows Server 2012 R2, Windows 10 (32 ou 64 bits)

Logiciel Horizon Client

Unity Touch est pris en charge par les versions Horizon Client suivantes :

- Horizon Client 2.0 pour iOS ou versions ultérieures
- Horizon Client 2.0 pour Android ou versions ultérieures

Systèmes d'exploitation des appareils portables

Unity Touch est pris en charge sur les systèmes d'exploitation des appareils portables :

- iOS 5.0 et versions ultérieures
- Android 3 (Honeycomb), Android 4 (Ice Cream Sandwich) et Android 4.1 et 4.2 (Jelly Bean).

Configurer les applications préférées affichées par Unity Touch

Grâce à la fonctionnalité Unity Touch, les utilisateurs de tablettes et de smartphones peuvent naviguer rapidement vers une application ou un fichier d'un poste de travail Horizon 7 à partir d'une barre latérale Unity Touch. Même si les utilisateurs peuvent spécifier les applications préférées qui apparaissent dans la barre latérale, pour une utilisation plus aisée, les administrateurs peuvent configurer une liste d'applications préférées par défaut.

Si vous utilisez des pools de postes de travail à attribution flottante, les applications et fichiers préférés spécifiés par les utilisateurs finaux seront perdus à chaque déconnexion du poste de travail, sauf si les profils d'utilisateur itinérants sont activés dans Active Directory.

La liste par défaut des applications préférées reste utilisable lorsqu'un utilisateur se connecte pour la première fois à un poste de travail sur lequel Unity Touch est activé. Mais si l'utilisateur configure sa propre liste d'applications préférées, la liste par défaut sera ignorée. La liste d'applications préférées de l'utilisateur, qui est conservée dans le profil itinérant de l'utilisateur, est disponible lorsque l'utilisateur se connecte à d'autres machines d'un pool flottant ou dédié.

Si vous créez une liste d'applications préférées par défaut et qu'une ou plusieurs applications ne sont pas installées sur le système d'exploitation du poste de travail Horizon 7, ou que les chemins de ces applications sont introuvables dans le menu Démarrer, les applications n'apparaissent pas dans la liste des applications préférées. Vous pouvez utiliser ce comportement pour configurer une liste de référence par défaut des applications préférées pouvant être appliquée à plusieurs images de machine virtuelle ayant différents ensembles d'applications installées.

Par exemple, si Microsoft Office et Microsoft Visio sont installés sur une machine virtuelle, et que Windows Powershell et VMware vSphere Client sont installés sur une deuxième machine virtuelle, vous pouvez créer une liste comprenant les quatre applications. Seules les applications installées apparaissent en tant qu'applications préférées par défaut sur chaque poste de travail.

Il existe d'autres méthodes permettant de spécifier une liste d'applications préférées par défaut :

- Ajouter une valeur au Registre Windows sur les machines virtuelles de pool de postes de travail
- Créer un module d'installation administrative à partir du programme d'installation d'Horizon Agent et distribuer le module aux machines virtuelles
- Exécuter le programme d'installation d'Horizon Agent à partir de la ligne de commande sur les machines virtuelles

---

Remarque Unity Touch suppose que les raccourcis des applications sont situés dans le dossier Programmes du menu **Démarrer**. Si un raccourci est situé en dehors du dossier Programmes, ajoutez le préfixe **`Programs`** au chemin du raccourci. Par exemple, `Windows Update.lnk` se trouve dans le dossier `ProgramData\Microsoft\Windows\Menu Démarrer`. Pour publier ce raccourci sous forme d'application préférée par défaut, ajoutez le préfixe **`Programs`** au chemin du raccourci. Par exemple : `"Programs/Windows Update.lnk"`.

Prérequis

- Vérifiez qu'Horizon Agent est installé sur la machine virtuelle.
- Vérifiez que vous disposez des droits d'administration sur la machine virtuelle. Pour cette procédure, vous devrez peut-être modifier un paramètre de registre.
- Si vous disposez de pools de postes de travail à attribution flottante, utilisez Active Directory pour configurer les profils d'utilisateur itinérant. Suivez les instructions fournies par Microsoft.

  Les utilisateurs de pools de postes de travail à attribution flottante pourront consulter leur liste d'applications et de fichiers préférés à chaque connexion.

Procédure

- (Facultatif) Créez une liste d'applications préférées par défaut en ajoutant une valeur au registre Windows.

  a Ouvrez `regedit` et accédez au paramètre de registre `HKLM\Software\VMware, Inc.\VMware Unity`.

  Sur une machine virtuelle 64 bits, accédez au dossier `HKLM\Software\Wow6432Node\VMware, Inc.\VMware Unity`.

  b Créez une valeur de chaîne appelée `FavAppList`.

  c Spécifiez les applications préférées par défaut.

  Utilisez le format suivant pour spécifier les chemins de raccourci vers les applications utilisées dans le menu **Démarrer**.

  path-to-app-1|path-to-app-2|path-to-app-3|…

  Par exemple :

  `Programs/Accessories/Accessibility/Speech Recognition.lnk|Programs/VMware/VMware vSphere Client.lnk|Programs/Microsoft Office/Microsoft Office 2010 Tools/Microsoft Office 2010 Language Preferences.lnk`

- (Facultatif) Créez une liste d'applications préférées par défaut en créant un module d'installation administrative à partir du programme d'installation d'Horizon Agent.

  a A partir de la ligne de commande, utilisez le format suivant pour créer le package d'installation administrative.

  `VMware-viewagent-x86_64-`*`y.y.y-xxxxxx`*`.exe /s /a /v"/qn TARGETDIR=""`*`partage de réseau pour stocker le module d'installation administrative`*`"" UNITY_DEFAULT_APPS=""`*`liste d'applications favorites par défaut devant être définies dans le registre`*`"""`

  Par exemple :

  `VMware-viewagent-x86_x64-`*`y.y.y-xxxxxx`*`.exe /s /a /v"/qn TARGETDIR=""\\foo-installer-share\ViewFeaturePack\"" UNITY_DEFAULT_APPS=""Programs/Accessories/Accessibility/Ease of Access.lnk|Programs/Accessories/System Tools/Character Map.lnk|Programs/Accessories/Windows PowerShell/Windows PowerShell.lnk|Programs/Internet Explorer (64-bit).lnk|Programs/Google Chrome/Google Chrome.lnk|Programs/iTunes/iTunes.lnk|Programs/Microsoft Office/Microsoft SharePoint Workspace 2010.lnk|Programs/PuTTY/PuTTY.lnk|Programs/Skype/Skype.lnk|Programs/WebEx/Productivity Tools/WebEx Settings.lnk|"""`

  b Distribuez le package d'installation administrative à partir du partage de réseau vers les machines virtuelles de poste de travail à l'aide d'une méthode de déploiement MSI (Microsoft Windows Installer) standard utilisée dans votre organisation.

- (Facultatif) Créez une liste d'applications préférées par défaut en exécutant le programme d'installation d'Horizon Agent directement sur une ligne de commande d'une machine virtuelle.

  Utilisez le format suivant.

  `VMware-viewagent-x86_64-`*`y.y.y-xxxxxx`*`.exe /s /v"/qn UNITY_DEFAULT_APPS=""`*`liste d'applications favorites par défaut devant être définies dans le registre`*`"""`

  Remarque La commande précédente combine l'installation d'Horizon Agent à la spécification de la liste d'applications préférées par défaut. Vous n'avez pas à installer Horizon Agent avant d'exécuter cette commande.

Suivant

Si vous avez effectué cette tâche directement sur une machine virtuelle (en modifiant le Registre Windows ou en installant Horizon Agent à partir de la ligne de commande), vous devez déployer la machine virtuelle que vous venez de configurer. Vous pouvez créer un snapshot ou un modèle et créer un pool de postes de travail ou recomposer un pool existant. Vous pouvez également créer une stratégie de groupe Active Directory pour déployer la nouvelle configuration.

Configuration de la redirection d'URL flash pour les flux de multidiffusion ou de monodiffusion

Les clients peuvent désormais utiliser Adobe Media Server et la multidiffusion ou la monodiffusion pour diffuser des événements vidéo en direct dans un environnement d'infrastructure de poste de travail virtuel (VDI). Pour fournir des flux vidéo en direct en multidiffusion ou en monodiffusion dans un environnement VDI, le flux de données multimédia doit être envoyé directement de la source multimédia aux points de terminaison, en contournant les postes de travail distants. La fonctionnalité Redirection d'URL Flash permet d'effectuer cette opération en interceptant et en redirigeant le fichier Shockwave Flash (SWF) du poste de travail distant vers le point de terminaison client.

Les contenus Flash peuvent être affichés à l'aide des lecteurs multimédias flash locaux des clients.

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 un contenu Flash 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 la page Web. Chaque fois que l'utilisateur d'un poste de travail distant clique sur le lien URL désigné sur une page Web, JavaScript intercepte et redirige le fichier SWF à partir de la session de poste de travail distant vers le point de terminaison client. Le point de terminaison ouvre alors un projecteur Flash local hors de la session de poste de travail distant pour lire le flux multimédia en local.

Pour configurer la redirection d'URL Flash, vous devez configurer le HTML de votre page Web et vos périphériques client.

Procédure

1. Configuration système requise pour la redirection d'URL flash page 12

   Pour prendre en charge la redirection d'URL Flash, le déploiement de votre Horizon 7 doit répondre à certaines exigences matérielles et logicielles.

2. Vérifier que la fonctionnalité redirection d'URL flash est installée page 13

   Avant d'utiliser cette fonctionnalité, vérifiez que la fonctionnalité Redirection d'URL Flash est installée et en cours d'exécution sur vos postes de travail virtuels.

3. Configurer les pages Web qui fournissent des flux de multidiffusion ou de monodiffusion page 13

   Pour permettre la redirection d'URL Flash, vous devez inclure une commande JavaScript dans les pages Web MIME HTML (MHTML) qui fournissent les liens vers les flux de multidiffusion ou de monodiffusion. Les utilisateurs peuvent afficher ces pages Web dans les navigateurs de leurs postes de travail distants pour accéder aux flux vidéo.

4. Configurer des périphériques client pour la redirection d'URL Flash page 14

   La fonctionnalité Redirection d'URL Flash redirige le fichier SWF des postes de travail distants vers les périphériques clients. Pour que ces périphériques client puissent lire des vidéos Flash à partir d'un flux de multidiffusion ou de monodiffusion, vous devez vérifier qu'Adobe Flash Player est installé sur les périphériques client. Les clients doivent également avoir une connectivité IP vers la source multimédia.

5 Activer/désactiver la redirection d'URL Flash page 14

La redirection d'URL Flash est activée lorsque vous effectuez une installation silencieuse d'Horizon Agent avec la propriété `VDM_FLASH_URL_REDIRECTION=1`. Vous pouvez désactiver ou réactiver la fonctionnalité Redirection d'URL Flash sur certains postes de travail distants en définissant une valeur sur une clé de Registre Windows sur ces machines virtuelles.

Configuration système requise pour la redirection d'URL flash

Pour prendre en charge la redirection d'URL Flash, le déploiement de votre Horizon 7 doit répondre à certaines exigences matérielles et logicielles.

Poste de travail Horizon 7

- Vous installez la redirection d'URL Flash en saisissant la propriété `VDM_FLASH_URL_REDIRECTION` sur la ligne de commande lors d'une installation silencieuse de View Agent 6.0 ou version ultérieure. Reportez-vous à la section « Propriétés de l'installation silencieuse pour Horizon Agent » dans le document *Configuration des postes de travail virtuels dans Horizon 7*.
- Les postes de travail doivent tourner sur des systèmes d'exploitation Windows 7, 64 ou 32 bits.
- Internet Explorer 8, 9 et 10, Chrome 29.*x* et Firefox 20.*x* sont parmi les navigateurs de poste de travail pris en charge.

Lecteur multimédia flash et ShockWave Flash (SWF)

Vous devez intégrer un lecteur multimédia Flash approprié tel que Strobe Media Playback dans votre site Web. Pour délivrer un contenu multidiffusion, vous pouvez utiliser `multicastplayer.swf` ou `StrobeMediaPlayback.swf` dans vos pages Web. Pour délivrer un contenu monodiffusion, vous devez utiliser `StrobeMediaPlayback.swf`. Vous pouvez également utiliser `StrobeMediaPlayback.swf` pour d'autres fonctionnalités prises en charge telles que la diffusion de flux RTMP et la diffusion dynamique HTTP.

Logiciel Horizon Client

Les versions suivantes d'Horizon Client prennent en charge la multidiffusion et la monodiffusion :

- Horizon Client 2.2 pour Linux ou versions ultérieures
- Horizon Client 2.2 pour Windows ou versions ultérieures

Les versions suivantes d'Horizon Client ne prennent en charge que la multidiffusion :

- Horizon Client 2.0 ou 2.1 pour Linux
- Horizon Client 5.4 pour Windows

Ordinateur Horizon Client ou périphérique d'accès client

- La redirection d'URL Flash est prise en charge par tous les systèmes d'exploitation qui exécutent Horizon Client pour Linux sur les périphériques client légers x86. Cette fonctionnalité n'est pas prise en charge par les processeurs ARM.
- La redirection d'URL Flash est prise en charge par tous les systèmes d'exploitation qui exécutent Horizon Client pour Windows. Pour plus de détails, reportez-vous au document *Utilisation de VMware Horizon Client pour Windows*.
- Sur les périphériques client Windows, vous devez installer Adobe Flash Player 10.1 ou versions ultérieures pour Internet Explorer.

- Sur les périphériques clients légers Linux, vous devez installer les fichiers `libexpat.so.0` et `libflashplayer.so`. Reportez-vous à la section « Configurer des périphériques client pour la redirection d'URL Flash », page 14.

Remarque Avec la redirection d'URL Flash, le flux de multidiffusion ou de monodiffusion est redirigé vers les périphériques clients qui pourraient être en dehors du pare-feu de votre organisation. Vos clients doivent avoir accès au serveur Web d'Adobe hébergeant le fichier Shockwave Flash (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.

Vérifier que la fonctionnalité redirection d'URL flash est installée

Avant d'utiliser cette fonctionnalité, vérifiez que la fonctionnalité Redirection d'URL Flash est installée et en cours d'exécution sur vos postes de travail virtuels.

La fonctionnalité de redirection d'URL Flash doit être présente sur chaque poste de travail avec lequel vous souhaitez prendre en charge la redirection de multidiffusion ou de monodiffusion. Pour voir des instructions sur l'installation d'Horizon Agent, reportez-vous à la section « Propriétés de l'installation silencieuse pour Horizon Agent » dans le document *Configuration des postes de travail virtuels dans Horizon 7*.

Procédure

1. Démarrez une session de poste de travail distant qui utilise PCoIP.
2. Ouvrez le Gestionnaire des tâches.
3. Vérifiez que le processus `ViewMPServer.exe` est en cours d'exécution sur le poste de travail.

Configurer les pages Web qui fournissent des flux de multidiffusion ou de monodiffusion

Pour permettre la redirection d'URL Flash, vous devez inclure une commande JavaScript dans les pages Web MIME HTML (MHTML) qui fournissent les liens vers les flux de multidiffusion ou de monodiffusion. Les utilisateurs peuvent afficher ces pages Web dans les navigateurs de leurs postes de travail distants pour accéder aux flux vidéo.

En outre, vous pouvez personnaliser le message d'erreur en anglais que voient les utilisateurs en cas de problème avec la redirection d'URL Flash. Choisissez cette option si vous souhaitez afficher un message d'erreur dans la langue locale pour les utilisateurs finaux. Vous devez incorporer la configuration `var vmwareScriptErroMessage` ainsi que votre chaîne de texte localisé dans la page Web MHTML.

Prérequis

Assure-vous que la bibliothèque `swfobject.js` est importée dans la page Web MHTML.

Procédure

1. Insérez la commande JavaScript `viewmp.js` dans la page Web MHTML.

   Par exemple : `<script type="text/javascript" src="http://localhost:33333/viewmp.js"></script>`

2. (Facultatif) Personnalisez le message d'erreur de redirection d'URL Flash envoyé aux utilisateurs finaux.

   Par exemple : "`var vmwareScriptErroMessage=`*`message d'erreur localisé`*"

3 Veillez à incorporer la commande JavaScript `viewmp.js` et personnalisez éventuellement le message d'erreur de redirection d'URL Flash avant que le fichier ShockWave Flash (SWF) ne soit importé dans la page Web MHTML.

Lorsqu'un utilisateur affiche la page Web dans un poste de travail distant, la commande JavaScript `viewmp.js` invoque sur le poste de travail distant le mécanisme de redirection d'URL Flash qui redirige le fichier SWF du poste de travail vers le périphérique d'hébergement client.

Configurer des périphériques client pour la redirection d'URL Flash

La fonctionnalité Redirection d'URL Flash redirige le fichier SWF des postes de travail distants vers les périphériques clients. Pour que ces périphériques client puissent lire des vidéos Flash à partir d'un flux de multidiffusion ou de monodiffusion, vous devez vérifier qu'Adobe Flash Player est installé sur les périphériques client. Les clients doivent également avoir une connectivité IP vers la source multimédia.

Remarque Avec la redirection d'URL Flash, le flux de multidiffusion ou de monodiffusion est redirigé vers les périphériques clients qui pourraient être en dehors du pare-feu de votre organisation. Vos clients doivent avoir accès au serveur Web d'Adobe qui héberge le fichier 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.

Procédure

◆ Installer Adobe Flash Player sur vos périphériques client.

Système d'exploitation	Action
Windows	Installez Adobe Flash Player 10.1 ou versions ultérieures pour Internet Explorer.
Linux	a Installez le fichier `libexpat.so.0` ou assurez-vous que ce fichier est déjà installé. Vérifiez que le fichier est installé dans le répertoire `/usr/lib` ou `/usr/local/lib`. b Installez le fichier `libflashplayer.so`, ou assurez-vous que ce fichier est déjà installé. Assurez-vous que le fichier est installé dans le répertoire du plug-in Flash approprié de votre système d'exploitation Linux. c Installez le programme `wget`, ou assurez-vous que le fichier de ce programme est déjà installé.

Activer/désactiver la redirection d'URL Flash

La redirection d'URL Flash est activée lorsque vous effectuez une installation silencieuse d'Horizon Agent avec la propriété `VDM_FLASH_URL_REDIRECTION=1`. Vous pouvez désactiver ou réactiver la fonctionnalité Redirection d'URL Flash sur certains postes de travail distants en définissant une valeur sur une clé de Registre Windows sur ces machines virtuelles.

Procédure

1 Démarrez l'éditeur du Registre Windows sur la machine virtuelle.

2 Accédez à la clé du Registre Windows qui commande la Redirection d'URL Flash.

Option	Description
Windows 7 64 bits	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware ViewMP\enabled = value`
Windows 7 32 bits	`HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware ViewMP\enabled = value`

3 Définissez la valeur pour désactiver ou activer Redirection d'URL Flash.

Option	Valeur
Désactivé	`0`
Activé	`1`

Par défaut, la valeur est définie sur `1`.

Configuration de la redirection Flash

Avec la fonctionnalité de redirection Flash, le contenu Flash est envoyé au système client et lu dans une fenêtre de conteneur Flash à l'aide de la version ActiveX de Flash Player.

Remarque Dans Horizon 7.0, la redirection Flash est une fonctionnalité en version préliminaire. Dans Horizon 7.0.1, elle est entièrement prise en charge.

Même si le nom de cette fonctionnalité est semblable à celui de la fonctionnalité Redirection d'URL Flash, il existe des différences importantes, comme décrit dans le tableau suivant.

Tableau 2-1. Comparaison entre les fonctionnalités Redirection Flash et Redirection d'URL Flash

Élément de différenciation	Redirection Flash	Redirection d'URL Flash
Niveau de prise en charge	Fonctionnalité en version préliminaire dans Horizon 7.0 sans support technique. Entièrement prise en charge dans Horizon 7.0.1.	Entièrement prise en charge
Types d'Horizon Client prenant en charge cette fonctionnalité	Client Windows uniquement	Client Windows et client Linux
Protocole d'affichage	Dans Horizon 7.0, PCoIP uniquement. Dans Horizon 7.0.1, PCoIP et VMware Blast.	PCoIP
Navigateurs	Internet Explorer 9, 10 ou 11 pour l'agent (poste de travail distant)	Tous les navigateurs qui sont actuellement pris en charge sur Horizon Client et Horizon Agent
Mécanisme de configuration	Utilisez un GPO côté agent pour spécifier une liste blanche ou noire de sites Web qui utiliseront ou non la redirection Flash	Modifiez le code source sur la page Web pour intégrer le JavaScript requis

Limites des fonctionnalités

La fonctionnalité de redirection Flash présente les limites suivantes :

- Cliquer sur un lien URL dans la fenêtre de Flash Player ouvre un navigateur sur le client plutôt que sur le poste de travail distant (côté agent).
- Certains sites Web ne fonctionnent pas avec la redirection Flash sur certaines versions de navigateur. Par exemple, le site vimeo.com ne fonctionne pas si vous utilisez Internet Explorer 11.

- Dans Horizon 7.0, il est possible que Flash et le script Java ne fonctionnent pas comme prévu.
- La fenêtre d'Horizon Client peut se figer lors de la lecture du contenu Flash, même si vous pouvez définir une clé de registre Windows pour résoudre ce problème.

  Sur un client 32 bits, définissez la valeur `HKLM\Software\VMware, Inc.\VMware VDM\Client\EnableD3DRenderer` sur « FALSE » et, sur un client 64 bits, définissez `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\EnableD3DRenderer` sur « FALSE ».
- Pour le site Web YouTube, l'interface externe est désactivée par défaut pour éviter les problèmes de lecture. Par conséquent, les fonctionnalités suivantes sont inutilisables : lecture automatique, boutons Précédent et Suivant et mode cinéma. Pour activer Flash Media pour la dernière mise à jour du site Web YouTube, vous devez supprimer youtube.com de **Paramètres d'affichage de compatibilité** et ajouter `&nohtml5=1` manuellement à l'URL de la vidéo. Par exemple, `https://www.youtube.com/watch?v=NwmRD25HWGE&nohtml5=1`.
- Vous ne pouvez pas cliquer sur des vidéos recommandées sur le site YouTube, sauf si vous définissez `appMode=1` comme clé de Registre Windows sur le poste de travail distant.
- S'il n'y a pas de périphérique audio sur le client, des erreurs se produiront lors de la lecture multimédia sur YouTube.
- La redirection Flash ne fonctionne pas pour redbox.com.
- Le menu contextuel de Flash (activé par un clic droit) est désactivé.
- Si une version 4.1 d'Horizon Client se connecte à un poste de travail Horizon 7.0 avec PCoIP, la redirection Flash échouera. Soit le contenu Flash est lu par le lecteur natif du poste de travail, soit l'utilisateur voit s'afficher un écran blanc.

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.

  Reportez-vous à la section « Options d'installation personnalisée 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. Reportez-vous à la section « Installer et configurer la redirection Flash », page 17.
- 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

- Horizon Client 4.0 ou version ultérieure doit être installé. L'option de redirection Flash est activée par défaut.

  Consultez la rubrique sur l'installation d'Horizon Client dans le document *Utilisation de VMware Horizon Client pour Windows*.

	■ 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

Installer et configurer la redirection Flash

La redirection du contenu Flash à partir d'un poste de travail distant vers une fenêtre de Flash Player sur le système client local requiert l'installation de la fonctionnalité de redirection Flash et d'Internet Explorer sur le poste de travail distant et sur le système client ainsi que la spécification des sites Web qui utiliseront cette fonctionnalité.

Pour installer cette fonctionnalité sur le système client, vous devez utiliser un programme d'installation Horizon Client 4.0 ou version ultérieure. Pour installer cette fonctionnalité sur un poste de travail distant, vous devez utiliser un programme d'installation Horizon Agent 7.0 ou version ultérieure et sélectionner l'option d'installation correcte, qui n'est pas sélectionnée par défaut. Pour activer cette fonctionnalité et spécifier quels sites Web l'utiliseront, vous utilisez une stratégie de groupe.

Remarque Vous pouvez également utiliser des paramètres de registre Windows sur le poste de travail distant pour configurer une liste blanche de sites Web à utiliser pour la redirection Flash. Reportez-vous à la section « Utiliser des paramètres de registre Windows pour configurer la redirection Flash », page 19.

Prérequis

- Vérifiez que vous pouvez vous connecter en tant qu'utilisateur de domaine Administrateur sur la machine qui héberge votre serveur Active Directory.
- Vérifiez que les composants logiciels enfichables MMC (Microsoft Management Console) et l'Éditeur d'objets de stratégie de groupe sont disponibles sur votre serveur Active Directory.
- Vérifiez que le fichier de modèle d'administration ADMX `vdm_agent.admx` pour la configuration d'Horizon Agent a été ajouté à l'unité d'organisation pour le poste de travail distant.
- Compilez une liste des sites Web qui peuvent ou pas rediriger le contenu Flash. Compilez une liste blanche pour vous assurer que seules les URL spécifiées dans la liste pourront rediriger du contenu Flash. Compilez une liste noire pour vous assurer que les URL spécifiées dans la liste ne pourront pas rediriger du contenu Flash.
- Vérifiez que Flash ActiveX est installé et qu'il fonctionne correctement. Pour vérifier l'installation, exécutez Internet Explorer et accédez à https://helpx.adobe.com/flash-player.html.

Procédure

1. Sur un système client Windows 7, Windows 8, Windows 8.1 ou Windows 10, installez la version requise d'Horizon Client et Flash Player version ActiveX.
   - Installez Horizon Client 4.0 ou version ultérieure. Consultez la rubrique sur l'installation d'Horizon Client dans le document *Utilisation de VMware Horizon Client pour Windows*.
   - Si nécessaire, installez la version ActiveX de Flash Player (plutôt que la version NPAPI). Flash Player est installé par défaut dans Internet Explorer 10 et 11. Pour Internet Explorer 9, vous devrez peut-être aller sur le site suivant pour télécharger et installer Flash Player : https://get.adobe.com/flashplayer/.

2 Sur un poste de travail distant Windows 7, Windows 8, Windows 8.1 ou Windows 10, installez la version requise d'Horizon Agent et d'Internet Explorer, avec Flash Player.

- Installez Horizon Agent 7.0 ou version ultérieure et veillez à sélectionner l'option pour la redirection Flash (expérimentale). Cette option n'est pas sélectionnée par défaut.
- Installez Internet Explorer 9, 10 ou 11.
- Si nécessaire, installez la version ActiveX de Flash Player (plutôt que la version NPAPI). Flash Player est installé par défaut dans Internet Explorer 10 et 11. Pour Internet Explorer 9, vous devrez peut-être aller sur le site suivant pour télécharger et installer Flash Player : https://get.adobe.com/flashplayer/.

3 Sur le poste de travail distant, dans Internet Explorer, sélectionnez **Outils > Gérer les modules complémentaires** dans la barre de menus et vérifiez que **VMware View FlashMMR Server** est répertorié et activé.

4 Sur le serveur Active Directory, ouvrez l'Éditeur de gestion de stratégie de groupe et modifiez les paramètres de stratégie de redirection Flash sous **Configuration ordinateur**.

Les paramètres se trouvent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Modèles d'administration classiques > Configuration de VMware Horizon Agent > VMware FlashMMR**.

Paramètre	Description
Activer la redirection multimédia Flash	Spécifie si la redirection Flash (FlashMMR) est activée sur le poste de travail distant (côté agent). Lorsqu'elle est activée, cette fonctionnalité transmet les données multimédia Flash depuis les URL désignées via un canal TCP au client, et appelle le Flash Player local sur le système client. Cette fonctionnalité réduit grandement la demande sur le CPU côté agent et sur la bande passante réseau.
Taille de rectangle minimale pour activer FlashMMR	Spécifie la largeur et la hauteur minimales, en pixels, du rectangle dans lequel est lu le contenu Flash. Par exemple, `400,300` spécifie une largeur de 400 pixels et une hauteur de 300 pixels. La redirection Flash sera utilisée uniquement si le contenu Flash est égal ou supérieur aux valeurs spécifiées dans cette stratégie. Si ce GPO n'est pas configuré, la valeur par défaut utilisée est `320,200`.

5 Dans l'Éditeur de gestion de stratégie de groupe, modifiez les paramètres de stratégie de redirection Flash sous **Configuration d'utilisateur**.

Les paramètres se trouvent dans le dossier **Configuration d'utilisateur > Stratégies > Modèles d'administration > Modèles d'administration classiques > Configuration de VMware Horizon Agent > VMware FlashMMR**.

a (Horizon 7.0.3 ou version ultérieure) Ouvrez le paramètre **Définition pour l'utilisation de la liste d'URL FlashMMR** pour définir une liste d'URL d'hôte que vous voulez utiliser avec la redirection Flash et sélectionnez le bouton radio **Activé**.

b Dans la liste déroulante d'utilisation des URL, choisissez d'activer une liste blanche ou une liste noire.

- Pour activer une liste blanche, sélectionnez **Activer une liste blanche**.
- Pour activer une liste noire, sélectionnez **Activer une liste noire**.

Par défaut, une liste blanche est activée.

c Ouvrez le paramètre **Listes d'URL d'hôte pour activer/désactiver FlashMMR** pour ajouter la liste d'URL d'hôte qui utiliseront ou pas la redirection Flash et sélectionnez le bouton radio **Activé**.

d Cliquez sur le bouton **Afficher**.

e Entrez les URL complètes que vous avez compilées comme condition préalable dans la colonne Nom et laissez la colonne Valeur vide.

Veillez à inclure **http:**// ou **https:**//. Vous pouvez utiliser des expressions régulières. Par exemple, vous pouvez spécifier **`https://*.google.com`** et **`http://www.cnn.com`**.

(Horizon 7.0) Laissez la colonne Valeur vide.

(Horizon 7.0.1 ou version ultérieure) Dans la colonne Valeur, vous pouvez éventuellement spécifier **`requireIECompatibility=true`**, **`appMode=0`** ou les deux (utilisez une virgule pour séparer les deux chaînes).

Les sites Web prennent en charge HTML5 par défaut. La redirection Flash ne fonctionne pas sur ces sites Web. Vous devez définir **`requireIECompatibility=true`** pour que ces sites fonctionnent. Ce paramètre n'est pas requis pour le site Web YouTube.

Par défaut, l'interface externe est activée lorsque la redirection Flash s'exécute. Cela peut dégrader les performances. Dans certaines situations, la configuration **`appMode=0`** peut améliorer les performances et conduire à une meilleure expérience utilisateur.

6 Sur la machine agent, ouvrez une invite de commande et passez sur le répertoire suivant :

```
%Program Files%\Common Files\VMware\Remote Experience
```

7 Exécutez la commande suivante pour ajouter la liste blanche ou noire à Internet Explorer.

```
cscript  mergeflashmmrwhitelist.vbs
```

8 Redémarrez Internet Explorer.

Les sites définis avec le paramètre **`requireIECompatibility=true`** sont ajoutés à l'affichage de compatibilité d'Internet Explorer. Vous pouvez le vérifier en sélectionnant **Outils > Paramètres d'affichage de compatibilité** dans la barre de menus.

Dans Horizon 7.0 uniquement, les sites sont également ajoutés à la liste de sites de confiance d'Internet Explorer. Vous pouvez vérifier les sites de confiance en sélectionnant **Outils > Options Internet** dans la barre de menus d'Internet Explorer et, dans l'onglet **Sécurité**, cliquez sur le bouton **Sites**.

Utiliser des paramètres de registre Windows pour configurer la redirection Flash

Si vous êtes un utilisateur de domaine sans privilèges d'administrateur sur le serveur Active Directory, vous pouvez également configurer la redirection Flash en définissant les valeurs appropriées dans des clés de registre Windows sur le poste de travail distant.

Vous pouvez utiliser cette procédure comme alternative à l'utilisation des paramètres GPO pour configurer la redirection Flash.

Prérequis

- Compilez une liste blanche de sites Web pour vous assurer que seules les URL spécifiées dans la liste pourront rediriger du contenu Flash. Même si vous pouvez compiler une liste noire de sites Web, vous ne pouvez pas utiliser les paramètres de Registre Windows pour activer la liste noire. Une liste noire garantit que seules les URL spécifiées dans la liste ne pourront pas rediriger du contenu Flash. Pour activer une liste noire, vous devez utiliser les paramètres GPO pour la redirection Flash.
- Vérifiez qu'Horizon Agent 7.0 ou version ultérieure est installé sur le poste de travail distant, ainsi que Flash Player et Internet Explorer 9, 10 ou 11. Reportez-vous à la section « Installer et configurer la redirection Flash », page 17.
- Vérifiez que vous utilisez Horizon Client 4.0 ou version ultérieure, ainsi que la version ActiveX de Flash Player.

Procédure

1 Utilisez Horizon Client pour accéder au poste de travail distant (machine agent).

2 Ouvrez l'Éditeur du Registre Windows (`regedit.exe`) sur la machine agent, accédez au dossier suivant et définissez **FlashRedirection** sur **`1`** :

```
HKLM\Software\VMware, Inc.\VMware FlashMMR
```

Remarque Ce paramètre active la fonctionnalité de redirection Flash, mais si ce paramètre est désactivé (défini sur 0) dans `HKLM\Software\Policies\VMware, Inc.\VMware FlashMMR`, cela signifie que la redirection Flash est désactivée dans tout le domaine et qu'un administrateur de domaine doit l'activer.

---

3 Accédez au dossier suivant :

```
HKEY_CURRENT_USER\SOFTWARE\VMware, Inc.\VMware FlashMMR
```

Si ce dossier n'existe pas déjà, créez-le.

4 Dans le dossier `VMware FlashMMR`, créez une sous-clé **UrlWhiteList**.

5 Cliquez avec le bouton droit sur la clé **UrlWhiteList**, sélectionnez **Nouveau > Valeur de chaîne** et, pour le nom, entrez l'URL d'un site Web qui utilisera la redirection Flash.

Vous pouvez utiliser des expressions régulières. Par exemple, vous pouvez spécifier **`https://*.google.com`**. Veillez à laisser la valeur **Données** vide.

6 (Facultatif) (Horizon 7.0.1 et 7.0.2 uniquement) Dans le champ de données de la nouvelle valeur de registre, ajoutez les données **`requireIECompatibility=true`**, **`appMode=0`** ou les deux (utilisez une virgule pour séparer les deux chaînes).

Les sites Web prennent en charge HTML5 par défaut. La redirection Flash ne fonctionne pas sur ces sites Web. Vous devez définir **`requireIECompatibility=true`** pour que ces sites fonctionnent. Ce paramètre n'est pas requis pour le site Web YouTube.

Par défaut, l'interface externe est activée lorsque la redirection Flash s'exécute. Cela peut dégrader les performances. Pour Horizon 7.0.1 ou version ultérieure, dans certaines situations, le paramètre **`appMode=0`** peut améliorer les performances et le paramètre **`appMode=1`** peut conduire à une meilleure expérience utilisateur.

7 Répétez l'étape précédente pour ajouter des URL supplémentaires et, lorsque vous avez terminé, fermez l'Éditeur du Registre.

8 Sur la machine agent, ouvrez une invite de commande et passez sur le répertoire suivant :

```
%Program Files%\Common Files\VMware\Remote Experience
```

9 Exécutez la commande suivante pour ajouter la liste blanche à Internet Explorer.

```
cscript  mergeflashmmrwhitelist.vbs
```

10 Redémarrez Internet Explorer.

Les sites définis avec le paramètre **`requireIECompatibility=true`** sont ajoutés à l'affichage de compatibilité d'Internet Explorer. Vous pouvez le vérifier en sélectionnant **Outils > Paramètres d'affichage de compatibilité** dans la barre de menus.

Dans Horizon 7.0 uniquement, les sites sont également ajoutés à la liste de sites de confiance d'Internet Explorer. Vous pouvez vérifier les sites de confiance en sélectionnant **Outils > Options Internet** dans la barre de menus d'Internet Explorer et, dans l'onglet **Sécurité**, cliquez sur le bouton **Sites**.

Configuration de l'Audio/Vidéo en temps réel

Audio/Vidéo en temps réel permet aux utilisateurs d'Horizon 7 d'exécuter Skype, Webex, Google Hangouts et d'autres applications de conférence en ligne sur leur poste de travail distant. Avec l'Audio/Vidéo en temps réel, les webcams et les périphériques audio qui sont connectés localement au système client sont redirigés vers le poste de travail distant. Cette fonctionnalité redirige les données vidéo et audio vers le poste de travail avec une bande passante beaucoup plus faible que celle utilisée par la redirection USB.

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.

Cette fonctionnalité installe une webcam virtuelle et un microphone virtuel VMware sur le système d'exploitation du poste de travail. La webcam virtuelle VMware utilise un pilote de webcam en mode noyau qui offre une compatibilité améliorée avec les applications vidéo basées sur un navigateur et avec d'autres logiciels de conférence tiers.

Lorsqu'une application de conférence ou vidéo est lancée, elle affiche et utilise ces périphériques virtuels VMware qui gèrent la redirection audio-vidéo à partir des périphériques connectés localement sur le client. La webcam et le microphone virtuels VMware s'affichent dans le Gestionnaire de périphériques sur le système d'exploitation du poste de travail.

Les pilotes des webcams et des périphériques audio doivent être installés sur vos systèmes Horizon Client pour permettre la redirection.

Options de configuration de la fonctionnalité Audio-vidéo en temps réel

Lorsque vous installez Horizon Agent avec Audio/Vidéo en temps réel, la fonctionnalité s'utilise sur vos postes de travail Horizon 7 sans autre configuration. Il est recommandé d'utiliser les valeurs par défaut de la fréquence et de la résolution d'images pour la plupart des périphériques et applications courantes.

Vous pouvez configurer les paramètres de stratégie de groupe pour modifier ces valeurs par défaut et les adapter à des applications, webcams ou environnements particuliers. Vous pouvez également définir une stratégie pour désactiver ou activer la fonctionnalité. Un fichier de modèle d'administration ADMX vous permet d'installer les paramètres de stratégie de groupe Audio/Vidéo en temps réel sur Active Directory ou sur des postes de travail individuels. Reportez-vous à la section « Configuration des paramètres de stratégie de groupe de l'Audio/Vidéo en temps réel », page 32.

Si vous disposez de plusieurs webcams et périphériques d'entrée audio intégrés ou connectés à vos ordinateurs client, vous pouvez configurer des webcams et des périphériques d'entrée audio préférés qui seront redirigés vers vos postes de travail. Reportez-vous à la section « Sélection de webcams et microphones préférés », page 23.

Remarque Vous pouvez sélectionner un périphérique audio préféré, mais aucune autre option de configuration audio n'est disponible.

Lorsque les images de la webcam et l'entrée audio sont redirigées vers un poste de travail distant, vous ne pouvez pas accéder à la webcam et aux périphériques audio de l'ordinateur local. Inversement, lorsque ces périphériques sont utilisés sur l'ordinateur local, vous ne pouvez pas y accéder via le poste de travail distant.

Pour plus d'informations sur les applications prises en charge, consultez l'article de la base de connaissances VMware *Directives pour l'utilisation de l'Audio/Vidéo en temps réel avec des applications tierces sur les postes de travail Horizon View*, à l'adresse http://kb.vmware.com/kb/2053754.

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

Vous installez la fonctionnalité Audio/Vidéo en temps réel en installant View Agent 6.0 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure. Pour utiliser cette fonctionnalité avec des applications et des postes de travail publiés, vous devez installer Horizon Agent 7.0.2 ou version ultérieure. Consultez le document Configuration pour plus d'informations sur l'installation d'Horizon Agent.

Logiciel Horizon Client

Horizon Client 2.2 pour Windows ou versions ultérieures

Horizon Client 2.2 pour Linux ou version ultérieure. S'agissant de Horizon Client pour Linux 3.1 ou d'une version antérieure, cette fonctionnalité n'est disponible que pour la version de Horizon Client pour Linux fournie par des fournisseurs tiers. S'agissant de Horizon Client pour Linux 3.2 et versions ultérieures, cette fonction est également disponible pour les versions du client distribuées par VMware.

Horizon Client 2.3 pour Mac ou version ultérieure

Horizon Client 4.0 pour iOS ou version ultérieure.

Horizon Client 4.0 pour Android ou version ultérieure.

Ordinateur Horizon Client ou périphérique d'accès client

- Tous les systèmes d'exploitation exécutant Horizon Client pour Windows.
- Tous les systèmes d'exploitation exécutant Horizon Client pour Linux sur des périphériques x86. Cette fonctionnalité n'est pas prise en charge par les processeurs ARM.
- Mac OS X Mountain Lion (10.8) et versions ultérieures. Elle est désactivée sur tous les systèmes d'exploitation Mac OS X antérieurs.
- Tous les systèmes d'exploitation exécutant Horizon Client pour iOS.
- Tous les systèmes d'exploitation exécutant Horizon Client pour Android.
- Pour plus d'informations sur les systèmes d'exploitation client pris en charge, reportez-vous au document *Utilisation de VMware Horizon Client* concernant le système ou périphérique approprié.
- 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)

Garantir que l'Audio/Vidéo en temps réel est utilisée plutôt que la redirection USB

Audio/Vidéo en temps réel prend en charge la redirection de webcam et d'entrée audio pour une utilisation dans des applications de conférence. La fonctionnalité Redirection USB qui peut être installée avec Horizon Agent ne prend pas en charge la redirection de webcam. Si vous redirigez des périphériques d'entrée audio au moyen de la redirection USB, le flux audio ne se synchronise pas correctement avec la vidéo pendant les sessions Audio/Vidéo en temps réel, et vous perdez l'avantage de la réduction de la demande sur la bande passante réseau. Vous pouvez prendre des mesures pour garantir que les webcams et les périphériques d'entrée audio sont redirigés vers vos postes de travail au moyen d'Audio/Vidéo en temps réel, et non avec Redirection USB.

Si vos postes de travail sont configurés avec la redirection USB, les utilisateurs finaux peuvent connecter et afficher leurs périphériques USB connectés localement en sélectionnant l'option **Connecter un périphérique USB** dans la barre de menus du client Windows ou dans le menu **Poste de travail > USB** du client Mac. Les clients Linux bloquent la redirection USB des périphériques audio et vidéo par défaut et ne fournissent pas d'options de périphériques USB aux utilisateurs finaux.

Si l'utilisateur final sélectionne un périphérique USB dans le menu **Connecter un périphérique USB** ou la liste **Poste de travail > USB**, ce périphérique devient inutilisable pour la conférence vidéo ou audio. Par exemple, si un utilisateur passe un appel Skype, l'image de la vidéo peut ne pas s'afficher ou le flux audio peut être dégradé. Si un utilisateur final sélectionne un périphérique pendant une session de conférence, la redirection de webcam ou audio est interrompue.

Pour masquer ces périphériques aux utilisateurs finaux et éviter des perturbations potentielles, vous pouvez configurer les paramètres de la stratégie de groupe Redirection USB pour désactiver l'affichage des webcam et des périphériques d'entrée audio dans VMware Horizon Client.

Vous pouvez notamment créer des règles de filtrage de redirection USB pour Horizon Agent et spécifier les noms de famille de périphériques `audio-in` et `video` à désactiver. Pour plus d'informations sur la définition de stratégies de groupe et la spécification de règles de filtrage pour la redirection USB, reportez-vous à « Utilisation de règles pour contrôler la redirection USB », page 85.

Avertissement Si vous ne configurez pas de règles de filtrage de redirection USB pour désactiver des familles de périphériques USB, informez vos utilisateurs finaux qu'ils ne peuvent pas sélectionner des périphériques webcam ou audio dans le menu **Connecter un périphérique USB** ou la liste **Poste de travail > USB** dans la barre de menus de VMware Horizon Client.

Sélection de webcams et microphones préférés

Si un ordinateur client dispose de plus d'une webcam et d'un microphone, vous pouvez configurer une webcam et un microphone par défaut que la fonctionnalité audio/vidéo en temps réel redirige vers le poste de travail. Ces périphériques peuvent être intégrés ou connectés à l'ordinateur client local.

Sur un ordinateur client Windows sur lequel Horizon Client pour Windows 4.2 ou version ultérieure est installé, vous pouvez sélectionner une webcam ou un microphone préféré en configurant des paramètres Audio/Vidéo en temps réel dans la boîte de dialogue Paramètres d'Horizon Client. Avec les versions antérieures d'Horizon Client, vous modifiez les paramètres de Registre pour sélectionner une webcam préférée et utilisez le contrôle du son dans le système d'exploitation Windows pour sélectionner un microphone par défaut.

Sur un ordinateur client Mac, vous pouvez spécifier une webcam ou un microphone préféré à l'aide du système de valeurs par défaut de Mac.

Sur un ordinateur client Linux, vous pouvez spécifier une webcam préférée en modifiant un fichier de configuration. Pour sélectionner un microphone par défaut, vous pouvez configurer le contrôle du son dans le système d'exploitation Linux sur l'ordinateur client.

La fonctionnalité audio/vidéo en temps réel redirige la webcam préférée si elle est disponible. Autrement, la fonctionnalité audio/vidéo en temps réel utilise la première webcam énumérée par le système.

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.

Cette procédure s'applique uniquement à Horizon Client pour Windows 4.2 et versions ultérieures. Pour les versions de client antérieures, vous devez modifier les paramètres de Registre pour sélectionner une webcam préférée et utiliser le contrôle du son dans le système d'exploitation Windows pour sélectionner un microphone par défaut. Pour plus d'informations, consultez le document *Utilisation de VMware Horizon Client pour Windows* correspondant à votre version d'Horizon Client.

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.

Sélectionner un microphone par défaut sur un système client Mac

Si plusieurs microphones sont connectés à votre système client, un seul d'entre eux peut être utilisé sur votre poste de travail distant. Vous pouvez spécifier le microphone par défaut à utiliser sur le poste de travail distant dans les Préférences système du système client.

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

Cette procédure explique comment choisir un microphone par défaut dans l'interface utilisateur du système client. Les administrateurs peuvent également configurer un microphone préféré en utilisant le système de valeurs par défaut de Mac. Reportez-vous à la section « Configurer une webcam ou un microphone préféré sur un système client Mac », page 26.

Important Si vous utilisez un microphone USB, ne le connectez pas via le menu **Connexion > USB** d'Horizon Client. En effet, cette opération achemine le périphérique via la redirection USB, si bien qu'il ne pourra pas utiliser la fonctionnalité Audio/Vidéo en temps réel.

Prérequis

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

Procédure

1. Sur votre système client, sélectionnez **Menu Apple > Préférences système**, puis cliquez sur **Son**.
2. Ouvrez le volet Entrée des préférences de son.
3. Sélectionnez le microphone de votre choix.

Ainsi, dès que vous vous connecterez à un poste de travail distant et effectuerez un appel, le poste de travail utilisera le microphone que vous avez sélectionné sur le système client.

Configuration de l'Audio/Vidéo en temps réel sur un client Mac

Vous pouvez configurer les paramètres Audio/Vidéo en temps réel sur la ligne de commande en utilisant le système de valeurs par défaut de Mac. Le système de valeurs par défaut vous permet de lire, d'écrire et de supprimer des valeurs d'utilisateur par défaut Mac à l'aide de l'application Terminal (`/Applications/Utilities/Terminal.app`).

Les valeurs par défaut de Mac appartiennent à des domaines. Les domaines correspondent généralement à des applications individuelles. Le domaine de la fonctionnalité Audio/Vidéo en temps réel est com.vmware.rtav.

Syntaxe de configuration de la fonctionnalité Audio/Vidéo en temps réel

Pour configurer la fonctionnalité Audio/Vidéo en temps réel, vous pouvez utiliser les commandes suivantes.

Tableau 2-2. Syntaxe des commandes de configuration de la fonctionnalité Audio/Vidéo en temps réel

vdmadmin	Description
`defaults write com.vmware.rtav scrWCamId "`*webcam-userid*`"`	Définit la webcam préférée à utiliser sur des postes de travail distants. Si cette valeur n'est pas définie, la webcam est automatiquement sélectionnée par l'énumération système. Vous pouvez spécifier n'importe quelle webcam connectée (ou intégrée) au système client.
`defaults write com.vmware.rtav srcAudioInId "`*audio-device-userid*`"`	Définit le microphone (périphérique d'entrée audio) préféré à utiliser sur des postes de travail distants. Si cette valeur n'est pas définie, les postes de travail distants utilisent le périphérique d'enregistrement par défaut du système client. Vous pouvez spécifier n'importe quel microphone connecté (ou intégré) au système client.
`defaults write com.vmware.rtav srcWCamFrameWidth` *pixels*	Définit la largeur de l'image. La valeur par défaut est une valeur codée en dur de 320 pixels. Vous pouvez modifier la largeur de l'image par n'importe quelle valeur de pixel.
`defaults write com.vmware.rtav srcWCamFrameHeight` *pixels*	Définit la hauteur de l'image. La valeur par défaut est une valeur codée en dur de 240 pixels. Vous pouvez modifier la hauteur de l'image par n'importe quelle valeur de pixel.
`defaults write com.vmware.rtav srcWCamFrameRate` *fps*	Définit la fréquence d'images. La valeur par défaut est de 15 ips. Vous pouvez modifier la fréquence d'images par n'importe quelle valeur.
`defaults write com.vmware.rtav LogLevel "`*level*`"`	Définit le niveau de journalisation du fichier journal de la fonctionnalité Audio/Vidéo en temps réel (`~/Library/Logs/VMware/vmware-RTAV-`*`pid`*`.log`). Vous pouvez définir le niveau de journalisation sur le suivi ou le débogage.
`defaults write com.vmware.rtav IsDisabled` *value*	Détermine si la fonctionnalité Audio/Vidéo en temps réel est activée ou désactivée. La fonctionnalité Audio/Vidéo en temps réel est activée par défaut. (Cette valeur n'est pas appliquée.) Pour désactiver la fonctionnalité Audio/Vidéo en temps réel sur le client, définissez la valeur sur True.
`defaults read com.vmware.rtav`	Affiche les paramètres de configuration de la fonctionnalité Audio/Vidéo en temps réel.
`defaults delete com.vmware.rtav` *setting*	Supprime un paramètre de configuration de la fonctionnalité Audio/Vidéo en temps réel. Par exemple : `defaults delete com.vmware.rtav srcWCamFrameWidth`

Remarque Vous pouvez définir une fréquence d'images comprise entre 1 et 25 ips et une résolution maximale de 1 920 x 1 080. Une résolution élevée à une fréquence d'images rapide peut ne pas être prise en charge par tous les périphériques de vos environnements.

Configurer une webcam ou un microphone préféré sur un système client Mac

Avec la fonctionnalité Audio/Vidéo en temps réel, si vous disposez de plusieurs webcams et microphones sur votre système client, vous ne pouvez en utiliser qu'un seul sur votre poste de travail distant. Vous pouvez spécifier vos webcam et microphone préférés sur la ligne de commande en utilisant le système de valeurs par défaut de Mac.

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

Dans la plupart des environnements, il n'est pas nécessaire de configurer une webcam ou un microphone préféré. Si vous ne définissez pas de microphone préféré, les postes de travail distants utilisent le périphérique audio par défaut défini dans les Préférences systèmes du système client. Reportez-vous à

« Sélectionner un microphone par défaut sur un système client Mac », page 25. Si vous ne configurez pas de webcam préférée, les postes de travail distants sélectionnent la webcam par énumération.

Prérequis

- Si vous configurez une webcam USB préférée, vérifiez que cette dernière est installée et opérationnelle sur le système client.
- Si vous configurez un microphone USB (ou un autre type) préféré, vérifiez que ce dernier est installé et opérationnel sur le système client.
- Vérifiez que vous utilisez le protocole d'affichage VMware Blast ou PCoIP pour votre poste de travail distant.

Procédure

1 Sur votre système client Mac, démarrez une application de webcam ou de microphone pour déclencher une énumération des périphériques de caméra ou audio dans le fichier journal de la fonctionnalité Audio/Vidéo en temps réel.

   a Connectez la webcam ou le périphérique audio.

   b Dans le dossier **Applications**, double-cliquez sur **VMware Horizon Client** pour démarrer Horizon Client.

   c Démarrez un appel, puis arrêtez-le.

2 Recherchez les entrées de journal correspondant à la webcam ou au microphone dans le fichier journal de la fonctionnalité Audio/Vidéo en temps réel.

   a Dans un éditeur de texte, ouvrez le fichier journal de la fonctionnalité Audio/Vidéo en temps réel.

      Le fichier journal de la fonctionnalité Audio/Vidéo en temps réel se nomme `~/Library/Logs/VMware/vmware-RTAV-`*`pid`*`.log`, où *pid* est l'ID de processus de la session actuelle.

   b Recherchez dans le fichier journal de la fonctionnalité Audio/Vidéo en temps réel les entrées qui identifient les webcams ou microphones connectés.

   L'exemple suivant montre comment les entrées de webcam peuvent s'afficher dans le fichier journal de la fonctionnalité Audio/Vidéo en temps réel :

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() -
1 Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() -
Name=FaceTime HD Camera (Built-in)   UserId=FaceTime HD Camera (Built-
in)#0xfa20000005ac8509   SystemId=0xfa20000005ac8509
```

   L'exemple suivant montre comment les entrées de microphone peuvent s'afficher dans le fichier journal de la fonctionnalité Audio/Vidéo en temps réel :

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: int
AVCaptureEnumerateAudioDevices(MMDev::DeviceList&) -
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum()
- 2 Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum()
- Index=255   Name=Built-in Microphone   UserId=Built-in Microphone#AppleHDAEngineInput:1B,
```

```
0,1,0:1   SystemId=AppleHDAEngineInput:1B,0,1,0:1
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum()
- Index=255   Name=Built-in Input   UserId=Built-in Input#AppleHDAEngineInput:1B,0,1,1:2
SystemId=AppleHDAEngineInput:1B,0,1,1:2
```

3 Recherchez dans le fichier journal de la fonctionnalité Audio/Vidéo en temps réel la webcam ou le microphone que vous préférez et notez son ID d'utilisateur.

   L'ID d'utilisateur est affiché dans le fichier journal après la chaîne UserId=. Par exemple, l'ID d'utilisateur de la caméra FaceTime interne est « FaceTime HD Camera (Built-in) » et celui du microphone interne est « Built-in Microphone ».

4 Dans Terminal (`/Applications/Utilities/Terminal.app`), utilisez la commande `defaults write` pour définir la webcam ou le microphone préféré.

Option	Action
Définir la webcam préférée	Tapez **`defaults write com.vmware.rtav srcWCamId "webcam-userid"`**, où *webcam-userid* correspond à l'ID d'utilisateur de la webcam préférée que vous pouvez trouver dans le fichier journal de la fonctionnalité Audio/Vidéo en temps réel. Par exemple : `defaults write com.vmware.rtav srcWCamId "HD Webcam C525”`
Définir le microphone préféré	Tapez **`defaults write com.vmware.rtav srcAudioInId "audio-device-userid"`**, où *audio-device-userid* correspond à l'ID d'utilisateur du microphone préféré que vous pouvez trouver dans le fichier journal de la fonctionnalité Audio/Vidéo en temps réel. Par exemple : `defaults write com.vmware.rtav srcAudioInId "Built-in Microphone"`

5 (Facultatif) Utilisez la commande `defaults read` pour vérifier les modifications que vous avez apportées à la fonctionnalité Audio/Vidéo en temps réel.

   Par exemple : **`defaults read com.vmware.rtav`**

   Cette commande répertorie l'ensemble des paramètres de la fonctionnalité Audio/Vidéo en temps réel.

Désormais, lors de la connexion à un poste de travail distant ou du démarrage d'un appel, le poste de travail utilisera la webcam ou le microphone préféré que vous avez configurés, s'ils sont disponibles. S'ils ne sont pas disponibles, le poste de travail distant pourra utiliser une autre webcam ou un autre microphone disponible.

Sélectionner un microphone par défaut sur un système client Linux

Si plusieurs microphones sont connectés à votre système client, un seul d'entre eux peut être utilisé sur votre poste de travail Horizon 7. Pour spécifier le microphone par défaut, vous pouvez utiliser le contrôle du son de votre système client.

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

Cette procédure explique comment sélectionner un microphone par défaut depuis l'interface utilisateur du système client. Les administrateurs peuvent également configurer un microphone préféré en modifiant un fichier de configuration. Reportez-vous à la section « Sélectionner une webcam ou un microphone préféré sur un système client Linux », page 29.

Prérequis

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

Procédure

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

   Vous pouvez également cliquer sur l'icône **Son** à droite de la barre d'outils en haut de l'écran.

2 Cliquez sur l'onglet **Entrée** dans la boîte de dialogue Préférences de son.

3 Sélectionnez le périphérique préféré et cliquez sur **Fermer**.

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

Avec la fonctionnalité Audio/Vidéo en temps réel, si vous disposez de plusieurs webcams et microphones sur votre système client, vous ne pouvez en utiliser qu'un seul sur votre poste de travail Horizon 7. Pour désigner la webcam et le microphone préférés, vous pouvez modifier un fichier de configuration.

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

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

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

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

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

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

Prérequis

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

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

Procédure

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

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

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

   c Démarrez un appel, puis arrêtez-le.

   Ce processus crée un fichier journal.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Configuration des paramètres de stratégie de groupe de l’Audio/Vidéo en temps réel

Vous pouvez configurer les paramètres de stratégie de groupe qui permettent de contrôler le comportement de l’Audio/Vidéo en temps réel (RTAV) sur vos postes de travail Horizon 7. Ces paramètres définissent la fréquence et la résolution d'images maximales d'une webcam virtuelle. Ces paramètres vous permettent de définir la bande passante maximale qu'un utilisateur peut utiliser. Un paramètre supplémentaire permet de désactiver/activer la fonctionnalité Audio/Vidéo en temps réel (RTAV).

Vous n'avez pas à configurer ces paramètres de stratégie. L’Audio/Vidéo en temps réel utilise la fréquence et la résolution d'images qui sont fixées pour la webcam des systèmes client. Les paramètres par défaut sont recommandés pour la plupart des applications webcam et audio.

Pour voir des exemples d'utilisation de bande passante pour l’Audio/Vidéo en temps réel, reportez-vous à « Bande passante de l'Audio/Vidéo en temps réel », page 35.

Ces paramètres de stratégie affectent vos postes de travail Horizon 7 et non les systèmes client auxquels les périphériques physiques sont connectés. Pour configurer ces paramètres sur vos postes de travail, ajoutez le fichier de modèle d'administration (ADMX) de stratégie de groupe pour l'Audio/Vidéo en temps réel (RTAV) dans Active Directory.

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.

Ajouter le modèle d'administration ADMX pour l'Audio/Vidéo en temps réel (RTAV) dans Active Directory et configurer les paramètres

Vous pouvez ajouter les paramètres de stratégie dans le fichier ADMX RTAV (`vdm_agent_rtav.admx`) à des objets de stratégie de groupe (GPO) dans Active Directory et configurer les paramètres dans l'Éditeur d'objets de stratégie de groupe.

Prérequis

- Vérifiez que l'option de configuration RTAV est installée sur vos postes de travail. Cette option de configuration est installée par défaut mais peut être désélectionnée pendant l'installation. Les paramètres n'ont aucun effet si RTAV n'est pas installé. Consultez le document Configuration pour plus d'informations sur l'installation d'Horizon Agent.
- Vérifiez que les objets de stratégie de groupe (GPO) dans Active Directory sont créés pour les paramètres de stratégie de groupe RTAV. Les objets de stratégie de groupe (GPO) doivent être liés à l'unité d'organisation (UO) qui contient vos postes de travail. Reportez-vous à la section « Exemple de stratégie de groupe Active Directory », page 192.
- Vérifiez que les composants logiciels enfichables Microsoft MMC (Microsoft Management Console) et l'Éditeur d'objets de stratégie de groupe sont disponibles sur votre serveur Active Directory.
- Familiarisez-vous avec les paramètres de stratégie de groupe RTAV. Reportez-vous à la section « Paramètres de stratégie de groupe de l'Audio/Vidéo en temps réel », page 34.

Procédure

1. Téléchargez le fichier Horizon 7 GPO Bundle `.zip` 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 GPO Bundle.

   Le fichier se nomme `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, où *x.x.x* est la version et *yyyyyyy* le numéro de build. Tous les fichiers ADMX qui fournissent des paramètres de stratégie de groupe pour Horizon 7 sont disponibles dans ce fichier.

2. Décompressez le fichier `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip` et copiez les fichiers ADMX sur votre hôte Active Directory ou RDS.

   a. Copiez le fichier `vdm_agent_rtav.admx`, ainsi que le dossier `en-US` dans le dossier `C:\Windows\PolicyDefinitions` sur votre hôte Active Directory ou RDS.

   b. (Facultatif) Copiez le fichier de ressources de la langue (`vdm_agent_rtav.adml`) dans le sous-dossier correspondant dans `C:\Windows\PolicyDefinitions\` sur votre hôte Active Directory ou RDS.

3. Sur l'hôte Active Directory, ouvrez l'Éditeur de gestion de stratégie de groupe et entrez le chemin vers le fichier de modèle dans l'éditeur.

   Sur un hôte RDS individuel, vous pouvez ouvrir l'Éditeur de stratégie de groupe locale avec l'utilitaire `gpedit.msc`.

   Les paramètres se situent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Configuration de RTAV pour View**.

Suivant

Configurez les paramètres de stratégie de groupe.

Paramètres de stratégie de groupe de l'Audio/Vidéo en temps réel

Les paramètres de la stratégie de groupe Audio/Vidéo en temps réel (RTAV) contrôlent la fréquence et la résolution maximales des images d'une webcam virtuelle. Un paramètre supplémentaire permet de désactiver ou d'activer la fonctionnalité RTAV. Ces paramètres de stratégie affectent les postes de travail distants, et non les systèmes clients sur lesquels les périphériques physiques sont connectés.

Si vous ne configurez pas les paramètres de la stratégie de groupe RTAV, RTAV utilise les valeurs qui sont définies sur les systèmes clients. Sur les systèmes clients, la fréquence d'images par défaut de la webcam est de 15 images par seconde. La résolution d'image par défaut de la webcam est de 320 x 240 pixels.

Les paramètres de stratégie de groupe de résolution déterminent les valeurs maximales pouvant être utilisées. La fréquence d'images et la résolution d'image qui sont définies sur les systèmes clients sont des valeurs absolues. Par exemple, si vous configurez les paramètres RTAV pour une résolution d'image maximale de 640 x 480 pixels, la webcam affiche n'importe quelle résolution qui est définie sur le client jusqu'à 640 x 480 pixels. Si vous définissez la résolution d'image sur le client sur une valeur supérieure à 640 x 480 pixels, la résolution du client est limitée à 640 x 480 pixels.

Toutes les configurations ne peuvent pas atteindre les valeurs maximales de la stratégie de groupe, à savoir une résolution de 1920 x 1080 à 25 images par seconde. La fréquence d'images maximale que votre configuration peut atteindre pour une résolution donnée dépend de la webcam utilisée, du matériel du système client, du matériel virtuel d'Horizon Agent et de la bande passante disponible.

Les paramètres de la stratégie de groupe de résolution déterminent les valeurs par défaut qui sont utilisées lorsque les valeurs de résolution ne sont pas définies par l'utilisateur.

Paramètre de stratégie de groupe	Description
`Disable RTAV`	Lorsque vous activez ce paramètre, la fonctionnalité Audio/Vidéo en temps réel est désactivée. Lorsque ce paramètre n'est pas configuré ou est désactivé, Audio/Vidéo en temps réel est activé. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration de RTAV pour VMware** dans l'Éditeur de gestion de stratégie de groupe.
`Max frames per second`	Détermine le nombre maximal d'images par seconde auquel la webcam peut capturer des images. Vous pouvez utiliser ce paramètre pour limiter la fréquence d'images de la webcam dans des environnements à faible bande passante réseau. La valeur minimale est d'une image par seconde. La valeur maximale est de 25 images par seconde. Lorsque ce paramètre n'est pas configuré ou est désactivé, aucune fréquence d'images maximale n'est définie. Audio/Vidéo en temps réel utilise la fréquence d'images qui est sélectionnée pour la webcam sur le système client. Par défaut, les webcams clientes ont une fréquence d'images de 15 images par seconde. Si aucun paramètre n'est configuré sur le système client et si le paramètre **Nombre maximal d'images par seconde** n'est pas configuré ou est désactivé, la webcam capture 15 images par seconde. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration de RTAV pour VMware > Paramètres RTAV de la webcam VMware** dans l'Éditeur de gestion de stratégie de groupe.
`Resolution – Max image width in pixels`	Détermine la largeur maximale, en pixels, des images capturées par la webcam. En définissant une faible largeur maximale d'image, vous pouvez diminuer la résolution des images capturées et ainsi améliorer l'expérience de visualisation dans les environnements réseau à faible bande passante. Lorsque ce paramètre n'est pas configuré ou est désactivé, la largeur maximale d'image n'est pas définie. RTAV utilise la largeur d'image définie sur le système client. La largeur par défaut d'une image de webcam sur un système client est de 320 pixels. La limite maximale d'une image de webcam est de 1 920 x 1 080 pixels. Si vous configurez ce paramètre avec une valeur supérieure à 1 920 pixels, la largeur d'image maximale effective est de 1 920 pixels. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration de RTAV pour VMware > Paramètres RTAV de la webcam VMware** dans l'Éditeur de gestion de stratégie de groupe.

Paramètre de stratégie de groupe	Description
`Resolution – Max image height in pixels`	Détermine la hauteur maximale, en pixels, des images capturées par la webcam. En définissant une faible hauteur maximale d'image, vous pouvez diminuer la résolution des images capturées et ainsi améliorer l'expérience de visualisation dans des environnements réseau à faible bande passante. Lorsque ce paramètre n'est pas configuré ou est désactivé, la hauteur maximale d'image n'est pas définie. RTAV utilise la hauteur d'image définie sur le système client. La hauteur par défaut d'une image de webcam sur un système client est de 240 pixels. La limite maximale d'une image de webcam est de 1 920 x 1 080 pixels. Si vous configurez ce paramètre avec une valeur supérieure à 1 080 pixels, la hauteur d'image maximale effective est de 1 080 pixels. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration de RTAV pour VMware > Paramètres RTAV de la webcam VMware** dans l'Éditeur de gestion de stratégie de groupe.
`Resolution – Default image resolution width in pixels`	Détermine la largeur de la résolution par défaut, en pixels, des images capturées par la webcam. Ce paramètre est utilisé lorsqu'aucune valeur de résolution n'est définie par l'utilisateur. Lorsque ce paramètre n'est pas configuré ou est désactivé, la largeur d'image par défaut est de 320 pixels. La valeur qui est configurée par ce paramètre de stratégie s'applique uniquement si View Agent 6.0 ou version ultérieure et Horizon Client 3.0 ou version ultérieure sont utilisés. Pour des versions plus anciennes de View Agent et d'Horizon Client, ce paramètre de stratégie n'a aucun effet et la largeur d'image par défaut est de 320 pixels. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration de RTAV pour VMware > Paramètres RTAV de la webcam VMware** dans l'Éditeur de gestion de stratégie de groupe.
`Resolution – Default image resolution height in pixels`	Détermine la hauteur de la résolution par défaut, en pixels, des images capturées par la webcam. Ce paramètre est utilisé lorsqu'aucune valeur de résolution n'est définie par l'utilisateur. Lorsque ce paramètre n'est pas configuré ou est désactivé, la hauteur d'image par défaut est de 240 pixels. La valeur qui est configurée par ce paramètre de stratégie s'applique uniquement si View Agent 6.0 ou version ultérieure et Horizon Client 3.0 ou version ultérieure sont utilisés. Pour les versions plus anciennes de View Agent et d'Horizon Client, ce paramètre de stratégie n'a aucun effet et la hauteur d'image par défaut est de 240 pixels. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration de RTAV pour VMware > Paramètres RTAV de la webcam VMware** dans l'Éditeur de gestion de stratégie de groupe.

Bande passante de l'Audio/Vidéo en temps réel

La bande passante de la fonctionnalité Audio/Vidéo en temps réel varie selon la résolution et la fréquence d'image de la webcam, ainsi que des données images et audio en cours de capture.

Les exemples de tests présentés dans Tableau 2-3 mesurent la bande passante que la fonctionnalité Audio/Vidéo en temps réel utilise dans un environnement View avec une webcam et des périphériques d'entrée vidéo standard. Les tests mesurent la bande passante permettant d'envoyer des données vidéo et audio d'Horizon Client à Horizon Agent. La bande passante totale requise pour exécuter une session de poste de travail à partir d'Horizon Client peut être supérieure à ces chiffres. Au cours de ces tests, la webcam capture des images à 15 images/seconde pour la résolution de chaque image.

Tableau 2-3. Résultats de l'exemple de bande passante pour envoyer des données Audio/Vidéo en temps réel d' Horizon Client à Horizon Agent

Résolution de l'image (largeur x hauteur)	Bande passante utilisée (Kbits/s)
160 x 120	225
320 x 240	320
640 x 480	600

Configuration de la redirection de scanner

La redirection de scanner permet aux utilisateurs de Horizon 7 d'analyser les informations qui se trouvent sur leurs applications et postes de travail distants à l'aide de périphériques d'analyse et d'acquisition d'images connectés localement à leurs ordinateurs clients. La redirection de scanner est disponible dans Horizon 6.0.2 et versions ultérieures.

La redirection de scanner prend en charge les périphériques d'analyse et d'acquisition d'images standard compatibles avec les formats TWAIN et WIA.

Une fois que vous avez installé Horizon Agent avec l'option de configuration Redirection de scanner, la fonctionnalité est opérationnelle sur vos applications et postes de travail distants, sans configuration supplémentaire. Vous n'avez besoin de configurer aucun pilote spécifique au scanner sur les applications ou postes de travail distants.

Vous pouvez configurer les paramètres de stratégie de groupe et modifier les valeurs par défaut pour les adapter à des environnements ou applications d'acquisition d'images spécifiques. Vous pouvez également définir une stratégie pour désactiver ou activer la fonctionnalité. Un fichier de modèle d'administration ADMX vous permet d'installer des paramètres de stratégie de groupe de redirection de scanner dans Active Directory ou sur des postes de travail individuels. Reportez-vous à la section « Configuration des paramètres de stratégie de groupe de redirection de scanner », page 38.

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

Configuration système requise pour la redirection de scanner

Pour prendre en charge la redirection de scanner, le déploiement de votre Horizon 7 doit répondre à certaines exigences matérielles et logicielles.

Application ou poste de travail distant Horizon 7

Cette fonctionnalité est prise en charge sur les postes de travail RDS, les applications RDS et les postes de travail VDI déployés sur des machines virtuelles mono-utilisateur.

Vous devez installer View Agent 6.0.2 ou une version ultérieure sur les machines virtuelles parentes ou modèles, ou sur les hôtes RDS, et sélectionner l'option de configuration de redirection de scanner.

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.

Les systèmes d'exploitation invités suivants sont pris en charge sur les machines virtuelles mono-utilisateur et, si indiqué, sur les hôtes RDS :

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

	■ Windows Server 2012 R2 configuré en tant que poste de travail ou hôte RDS **Important** La fonctionnalité Expérience de poste de travail doit être installée sur les systèmes d'exploitation invités Windows Server, qu'ils soient configurés en tant que postes de travail ou hôtes RDS. Les pilotes du scanner n'ont pas à être installés sur le système d'exploitation du poste de travail où Horizon Agent est installé.
Logiciel Horizon Client	Horizon Client 3.2 pour Windows ou version ultérieure
Ordinateur Horizon Client ou périphérique d'accès client	Systèmes d'exploitation pris en charge : ■ Windows 7 32 ou 64 bits ■ Windows 8 32 ou 64 bits.*x* ■ Windows 10 32 ou 64 bits Les pilotes du scanner doivent être installés, et ce dernier doit être opérationnel sur l'ordinateur client.
Norme de scanner	TWAIN ou WIA
Protocole d'affichage pour Horizon 7	PCoIP La redirection de scanner n'est pas prise en charge dans les sessions de poste de travail RDP.

Opération utilisateur de la redirection de scanner

Grâce à la fonction de redirection de scanner, les utilisateurs peuvent connecter des scanners physiques et des périphériques d'imagerie à leurs ordinateurs client comme périphériques virtuels capables de réaliser des opérations d'analyse dans leurs applications et leurs postes de travail distants.

Les utilisateurs peuvent se servir des scanners virtuels presque comme ils se servent des scanners sur les ordinateurs client connectés localement.

- Une fois l'option Redirection de scanner installée avec Horizon Agent, une icône de barre d'état système de scanner ( ) est ajoutée au poste de travail. Sur les applications RDS, l'icône de barre d'état système de scanner est redirigée vers l'ordinateur client local.

  Vous n'avez pas à utiliser l'icône de barre d'état système de scanner. La redirection de scanner fonctionne sans autre configuration. Vous pouvez utiliser l'icône pour configurer des options telles que le périphérique à utiliser, lorsque plusieurs périphériques sont connectés à l'ordinateur client.
- Lorsque vous cliquez sur l'icône du scanner, le menu Redirection de scanner pour VMware Horizon s'affiche. Aucun scanner n'apparaît dans la liste de ce menu si des scanners incompatibles sont connectés à l'ordinateur client.
- Par défaut, les périphériques d'analyse sont sélectionnés automatiquement. Les scanners TWAIN et WIA sont sélectionnés séparément. Il se peut qu'un scanner TWAIN et un scanner WIA soient sélectionnés simultanément.
- Si plusieurs scanners connectés localement sont configurés, vous pouvez sélectionner un scanner différent de celui qui est sélectionné par défaut.
- Les scanners WIA s'affichent dans le menu du gestionnaire des périphériques du poste de travail distant, sous **Périphériques d'imagerie**. Le scanner WIA est appelé **VMware Virtual Scanner WIA**.

- Dans le menu Redirection de scanner pour VMware Horizon, vous pouvez cliquer sur l'option **Préférences** et sélectionner des options telles que masquer les webcams dans le menu de redirection de scanner et définir la sélection du scanner par défaut.

  Vous pouvez également contrôler ces fonctionnalités en configurant les paramètres de stratégie de groupe de la redirection de scanner dans Active Directory. Reportez-vous à la section « Paramètres de stratégie de groupe de redirection de scanner », page 40.

- Lorsque vous utilisez un scanner TWAIN, le menu Redirection de scanner TWAIN pour VMware Horizon offre des options supplémentaires pour la sélection des régions d'une image, l'analyse en couleur, en noir et blanc ou en nuances de gris, et le choix d'autres fonctions courantes.

- Pour afficher la fenêtre de l'interface utilisateur TWAIN si un logiciel d'analyse TWAIN ne l'affiche pas par défaut, sélectionnez l'option **Toujours afficher la boîte de dialogue des paramètres du scanner** dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner.

  Notez toutefois que la plupart des logiciels d'analyse TWAIN affichent cette fenêtre par défaut. Pour ce logiciel, la fenêtre est toujours affichée, que l'option **Toujours afficher la boîte de dialogue des paramètres du scanner** soit sélectionnée ou non.

Remarque Si vous exécutez deux applications RDS hébergées sur différentes batteries de serveurs, deux icônes de redirection de scanner apparaissent dans la barre d'état système de l'ordinateur client. Généralement, un seul scanner est connecté à un ordinateur client. Dans ce cas, les deux icônes utilisent le même périphérique, ce qui signifie que l'une comme l'autre sont valides. Dans certaines situations, vous pouvez disposer de deux scanners connectés localement et exécuter deux applications RDS qui s'exécutent à leur tour sur des batteries de serveurs différentes. Dans ce cas, vous devez ouvrir chaque icône pour savoir quel menu de redirection de scanner contrôle quelle application RDS.

Pour obtenir des instructions d'utilisateur final relatives à l'utilisation des scanners redirigés, consultez le document *Utilisation de VMware Horizon Client pour Windows*.

Configuration des paramètres de stratégie de groupe de redirection de scanner

Vous pouvez configurer les paramètres de stratégie de groupe qui contrôlent le comportement de la redirection de scanner sur vos applications et postes de travail Horizon 7. Avec ces paramètres de stratégie, vous pouvez contrôler de façon centralisée, depuis Active Directory, les options qui sont disponibles dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner, dans les applications et sur les postes de travail des utilisateurs.

Vous n'avez pas à configurer ces paramètres de stratégie. La redirection de scanner fonctionne avec les paramètres par défaut qui sont configurés pour analyser les périphériques sur les postes de travail distants et les systèmes clients.

Ces paramètres de stratégie ont un impact sur vos applications et postes de travail distants (pas sur les systèmes clients auxquels les scanners physiques sont connectés). Pour configurer ces paramètres sur vos postes de travail et applications, ajoutez le fichier de modèle d'administration (ADMX) de stratégie de groupe de redirection de scanner dans Active Directory.

Ajouter les modèles d'administration ADMX de redirection de scanner à Active Directory

Vous pouvez ajouter les paramètres de stratégie du fichier de modèle d'administration ADMX de redirection de scanner (`vdm_agent_scanner.admx`) à des objets de stratégie de groupe (GPO) dans Active Directory et configurer les paramètres dans l'Éditeur d'objets de stratégie de groupe.

Prérequis

- Vérifiez que l'option de configuration Redirection de scanner est installée sur vos hôtes RDS et vos postes de travail. Les paramètres de stratégie de groupe n'ont aucun effet si la redirection de scanner n'est pas installée. Consultez le document Configuration pour plus d'informations sur l'installation d'Horizon Agent.
- Vérifiez que les objets de stratégie de groupe (GPO) Active Directory sont créés pour les paramètres de stratégie de groupe de redirection de scanner. Les objets de stratégie de groupe (GPO) doivent être liés à l'unité d'organisation (UO) qui contient vos hôtes RDS et vos postes de travail. Reportez-vous à la section « Exemple de stratégie de groupe Active Directory », page 192.
- Vérifiez que les composants logiciels enfichables MMC (Microsoft Management Console) et l'Éditeur d'objets de stratégie de groupe sont disponibles sur votre serveur Active Directory.
- Familiarisez-vous avec les paramètres de stratégie de groupe de redirection de scanner. Reportez-vous à la section « Paramètres de stratégie de groupe de redirection de scanner », page 40.

Procédure

1. Téléchargez le fichier Horizon 7 GPO Bundle `.zip` 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 GPO Bundle.

   Le fichier se nomme `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, où *x.x.x* est la version et *yyyyyyy* le numéro de build. Tous les fichiers ADMX qui fournissent des paramètres de stratégie de groupe pour Horizon 7 sont disponibles dans ce fichier.

2. Décompressez le fichier `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip` et copiez les fichiers ADMX sur votre hôte Active Directory ou RDS.

   a. Copiez le fichier `vdm_agent_scanner.admx`, ainsi que le dossier `en-US` dans le dossier `C:\Windows\PolicyDefinitions` sur votre hôte Active Directory ou RDS.

   b. (Facultatif) Copiez le fichier de ressources de la langue (`vdm_agent_scanner.adml`) dans le sous-dossier correspondant dans `C:\Windows\PolicyDefinitions\` sur votre hôte Active Directory ou RDS.

3. Sur l'hôte Active Directory, ouvrez l'Éditeur de gestion de stratégie de groupe et entrez le chemin vers le fichier de modèle dans l'éditeur.

   Sur un hôte RDS individuel, vous pouvez ouvrir l'Éditeur de stratégie de groupe locale avec l'utilitaire `gpedit.msc`.

   Les paramètres se situent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Redirection de scanner**.

   La plupart des paramètres sont également ajoutés au dossier **Configuration utilisateur**, situé dans le dossier **Configuration utilisateur > Stratégies > Modèles d'administration > Redirection de scanner**.

Suivant

Configurez les paramètres de stratégie de groupe.

Paramètres de stratégie de groupe de redirection de scanner

Les paramètres de stratégie de groupe de redirection de scanner contrôlent les options qui sont disponibles dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner des postes de travail et applications des utilisateurs.

Le fichier de modèle d'administration ADMX de redirection de scanner contient les stratégies Configuration ordinateur et Configuration utilisateur. Les stratégies de configuration d'utilisateur vous permettent de définir des configurations différentes pour les utilisateurs de postes de travail VDI, de postes de travail RDS et d'applications RDS. Plusieurs stratégies de configuration d'utilisateur peuvent prendre effet, même lorsque les sessions de poste de travail et les applications des utilisateurs s'exécutent sur les mêmes hôtes RDS. Tous les paramètres se trouvent dans le dossier **Configuration de VMware Horizon Agent > Redirection de scanner** dans l'Éditeur de gestion de stratégie de groupe.

Paramètre de stratégie de groupe	Ordinateur	Utilisateur	Description
`Disable functionality`	X		Désactive la fonctionnalité de redirection de scanner. Lorsque vous activez ce paramètre, les scanners ne peuvent pas être redirigés et n'apparaissent pas dans le menu du scanner des postes de travail et des applications des utilisateurs. Lorsque vous désactivez ce paramètre ou ne le configurez pas, la redirection de scanner fonctionne et les scanners apparaissent dans le menu correspondant.
`Lock config`	X		Verrouille l'interface utilisateur de redirection de scanner et empêche les utilisateurs de modifier les options de configuration sur leurs postes de travail et dans leurs applications. Lorsque vous activez ce paramètre, les utilisateurs ne peuvent pas configurer les options disponibles dans le menu de la barre d'état de leurs postes de travail et de leurs applications. Les utilisateurs peuvent afficher la boîte de dialogue Préférences de redirection de VMware Horizon Scanner, mais les options sont désactivées et ne peuvent pas être modifiées. Lorsque vous désactivez ce paramètre ou ne le configurez pas, les utilisateurs peuvent configurer les options de la boîte de dialogue Préférences de redirection de VMware Horizon Scanner.
`Compression`		X	Définit le taux de compression d'image au cours du transfert d'image vers le poste de travail à distance ou l'application distante. Vous avez le choix parmi les modes de compression suivants : ■ **Désactiver**. La compression d'image est désactivée. ■ **Sans perte**. La compression sans perte (`zlib`) conserve la qualité de l'image d'origine. ■ **JPEG**. La compression JPEG est source de perte de qualité. Spécifiez le niveau de qualité d'image dans le champ **Qualité de compression JPEG**. La qualité de compression JPEG doit être une valeur comprise entre 0 et 100. Lorsque vous activez ce paramètre, le mode de compression sélectionné est défini pour tous les utilisateurs affectés par cette stratégie. Cependant, les utilisateurs peuvent modifier l'option **Compression** dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner et remplacer le paramètre de stratégie. Lorsque vous désactivez le paramètre de cette stratégie ou ne le configurez pas, le mode de compression **JPEG** est utilisé.

Paramètre de stratégie de groupe	Ordinateur	Utilisateur	Description
`Hide Webcam`	X	X	Empêche les webcams d'apparaître dans le menu de sélection de scanner de la boîte de dialogue Préférences de redirection de VMware Horizon Scanner. Par défaut, les webcams peuvent être redirigées vers les postes de travail et les applications. Les utilisateurs peuvent sélectionner des webcams et les utiliser comme scanners virtuels pour capturer des images. Lorsque vous activez ce paramètre en tant que stratégie Configuration d'ordinateur, les webcams sont masquées pour tous les utilisateurs des ordinateurs affectés. Les utilisateurs ne peuvent pas modifier l'option **Masquer la webcam** dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner. Lorsque vous activez ce paramètre en tant que stratégie Configuration d'utilisateur, les webcams sont masquées pour tous les utilisateurs affectés. Cependant, les utilisateurs peuvent modifier l'option **Masquer la webcam** dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner. Lorsque vous activez ce paramètre à la fois dans la configuration d'ordinateur et dans la configuration d'utilisateur, le paramètre **Masquer la webcam** de la configuration d'ordinateur remplace le paramètre de stratégie correspondant de la configuration d'utilisateur pour tous les utilisateurs des ordinateurs affectés. Lorsque vous désactivez ce paramètre ou ne le configurez pas dans l'une des configurations de stratégie, le paramètre **Masquer la webcam** est déterminé par le paramètre de stratégie correspondant (soit Configuration d'ordinateur, soit Configuration d'utilisateur) ou par la sélection de l'utilisateur dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner.

Paramètre de stratégie de groupe	Ordinateur	Utilisateur	Description
`Default Scanner`	X	X	Permet la gestion centralisée de sélection automatique de scanner. Les options de sélection automatique de scanner sont sélectionnées séparément pour les scanners TWAIN et WIA. Vous avez le choix parmi les options de sélection automatique suivantes : ■ **Aucune**. Ne pas sélectionner de scanner automatiquement. ■ **Sélection automatique**. Sélectionne automatiquement le scanner connecté localement. ■ **Dernier scanner utilisé**. Sélectionne automatiquement le dernier scanner utilisé. ■ **Spécifié**. Sélectionne le scanner dont vous avez entré le nom dans la zone de texte **Scanner spécifié**. Lorsque vous activez ce paramètre en tant que stratégie Configuration d'ordinateur, le paramètre détermine le mode de sélection automatique de scanner pour tous les utilisateurs des ordinateurs affectés. Les utilisateurs ne peuvent pas modifier l'option **Scanner par défaut** dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner. Lorsque vous activez ce paramètre en tant que stratégie Configuration d'utilisateur, le paramètre détermine le mode de sélection automatique de scanner pour tous les utilisateurs affectés. Cependant, les utilisateurs peuvent modifier l'option **Scanner par défaut** dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner. Lorsque vous activez ce paramètre à la fois dans la configuration d'ordinateur et dans la configuration d'utilisateur, le mode de sélection automatique de scanner de la configuration d'ordinateur remplace le paramètre de stratégie correspondant de la configuration d'utilisateur pour tous les utilisateurs des ordinateurs affectés. Lorsque vous désactivez ce paramètre ou ne le configurez pas dans l'une des configurations de stratégie, le mode de sélection automatique de scanner est déterminé par le paramètre de stratégie correspondant (soit Configuration d'ordinateur, soit Configuration d'utilisateur) ou par la sélection de l'utilisateur dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner.

Configuration de la redirection de port série

Avec la redirection de port série, les utilisateurs peuvent rediriger des ports série (COM) connectés en local, tels que les ports RS232 intégrés ou les 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.

La redirection de port série est disponible dans Horizon 6 version 6.1.1 et versions ultérieures avec Horizon Client pour Windows 3.4 et versions ultérieures.

Après avoir installé Horizon Agent et configuré la fonctionnalité de redirection de port série, cette dernière peut fonctionner sur vos postes de travail distants sans configuration supplémentaire. Par exemple, COM1 sur le système client local est redirigé en tant que COM1 sur le poste de travail distant, et COM2 est redirigé en tant que COM2, sauf si un port COM existe déjà sur le poste de travail distant. 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. Vous n'avez pas à configurer les ports COM ou à installer des pilotes de périphérique sur les postes de travail distants.

Pour activer un port COM redirigé, l'utilisateur sélectionne l'option **Se connecter** dans le menu sur l'icône de barre d'état système du port série lors d'une session de poste de travail. Un utilisateur peut également régler un périphérique de port COM pour qu'il se connecte automatiquement dès que l'utilisateur ouvre une session sur le poste de travail distant. Reportez-vous à la section « Opération utilisateur de la redirection de port série », page 44.

Vous pouvez configurer des paramètres de stratégie de groupe pour modifier la configuration par défaut. Par exemple, vous pouvez verrouiller les paramètres pour que les utilisateurs ne puissent pas modifier les mappages ou les propriétés du port COM. Vous pouvez également définir une stratégie pour désactiver ou activer la fonctionnalité. Un fichier de modèle d'administration ADMX vous permet d'installer des paramètres de stratégie de groupe de redirection de port série dans Active Directory ou sur des postes de travail individuels. Reportez-vous à la section « Configuration des paramètres de stratégie de groupe de redirection de port série », page 45.

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.

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.

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.

Opération utilisateur de la redirection de port série

Les utilisateurs peuvent faire fonctionner des périphériques de port COM physiques qui sont connectés à leurs ordinateurs clients et utiliser la virtualisation de port série pour connecter les périphériques à leurs postes de travail distants, lorsque les périphériques sont accessibles à des applications tierces.

- Une fois l'option Redirection de port série installée avec Horizon Agent, une icône de barre d'état système de port série ( ) est ajoutée au poste de travail distant. Pour les applications publiées, l'icône est redirigée vers l'ordinateur client local.

  L'icône apparaît uniquement si vous utilisez les versions requises d'Horizon Agent et d'Horizon Client pour Windows, et si vous vous connectez sur PCoIP. L'icône ne s'affiche pas si vous vous connectez à un poste de travail distant depuis un Mac, Linux ou un client mobile.

  Vous pouvez utiliser l'icône afin de configurer des options pour connecter, déconnecter et personnaliser les ports COM mappés.

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

- Par défaut, les ports COM connectés en local sont mappés vers les ports COM correspondants sur le poste de travail distant. Par exemple : **COM1 mappé vers COM3**. Les ports mappés ne sont pas connectés par défaut.

- Pour utiliser un port COM mappé, vous devez sélectionner manuellement l'option **Se connecter** dans le menu **Redirection série COM pour VMware Horizon** ou l'option **Se connecter automatiquement** doit être définie lors d'une session de poste de travail précédente ou en configurant un paramètre de stratégie de groupe. **Se connecter automatiquement** configure un port mappé pour qu'il se connecte automatiquement lorsqu'une session de poste de travail distant est démarrée.

- Lorsque vous sélectionnez l'option **Se connecter**, le port redirigé est actif. Dans le gestionnaire des périphériques du système d'exploitation invité sur le poste de travail distant, le port redirigé est indiqué par **Redirecteur de port série pour VMware Horizon (COM*n*)**.

  Lorsque le port COM est connecté, vous pouvez ouvrir le port dans une application tierce, qui peut échanger des données avec le périphérique de port COM connecté à la machine cliente. Lorsqu'un port est ouvert dans une application, vous ne pouvez pas le déconnecter dans le menu **Redirection série COM pour VMware Horizon**.

  Avant de pouvoir déconnecter le port COM, vous devez le fermer dans l'application ou fermer l'application. Vous pouvez ensuite sélectionner l'option **Déconnecter** pour déconnecter le port et rendre le port COM physique disponible pour utilisation sur la machine cliente.

- Dans le menu **Redirection série COM pour VMware Horizon**, vous pouvez cliquer avec le bouton droit sur un port redirigé pour sélectionner la commande **Propriétés du port**.

  Dans la boîte de dialogue Propriétés COM, vous pouvez configurer un port pour qu'il se connecte automatiquement lorsqu'une session de poste de travail distant est démarrée, ignorer le signal DSR (Data Set Ready) et mapper le port local sur le client vers un port COM différent sur le poste de travail distant en sélectionnant un port dans la liste déroulante **Personnaliser le nom de port**.

  Un port de poste de travail distant peut apparaître comme étant chevauché. Par exemple, vous pouvez voir **COM1 (chevauché)**. Dans ce cas, la machine virtuelle est configurée avec un port COM dans le matériel virtuel sur l'hôte ESXi. Vous pouvez utiliser un port redirigé même lorsqu'il est mappé vers un port chevauché sur la machine virtuelle. La machine virtuelle reçoit des données de série via le port depuis l'hôte ESXi ou le système client.

- Dans le gestionnaire des périphériques du système d'exploitation invité, vous pouvez utiliser l'onglet **Propriétés > Paramètres du port** pour configurer des paramètres d'un port COM redirigé. Par exemple, vous pouvez régler le débit en bauds et les bits de données par défaut. Toutefois, les paramètres que vous configurez dans le gestionnaire des périphériques sont ignorés si l'application spécifie les paramètres du port.

Pour obtenir des instructions d'utilisateur final relatives à l'utilisation des ports COM série redirigés, consultez le document *Utilisation de VMware Horizon Client pour Windows*.

Instructions relatives à configuration de la redirection de port série

Grâce aux paramètres de stratégie de groupe, vous pouvez configurer la redirection de port série et limiter la capacité des utilisateurs à personnaliser les ports COM redirigés. Vos choix dépendent des rôles d'utilisateur et des applications tierces de votre organisation.

Pour plus d'informations sur les paramètres de stratégie de groupe, reportez-vous à « Paramètres de stratégie de groupe de redirection de port série », page 47.

- Si vos utilisateurs exécutent les mêmes applications tierces et périphériques de port COM, assurez-vous que les ports redirigés sont configurés de la même façon. Par exemple, dans une banque ou une boutique qui utilise des périphériques de point de vente, assurez-vous que tous les périphériques de port COM sont connectés aux mêmes ports sur les points de terminaison clients, et que tous les ports sont mappés vers les mêmes ports COM redirigés sur les postes de travail distants.

  Réglez le paramètre de stratégie **PortSettings** pour mapper les ports clients vers les ports redirigés. Sélectionnez l'élément **Autoconnect** dans **PortSettings** pour vous assurer que les ports redirigés sont connectés au début de chaque session de poste de travail. Activez le paramètre de stratégie **Lock Configuration** pour empêcher les utilisateurs de modifier les mappages de port ou de personnaliser les configurations de port. Dans ce scénario, les utilisateurs n'ont jamais à se connecter ou à se déconnecter manuellement et ils ne peuvent pas accidentellement rendre un port COM redirigé inaccessible à une application tierce.

- Si vos utilisateurs sont des travailleurs du savoir qui utilisent diverses applications tierces et qui peuvent également utiliser leurs ports COM localement sur leurs machines clientes, assurez-vous que les utilisateurs peuvent se connecter et se déconnecter des ports COM redirigés.

  Vous pouvez régler le paramètre de stratégie **PortSettings** si les mappages de port par défaut sont incorrects. En fonction des exigences de vos utilisateurs, vous pouvez ou non régler l'élément **Autoconnect**. N'activez pas le paramètre de stratégie **Lock Configuration**.

- Assurez-vous que vos applications tierces ouvrent le port COM mappé vers le poste de travail distant.
- Assurez-vous que le débit en bauds utilisé pour un périphérique correspond au débit en bauds que l'application tierce tente d'utiliser.
- Vous pouvez rediriger jusqu'à cinq ports COM entre un système client et un poste de travail distant.

Configuration des paramètres de stratégie de groupe de redirection de port série

Vous pouvez configurer les paramètres de stratégie de groupe qui contrôlent le comportement de la redirection de port série sur vos postes de travail distants. Avec ces paramètres de stratégie, vous pouvez contrôler de façon centralisée, depuis Active Directory, les options disponibles dans le menu **Redirection série COM pour VMware Horizon** sur les postes de travail des utilisateurs.

Vous n'avez pas à configurer ces paramètres de stratégie. La redirection de port série fonctionne avec les paramètres par défaut qui sont configurés pour les ports COM redirigés sur les postes de travail distants et les systèmes clients.

Ces paramètres de stratégie affectent vos postes de travail, et non les systèmes clients sur lesquels les périphériques de port COM physiques sont connectés. Pour configurer ces paramètres sur vos postes de travail, ajoutez le fichier de modèle d'administration (ADMX) de stratégie de groupe pour la redirection de port série dans Active Directory.

Ajouter le modèle d'administration ADMX de redirection de port série à Active Directory

Vous pouvez ajouter les paramètres de stratégie du fichier ADMX de redirection de port série (`vdm_agent_serialport.admx`) à des objets de stratégie de groupe (GPO) dans Active Directory et configurer les paramètres dans l'Éditeur d'objets de stratégie de groupe.

Prérequis

- Vérifiez que l'option d'installation Redirection de port série est installée sur vos postes de travail. Les paramètres de stratégie de groupe n'ont aucun effet si la redirection de port série n'est pas installée. Consultez le document Configuration pour plus d'informations sur l'installation d'Horizon Agent.
- Vérifiez que les objets de stratégie de groupe (GPO) Active Directory sont créés pour les paramètres de stratégie de groupe de redirection de port série. Les objets de stratégie de groupe (GPO) doivent être liés à l'unité d'organisation (UO) qui contient vos postes de travail. Reportez-vous à la section « Exemple de stratégie de groupe Active Directory », page 192.
- Vérifiez que les composants logiciels enfichables MMC (Microsoft Management Console) et l'Éditeur d'objets de stratégie de groupe sont disponibles sur votre serveur Active Directory.
- Familiarisez-vous avec les paramètres de stratégie de groupe de redirection de port série. Reportez-vous à la section « Paramètres de stratégie de groupe de redirection de port série », page 47.

Procédure

1. Téléchargez le fichier Horizon 7 GPO Bundle `.zip` 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 GPO Bundle.

   Le fichier se nomme `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, où *x.x.x* est la version et *yyyyyyy* le numéro de build. Tous les fichiers ADMX qui fournissent des paramètres de stratégie de groupe pour Horizon 7 sont disponibles dans ce fichier.

2. Décompressez le fichier `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip` et copiez les fichiers ADMX sur votre hôte Active Directory ou RDS.

   a. Copiez le fichier `vdm_agent_serialport.admx`, ainsi que le dossier `en-US` dans le dossier `C:\Windows\PolicyDefinitions` sur votre hôte Active Directory ou RDS.

   b. (Facultatif) Copiez le fichier de ressources de la langue (`vdm_agent_serialport.adml`) dans le sous-dossier correspondant dans `C:\Windows\PolicyDefinitions\` sur votre hôte Active Directory ou RDS.

3. Sur l'hôte Active Directory, ouvrez l'Éditeur de gestion de stratégie de groupe et entrez le chemin vers le fichier de modèle dans l'éditeur.

   Sur un hôte RDS individuel, vous pouvez ouvrir l'Éditeur de stratégie de groupe locale avec l'utilitaire `gpedit.msc`.

   Les paramètres se situent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > COM série**.

   La plupart des paramètres sont également ajoutés au dossier **Configuration utilisateur**, situé dans le dossier **Configuration utilisateur > Stratégies > Modèles d'administration > COM série**.

Suivant

Configurez les paramètres de stratégie de groupe.

Paramètres de stratégie de groupe de redirection de port série

Les paramètres de stratégie de groupe de redirection de port série contrôlent la configuration du port COM redirigé, y compris les options qui sont disponibles dans le menu **Redirection série COM pour VMware Horizon** sur les postes de travail distants.

Le fichier d'administration ADMX de redirection de port série contient les stratégies Configuration ordinateur et Configuration utilisateur. Les stratégies Configuration d'utilisateur vous permettent de régler différentes configurations pour des utilisateurs spécifiés de postes de travail VDI. Les paramètres de stratégie configurés dans Configuration d'ordinateur sont prioritaires sur les paramètres correspondants configurés dans Configuration d'utilisateur.

Paramètre de stratégie de groupe	Ordinateur	Utilisateur	Description

`PortSettings1`
`PortSettings2`
`PortSettings3`
`PortSettings4`
`PortSettings5`
	X	X	Les paramètres de port déterminent le mappage entre le port COM sur le système client et le port COM redirigé sur le poste de travail distant et déterminent d'autres paramètres qui affectent le port COM redirigé. Vous configurez chaque port COM redirigé individuellement.
			Cinq paramètres de stratégie de paramètres de port sont disponibles, ce qui permet de mapper jusqu'à cinq ports COM entre le client et le poste de travail distant. Sélectionnez un paramètre de stratégie de paramètres de port pour chaque port COM que vous voulez configurer. Lorsque vous activez le paramètre de stratégie de paramètres de port, vous pouvez configurer les éléments suivants qui affectent le port COM redirigé :
			■ Le paramètre **Source port number** spécifie le numéro du port COM physique connecté au système client.
			■ Le paramètre **Destination virtual port number** spécifie le numéro du port COM virtuel redirigé sur le poste de travail distant.
			■ Le paramètre **Autoconnect** connecte automatiquement le port COM au port COM redirigé au début de chaque session de poste de travail.
			■ Avec le paramètre **IgnoreDSR**, le périphérique du port COM redirigé ignore le signal DSR (Data Set Ready).
			■ Le paramètre **Pause before close port (in milliseconds)** spécifie le temps d'attente (en millisecondes) entre la fermeture du port redirigé par un utilisateur et la fermeture réelle du port. Certains adaptateurs USB-série requièrent ce délai pour garantir que les données transmises sont conservées. Ce paramètre est conçu à des fins de dépannage.
			■ Le paramètre **Serial2USBModeChangeEnabled** résout les problèmes qui s'appliquent aux adaptateurs USB-série utilisant la puce Prolific, y compris l'adaptateur GlobalSat BU353 GPS. Si vous n'activez pas ce paramètre pour les adaptateurs de puce Prolific, les périphériques connectés peuvent transmettre des données mais pas en recevoir.
			■ Le paramètre **Disable errors in wait mask** désactive la valeur d'erreur dans le masque de port COM. Ce paramètre de dépannage est requis pour certaines applications. Pour plus de détails, consultez la documentation Microsoft de la fonction `WaitCommEvent` à l'adresse http://msdn.microsoft.com/en-us/library/windows/desktop/aa363479(v=vs.85).aspx.
			■ Le paramètre **HandleBtDisappear** prend en charge le comportement du port COM BlueTooth. Ce paramètre est conçu à des fins de dépannage.
			■ Le paramètre **UsbToComTroubleShooting** résout certains problèmes qui s'appliquent aux adaptateurs de port USB-série. Ce paramètre est conçu à des fins de dépannage.
			Lorsque vous activez le paramètre de stratégie de paramètres de port pour un port COM particulier, les utilisateurs peuvent se connecter et se déconnecter du port redirigé, mais ils ne peuvent pas configurer les propriétés du port sur le poste de travail distant. Par exemple, les utilisateurs ne peuvent pas régler le port pour qu'il soit redirigé automatiquement lorsqu'ils se connectent au poste de travail, et ils ne peuvent pas ignorer le signal DSR. Ces propriétés sont contrôlées par le paramètre de stratégie de groupe.
			Remarque Un port COM redirigé est connecté et actif uniquement si le port COM physique est connecté en local au système client. Si vous mappez un port COM qui n'existe pas sur le client, le port redirigé apparaît comme étant inactif et indisponible dans le menu de la barre d'état système sur le poste de travail distant.

Paramètre de stratégie de groupe	Ordinateur	Utilisateur	Description
			Lorsque le paramètre de stratégie de paramètres de port est désactivé ou non configuré, le port COM redirigé utilise les paramètres que les utilisateurs configurent sur le poste de travail distant. Les options du menu **Redirection série COM pour VMware Horizon** sont actives et disponibles pour les utilisateurs. Ces paramètres se trouvent dans le dossier **Configuration de VMware View Agent > COM série > PortSettings** dans l'Éditeur de gestion de stratégie de groupe.
`Local settings priority`	X	X	Donne la priorité aux paramètres configurés sur le poste de travail distant. Lorsque vous activez cette stratégie, les paramètres de redirection de port série qu'un utilisateur configure sur le poste de travail distant sont prioritaires sur les paramètres de stratégie de groupe. Un paramètre de stratégie de groupe prend effet uniquement si un paramètre n'est pas configuré sur le poste de travail distant. Lorsque ce paramètre est désactivé ou non configuré, les paramètres de stratégie de groupe sont prioritaires sur les paramètres configurés sur le poste de travail distant. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > COM série** dans l'Éditeur de gestion de stratégie de groupe.
`Disable functionality`	X		Désactive la fonctionnalité de redirection de port série. Lorsque vous activez ce paramètre, les ports COM ne sont pas redirigés vers le poste de travail distant. L'icône de barre d'état système du port série sur le poste de travail distant n'est pas affichée. Lorsque ce paramètre est désactivé, la redirection de port série fonctionne, l'icône de barre d'état système du port série est affichée et les ports COM apparaissent dans le menu **Redirection série COM pour VMware Horizon**. Lorsque ce paramètre n'est pas configuré, les paramètres locaux sur le poste de travail distant déterminent si la redirection de port série est désactivée ou activée. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > COM série** dans l'Éditeur de gestion de stratégie de groupe.
`Lock configuration`	X	X	Verrouille l'interface utilisateur de la redirection de port série et empêche les utilisateurs de modifier les options de configuration sur le poste de travail distant. Lorsque vous activez ce paramètre, les utilisateurs ne peuvent pas configurer les options disponibles dans le menu de la barre d'état système de leurs postes de travail. Les utilisateurs peuvent afficher le menu **Redirection série COM pour VMware Horizon**, mais les options sont inactives et ne peuvent pas être modifiées. Lorsque ce paramètre est désactivé, les utilisateurs peuvent configurer les options dans le menu **Redirection série COM pour VMware Horizon**. Lorsque ce paramètre n'est pas configuré, les paramètres de programme locaux sur le poste de travail distant déterminent si les utilisateurs peuvent configurer les paramètres de redirection de port COM. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > COM série** dans l'Éditeur de gestion de stratégie de groupe.

Paramètre de stratégie de groupe	Ordinateur	Utilisateur	Description
`Bandwidth limit`	X		Définit une limite sur la vitesse de transmission des données, en kilo-octets par seconde, entre le port série redirigé et les systèmes clients. Lorsque vous activez ce paramètre, vous pouvez définir une valeur dans la case **Bandwidth limit (in kilobytes per second)** qui détermine la vitesse de transmission des données maximale entre le port série redirigé et le client. La valeur de 0 désactive la limite de bande passante. Lorsque ce paramètre est désactivé, aucune limite de bande passante n'est définie. Lorsque ce paramètre n'est pas configuré, les paramètres de programme locaux sur le poste de travail distant déterminent si une limite de bande passante est définie. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > COM série** dans l'Éditeur de gestion de stratégie de groupe.

Configurer des adaptateurs USB-série

Vous pouvez configurer des adaptateurs USB-série utilisant une puce Prolific de façon à ce qu'ils soient redirigés vers des postes de travail distants par la fonctionnalité de redirection de port série.

Pour vérifier que les données sont bien transmises sur les adaptateurs de puce Prolific, vous pouvez activer un paramètre de stratégie de groupe de redirection de port série dans Active Directory ou sur une machine virtuelle de poste de travail individuel.

Si vous ne configurez pas le paramètre de stratégie de groupe pour résoudre les problèmes des adaptateurs de puce Prolific, les périphériques connectés peuvent transmettre des données mais pas en recevoir.

Vous n'avez pas à configurer un paramètre de stratégie ou une clé de registre sur les systèmes clients.

Prérequis

- Vérifiez que l'option d'installation Redirection de port série est installée sur vos postes de travail. Les paramètres de stratégie de groupe n'ont aucun effet si la redirection de port série n'est pas installée. Consultez le document Configuration pour plus d'informations sur l'installation d'Horizon Agent.
- Vérifiez que le fichier de modèle d'administration ADMX de redirection de port série est ajouté dans Active Directory ou sur la machine virtuelle de poste de travail.
- Familiarisez-vous avec l'élément **Serial2USBModeChangeEnabled** dans le paramètre de stratégie de groupe **PortSettings**. Reportez-vous à la section « Paramètres de stratégie de groupe de redirection de port série », page 47.

Procédure

1. Dans Active Directory ou sur la machine virtuelle, ouvrez l'Éditeur d'objets de stratégie de groupe.
2. Accédez au dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Modèles d'administration classiques > Configuration de VMware View Agent > Série COM**.
3. Sélectionnez le dossier **PortSettings**.
4. Sélectionnez et activez le paramètre de stratégie de groupe **PortSettings**.
5. Spécifiez les numéros des ports COM source et de destination pour mapper le port COM.
6. Cochez la case **Serial2USBModeChangeEnabled**.
7. Configurez d'autres éléments dans le paramètre de stratégie **PortSettings** si nécessaire.
8. Cliquez sur **OK** et fermez l'Éditeur d'objets de stratégie de groupe.

Les adaptateurs USB-série peuvent être redirigés vers des postes de travail distants. Ils peuvent recevoir des données lorsque les utilisateurs démarrent leurs prochaines sessions de poste de travail.

Gestion de l'accès à la redirection multimédia (MMR) Windows Media

Horizon 7 fournit la fonction Windows Media MMR pour les postes de travail VDI exécutés sur des machines mono-utilisateur et pour les postes de travail RDS.

MMR délivre le flux multimédia directement aux ordinateurs client. Avec MMR, le flux multimédia est traité, c'est-à-dire décodé, sur le système client. Le système client effectue la lecture du contenu multimédia, déchargeant ainsi la demande sur l'hôte ESXi.

Les données MMR sont envoyées sur le réseau sans cryptage au niveau de l'application et peuvent contenir des éléments sensibles, selon le contenu redirigé. Pour garantir que les données ne puissent pas être surveillées sur le réseau, utilisez MMR uniquement sur un réseau sécurisé.

Si le tunnel sécurisé est activé, les connexions MMR entre Horizon Clients et View Secure Gateway sont sécurisées, mais les connexions entre View Secure Gateway et les machines de poste de travail ne sont pas cryptées. Si le tunnel sécurisé est désactivé, les connexions MMR entre Horizon Clients et les machines de poste de travail ne sont pas cryptées.

Activation de la redirection multimédia dans Horizon 7

Vous pouvez prendre des mesures pour vous assurer que la Redirection multimédia (MMR) est accessible uniquement aux systèmes Horizon Client qui disposent de ressources suffisantes pour gérer le décodage multimédia local et qui sont connectés à Horizon 7 sur un réseau sécurisé.

Par défaut, la stratégie globale de View Administrator, **Redirection multimédia (MMR)** est définie sur **Refuser**.

Pour utiliser la fonctionnalité MMR, vous devez définir cette valeur de manière explicite sur **Autoriser**.

Pour contrôler l'accès à MMR, vous pouvez activer ou désactiver la stratégie **Redirection multimédia (MMR)** globalement, pour des pools de postes de travail individuels ou pour des utilisateurs spécifiques.

Pour obtenir des instructions relatives à la définition des stratégies globales dans Horizon Administrator, reportez-vous à « Règles Horizon 7 », page 101.

Configuration système requise pour la redirection multimédia (MMR) Windows Media

Pour prendre en charge la redirection multimédia (MMR) Windows Media, le déploiement de votre Horizon 7 doit répondre à certaines exigences matérielles et logicielles. La fonctionnalité MMR Windows Media est fournie dans Horizon 6.0.2 et versions ultérieures.

Poste de travail distant View

- Cette fonctionnalité est prise en charge sur les postes de travail de machine virtuelle qui sont déployés sur des machines virtuelles mono-utilisateur et sur des postes de travail RDS.

  View Agent 6.1.1 ou version ultérieure est requis pour prendre en charge cette fonctionnalité sur les postes de travail RDS.

  View Agent 6.0.2 ou version ultérieure est requis pour prendre en charge cette fonctionnalité sur les machines mono-utilisateur.

- Les systèmes d'exploitation invités suivants sont pris en charge :
  - Windows 10 64 ou 32 bits. Le Lecteur Windows Media est pris en charge. Le lecteur par défaut TV & Movies n'est pas pris en charge.

- Windows Server 2016 est une fonctionnalité de la version d'évaluation technique. Le Lecteur Windows Media est pris en charge. Le lecteur par défaut TV & Movies n'est pas pris en charge.
- Windows 7 SP1 Entreprise ou Intégrale 32 ou 64 bits (machine mono-utilisateur). Windows 7 Professionnel n'est pas pris en charge.
- Windows 8/8.1 Professionnel ou Entreprise 32 ou 64 bits (machine mono-utilisateur)
- Windows Server 2008 R2 configuré en tant qu'hôte RDS
- Windows Server 2012 et 2012 R2 configuré en tant qu'hôte RDS

- Le **rendu 3D** peut être activé ou désactivé sur le pool de postes de travail.
- Les utilisateurs doivent lire les vidéos sur Lecteur Windows Media 12 (ou version ultérieure) ou sur Internet Explorer 8 (ou version ultérieure).

  Si vous utilisez Internet Explorer, désactivez le mode protégé. Dans la boîte de dialogue Options Internet, cliquez sur l'onglet **Sécurité** et désélectionnez **Activer le mode protégé**.

Logiciel Horizon Client

Horizon Client 3.2 pour Windows ou une version ultérieure est requis pour prendre en charge Windows Media MMR sur les machines mono-utilisateur.

Ordinateur Horizon Client ou périphérique d'accès client

- Les clients doivent exécuter des systèmes d'exploitation Windows 7, Windows 8/8.1 ou Windows 10 (32 ou 64 bits).

Formats multimédias pris en charge

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

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

Stratégies Horizon

Dans Horizon Administrator, définissez la stratégie **Redirection multimédia (MMR)** sur **Autoriser**. La valeur par défaut est **Refuser**.

Pare-feu dorsal

Si le déploiement d'Horizon 7 inclut un pare-feu dorsal entre vos serveurs de sécurité de la zone DMZ et votre réseau interne, assurez-vous que le pare-feu dorsal autorise le trafic vers le port 9427 de vos postes de travail.

Déterminer s'il convient d'utiliser Windows Media MMR en fonction de la latence réseau

Par défaut, Windows Media MMR s'adapte aux conditions du réseau sur les postes de travail mono-utilisateur qui s'exécutent sous Windows 8 ou versions ultérieures et les postes de travail RDS qui s'exécutent sous Windows Server 2012 ou 2012 R2 ou versions ultérieures. Si la latence réseau entre Horizon Client et le poste de travail distant est de 29 millisecondes ou moins, la vidéo est redirigée avec Windows Media MMR. Si la latence réseau est de 30 millisecondes ou plus, la vidéo n'est pas redirigée. Elle est rendue sur l'hôte ESXi et envoyée au client sur PCoIP.

Cette fonction s'applique aux postes de travail mono-utilisateur Windows 8 ou versions ultérieures et aux postes de travail RDS Windows Server 2012 ou 2012 R2 ou versions ultérieures. Les utilisateurs peuvent exécuter n'importe quel système client pris en charge, Windows 7 ou Windows 8/8.1.

Cette fonction ne s'applique pas aux postes de travail mono-utilisateur Windows 7 ni aux postes de travail RDS Windows Server 2008 R2. Sur ces systèmes d'exploitation invités, Windows Media MMR effectue toujours la redirection multimédia, quelle que soit la latence réseau.

Vous pouvez remplacer cette fonction pour obliger Windows Media MMR à effectuer une redirection multimédia quelle que soit la latence réseau, en configurant le paramètre de registre `RedirectionPolicy` sur le poste de travail.

Procédure

1 Lancez l'éditeur du Registre Windows sur le poste de travail distant.

2 Accédez à la clé de registre Windows qui contrôle la stratégie de redirection.

La clé de Registre que vous configurez pour un poste de travail distant dépend du nombre de bits de la version du Lecteur Windows Media.

Option	Description
Lecteur Windows Media 64 bits	■ Pour un poste de travail 64 bits, utilisez la clé de Registre : `HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware tsmmr`
Lecteur Windows Media 32 bits	■ Pour un poste de travail 32 bits, utilisez la clé de Registre : `HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware tsmmr` ■ Pour un poste de travail 64 bits, utilisez la clé de Registre : `HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware tsmmr`

3 Définissez la valeur de `RedirectionPolicy` sur `always`.

```
Value name = RedirectionPolicy
Value Type = REG_SZ
Value data = always
```

4 Redémarrez Windows Media Player sur le poste de travail pour que la valeur mise à jour entre en vigueur.

Gestion de l'accès à la redirection de lecteur client

Lorsque vous déployez Horizon Client 3.5 ou version ultérieure, View Agent 6.2 ou version ultérieure et Horizon Agent 7.0 ou version ultérieure avec la redirection du lecteur client, les dossiers et les fichiers sont envoyés sur le réseau avec chiffrement. Les connexions de redirection du lecteur client entre les clients et View Secure Gateway et les connexions entre View Secure Gateway et les machines de poste de travail sont sécurisées.

Pour Horizon Client 4.2 ou Horizon 7 version 7.0.2 ou ultérieure, si VMware Blast Extreme est activé, les fichiers et les dossiers sont transférés via un canal virtuel avec chiffrement.

Avec des versions de client ou d'agent antérieures, les dossiers et les fichiers de redirection de lecteur client sont envoyés sur le réseau sans chiffrement et peuvent contenir des données sensibles, selon le contenu redirigé. Si le tunnel sécurisé est activé, les connexions de redirection du lecteur client entre Horizon Client et View Secure Gateway sont sécurisées, mais les connexions entre View Secure Gateway et les machines de poste de travail ne sont pas chiffrées. Si le tunnel sécurisé est désactivé, les connexions de redirection du lecteur client entre Horizon Client et les machines de poste de travail ne sont pas chiffrées. Pour vous assurer que ces données ne peuvent pas être surveillées sur le réseau, utilisez la redirection du lecteur client uniquement sur un réseau sécurisé si Horizon Client est antérieur à la version 3.5 ou si l'agent est antérieur à la version 6.2.

L'option d'installation **Redirection du lecteur client** dans le programme d'installation de l'agent est sélectionnée par défaut. Il vous est conseillé d'activer l'option d'installation **Redirection du lecteur client** uniquement sur les pools de postes de travail où les utilisateurs requièrent cette fonctionnalité.

Utiliser une stratégie de groupe pour désactiver la redirection du lecteur client

Vous pouvez désactiver la redirection du lecteur client en configurant un paramètre de stratégie de groupe Services Bureau à distance Microsoft pour des postes de travail distants et des hôtes RDS dans Active Directory.

Pour plus d'informations sur la redirection du lecteur client, consultez le document *Utilisation de VMware Horizon Client* pour le type spécifique de périphérique client de poste de travail. Allez sur https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Remarque Ce paramètre remplace le registre local et les paramètres des Stratégies de carte à puce qui activent la fonctionnalité de redirection du lecteur client.

Prérequis

Si le déploiement d'View inclut un pare-feu dorsal entre vos serveurs de sécurité de la zone DMZ et votre réseau interne, assurez-vous que le pare-feu dorsal autorise le trafic vers le port 9427 de vos postes de travail mono-utilisateur et RDS. Des connexions TCP sur le port 9427 sont requises pour prendre en charge la redirection du lecteur client.

Pour Horizon Client 4.2 ou Horizon 7 version 7.0.2 ou ultérieure, le port 9427 n'a pas besoin d'être ouvert si VMware Blast Extreme est activé, car la redirection du lecteur client transfère les données via le canal virtuel.

Procédure

1. Dans l'Éditeur de stratégie de groupe, accédez à **Configuration de l'ordinateur\Règles\Modèles d'administration\Composants Windows\Services Bureau à distance\Hôte de session de poste de travail distant\Redirection de périphériques et de ressources**.

   Ce chemin de navigation concerne Active Directory sur Windows Server 2012. Le chemin de navigation est différent sur d'autres systèmes d'exploitation Windows.

2. Activez le paramètre de stratégie de groupe **Ne pas autoriser la redirection de lecteur**.

Utiliser des paramètres de registre pour configurer la redirection du lecteur client

Vous pouvez utiliser des paramètres de clé de registre Windows pour contrôler le comportement de la redirection du lecteur client sur un poste de travail distant. Cette fonctionnalité requiert Horizon Agent 7.0 ou version ultérieure et Horizon Client 4.0 ou version ultérieure.

Les paramètres de registre Windows qui contrôlent le comportement de la redirection du lecteur client sur un poste de travail distant se trouvent dans le chemin d'accès suivant :

```
HKLM\Software\VMware, Inc.\VMware TSDR
```

Vous pouvez utiliser l'Éditeur du Registre Windows sur le poste de travail distant pour modifier les paramètres de registre locaux.

Remarque Les stratégies de redirection du lecteur client définies avec Stratégies de carte à puce sont prioritaires sur les paramètres de registre locaux.

Désactivation de la redirection du lecteur client

Pour désactiver la redirection du lecteur client, créez une valeur de chaîne `disabled` et définissez-la sur `true`.

```
HKLM\Software\VMware, Inc.\VMware TSDR\disabled=true
```

La valeur est `false` (activée) par défaut.

Empêcher l'accès en écriture à des dossiers partagés

Pour empêcher l'accès en écriture à tous les dossiers partagés avec le poste de travail distant, créez une valeur de chaîne `permissions` et définissez-la sur une chaîne qui commence par `r`, sauf pour `rw`.

```
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
```

La valeur est `rw` (tous les dossiers partagés sont accessibles en lecture et en écriture) par défaut.

Partage de dossiers spécifiques

Pour partager des dossiers spécifiques avec le poste de travail distant, créez une clé `default shares` et créez une sous-clé pour chaque dossier à partager avec le poste de travail distant. Pour chaque sous-clé, créez une valeur de chaîne `name` et définissez-la sur le chemin d'accès du dossier à partager. L'exemple suivant partage les dossiers `C:\ebooks` et `C:\spreadsheets`.

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f1\name=C:\ebooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f2\name=C:\spreadsheets
```

Si vous définissez `name` sur `*all`, tous les lecteurs clients sont partagés avec le poste de travail distant. Le paramètre `*all` n'est pris en charge que sur les systèmes clients Windows.

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\1st\name=*all
```

Pour empêcher le client de partager d'autres dossiers (c'est-à-dire des dossiers non spécifiés avec la clé `default shares`), créez une valeur de chaîne `ForcedByAdmin` et définissez-la sur `true`.

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
```

Lorsque la valeur est `true`, la boîte de dialogue Partage n'apparaît pas quand les utilisateurs se connectent au poste de travail distant dans Horizon Client. La valeur est `false` (les clients peuvent partager des dossiers supplémentaires) par défaut.

L'exemple suivant partage les dossiers `C:\ebooks` et `C:\spreadsheets`, met les deux dossiers en lecture seule et empêche le client de partager des dossiers supplémentaires.

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f1\name=C:\ebooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f2\name=C:\spreadsheets
```

Remarque N'utilisez pas la fonctionnalité `ForcedByAdmin` comme fonctionnalité de sécurité ou contrôle du partage. Un utilisateur peut contourner le paramètre `ForcedByAdmin=true` en créant un lien vers un partage existant qui renvoie aux dossiers non spécifiés par la clé `default shares`.

Configurer Skype Entreprise

Vous pouvez passer des appels audio et vidéo optimisés avec Skype Entreprise à l'intérieur d'un poste de travail virtuel sans affecter négativement l'infrastructure virtuelle et sans surcharger le réseau.

Tout le traitement multimédia a lieu sur la machine cliente plutôt que dans le poste de travail virtuel lors des appels audio et vidéo Skype.

Pour utiliser Skype Entreprise, vous devez installer le pack de virtualisation pour Skype Entreprise sur la machine cliente lors de l'installation d'Horizon Client pour Windows. Consultez le document *Utilisation de VMware Horizon Client pour Windows*.

Un administrateur Horizon doit installer le pack de virtualisation pour Skype Entreprise sur le poste de travail virtuel lors de l'installation d'Horizon Agent.

Fonctionnalités de Skype Entreprise

Skype Entreprise offre les fonctionnalités suivantes :

- Appels audio point à point
- Appels vidéo point à point
- Appels PSTN via un pavé de numérotation
- Transfert, coupure du son, mise en attente et reprise d'un appel
- Commandes HID
- Appels PSTN via un serveur de médiation
- Connectivité à distance et appels via le serveur Edge
- Attente musicale
- Intégration de la messagerie vocale

Configuration système requise de Skype Entreprise

Cette fonctionnalité prend en charge les configurations suivantes.

Tableau 2-4. Configuration système requise de Skype Entreprise

Système	Configuration requise
Server	Lync Server 2013, Skype Entreprise Server 2015, Office 365
Client	Skype Entreprise 2015 15.0.4675.1003 et versions ultérieures Skype Entreprise 2016 dans le cadre d'Office 365 Plus : 16.0.7571.2072 ou version ultérieure Skype Entreprise 2016 dans le cadre d'Office 2016 : 16.0.4534.1000 ou version ultérieure
Systèmes d'exploitation de postes de travail virtuels	Postes de travail persistants et non persistants Windows 7, Windows 8.1, Windows 10. Les postes de travail Windows 2008 R2 et Windows 2012 R2 sont également pris en charge.
Systèmes d'exploitation de machines clients	Windows 7, Windows 8.1, Windows 10
Protocoles d'affichage	VMware Blast et PCoIP
Ports réseau	Les mêmes ports que ceux utilisés par le client Skype Entreprise natif. Voir les ports clients dans https://technet.microsoft.com/en-us/library/gg398833.aspx
Webcam	Les mêmes périphériques qui sont compatibles avec Skype Entreprise. Voir les webcams répertoriées dans https://technet.microsoft.com/en-us/office/dn947482.aspx
Codecs audio et vidéo	Les mêmes que les codecs audio et vidéo utilisés par le client Skype Entreprise natif. Reportez-vous à la section https://technet.microsoft.com/en-us/library/gg425841.aspx?f=255&MSPPError=-2147217396.
Media Feature Pack	Doit être installé sur le poste de travail distant pour les versions N et KN de Windows 10. Vous pouvez installer Media Feature à partir de https://www.microsoft.com/en-us/download/details.aspx?id=48231

Limites de Skype Entreprise

Skype Entreprise présente les limites suivantes :

- Vous ne pouvez pas passer d'appels E.911.

- IPv6 n'est pas pris en charge.
- Vous ne pouvez pas personnaliser les sonneries.
- Les appels Response Group, le parcage d'appel, la prise d'appels depuis le parcage et les appels via le bureau ne sont pas pris en charge.
- L'utilisation d'un tableau blanc, l'affichage de la galerie, les webcams panoramiques et le partage d'écran ne sont pas pris en charge actuellement.
- Vous ne pouvez pas enregistrer les appels.
- L'utilisation du client Lync ou Skype Entreprise sur la machine cliente en même temps que le client Skype Entreprise optimisé dans le poste de travail distant n'est pas prise en charge.
- L'interface utilisateur du client Lync 2013 n'est pas prise en charge lors de la connexion du client Skype 2015 à un serveur Lync 2013. Un administrateur peut configurer l'interface utilisateur du client Skype sur le serveur :https://social.technet.microsoft.com/wiki/contents/articles/30282.switch-between-skype-for-business-and-lync-client-ui.aspx
- Les conférences audio et vidéo impliquant plus de deux utilisateurs ne sont actuellement pas prises en charge.
- Les réunions Conférence maintenant ne sont pas prises en charge.
- Dans la fenêtre d'aperçu vidéo, si vous souhaitez afficher un aperçu d'une caméra différente de celle répertoriée, sélectionnez le périphérique, puis fermez et rouvrez la boîte de dialogue pour afficher l'aperçu.
- Si vous êtes connecté à un réseau privé lorsque vous installez Skype Entreprise sur le poste de travail distant, le programme d'installation ajoute des règles de pare-feu entrant et sortant pour ce profil réseau. Lorsque vous ouvrez une session sur le poste de travail distant à partir d'un réseau de domaine, puis que vous utilisez Skype Entreprise, une exception de pare-feu s'affiche. Pour corriger le problème, ajoutez manuellement des exceptions de pare-feu pour le client Skype Entreprise dans les règles de pare-feu pour tous les profils réseau.
- L'option de contrôle du volume dans le système d'exploitation du poste de travail distant n'affecte pas le niveau de volume d'un appel Skype en cours. Utilisez le contrôle du volume dans l'appel Skype ou le contrôle du volume sur la machine cliente pour modifier le volume.

Configuration de la redirection de contenu URL 3

Avec la fonctionnalité de redirection de contenuURL, vous pouvez configurer des URL spécifiques pour qu'elles s'ouvrent sur la machine cliente ou dans une application ou un poste de travail distant. Vous pouvez rediriger des URL que les utilisateurs tapent dans la barre d'adresses Internet Explorer ou dans une application.

Ce chapitre aborde les rubriques suivantes :

Comprendre la redirection de contenu URL

La fonctionnalité de redirection de contenu URL prend en charge la redirection depuis une application ou un poste de travail distant vers un client et vice versa.

La redirection depuis une application ou un poste de travail distant vers un client est appelée redirection agent vers client. La redirection depuis un client vers une application ou un poste de travail distant est appelée redirection client vers agent.

Redirection agent vers client

Avec la redirection agent vers client, Horizon Agent envoie l'URL à Horizon Client, qui ouvre l'application par défaut pour le protocole dans l'URL sur la machine cliente.

Redirection client vers agent

Avec la redirection client vers agent, Horizon Client ouvre une application ou un poste de travail distant que vous spécifiez pour traiter l'URL. Si l'URL est redirigée vers un poste de travail distant, le lien est ouvert dans le navigateur par défaut pour le protocole sur le poste de travail. Si l'URL est redirigée vers une application distante, le lien est ouvert par l'application spécifiée. L'utilisateur final doit être autorisé à accéder au pool de postes de travail ou d'applications.

Vous pouvez rediriger certaines URL depuis une application ou un poste de travail distant vers un client et rediriger d'autres URL depuis un client vers une application ou un poste de travail distant. Vous pouvez rediriger n'importe quel nombre de protocoles, notamment HTTP, HTTPS, mailto et callto.

Configuration requise pour la redirection de contenu URL

Pour utiliser la fonctionnalité de redirection de contenu URL, vos machines clientes, vos machines de poste de travail distant et vos hôtes RDS doivent respecter certaines exigences.

Clients Windows	Horizon Client 4.0 pour Windows ou version ultérieure. Pour utiliser la redirection client vers agent, vous devez activer la fonctionnalité de redirection de contenu URL lors de l'installation d'Horizon Client pour Windows. Il n'est pas nécessaire d'activer la fonctionnalité de redirection de contenu URL dans Horizon Client pour Windows pour utiliser la redirection agent vers client.
clients Mac	Horizon Client 4.2 pour Mac ou version ultérieure. Dans Horizon Client 4.2 ou 4.3 pour Mac, la redirection de contenu URL est une fonctionnalité de la version d'évaluation technique qui ne prend en charge que la redirection agent vers client. Dans Horizon Client 4.4 pour Mac et versions ultérieures, la redirection de contenu URL est prise en charge officiellement et elle prend en charge les redirections agent vers client et client vers agent.
Machines virtuelles de poste de travail et hôtes RDS	Horizon Agent 7.0 ou version ultérieure dans des machines de poste de travail distant et des hôtes RDS qui fournissent des postes de travail et des applications. Vous devez activer la fonctionnalité de redirection de contenu URL lors de l'installation d'Horizon Agent.
Navigateurs Web	Internet Explorer 9, 10 et 11
Protocoles d'affichage	VMware Blast et PCoIP

Utilisation de la redirection de contenu URL dans un environnement Architecture Cloud Pod

Si vous disposez d'un environnement Architecture Cloud Pod, vous pouvez configurer des paramètres globaux de redirection de contenu URL en plus des paramètres locaux de redirection de contenu URL.

Contrairement aux paramètres locaux de redirection de contenu URL, qui sont visibles uniquement dans l'espace local, les paramètres globaux de redirection de contenu URL sont visibles dans la fédération d'espaces. Avec des paramètres globaux de redirection de contenu URL, vous pouvez rediriger des liens URL dans le client vers des ressources globales, telles que des droits de poste de travail globaux et des droits d'application globaux.

Lorsqu'un utilisateur utilise Horizon Client pour se connecter à une instance du Serveur de connexion dans la fédération d'espaces, l'instance du Serveur de connexion recherche tous les paramètres locaux et globaux de redirection de contenu URL attribués à l'utilisateur. Les paramètres locaux et globaux sont fusionnés et utilisés dès que l'utilisateur clique sur une URL sur la machine cliente.

Pour plus d'informations sur la configuration et la gestion d'un environnement Architecture Cloud Pod, consultez le document *Administration d'Architecture Cloud Pod dans Horizon 7*.

Installation d' Horizon Agent avec la fonctionnalité de redirection de contenu URL

Pour utiliser la redirection de contenu URL depuis une application ou un poste de travail distant vers un client (redirection agent vers client) ou depuis un client vers une application ou un poste de travail distant (redirection client vers agent), vous devez activer la fonctionnalité de redirection de contenu URL lorsque vous installez Horizon Agent.

Au lieu de double-cliquer sur le fichier du programme d'installation, démarrez l'installation d'Horizon Agent en exécutant la commande suivante dans une fenêtre d'invite de commande :

```
VMware-viewagent-x86_64-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

Suivez les invites et terminez l'installation.

Pour vérifier que la fonctionnalité de redirection de contenu URL est installée, assurez-vous que les fichiers `vmware-url-protocol-launch-helper.exe` et `vmware-url-filtering-plugin.dll` se trouvent dans le répertoire `%PROGRAMFILES%\VMware\VMware View\Agent\bin\UrlRedirection`. De plus, vérifiez que le module complémentaire Internet Explorer Plug-in de filtrage URL VMware Horizon View est activé.

Configuration de la redirection agent vers client

Avec la redirection agent vers client, Horizon Agent envoie l'URL à Horizon Client, qui ouvre l'application par défaut pour le protocole dans l'URL.

Pour activer la redirection agent vers client, exécutez les tâches de configuration suivantes.

- Activez la fonctionnalité de redirection de contenu URL dans Horizon Agent. Reportez-vous à la section « Installation d'Horizon Agent avec la fonctionnalité de redirection de contenu URL », page 61.
- Appliquez les paramètres de stratégie de groupe de redirection de contenu URL à vos applications et postes de travail distants. Reportez-vous à la section « Ajouter le modèle d'administration ADMX de redirection de contenu URL à un GPO », page 61.
- Configurez des paramètres de stratégie de groupe pour indiquer, pour chaque protocole, comment Horizon Agent doit rediriger l'URL. Reportez-vous à la section « Paramètres de stratégie de groupe de redirection de contenu URL », page 62.

Ajouter le modèle d'administration ADMX de redirection de contenu URL à un GPO

Le fichier de modèle d'administration ADMX de redirection de contenu URL, nommé `urlRedirection-enUS.admx`, contient des paramètres vous permettant de contrôler si un lien URL est ouvert sur le client (redirection agent vers client) ou dans une application ou un poste de travail distant (redirection client vers agent).

Pour appliquer les paramètres de stratégie de groupe de redirection de contenu URL à vos applications et postes de travail distants, ajoutez le fichier de modèle d'administration ADMX à des GPO sur votre serveur Active Directory. Pour des règles concernant des liens URL sur lesquels vous cliquez dans une application ou un poste de travail distant, les GPO doivent être liés à l'UO qui contient vos postes de travail virtuels et vos hôtes RDS.

Vous pouvez également appliquer les paramètres de stratégie de groupe à un GPO lié à l'UO qui contient vos ordinateurs clients Windows, mais la méthode préférée pour la configuration de la redirection client vers agent consiste à utiliser l'utilitaire de ligne de commande `vdmutil`. Comme macOS ne prend pas en charge les GPO, vous devez utiliser `vmdutil` si vous disposez de clients Mac.

Prérequis

- Vérifiez que la fonctionnalité de redirection de contenu URL est incluse lorsque vous installez Horizon Agent. Reportez-vous à la section « Installation d'Horizon Agent avec la fonctionnalité de redirection de contenu URL », page 61.
- Vérifiez que les objets de stratégie de groupe (GPO) Active Directory sont créés pour les paramètres de stratégie de groupe de redirection de contenu URL.
- Vérifiez que les composants logiciels enfichables MMC (Microsoft Management Console) et Éditeur de gestion de stratégie de groupe sont disponibles sur votre serveur Active Directory.

Procédure

1. Téléchargez le fichier Horizon 7 GPO Bundle `.zip` 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 GPO Bundle.

   Le fichier se nomme `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, où *x.x.x* est la version et *yyyyyyy* le numéro de build. Tous les fichiers ADMX qui fournissent des paramètres de stratégie de groupe pour Horizon 7 sont disponibles dans ce fichier.

2. Décompressez le fichier `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip` et copiez le fichier ADMX de redirection de contenu URL sur votre serveur Active Directory.

   a. Copiez le fichier `urlRedirection-enUS.admx` dans le dossier `C:\Windows\PolicyDefinitions\`.

   b. Copiez le fichier de ressources de la langue `urlRedirection.adml` dans le sous-dossier correspondant dans le répertoire `C:\Windows\PolicyDefinitions`.

      Par exemple, pour l'anglais, copiez le fichier `urlRedirection-enUS.adml` dans le dossier `C:\Windows\PolicyDefinitions\en-US`.

3. Sur votre serveur Active Directory, ouvrez l'Éditeur de gestion de stratégie de groupe.

   Les paramètres de stratégie de groupe de redirection de contenu URL sont installés dans **Configuration ordinateur > Stratégies > Modèles d'administration > Redirection URL de VMware Horizon**.

Suivant

Configurez les paramètres de stratégie de groupe.

Paramètres de stratégie de groupe de redirection de contenu URL

Le fichier de modèle de redirection de contenu URL contient des paramètres de stratégie de groupe qui vous permettent de créer des règles pour la redirection agent vers client et client vers agent. Le fichier de modèle ne contient que des paramètres de Configuration d'ordinateur. Tous les paramètres se trouvent dans le dossier **Redirection URL de VMware Horizon** dans l'Éditeur de gestion de stratégie de groupe.

Le tableau suivant décrit les paramètres de stratégie de groupe dans le fichier de modèle de redirection de contenu URL.

Tableau 3-1. Paramètres de stratégie de groupe de redirection de contenu URL

Paramètre	Propriétés
`IE Policy: Prevent users from changing URL Redirection plugin loading behavior`	Détermine si les utilisateurs peuvent désactiver la fonctionnalité de redirection de contenu URL. Ce paramètre n'est pas configuré par défaut.
`IE Policy: Automatically enable URL Redirection plugin`	Détermine si les plug-ins Internet Explorer qui viennent d'être installés sont automatiquement activés. Ce paramètre n'est pas configuré par défaut.

Tableau 3-1. Paramètres de stratégie de groupe de redirection de contenu URL (suite)

Paramètre	Propriétés
`Url Redirection Enabled`	Détermine si la fonctionnalité de redirection de contenu URL est activée. Vous pouvez utiliser ce paramètre pour désactiver la fonctionnalité de redirection de contenu URL même si la fonctionnalité a été installée sur le client ou l'agent. Ce paramètre n'est pas configuré par défaut.
`Url Redirection Protocol 'http'`	Pour toutes les URL qui utilisent le protocole HTTP, spécifie les URL qui doivent être redirigées. Ce paramètre dispose des options suivantes : ■ **brokerHostname** : adresse IP ou nom complet de l'hôte de Serveur de connexion à utiliser lors de la redirection d'URL vers une application ou un poste de travail distant. ■ **remoteItem** : nom complet du pool d'applications ou de postes de travail distants qui peut traiter les URL spécifiées dans **agentRules**. ■ **clientRules** : URL devant être redirigées vers le client. Par exemple, si vous définissez **clientRules** sur **`.*.mycompany.com`**, toutes les URL contenant le texte `mycompany.com` sont redirigées vers le client Windows et sont ouvertes dans le navigateur par défaut sur le client. ■ **agentRules** : URL devant être redirigées vers l'application ou le poste de travail distant spécifié dans **remoteItem**. Par exemple, si vous définissez **agentRules** sur **`.*.mycompany.com`**, toutes les URL qui contiennent le texte « mycompany.com » sont redirigées vers l'application ou le poste de travail distant. Lorsque vous créez des règles d'agent, vous devez également utiliser l'option **brokerHostname** pour spécifier l'adresse IP ou le nom de domaine complet de l'hôte du Serveur de connexion et l'option **remoteItem** pour spécifier le nom complet du pool de postes de travail ou d'applications. **Remarque** La méthode préférée pour configurer des règles de client consiste à utiliser l'utilitaire de ligne de commande `vdmutil`. Ce paramètre est activé par défaut.
`Url Redirection Protocol '[...]'`	Utilisez ce paramètre pour n'importe quel protocole autre que HTTP, tel que HTTPS, email ou callto. Les options sont les mêmes que pour `Url Redirection Protocol 'http'`. Si vous n'avez pas besoin de configurer d'autres protocoles, vous pouvez supprimer ou commenter cette entrée avant d'ajouter le fichier de modèle de redirection de contenu URL à Active Directory. Il est recommandé de configurer les mêmes paramètres de redirection pour les protocoles HTTP et HTTPS. Ainsi, si un utilisateur saisit une URL partielle dans Internet Explorer, telle que `mycompany.com` et que ce site redirige automatiquement de HTTP vers HTTPS, la redirection de contenu URL fonctionnera comme prévu. Dans cet exemple, si vous définissez une règle pour HTTPS, mais que vous ne définissez pas le même paramètre de redirection pour HTTP, l'URL partielle que l'utilisateur saisit n'est pas redirigée. Ce paramètre n'est pas configuré par défaut.

Pour la redirection client vers agent, si vous configurez un protocole sans gestionnaire par défaut, après avoir configuré un paramètre de stratégie de groupe pour ce protocole, vous devez démarrer Horizon Client une fois avant que les URL qui spécifient ce protocole soient redirigées.

Syntaxe pour créer des règles de redirection de contenu URL

Vous pouvez utiliser des expressions régulières lorsque vous spécifiez les URL à ouvrir sur le client ou dans une application ou un poste de travail distant. Utilisez des points-virgules pour séparer plusieurs entrées. Les espaces ne sont pas autorisés entre les entrées.

Le tableau suivant décrit des exemples d'entrées.

Entrée	Description
`.*`	Spécifie que toutes les URL sont redirigées. Si vous utilisez ce paramètre pour des règles d'agent (option **agentRules**), toutes les URL sont ouvertes dans l'application ou le poste de travail distant spécifié. Si vous utilisez ce paramètre pour des règles de client (option **clientRules**), toutes les URL sont redirigées vers le client.
`.*.acme.com;.*.exemple.com`	Spécifie que toutes les URL qui contiennent le texte `.acme.com` ou `example.com` sont redirigées.
[espace ou laissez vide]	Spécifie qu'aucune URL n'est redirigée. Par exemple, laisser l'option **clientRules** vide spécifie qu'aucune URL n'est redirigée vers le client.

Exemple de stratégie de groupe de redirection agent vers client

Vous voulez peut-être utiliser la redirection agent vers client pour conserver des ressources ou en tant que couche de sécurité ajoutée. Si des employés travaillent sur une application ou un poste de travail distant et qu'ils veulent regarder des vidéos, par exemple, vous pouvez rediriger ces URL vers la machine cliente afin qu'aucune charge supplémentaire ne soit placée sur le centre de données. Ou bien, pour des raisons de sécurité, pour les employés qui travaillent à l'extérieur du réseau d'entreprise, vous pouvez préférer que toutes les URL qui pointent vers des emplacements externes au réseau d'entreprise soient ouvertes sur la propre machine cliente d'un employé.

Vous pouvez, par exemple, configurer des règles pour que le contenu non lié à l'entreprise, c'est-à-dire des URL qui ne pointent pas vers le réseau d'entreprise, soit redirigé pour s'ouvrir sur la machine cliente. Dans ce cas, vous pouvez utiliser les paramètres suivants, qui incluent des expressions régulières :

- Pour **agentRules** : `.*.mycompany.com`

  Cette règle redirige toutes les URL qui contiennent le texte `mycompany.com` pour les ouvrir sur l'application ou le poste de travail distant spécifié (agent).

- Pour **clientRules** : `.*`

  Cette règle redirige toutes les URL vers le client pour les ouvrir avec le navigateur client par défaut.

La fonctionnalité de redirection de contenu URL utilise le processus suivant pour appliquer des règles de client et d'agent :

1. Lorsqu'un utilisateur clique sur un lien dans une application ou un poste de travail distant, les règles du client sont vérifiées en premier.
2. Si l'URL correspond à une règle de client, les règles d'agent sont vérifiées par la suite.
3. S'il existe un conflit entre les règles d'agent et les règles de client, le lien est ouvert localement. Dans ce cas, l'URL est ouverte sur la machine agent.
4. S'il n'y a pas de conflit, l'URL est redirigée vers le client.

Dans l'exemple, il existe un conflit entre les règles de client et les règles d'agent, car les URL contenant **`mycompany.com`** sont un sous-ensemble de toutes les URL. À cause de ce conflit, les URL contenant **`mycompany.com`** sont ouvertes localement. Si vous cliquez sur un lien contenant **`mycompany.com`** dans l'URL alors que vous vous trouvez sur un poste de travail distant, l'URL est ouverte sur ce poste de travail distant. Si vous cliquez sur un lien contenant **`mycompany.com`** dans l'URL alors que vous vous trouvez sur un système client, l'URL est ouverte sur le client.

Configuration de la redirection client vers agent

Avec la redirection client vers agent, Horizon Client ouvre une application ou un poste de travail distant pour traiter un lien URL sur lequel un utilisateur clique sur le client. Si un poste de travail distant est ouvert, l'application par défaut pour le protocole dans l'URL traite l'URL. Si une application distante est ouverte, l'application traite l'URL.

Pour utiliser la redirection client vers agent, exécutez les tâches de configuration suivantes.

- Activez la fonctionnalité de redirection de contenu URL dans Horizon Agent. Reportez-vous à la section « Installation d'Horizon Agent avec la fonctionnalité de redirection de contenu URL », page 61.
- (Clients Windows uniquement) Activez la fonctionnalité de redirection de contenu URL dans Horizon Client pour Windows. Reportez-vous à la section « Installation d'Horizon Client pour Windows avec la fonctionnalité de redirection de contenu URL », page 65.
- Utilisez l'utilitaire de ligne de commande `vdmutil` pour créer un paramètre de redirection de contenu URL qui indique, pour chaque protocole, comment Horizon Client doit rediriger les URL. Reportez-vous à la section « Créer un paramètre local de redirection de contenu URL », page 67 ou « Créer un paramètre global de redirection de contenu URL », page 69.
- Utilisez l'utilitaire de ligne de commande `vdmutil` pour attribuer le paramètre de redirection de contenu URL à des utilisateurs ou des groupes Active Directory. Reportez-vous à la section « Attribuer un paramètre de redirection de contenu URL à un utilisateur ou un groupe », page 71.
- Vérifiez le paramètre de redirection de contenu URL. Reportez-vous à la section « Tester un paramètre de redirection de contenu URL », page 72.

Remarque Vous pouvez utiliser des paramètres de stratégie de groupe pour configurer des règles de redirection client vers agent, mais l'utilisation de l'utilitaire de ligne de commande `vdmutil` est la méthode préférée. Pour plus d'informations, reportez-vous à la section « Utilisation de paramètres de stratégie de groupe pour configurer la redirection client vers agent », page 74.

Installation d' Horizon Client pour Windows avec la fonctionnalité de redirection de contenu URL

Pour utiliser la redirection de contenu URL à partir d'un client Windows vers une application ou un poste de travail distant (redirection client vers agent), vous devez installer Horizon Client pour Windows avec la fonctionnalité de redirection de contenu URL.

Pour activer la fonctionnalité de redirection de contenu URL, vous devez utiliser le programme d'installation d'Horizon Client pour Windows avec une option de ligne de commande. Au lieu de double-cliquer sur le fichier du programme d'installation, démarrez l'installation en exécutant la commande suivante dans une fenêtre d'invite de commande :

```
VMware-Horizon-Client-x86-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

Pour vérifier que la fonctionnalité est installée, assurez-vous que les fichiers `vmware-url-protocol-launch-helper.exe` et `vmware-url-filtering-plugin.dll` se trouvent dans le répertoire `%PROGRAMFILES%\VMware\VMware Horizon View Client`. De plus, vérifiez que le module complémentaire Internet Explorer Plug-in de filtrage URL VMware Horizon View est installé.

Remarque Horizon Client 4.4 pour Mac prend en charge la redirection client vers agent par défaut. Aucune autre étape d'installation n'est requise. Horizon Client 4.2 et 4.3 pour Mac ne prennent pas en charge la redirection client vers agent.

Utilisation de l'utilitaire de ligne de commande vdmutil

Vous pouvez utiliser l'interface de ligne de commande `vdmutil` afin de créer, attribuer et gérer les paramètres de redirection de contenu URL pour la redirection client vers agent.

Utilisation de la commande

La syntaxe de la commande `vdmutil` contrôle son fonctionnement depuis une invite de commande Windows.

```
vdmutil command_option [additional_option argument] ...
```

Les options supplémentaires que vous pouvez utiliser dépendent de l'option de commande.

Par défaut, le chemin d'accès au fichier exécutable de la commande `vdmutil` est `C:\Program Files\VMware\VMware View\Server\tools\bin`. Pour éviter d'entrer le chemin d'accès sur la ligne de commande, ajoutez-le à la variable d'environnement PATH.

Authentification de la commande

Vous devez exécuter la commande `vdmutil` en tant qu'utilisateur disposant du rôle Administrateurs.

Vous pouvez utiliser Horizon Administrator pour attribuer le rôle Administrateurs à un utilisateur. Pour plus d'informations, reportez-vous au document *Administration de View*.

La commande `vdmutil` inclut des options pour spécifier le nom d'utilisateur, le domaine et le mot de passe à utiliser pour l'authentification. Vous devez utiliser ces options d'authentification avec toutes les options de la commande `vdmutil`, à l'exception de `--help` et de `--verbose`.

Tableau 3-2. options d'authentification de la commande vdmutil

Option	Description
`--authAs`	Nom d'utilisateur d'un utilisateur administrateur Horizon pour s'authentifier sur l'instance du Serveur de connexion. N'utilisez ni le format **`domain\username`** ni le format de nom principal d'utilisateur (UPN).
`--authDomain`	Nom de domaine complet de l'utilisateur administrateur Horizon spécifié dans l'option `--authAs`.
`--authPassword`	Mot de passe de l'administrateur Horizon spécifié dans l'option `--authAs`. Si vous entrez **`"*"`** plutôt qu'un mot de passe, la commande `vdmutil` affiche une invite de mot de passe et ne conserve pas les mots de passe sensibles dans l'historique des commandes sur la ligne de commande.

Par exemple, la commande `vdmutil` suivante connecte l'utilisateur mydomain\johndoe.

```
vdmutil --listURLSetting --authAs johndoe --authDomain mydomain --authPassword secret
```

Sortie de commande

La commande `vdmutil` renvoie 0 lorsqu'une opération réussit et un code différent de zéro spécifique d'un échec lorsqu'une opération échoue. La commande `vdmutil` écrit des messages d'erreur en format d'erreur standard. Lorsqu'une opération produit une sortie ou lorsque la journalisation détaillée est activée à l'aide de l'option `--verbose`, la commande `vdmutil` écrit la sortie en format de sortie standard en anglais américain.

Options pour la redirection de contenu URL

Vous pouvez utiliser les options de la commande `vdmutil` suivante pour créer, attribuer et gérer des paramètres de redirection de contenu URL. Toutes les options sont précédées de deux tirets (--).

Tableau 3-3. Options de la commande vdmutil pour la redirection de contenu URL

Option	Description
`--addGroupURLSetting`	Attribue un groupe à un paramètre de redirection de contenu URL particulier.
`--addUserURLSetting`	Attribue un utilisateur à un paramètre de redirection de contenu URL particulier.
`--createURLSetting`	Crée un paramètre de redirection de contenu URL.
`--deleteURLSetting`	Supprime un paramètre de redirection de contenu URL.
`--disableURLSetting`	Désactive un paramètre de redirection de contenu URL.
`--enableURLSetting`	Active un paramètre de redirection de contenu URL qui était précédemment désactivé avec l'option `--disableURLSetting`.
`--listURLSetting`	Répertorie tous les paramètres de redirection de contenu URL sur l'instance du Serveur de connexion.
`--readURLSetting`	Affiche des informations sur un paramètre de redirection de contenu URL.
`--removeGroupURLSetting`	Supprime une attribution de groupe d'un paramètre de redirection de contenu URL.
`--removeUserURLSetting`	Supprime une attribution d'utilisateur d'un paramètre de redirection de contenu URL.
`--updateURLSetting`	Met à jour un paramètre de redirection de contenu URL existant.

Vous pouvez afficher des informations sur la syntaxe pour toutes les options `vdmutil` en tapant **`vdmutil --help`**. Pour afficher des informations détaillées sur la syntaxe pour une option particulière, tapez **`vdmutil --`*`option`*` --help`**.

Créer un paramètre local de redirection de contenu URL

Vous pouvez créer un paramètre local de redirection de contenu URL qui redirige des URL spécifiques pour qu'elles s'ouvrent sur une application ou un poste de travail distant. Un paramètre local de redirection de contenu URL n'est visible que dans l'espace local.

Vous pouvez configurer n'importe quel nombre de protocoles, notamment HTTP, HTTPS, mailto et callto.

Il est recommandé de configurer les mêmes paramètres de redirection pour les protocoles HTTP et HTTPS. Ainsi, si un utilisateur saisit une URL partielle dans Internet Explorer, telle que `mycompany.com` et que ce site redirige automatiquement de HTTP vers HTTPS, la redirection de contenu URL fonctionnera comme prévu. Dans cet exemple, si vous définissez une règle pour HTTPS, mais que vous ne définissez pas le même paramètre de redirection pour HTTP, l'URL partielle que l'utilisateur saisit n'est pas redirigée.

Pour créer un paramètre global de redirection de contenu URL, qui est visible dans la fédération d'espaces, reportez-vous à la section « Créer un paramètre global de redirection de contenu URL », page 69.

Prérequis

Familiarisez-vous avec les options et les exigences de l'interface de ligne de commande `vdmutil` et vérifiez que vous disposez de privilèges suffisants pour exécuter la commande `vdmutil`. Reportez-vous à la section « Utilisation de l'utilitaire de ligne de commande vdmutil », page 66.

Procédure

1 Connectez-vous à l'instance du Serveur de connexion.

2 Exécutez la commande `vdmutil` avec l'option `--createURLSetting` pour créer le paramètre de redirection de contenu URL.

```
vdmutil --createURLSetting --urlSettingName value --urlRedirectionScope LOCAL
[--description value] [--urlScheme value] [--entitledApplication value | --entitledDesktop
value] [--agentURLPattern value]
```

Option	Description
--urlSettingName	Nom unique du paramètre de redirection de contenu URL. Le nom peut contenir entre 1 et 64 caractères.
--urlRedirectionScope	Portée du paramètre de redirection de contenu URL. Spécifiez LOCAL pour rendre le paramètre visible uniquement dans l'espace local.
--description	Description du paramètre de redirection de contenu URL. La description peut contenir entre 1 et 1 024 caractères.
--urlScheme	Protocole auquel le paramètre de redirection de contenu URL s'applique, par exemple, http, https, mailto ou callto.
--entitledApplication	Nom complet d'un pool d'applications local à utiliser pour ouvrir les URL spécifiées, par exemple `iexplore-2012`. Vous pouvez également utiliser cette option pour spécifier le nom complet d'un pool de postes de travail RDS local.
--entitledDesktop	Nom complet d'un pool de postes de travail local à utiliser pour ouvrir les URL spécifiées, par exemple xx. Pour les pools de postes de travail RDS, utilisez l'option `--entitledApplication`.
--agentURLPattern	Chaîne entre guillemets qui spécifie l'URL devant être ouverte sur l'application ou le poste de travail distant. Vous devez inclure le préfixe de protocole. Vous pouvez utiliser des caractères génériques pour spécifier un modèle d'URL qui correspond à plusieurs URL. Par exemple, si vous tapez **`"http://google.*"`**, toutes les URL contenant le texte **`google`** sont redirigées vers l'application ou le poste de travail distant que vous avez spécifié. Si vous tapez **`.*`** (point étoile), toutes les URL sont redirigées vers l'application ou le poste de travail distant.

3 (Facultatif) Exécutez la commande `vdmutil` avec l'option `--updateURLSetting` pour ajouter plus de protocoles, d'URL et de ressources locales au paramètre de redirection de contenu URL que vous avez créé.

```
vdmutil --updateURLSetting --urlSettingName value --urlRedirectionScope LOCAL
[--description value][--urlScheme value][--entitledApplication value | --entitledDesktop
value] [--agentURLPattern value]
```

Les options sont les mêmes que pour la commande `vdmutil` avec l'option `--createURLSetting`.

Exemple : Création d'un paramètre local de redirection de contenu URL

L'exemple suivant crée un paramètre local de redirection de contenu URL appelé `url-filtering` qui redirige toutes les URL de client contenant le texte `http://google.*` vers le pool d'applications appelé `iexplore2012`.

```
VdmUtil --createURLSetting --urlSettingName url-filtering --urlScheme http
--entitledApplication iexplore2012 --agentURLPattern "http://google.*"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

L'exemple suivant met à jour le paramètre `url-filtering` pour rediriger également toutes les URL de client qui contiennent le texte `https://google.*` vers le pool d'applications appelé `iexplore2012`.

```
vdmutil --updateURLSetting --urlSettingName url-filtering --urlScheme https
--entitledApplication iexplore2012 --agentURLPattern "https://google.*"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

L'exemple suivant met à jour le paramètre `url-filtering` pour rediriger toutes les URL de client qui contiennent le texte `mailto://.*.mycompany.com` vers le pool d'applications appelé `Outlook2008`.

```
vdmutil --updateURLSetting --urlSettingName url-filtering --urlScheme mailto
--entitledApplication Outlook2008 --agentURLPattern "mailto://.*.mycompany.com"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

Suivant

Attribuez le paramètre de redirection de contenu URL à un utilisateur ou un groupe. Reportez-vous à la section « Attribuer un paramètre de redirection de contenu URL à un utilisateur ou un groupe », page 71.

Créer un paramètre global de redirection de contenu URL

Si vous disposez d'un environnement Architecture Cloud Pod, vous pouvez créer un paramètre global de redirection de contenu URL qui redirige des URL spécifiques pour qu'elles s'ouvrent sur une application ou un poste de travail distant dans n'importe quel espace de la fédération d'espaces.

Un paramètre global de redirection de contenu URL est visible dans la fédération d'espaces. Lorsque vous créez un paramètre global de redirection de contenu URL, vous pouvez rediriger les URL vers des ressources globales, telles que des droits de poste de travail globaux et des droits d'application globaux.

Vous pouvez configurer n'importe quel nombre de protocoles, notamment HTTP, HTTPS, mailto et callto.

Il est recommandé de configurer les mêmes paramètres de redirection pour les protocoles HTTP et HTTPS. Ainsi, si un utilisateur saisit une URL partielle dans Internet Explorer, telle que `mycompany.com` et que ce site redirige automatiquement de HTTP vers HTTPS, la redirection de contenu URL fonctionnera comme prévu. Dans cet exemple, si vous définissez une règle pour HTTPS, mais que vous ne définissez pas le même paramètre de redirection pour HTTP, l'URL partielle que l'utilisateur saisit n'est pas redirigée.

Pour plus d'informations sur la configuration et la gestion d'un environnement Architecture Cloud Pod, consultez le document *Administration d'Architecture Cloud Pod dans Horizon 7*.

Pour créer un paramètre local de redirection de contenu URL, reportez-vous à la section « Créer un paramètre local de redirection de contenu URL », page 67.

Prérequis

Familiarisez-vous avec les options et les exigences de l'interface de ligne de commande `vdmutil` et vérifiez que vous disposez de privilèges suffisants pour exécuter la commande `vdmutil`. Reportez-vous à la section « Utilisation de l'utilitaire de ligne de commande vdmutil », page 66.

Procédure

1 Connectez-vous à une instance du Serveur de connexion dans la fédération d'espaces.

2 Exécutez la commande `vdmutil` avec l'option `--createURLSetting` pour créer le paramètre de redirection de contenu URL.

```
vdmutil --createURLSetting --urlSettingName value --urlRedirectionScope GLOBAL
[--description value] [--urlScheme value] [--entitledApplication value | --entitledDesktop
value] [--agentURLPattern value]
```

Option	Description
--urlSettingName	Nom unique du paramètre de redirection de contenu URL. Le nom peut contenir entre 1 et 64 caractères.
--urlRedirectionScope	Portée du paramètre de redirection de contenu URL. Spécifiez GLOBAL pour rendre le paramètre visible dans la fédération d'espaces.
--description	Description du paramètre de redirection de contenu URL. La description peut contenir entre 1 et 1 024 caractères.
--urlScheme	Protocole auquel le paramètre de redirection de contenu URL s'applique, par exemple, http, https, mailto ou callto.
--entitledApplication	Nom complet d'un droit d'application global à utiliser pour ouvrir les URL spécifiées.
--entitledDesktop	Nom complet d'un droit de poste de travail global à utiliser pour ouvrir les URL spécifiées, par exemple GE-1.
--agentURLPattern	Chaîne entre guillemets qui spécifie l'URL devant être ouverte sur l'application ou le poste de travail distant. Vous devez inclure le préfixe de protocole. Vous pouvez utiliser des caractères génériques pour spécifier un modèle d'URL qui correspond à plusieurs URL. Par exemple, si vous tapez « http://google.* », toutes les URL qui incluent le texte google sont redirigées vers l'application ou le poste de travail distant. Si vous tapez .* (point étoile), toutes les URL sont redirigées vers l'application ou le poste de travail distant.

3 (Facultatif) Exécutez la commande `vdmutil` avec l'option `--updateURLSetting` pour ajouter plus de protocoles, d'URL et de ressources globales au paramètre de redirection de contenu URL que vous avez créé.

```
vdmutil --updateURLSetting --urlSettingName value --urlRedirectionScope GLOBAL
[--description value][--urlScheme value][--entitledApplication value | --entitledDesktop
value] [--agentURLPattern value]
```

Les options sont les mêmes que pour la commande `vdmutil` avec l'option `--createURLSetting`.

Exemple : Configuration d'un paramètre global de redirection de contenu URL

L'exemple suivant crée un paramètre global de redirection de contenu URL appelé `Operations-Setting` qui redirige toutes les URL de client contenant le texte `http://google.*` vers le droit d'application global appelé `GAE1`.

```
vdmutil --createURLSetting --urlSettingName Operations-Setting --urlRedirectionScope GLOBAL
--urlScheme http --entitledApplication GAE1 --agentURLPattern "http://google.*" --authAs johndoe
--authDomain mydomain --authPassword secret
```

L'exemple suivant met à jour le paramètre `Operations-Setting` pour rediriger également toutes les URL qui contiennent le texte `https://google.*` vers le droit d'application global appelé `GAE1`.

```
vdmutil --updateURLSetting --urlSettingName Operations-Setting --urlRedirectionScope GLOBAL
--urlScheme https --entitledApplication GAE1 --agentURLPattern "https://google.*" -authAs
johndoe
--authDomain mydomain --authPassword secret
```

L'exemple suivant met à jour le paramètre `Operations-Setting` pour rediriger toutes les URL qui contiennent le texte "`mailto://.*.mycompany.com`" vers le droit d'application global appelé `GA2`.

```
vdmutil --updateURLSetting --urlSettingName Operations-Setting --urlRedirectionScope GLOBAL
--urlScheme mailto --entitledApplication GAE2 --agentURLPattern "mailto://.*.mycompany.com"
--authAs johndoe --authDomain mydomain --authPassword secret
```

Suivant

Attribuez le paramètre de redirection de contenu URL à un utilisateur ou un groupe. Reportez-vous à la section « Attribuer un paramètre de redirection de contenu URL à un utilisateur ou un groupe », page 71.

Attribuer un paramètre de redirection de contenu URL à un utilisateur ou un groupe

Une fois que vous avez créé un paramètre de redirection de contenu URL, vous pouvez l'attribuer à un utilisateur ou un groupe Active Directory.

Prérequis

Familiarisez-vous avec les options et les exigences de l'interface de ligne de commande `vdmutil` et vérifiez que vous disposez de privilèges suffisants pour exécuter la commande `vdmutil`. Reportez-vous à la section « Utilisation de l'utilitaire de ligne de commande vdmutil », page 66.

Procédure

- Pour attribuer un paramètre de redirection de contenu URL à un utilisateur, exécutez la commande `vdmutil` avec l'option `--addUserURLSetting`.

  ```
  vdmutil --addUserURLSetting --urlSettingName value --userName value
  ```

Option	Description
--urlSettingName	Nom du paramètre de redirection de contenu URL à attribuer.
--userName	Nom de l'utilisateur Active Directory au format `domain\username`.

- Pour attribuer un paramètre de redirection de contenu URL à un groupe, exécutez la commande `vdmutil` avec l'option `--addGroupURLSetting`.

  ```
  vdmutil --addGroupURLSetting --urlSettingName value --groupName value
  ```

Option	Description
--urlSettingName	Nom du paramètre de redirection de contenu URL à attribuer.
--groupName	Nom du groupe Active Directory au format `domain\group`.

Exemple : Attribution d'un paramètre de redirection de contenu URL

L'exemple suivant attribue le paramètre de redirection de contenu URL nommé `url-filtering` à l'utilisateur nommé `mydomain\janedoe`.

```
vdmutil --addUserURLSetting --authAs johndoe --authDomain mydomain
--authPassword secret --urlSettingName url-filtering --userName mydomain\janedoe
```

L'exemple suivant attribue le paramètre de redirection de contenu URL nommé `url-filtering` au groupe nommé `mydomain\usergroup`.

```
vdmutil --addGoupURLSetting --authAs johndoe --authDomain mydomain
--authPassword secret --urlSettingName url-filtering --groupName mydomain\usergroup
```

Suivant

Vérifiez vos paramètres de redirection de contenu URL. Reportez-vous à la section « Tester un paramètre de redirection de contenu URL », page 72.

Tester un paramètre de redirection de contenu URL

Une fois que vous avez créé et attribué un paramètre de redirection de contenu URL, effectuez certaines étapes pour vérifier que le paramètre fonctionne correctement.

Prérequis

Familiarisez-vous avec les options et les exigences de l'interface de ligne de commande `vdmutil` et vérifiez que vous disposez de privilèges suffisants pour exécuter la commande `vdmutil`. Reportez-vous à la section « Utilisation de l'utilitaire de ligne de commande vdmutil », page 66.

Procédure

1 Connectez-vous à l'instance du Serveur de connexion.

2 Exécutez la commande `vdmutil` avec l'option `--readURLSetting`.

Par exemple :

```
vdmutil --readURLSetting --urlSettingName url-filtering --authAs johndoe
--authDomain mydomain --authPassword secret
```

La commande affiche des informations détaillées sur le paramètre de redirection de contenu URL. Par exemple, la sortie de commande suivante du paramètre `url-filtering` indique que les URL HTTP et HTTPS contenant le texte `google.*` sont redirigées depuis le client vers le pool d'applications local nommé `iexplore2012`.

```
URL Redirection setting url-filtering
   Description                                    : null
   Enabled                                        : true
   Scope of URL Redirection Setting               : LOCAL
   URL Scheme And Local Resource handler pairs
      URL Scheme                                  : http
      Handler type                                : APPLICATION
      Handler Resource name                       : iexplore2012
      URL Scheme                                  : https
      Handler type                                : APPLICATION
      Handler Resource name                       : iexplore2012
   AgentPatterns
        https://google.*
        http://google.*
   ClientPatterns
      No client patterns configured
```

3 Sur une machine cliente Windows, ouvrez Horizon Client, connectez-vous à l'instance du Serveur de connexion, cliquez sur les URL qui correspondent aux modèles d'URL configurés dans le paramètre et vérifiez que les URL sont redirigées comme prévu.

4 Sur la même machine cliente Windows, ouvrez l'éditeur du registre (`regedit`) et vérifiez les clés de registre dans le chemin `\Computer\HKEY_CURRENT_USER\Software\VMware. Inc.\VMware VDM\URLRedirection\`.

   Vous devriez voir une clé pour chaque protocole spécifié dans le paramètre. Vous pouvez cliquer sur un protocole pour voir les règles qui lui sont associées. Par exemple, `agentRules` indique les URL qui sont redirigées, `brokerHostName` indique l'adresse IP ou le nom d'hôte complet de l'instance du Serveur de connexion utilisée lors de la redirection des URL et `remoteItem` indique le nom complet du pool de postes de travail ou d'applications qui traite les URL redirigées.

Gestion de paramètres de redirection de contenu URL

Vous pouvez utiliser des commandes `vdmutil` pour gérer vos paramètres de redirection de contenu URL.

Vous devez spécifier les options `--authAs`, `--authDomain` et `--authPassword` avec toutes les commandes. Pour plus d'informations, reportez-vous à la section « Utilisation de l'utilitaire de ligne de commande vdmutil », page 66.

Affichage des paramètres

Exécutez la commande `vdmutil` avec l'option `--listURLSetting` pour répertorier les noms de tous les paramètres de redirection de contenu URL configurés.

```
vdmutil --listURLSetting
```

Exécutez la commande `vdmutil` avec l'option `--readURLSetting` pour afficher les informations détaillées sur un paramètre de redirection de contenu URL particulier.

```
vdmutil --readURLSetting --urlSettingName value
```

Suppression d'un paramètre

Exécutez la commande `vdmutil` avec l'option `--deleteURLSetting` pour supprimer un paramètre de redirection de contenu URL.

```
vdmutil --deleteURLSetting --urlSettingName value
```

Désactivation et activation d'un paramètre

Exécutez la commande `vdmutil` avec l'option `--disableURLSetting` pour désactiver un paramètre de redirection de contenu URL.

```
vdmutil --disableURLSetting --urlSettingName value
```

Exécutez la commande `vdmutil` avec l'option --enableURLSetting pour activer un paramètre de redirection de contenu URL qui était désactivé.

```
vdmutil --enableURLSetting --urlSettingName value
```

Suppression d'un utilisateur ou d'un groupe d'un paramètre

Exécutez la commande `vdmutil` avec l'option `--removeUserURLSetting` pour supprimer un utilisateur d'un paramètre de redirection de contenu URL.

```
vdmutil --removeUserURLSetting --urlSettingName value --userName value
```

Exécutez la commande `vdmutil` avec l'option `--removeGroupURLSetting` pour supprimer un groupe d'un paramètre de redirection de contenu URL.

```
vdmutil --removeGroupURLSetting --urlSettingName value --userGroup value
```

Utilisez le format `domain\username` ou `domain\groupname` lorsque vous spécifiez un nom d'utilisateur ou de groupe.

Utilisation de paramètres de stratégie de groupe pour configurer la redirection client vers agent

Le fichier de modèle d'administration ADMX de redirection de contenu URL (`urlRedirection-enUS.admx`) contient des paramètres de stratégie de groupe que vous pouvez utiliser pour créer des règles qui redirigent des URL du client vers une application ou un poste de travail distant (redirection client vers agent).

Remarque La méthode préférée pour configurer la redirection client vers agent consiste à utiliser l'interface de ligne de commande `vdmutil`. Comme les GPO ne sont pas pris en charge par macOS, vous ne pouvez pas les utiliser pour régler la configuration client vers agent si vous disposez de clients macOS.

Pour créer une règle pour la redirection client vers agent, vous utilisez l'option **remoteItem** pour spécifier le nom complet d'un pool d'applications ou de postes de travail distants et l'option **agentRules** pour spécifier les URL qui doivent être redirigées vers l'application ou le poste de travail distant. Vous devez également utiliser l'option **brokerHostname** pour spécifier l'adresse IP ou le nom de domaine complet de l'hôte de Serveur de connexion à utiliser lors de la redirection des URL vers une application ou un poste de travail distant.

Par exemple, pour des raisons de sécurité, vous pourriez vouloir que toutes les URL HTTP qui pointent vers le réseau d'entreprise soient ouvertes dans une application ou un poste de travail distant. Dans ce cas, vous pouvez définir l'option **agentRules** sur **`.*.mycompany.com`**.

Pour obtenir des instructions d'installation du fichier de modèle de redirection de contenu URL, reportez-vous à la section « Ajouter le modèle d'administration ADMX de redirection de contenu URL à un GPO », page 61.

Limites de la redirection de contenu URL

La fonctionnalité de redirection de contenu URL peut se comporter de façon inattendue.

- Si l'URL ouvre une page spécifique d'un pays en fonction des paramètres régionaux, la source du lien détermine la page régionale qui est ouverte. Par exemple, si le poste de travail distant (source agent) réside dans un centre de données au Japon et que l'ordinateur de l'utilisateur se trouve aux États-Unis, si l'URL est redirigée depuis l'agent vers la machine cliente, la page qui s'ouvre sur le client aux États-Unis est la page japonaise.
- Si les utilisateurs créent des favoris de pages Web, ils sont créés après la redirection. Par exemple, si un utilisateur clique sur un lien sur la machine cliente, que l'URL est redirigée vers un poste de travail distant (agent) et que l'utilisateur crée un favori pour cette page, le favori est créé sur l'agent. Lorsque l'utilisateur ouvre à nouveau le navigateur sur la machine cliente, il peut s'attendre à trouver le favori sur la machine cliente, mais le favori a été stocké sur le poste de travail distant (source agent).
- Les fichiers que les utilisateurs téléchargent s'affichent sur la machine sur laquelle le navigateur a été utilisé pour ouvrir l'URL, par exemple, lorsqu'un utilisateur clique sur un lien sur la machine cliente et que l'URL est redirigée vers un poste de travail distant. Si le lien a téléchargé un fichier, ou s'il s'agit du lien d'une page Web sur laquelle l'utilisateur télécharge un fichier, le fichier est téléchargé sur le poste de travail distant plutôt que sur la machine cliente.
- Si vous installez Horizon Agent et Horizon Client sur la même machine, vous pouvez activer la redirection de contenu URL dans Horizon Agent ou dans Horizon Client, mais pas dans les deux. Sur cette machine, vous pouvez configurer la redirection client vers agent ou la redirection agent vers client, mais pas les deux.

Fonctionnalités de redirection de contenu URL non prises en charge

La redirection de contenu URL ne fonctionne pas dans certaines circonstances.

URL raccourcies

Les URL raccourcies, telles que `https://goo.gl/abc`, peuvent être redirigées en fonction de règles de filtrage, mais le mécanisme de filtrage n'examine pas l'URL non raccourcie d'origine.

Par exemple, si vous disposez d'une règle qui redirige les URL contenant `acme.com`, une URL d'origine, telle que `http://www.acme.com/some-really-long-path`, et une URL raccourcie de l'URL d'origine, telle que `https://goo.gl/xyz`, l'URL d'origine est redirigée, mais pas l'URL raccourcie.

Vous pouvez contourner cette limite en créant des règles pour bloquer ou rediriger des URL depuis les sites Web les plus souvent utilisés pour raccourcir les URL.

Pages HTML intégrées

Les pages HTML intégrées contournent la redirection URL, par exemple, lorsqu'un utilisateur accède à une URL qui ne correspond pas à une règle de redirection URL. Si une page contient une page HTML intégrée (iFrame ou cadre en ligne) qui contient une URL ne correspondant pas à une règle de redirection, la règle de redirection URL ne fonctionne pas. La règle ne fonctionne que sur l'URL de niveau supérieur.

Plug-ins Internet Explorer désactivés

La redirection de contenu URL ne fonctionne pas si les plug-ins Internet Explorer sont désactivés, par exemple, lorsqu'un utilisateur passe à la navigation InPrivate dans Internet Explorer. On utilise la navigation privée pour que les pages Web et les fichiers téléchargés depuis des pages Web n'apparaissent pas dans l'historique de navigation et de téléchargement de l'ordinateur. Cette limite se produit, car la fonctionnalité de redirection URL requiert l'activation d'un certain plug-in Internet Explorer, et la navigation privée désactive ces plug-ins.

Vous pouvez contourner cette limite en utilisant le paramètre GPO afin d'empêcher les utilisateurs de désactiver les plug-ins. Ces paramètres incluent « Ne pas autoriser les utilisateurs à activer ou désactiver les modules complémentaires » et « Activer automatiquement les modules complémentaires nouvellement installés ». Dans l'Éditeur de gestion de stratégie de groupe, ces paramètres se trouvent sous **Configuration ordinateur > Modèles d'administration > Composants Windows > Internet Explorer**.

Pour contourner cette limite en particulier dans Internet Explorer, utilisez le paramètre GPO pour désactiver le mode InPrivate. Il s'agit du paramètre « Désactiver la navigation InPrivate ». Dans l'Éditeur de gestion de stratégie de groupe, ces paramètres se trouvent sous **Configuration ordinateur > Modèles d'administration > Composants Windows > Internet Explorer > Confidentialité**.

Ces solutions sont des meilleures pratiques et elles peuvent éviter des problèmes avec la redirection que des situations autres que la navigation privée peuvent provoquer.

Une application universelle Windows 10 est le gestionnaire par défaut d'un protocole

La redirection URL ne fonctionne pas si une application universelle Windows 10 est le gestionnaire par défaut d'un protocole spécifié dans un lien. Les applications universelles, basées sur la plate-forme Windows universelle pour pouvoir être téléchargées vers des PC, des tablettes et des téléphones, incluent le navigateur Microsoft Edge, Courrier, Cartes, Photos, Groove Musique, etc.

Si vous cliquez sur un lien pour lequel l'une de ces applications est le gestionnaire par défaut, l'URL n'est pas redirigée. Par exemple, si un utilisateur clique sur un lien d'e-mail dans une application et que l'application de messagerie par défaut est l'application universelle Courrier, l'URL spécifiée dans le lien n'est pas redirigée.

Vous pouvez contourner cette limite en transformant une autre application en gestionnaire par défaut du protocole des URL que vous voulez rediriger. Par exemple, si Edge est le navigateur par défaut, définissez Internet Explorer comme navigateur par défaut.

Machines avec démarrage sécurisé activé

Les machines sur lesquelles le démarrage sécurisé est activé laissent la fonctionnalité de redirection de contenu URL désactivée. Les URL ne peuvent pas être redirigées depuis ces machines. Les URL peuvent être redirigées vers ces machines.

Utilisation de périphériques USB avec des applications et postes de travail distants

4

Les administrateurs peuvent configurer l'utilisation des périphériques USB, tels que des clés USB, des caméras, des périphériques VoIP (voice-over-IP) et des imprimantes, à partir d'un poste de travail distant. Cette fonctionnalité est appelée redirection USB, et elle prend en charge l'utilisation des protocoles d'affichage Blast Extreme, PCoIP et Microsoft RDP. Un poste de travail distant peut recevoir jusqu'à 128 périphériques USB.

Vous pouvez également rediriger des clés et des disques durs USB localement connectés pour une utilisation dans des postes de travail et des applications RDS. D'autres types de périphériques USB, notamment des périphériques de stockage, ne sont pas pris en charge dans des postes de travail et des applications RDS.

Lorsque vous utilisez cette fonctionnalité dans des pools de postes de travail qui sont déployés sur des machines mono-utilisateur, la plupart des périphériques USB raccordés au système client local deviennent disponibles à partir d'un poste de travail distant. Vous pouvez même vous connecter à un iPad et le gérer depuis un poste de travail distant. Par exemple, vous pouvez synchroniser votre iPad avec l'application iTunes installée sur votre poste de travail distant. Sur certains périphériques clients, comme les ordinateurs Windows et Mac, les périphériques USB sont répertoriés dans un menu d'Horizon Client. Vous utilisez le menu pour connecter et déconnecter les périphériques.

Dans la plupart des cas, vous ne pouvez pas utiliser simultanément un périphérique USB sur votre système client et sur votre application ou poste de travail distant. Seuls quelques types de périphériques USB peuvent être partagés entre un poste de travail distant et l'ordinateur local. Ces périphériques sont notamment les lecteurs de carte à puce et les périphériques d'interface utilisateur tels que les claviers et les dispositifs de pointage.

Les administrateurs peuvent spécifier à quels types de périphériques USB les utilisateurs finaux sont autorisés à se connecter. Pour les périphériques composites qui contiennent plusieurs types de périphériques, tels qu'un périphérique d'entrée vidéo et un périphérique de stockage, sur certains systèmes clients, les administrateurs peuvent diviser le périphérique pour qu'un périphérique (par exemple, le périphérique d'entrée vidéo) soit autorisé mais pas l'autre (par exemple, le périphérique de stockage).

La fonction de redirection USB n'est disponible que sur certains types de clients. Pour savoir si cette fonctionnalité est prise en charge sur un type de client particulier, consultez la matrice de prise en charge des fonctionnalités incluse dans le document « Utilisation de VMware Horizon Client » pour le type spécifique de poste de travail ou d'appareil mobile client. Allez sur https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Important Lorsque vous déployez la fonctionnalité de redirection USB, vous pouvez effectuer des opérations pour protéger votre organisation des vulnérabilités de sécurité pouvant affecter les périphériques USB. Reportez-vous à la section « Déploiement de périphériques USB dans un environnement Horizon 7 sécurisé », page 82.

Ce chapitre aborde les rubriques suivantes :

Limitations concernant les types de périphérique USB

Bien qu'Horizon 7 n'empêche pas de manière explicite les périphériques de fonctionner sur un poste de travail distant, des facteurs tels que la latence et la bande passante réseau permettent à certains périphériques de fonctionner mieux que d'autres. Par défaut, l'utilisation de certains périphériques est automatiquement filtrée ou bloquée.

Dans Horizon 6.0.1, avec Horizon Client 3.1 ou version ultérieure, vous pouvez brancher des périphériques USB 3.0 sur les ports USB 3.0 sur la machine cliente, sur des clients Windows, Linux et Mac. Les périphériques USB 3.0 sont uniquement pris en charge avec un flux unique. Dans la mesure où la prise en charge de flux multiples n'est pas mise en œuvre dans cette version, les performances des périphériques USB ne sont pas améliorées. Certains périphériques USB 3.0 qui nécessitent un haut débit constant pour fonctionner correctement risquent de ne pas fonctionner dans une session VDI en raison de la latence réseau.

Dans les versions antérieures de View, bien que les périphériques USB 3.0 super rapides ne soient pas pris en charge, ils fonctionnent lorsqu'ils sont connectés à un port USB 2.0 sur la machine cliente. Cependant, il peut y avoir des exceptions, selon le type de jeu de puces USB sur la carte mère du système client.

Les types de périphériques suivants ne conviennent pas à la redirection USB vers un poste de travail distant qui est déployé sur une machine mono-utilisateur :

- En raison des besoins en bande passante des webcams qui consomment généralement plus 60 Mbits/s de bande passante, les webcams ne sont pas prises en charge via la redirection USB. Pour les webcams, vous pouvez utiliser la fonctionnalité Audio-vidéo en temps réel.
- 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, les périphériques d'entrée et de sortie audio fonctionneront correctement à l'aide de cette fonctionnalité et vous n'avez pas besoin d'utiliser la redirection USB pour ces périphériques.
- La gravure de CD/DVD USB n'est pas prise en charge.
- Les performances de certains périphériques USB varient considérablement, en fonction de la latence et de la fiabilité du réseau, en particulier sur un réseau étendu. Par exemple, une demande de lecture d'un seul périphérique de stockage USB nécessite trois allers-retours entre le client et le poste de travail distant. La lecture d'un fichier complet peut nécessiter plusieurs opérations de lecture USB, et plus la latence est grande, plus l'aller-retour prendra du temps.

Selon le format utilisé, la structure du fichier peut être très volumineuse. Des lecteurs de disques USB de taille importante peuvent nécessiter plusieurs minutes avant d'apparaître sur le poste de travail. Le formatage d'un périphérique USB en NTFS plutôt qu'en FAT permet de diminuer le délai de connexion initial. Un lien réseau non fiable peut entraîner plusieurs tentatives, ce qui diminue davantage les performances.

De la même façon, les lecteurs de CD/DVD USB, ainsi que les scanners et les périphériques tactiles comme les tablettes de signature, ne fonctionnent pas correctement sur un réseau latent tel qu'un réseau étendu.

- La redirection de scanners USB dépend de l'état du réseau, et les numérisations peuvent être anormalement longues.

Vous pouvez rediriger les types de périphériques suivants vers une application ou un poste de travail publié sur un hôte RDS :

- clés USB
- disques durs USB

À partir d'Horizon 7 version 7.0.2, vous pouvez rediriger des tablettes de signature, des pédales de dictée et certaines tablettes Wacom vers une application ou un poste de travail publié. Ces périphériques sont désactivés par défaut dans Horizon 7 version 7.0.2. Pour activer ces périphériques, supprimez les paramètres de clé de Registre Windows `ExcludeAllDevices` et `IncludeFamily` du chemin suivant : `HKLM\Software\Policies\VMware, Inc\VMware VDM\Agent\USB`. Ces périphériques sont activés par défaut dans Horizon 7 version 7.0.3 et versions ultérieures.

Vous ne pouvez pas rediriger d'autres types de périphériques USB (par exemple, d'autres types de périphériques de stockage USB tels que les lecteurs de stockage de sécurité et les CD-ROM USB) vers une application ou un poste de travail publié.

Présentation de la configuration de la redirection USB

Pour configurer votre déploiement afin que les utilisateurs finaux puissent connecter des périphériques amovibles, par exemple des clés USB, des appareils photo et des casques audio, vous devez installer certains composants sur le poste de travail distant ou l'hôte RDS et le périphérique client, et vérifier que le paramètre général des périphériques USB est activé dans View Administrator.

Cette liste de contrôle inclut des tâches obligatoires et facultatives pour la configuration de la redirection USB dans votre entreprise.

La fonctionnalité de redirection USB n'est disponible que sur certains types de clients, par exemple Windows, Mac et des clients Linux fournis par des partenaires. Pour savoir si cette fonctionnalité est prise en charge sur un type de client particulier, reportez-vous à la matrice de prise en charge des fonctionnalités incluse dans le document « Utilisation de VMware Horizon Client » pour le type spécifique de périphérique client. Allez sur https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Important Lorsque vous déployez la fonctionnalité de redirection USB, vous pouvez effectuer des opérations pour protéger votre organisation des vulnérabilités de sécurité pouvant affecter les périphériques USB. Par exemple, vous pouvez utiliser des paramètres de stratégie de groupe pour désactiver Redirection USB pour certains postes de travail distants et utilisateurs, ou pour limiter les types de périphériques USB pouvant être redirigés. Reportez-vous à la section « Déploiement de périphériques USB dans un environnement Horizon 7 sécurisé », page 82.

---

1. Lors de l'exécution de l'assistant d'installation d'Horizon Agent sur la source du poste de travail distant ou l'hôte RDS, veillez à inclure le composant Redirection USB.

   par défaut. Ce composant est désélectionné par défaut. Vous devez sélectionner le composant pour l'installer.

2 Lors de l'exécution de l'assistant d'installation de VMware Horizon Client sur le système client, veillez à inclure le composant Redirection USB.

   Ce composant est inclus par défaut.

3 Vérifiez que l'accès aux périphériques USB à partir d'un poste de travail distant ou une application est activé dans View Administrator.

   Dans View Administrator, accédez à **Règles > Règles générales** et vérifiez que **Accès USB** est défini sur **Autoriser**.

4 (Facultatif) Configurez les stratégies de groupe d'Horizon Agent pour spécifier les types de périphériques qui peuvent être redirigés.

   Reportez-vous à la section « Utilisation de règles pour contrôler la redirection USB », page 85.

5 (Facultatif) Configurez des paramètres similaires sur le périphérique client.

   Vous pouvez également préciser si les périphériques sont automatiquement connectés lorsque Horizon Client se connecte à l'application ou au poste de travail distant, ou lorsque l'utilisateur final branche un périphérique USB. La méthode de configuration des paramètres USB sur le périphérique client dépend du type de périphérique. Par exemple, pour les points de terminaison clients Windows, vous pouvez configurer des stratégies de groupe, tandis que pour les points de terminaison Mac, vous utilisez une commande de ligne de commande. Pour obtenir des instructions, reportez-vous au document « Utilisation de VMware Horizon Client » pour le type de périphérique client spécifique.

6 Demandez aux utilisateurs finaux de se connecter à une application ou un poste de travail distant, et de brancher leur périphérique USB sur leur système client local.

   Si le pilote du périphérique USB n'est pas déjà installé sur le poste de travail distant ou l'hôte RDS, le système d'exploitation invité détecte le périphérique USB et recherche un pilote adéquat, comme il le ferait sur un ordinateur Windows physique.

Trafic réseau et redirection USB

La redirection USB fonctionne indépendamment du protocole d'affichage (RDP ou PCoIP) et le trafic USB utilise habituellement le port TCP 32111.

Le trafic réseau entre un système client et une application ou un poste de travail distant peut prendre différentes routes, selon que le système client se trouve sur le réseau de l'entreprise et en fonction de la façon dont l'administrateur a choisi de configurer la sécurité.

1 Si le système client se trouve sur le réseau de l'entreprise, pour qu'une connexion directe puisse s'établir entre le client et le poste de travail ou l'application, le trafic USB utilise le port TCP 32111.

2 Si le système client se trouve à l'extérieur du réseau de l'entreprise, le client peut se connecter via un serveur de sécurité View.

   Un serveur de sécurité réside dans une zone DMZ et agit comme un hôte proxy pour les connexions dans votre réseau approuvé. Cette conception fournit une couche supplémentaire de sécurité en protégeant l'instance du Serveur de connexion View contre l'Internet public et en forçant toutes les demandes de session non protégées via le serveur de sécurité.

   Un déploiement de serveur de sécurité basé sur une zone DMZ requiert l'ouverture de quelques ports sur le pare-feu afin d'autoriser des clients à se connecter à des serveurs de sécurité dans la zone DMZ. Vous devez également configurer des ports pour la communication entre des serveurs de sécurité et les instances du Serveur de connexion View sur le réseau interne.

   Pour plus d'informations sur les ports spécifiques, reportez-vous à « Règles de pare-feu pour les serveurs de sécurité basés sur une zone DMZ » dans le document *Guide de planification de l'architecture de View*.

3 Si le système client se trouve à l'extérieur du réseau de l'entreprise, vous pouvez utiliser View Administrator pour activer le tunnel sécurisé HTTPS. Le client établit ensuite une autre connexion HTTPS avec l'hôte du Serveur de connexion View ou du serveur de sécurité lorsque des utilisateurs se connectent à une application ou un poste de travail distant. La connexion est établie par tunnel à l'aide du port HTTPS 443 vers le serveur de sécurité, puis les connexions ultérieures pour le trafic USB entre le serveur et l'application ou le poste de travail distant utilisent le port TCP 32111. Les performances du périphérique USB sont légèrement dégradées lors de l'utilisation de ce tunnel.

Remarque Si vous utilisez un client ultra léger, le trafic USB est redirigé à l'aide d'un canal virtuel PCoIP et ne passe pas par le port TCP 32111. Les données sont encapsulées et chiffrées par PCoIP Secure Gateway à l'aide du port TCP/UDP 4172. Si vous utilisez uniquement des clients ultra légers, il n'est pas nécessaire d'ouvrir le port TCP 32111.

Connexions automatiques aux périphériques USB

Sur certains systèmes clients, les administrateurs, les utilisateurs finaux ou les deux peuvent configurer des connexions automatiques de périphériques USB à un poste de travail distant. Il est possible d'établir une connexion automatique lorsque l'utilisateur branche un périphérique USB sur le système client ou lorsque le client se connecte au poste de travail distant.

Certains périphériques comme les smartphones et les tablettes ont besoin de connexions automatiques, car ils sont redémarrés, et donc déconnectés, pendant une mise à niveau. Si ces périphériques ne sont pas configurés pour se reconnecter automatiquement au poste de travail distant, après avoir redémarré suite à la mise à niveau ils se connecteront plutôt au système client local.

Les propriétés de configuration des connexions USB automatiques que les administrateurs définissent sur le client ou que les utilisateurs finaux définissent à l'aide d'un élément de menu d'Horizon Client s'appliquent à tous les périphériques USB, sauf si ceux-ci sont configurés pour être exclus de la redirection USB. Par exemple, dans certaines versions de clients, les webcams et les microphones sont exclus de la redirection USB par défaut, car ces périphériques fonctionnent mieux avec la fonctionnalité Audio-vidéo en temps réel. Dans certains cas, un périphérique USB peut ne pas être exclu de la redirection par défaut, mais nécessiter que les administrateurs l'excluent de façon explicite de la redirection. Par exemple, les types de périphériques USB suivants ne sont pas recommandés pour la redirection USB et ne doivent pas être connectés automatiquement à un poste de travail distant :

- Périphériques Ethernet USB. Si vous redirigez un périphérique Ethernet USB, votre système client peut perdre la connectivité réseau si ce périphérique est le seul périphérique Ethernet.
- Périphériques à écran tactile. Si vous redirigez un périphérique à écran tactile, le poste de travail distant recevra une entrée tactile mais pas une entrée de clavier.

Si vous avez défini le poste de travail distant pour qu'il se connecte automatiquement aux périphériques USB, vous pouvez configurer une stratégie visant à exclure des périphériques spécifiques, comme les écrans tactiles et les périphériques réseau. Pour plus d'informations, reportez-vous à la section « Configuration de paramètres de règle de filtre pour des périphériques USB », page 89.

Sur les clients Windows, plutôt que de définir des paramètres qui connectent automatiquement tous les périphériques à l'exception de ceux qui sont exclus, vous pouvez modifier un fichier de configuration sur le client qui définit Horizon Client de sorte qu'il reconnecte uniquement un ou plusieurs périphériques spécifiques, comme les smartphones et les tablettes, au poste de travail distant. Pour plus d'information, reportez-vous à *Utilisation de VMware Horizon Client pour Windows*.

Déploiement de périphériques USB dans un environnement Horizon 7 sécurisé

Les périphériques USB peuvent être vulnérables à une menace de sécurité nommée BadUSB, dans laquelle le microprogramme de certains périphériques USB peut être piraté et remplacé par un logiciel malveillant. Par exemple, un périphérique peut ainsi être amené à rediriger le trafic réseau, ou à émuler un clavier et capturer la frappe effectuée. Vous pouvez configurer la fonctionnalité de redirection USB de manière à protéger votre déploiement Horizon 7 contre cette vulnérabilité de sécurité.

En désactivant la redirection USB, vous pouvez empêcher toute redirection de périphérique USB vers les postes de travail et les applications Horizon 7 de vos utilisateurs. Vous pouvez également désactiver la redirection de périphériques USB spécifiques, pour permettre aux utilisateurs d'avoir uniquement accès à des périphériques spécifiques sur leurs postes de travail et leurs applications.

Le choix de prendre ou non ces mesures dépend des exigences de sécurité de votre organisation. Ces étapes ne sont pas obligatoires. Vous pouvez installer la redirection USB et laisser la fonctionnalité activée pour tous les périphériques USB de votre déploiement Horizon 7. Au minimum, analysez sérieusement à quel degré votre organisation doit tenter de limiter son exposition à cette vulnérabilité de sécurité.

Désactivation de la redirection USB pour tous les types de périphériques

Certains environnements hautement sécurisés nécessitent que vous empêchiez tous les périphériques USB que les utilisateurs peuvent avoir connectés à leurs périphériques clients d'être redirigés vers leurs applications et postes de travail distants. Vous pouvez désactiver la redirection USB pour tous les pools de postes de travail, des pools de postes de travail spécifiques ou des utilisateurs spécifiques dans un pool de postes de travail.

Utilisez l'une des stratégies suivantes, selon votre situation :

- Lorsque vous installez Horizon Agent sur une image de poste de travail ou un hôte RDS, désactivez l'option de configuration **Redirection USB**. (L'option est décochée par défaut.) Cette approche empêche d'accéder à des périphériques USB sur l'ensemble des applications et des postes de travail distants qui sont déployés à partir de l'image du poste de travail ou de l'hôte RDS.
- Dans Horizon Administrator, modifiez la stratégie **Accès USB** pour autoriser ou refuser l'accès sur un pool spécifique. Avec cette approche, vous n'avez pas besoin de modifier l'image du poste de travail et pouvez accéder aux périphériques USB de pools d'applications et de postes de travail spécifiques.

  Seule la stratégie globale **Accès USB** est disponible pour les pools d'applications et de postes de travail RDS. Vous ne pouvez pas définir cette stratégie pour des pools d'applications ou de postes de travail RDS individuels.
- Dans View Administrator, dès que vous avez défini la stratégie au niveau du pool de postes de travail ou d'applications, vous pouvez remplacer la stratégie d'un utilisateur spécifique du pool en sélectionnant le paramètre **Remplacements d'utilisateur** et en sélectionnant un utilisateur.
- Définissez la stratégie `Exclude All Devices` sur **`true`**, du côté Horizon Agent ou du côté client, selon le cas.
- Utilisez Stratégies de carte à puce pour créer une stratégie qui désactive le paramètre de stratégie Horizon **Redirection USB**. Avec cette approche, vous pouvez désactiver la redirection USB sur un poste de travail distant spécifique si certaines conditions sont respectées. Par exemple, vous pouvez configurer une stratégie qui désactive la redirection USB lorsque des utilisateurs se connectent à un poste de travail distant depuis l'extérieur du réseau d'entreprise.

Si vous définissez la stratégie `Exclude All Devices` sur **`true`**, Horizon Client empêche la redirection de tous les périphériques USB. Vous pouvez utiliser d'autres paramètres de règle pour autoriser la redirection de périphériques spécifiques ou de familles de périphériques. Si vous définissez la stratégie sur **`false`**, Horizon Client autorise la redirection de tous les périphériques USB sauf ceux qui sont bloqués par d'autres

paramètres de stratégie. Vous pouvez définir la stratégie dans Horizon Agent et Horizon Client. Le tableau suivant décrit comment la stratégie `Exclude All Devices` que vous pouvez définir pour Horizon Agent et Horizon Client se combinent pour produire une stratégie efficace pour l'ordinateur client. Par défaut, tous les périphériques USB sont autorisés à être redirigés, sauf blocage contraire.

Tableau 4-1. Effet de la combinaison de règles Exclure tous les périphériques

Stratégie Exclure tous les périphériques sur Horizon Agent	Stratégie Exclure tous les périphériques dans Horizon Client	Règle Exclure tous les périphériques effective combinée
`false` ou non défini (inclure tous les périphériques USB)	**`false`** ou non défini (inclure tous les périphériques USB)	Inclure tous les périphériques USB
`false` (inclure tous les périphériques USB)	**`true`** (exclure tous les périphériques USB)	Exclure tous les périphériques USB
`true` (exclure tous les périphériques USB)	Aucun ou non défini	Exclure tous les périphériques USB

Si vous avez défini la stratégie `Disable Remote Configuration Download` sur **`true`**, la valeur d'`Exclude All Devices` dans Horizon Agent n'est pas transmise à Horizon Client, mais Horizon Agent et Horizon Client appliquent la valeur locale d'`Exclude All Devices`.

Ces stratégies sont incluses dans le fichier de modèle d'administration ADMX pour la configuration d'Horizon Agent (`vdm_agent.admx`).

Désactivation de la redirection USB pour des périphériques spécifiques

Certains utilisateurs peuvent devoir rediriger des périphériques USB localement connectés afin de pouvoir effectuer des tâches sur leurs applications ou postes de travail distants. Par exemple, un médecin peut devoir utiliser un périphérique dictaphone USB pour enregistrer des informations médicales dans le dossier d'un patient. Dans ce cas, vous ne pouvez pas désactiver l'accès à tous les périphériques USB. Vous pouvez utiliser les paramètres de stratégie de groupe pour activer ou désactiver une redirection USB pour des périphériques spécifiques.

Avant d'activer la redirection USB pour des périphériques spécifiques, assurez-vous que vous approuvez les périphériques physiques connectés à des machines clientes dans votre entreprise. Assurez-vous de pouvoir approuver votre chaîne d'approvisionnement. Si possible, assurez le suivi d'une chaîne de sécurité pour les périphériques USB.

En outre, formez vos employés pour vous assurer qu'ils ne connectent pas des périphériques provenant de sources inconnues. Si possible, restreignez les périphériques de votre environnement à ceux qui acceptent uniquement des mises à jour de microprogramme signées, bénéficient d'une certification FIPS 140-2 Niveau 3 et ne prennent pas en charge tout type de microprogramme autorisant la mise à jour sur site. Ces types de périphériques USB peuvent poser des problèmes d'approvisionnement et, selon la configuration requise de vos périphériques, peuvent s'avérer impossibles à trouver. Ces choix peuvent être difficiles à mettre en œuvre dans la pratique, mais ils méritent d'être envisagés.

Chaque périphérique USB a son propre fournisseur et ID de produit qui l'identifie sur l'ordinateur. En configurant les paramètres de la stratégie de groupe Configuration d'Horizon Agent, vous pouvez définir une stratégie d'inclusion de ces types de périphériques connus. Avec cette approche, vous éliminez le risque d'autoriser l'insertion de périphériques inconnus dans votre environnement.

Par exemple, vous pouvez empêcher tous les périphériques, à l'exception de ceux associés à un fournisseur de périphériques et à un ID de produit connus, `vid/pid=0123/abcd`, d'être redirigés vers l'application ou le poste de travail distant :

```
ExcludeAllDevices   Enabled

IncludeVidPid       o:vid-0123_pid-abcd
```

Remarque Cet exemple de configuration fournit une protection, mais comme un périphérique compromis peut communiquer n'importe quel vid/pid, une attaque peut toujours éventuellement se produire.

Par défaut, Horizon 7 interdit la redirection de certaines familles de périphériques vers l'application ou le poste de travail distant. Par exemple, les périphériques d'interface utilisateur et les claviers sont interdits d'affichage dans l'invité. Certains codes BadUSB récemment publiés ciblent les claviers USB.

Vous pouvez interdire la redirection de familles spécifiques de périphériques vers l'application ou le poste de travail distant. Par exemple, vous pouvez bloquer tous les périphériques vidéo, audio et de stockage de masse :

```
ExcludeDeviceFamily   o:video;audio;storage
```

À l'inverse, vous pouvez créer une liste blanche interdisant la redirection de tous les périphériques mais autorisant l'utilisation d'une famille spécifique de périphériques. Par exemple, vous pouvez bloquer tous les périphériques à l'exception des périphériques de stockage :

```
ExcludeAllDevices     Enabled

IncludeDeviceFamily   o:storage
```

Un autre risque peut survenir lorsqu'un utilisateur distant se connecte à un poste de travail ou à une application et l'infecte. Vous pouvez empêcher l'accès USB à toute connexion Horizon 7 provenant de l'extérieur du pare-feu de l'entreprise. Le périphérique USB peut être utilisé en interne, mais pas en externe.

Sachez que si vous bloquez le port TCP 32111 pour désactiver l'accès externe aux périphériques USB, la synchronisation de fuseau horaire ne fonctionnera pas, car le port 32111 est également utilisé pour la synchronisation de fuseau horaire. Pour les clients zéro, le trafic USB est intégré dans un canal virtuel sur le port UDP 4172. Comme le port 4172 est utilisé pour le protocole d'affichage ainsi que pour la redirection USB, vous ne pouvez pas bloquer le port 4172. Si nécessaire, vous pouvez désactiver la redirection USB sur les clients zéro. Pour plus d'informations, reportez-vous à la documentation du produit client zéro et contactez son fournisseur.

La définition de stratégies pour bloquer certaines familles de périphériques ou des périphériques spécifiques peut contribuer à réduire les risques d'infection avec le logiciel malveillant BadUSB. Ces stratégies ne réduisent pas tous les risques, mais peuvent s'inscrire dans une stratégie de sécurité globale.

Utilisation de fichiers journaux pour le dépannage et pour déterminer les ID de périphérique USB

Des fichiers journaux pour USB très utiles se trouvent sur le système client et sur le système d'exploitation du poste de travail distant ou l'hôte RDS. Utilisez les fichiers journaux de ces deux emplacements à des fins de dépannage. Pour trouver les ID de produits de périphériques spécifiques, utilisez les journaux côté client.

Si vous tentez de configurer les fonctionnalités de partitionnement et de filtre de périphériques USB, ou si vous tentez de déterminer pourquoi un périphérique particulier ne s'affiche pas dans un menu Horizon Client, effectuez une recherche dans les journaux côté client. Des journaux clients sont produits pour l'arbitrage USB et le service USB d'Horizon View. La journalisation sur les clients Windows et Linux est activée par défaut. Sur les clients Mac, la journalisation est désactivée par défaut. Pour activer la journalisation sur les clients Mac, consultez le document *Utilisation de VMware Horizon Client pour Mac*.

Lorsque vous configurez des stratégies pour le fractionnement et le filtrage de périphériques USB, certaines valeurs que vous définissez nécessitent le VID (ID de fournisseur) et le PID (ID de produit) du périphérique USB. Pour connaître le VID et le PID, vous pouvez rechercher le nom du produit sur Internet, associé à `vid` et `pid`. Vous pouvez également consulter le fichier journal côté client après la connexion du périphérique USB au système local lorsqu'Horizon Client est en cours d'exécution. Le tableau suivant montre l'emplacement par défaut des fichiers journaux.

Tableau 4-2. Emplacements des fichiers journaux

Client ou Agent	Chemin d'accès aux fichiers journaux
Client Windows	`%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt` `C:\Windows\Temp\vmware-SYSTEM\vmware-usbarb-*.log`
Horizon Agent	`%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt`
Client Mac	`/var/root/Library/Logs/VMware/vmware-view-usbd-xxxx.log` `/Library/Logs/VMware/vmware-usbarbitrator-xxxx.log`
Client Linux	(Emplacement par défaut) `/tmp/vmware-root/vmware-view-usbd-*.log`

Si un problème sur le périphérique se produit après la redirection de ce dernier vers l'application ou le poste de travail distant, consultez les journaux côté client et côté agent.

Utilisation de règles pour contrôler la redirection USB

Vous pouvez configurer des stratégies USB pour l'application ou le poste de travail distant (Horizon Agent) et Horizon Client. Ces stratégies spécifient si le périphérique client doit fractionner des périphériques USB composites en composants distincts pour la redirection. Vous pouvez fractionner les périphériques pour limiter les types de périphériques USB que le client met à disposition pour la redirection et pour qu'Horizon Agent empêche le transfert de certains périphériques USB à partir d'un ordinateur client.

Si d'anciennes versions d'Horizon Agent ou d'Horizon Client sont installées, certaines fonctionnalités des stratégies de redirection USB ne sont pas disponibles. Tableau 4-3 indique comment Horizon 7 applique les stratégies pour différentes combinaisons d'Horizon Agent et d'Horizon Client.

Tableau 4-3. Compatibilité des paramètres de stratégie USB

Version d'Horizon Agent	Version d'Horizon Client	Effet des paramètres de stratégie USB sur la redirection USB
5.1 ou version ultérieure	5.1 ou version ultérieure	Les paramètres de stratégie USB s'appliquent à Horizon Agent et à Horizon Client. Vous pouvez utiliser les paramètres de stratégie USB d'Horizon Agent pour empêcher le transfert de périphériques USB vers un poste de travail. Horizon Agent peut envoyer des paramètres de stratégie de fractionnement et de filtrage de périphériques à Horizon Client. Vous pouvez utiliser les paramètres de stratégie USB d'Horizon Client pour empêcher la redirection de périphériques USB d'un ordinateur client vers un poste de travail. **Remarque** Dans View Agent 6.1 ou version ultérieure et Horizon Client 3.3 ou version ultérieure, ces paramètres de stratégie de redirection USB s'appliquent aux postes de travail et applications RDS ainsi qu'aux postes de travail distants qui s'exécutent sur des machines mono-utilisateur.
5.1 ou version ultérieure	5.0.x ou version antérieure	Les paramètres de stratégie USB s'appliquent uniquement à Horizon Agent. Vous pouvez utiliser les paramètres de stratégie USB d'Horizon Agent pour empêcher le transfert de périphériques USB vers un poste de travail. Vous ne pouvez pas utiliser les paramètres de stratégie USB d'Horizon Client pour contrôler les périphériques pouvant être redirigés d'un ordinateur client vers un poste de travail. Horizon Client ne peut pas recevoir de paramètres de stratégie de fractionnement et de filtrage de périphériques provenant d'Horizon Agent. Les paramètres de Registre existants pour la redirection USB par Horizon Client demeurent valides.

Tableau 4-3. Compatibilité des paramètres de stratégie USB (suite)

Version d'Horizon Agent	Version d'Horizon Client	Effet des paramètres de stratégie USB sur la redirection USB
5.0.x ou version antérieure	5.1 ou version ultérieure	Les paramètres de stratégie USB s'appliquent uniquement à Horizon Client. Vous pouvez utiliser les paramètres de stratégie USB d'Horizon Client pour empêcher la redirection de périphériques USB d'un ordinateur client vers un poste de travail. Vous ne pouvez pas utiliser les paramètres de stratégie USB d'Horizon Agent pour empêcher le transfert de périphériques USB vers un poste de travail. Horizon Agent ne peut pas envoyer des paramètres de stratégie de fractionnement et de filtrage de périphériques à Horizon Client.
5.0.x ou version antérieure	5.0.x ou version antérieure	Les paramètres de stratégie USB ne s'appliquent pas. Les paramètres de Registre existants pour la redirection USB par Horizon Client demeurent valides.

Si vous mettez à niveau Horizon Client, tous les paramètres de Registre existants pour la redirection USB, par exemple `HardwareIdFilters`, restent valides jusqu'à ce que vous définissiez des stratégies USB pour Horizon Client.

Sur les périphériques clients qui ne prennent pas en charge les stratégies USB côté client, vous pouvez utiliser les stratégies USB pour Horizon Agent afin de contrôler les périphériques USB autorisés à être transférés du client vers un poste de travail.

Configuration de paramètres de règle de fractionnement de périphérique pour des périphériques USB composites

Les périphériques USB composites sont composés d'au moins deux périphériques distincts, tels qu'un périphérique d'entrée vidéo et un périphérique de stockage, ou un microphone et une souris. Si vous souhaitez rendre un ou plusieurs des composants disponibles pour la redirection, vous pouvez fractionner le périphérique composite en interfaces de son composant, exclure certaines interfaces de la redirection et en inclure d'autres.

Vous pouvez définir une stratégie qui fractionne automatiquement les périphériques composites. Si le fractionnement automatique de périphériques ne fonctionne pas pour un périphérique spécifique ou s'il ne produit pas les résultats requis par votre application, vous pouvez fractionner manuellement les périphériques composites.

Fractionnement automatique de périphérique

Si vous activez le fractionnement automatique de périphérique, Horizon 7 tente de fractionner les fonctions ou les périphériques en un périphérique composite selon les règles de filtre en vigueur. Par exemple, un dictaphone peut être fractionné automatiquement de sorte que la souris demeure locale pour le client, mais que le reste des périphériques soit transmis au poste de travail distant.

Le tableau suivant indique comment la valeur du paramètre `Allow Auto Device Splitting` détermine si Horizon Client tente de fractionner automatiquement des périphériques USB composites. Par défaut, le fractionnement automatique est désactivé.

Tableau 4-4. Effet de la combinaison de règles de désactivation du fractionnement automatique

Stratégie Autoriser le fractionnement automatique de périphérique sur Horizon Agent	Stratégie Autoriser le fractionnement automatique de périphérique sur Horizon Client	Règle Autoriser le fractionnement automatique de périphérique effective combinée
`Allow – Default Client Setting`	**`false`** (fractionnement automatique désactivé)	Fractionnement automatique désactivé
`Allow – Default Client Setting`	**`true`** (fractionnement automatique activé)	Fractionnement automatique activé
`Allow – Default Client Setting`	Non défini	Fractionnement automatique activé

Tableau 4-4. Effet de la combinaison de règles de désactivation du fractionnement automatique (suite)

Stratégie Autoriser le fractionnement automatique de périphérique sur Horizon Agent	Stratégie Autoriser le fractionnement automatique de périphérique sur Horizon Client	Règle Autoriser le fractionnement automatique de périphérique effective combinée
`Allow – Override Client Setting`	Aucun ou non défini	Fractionnement automatique activé
Non défini	Non défini	Fractionnement automatique désactivé

Remarque Ces stratégies sont incluses dans le fichier de modèle d'administration ADMX pour la configuration d'Horizon Agent. Le fichier de modèle d'administration ADMX se nomme (`vdm_agent.admx`).

Par défaut, Horizon 7 désactive le fractionnement automatique et exclut de la redirection tous les composants de sortie audio, de carte à puce, de clavier ou de souris d'un périphérique USB composite.

Horizon 7 applique les paramètres de stratégie de fractionnement de périphériques avant d'appliquer des paramètres de stratégie de filtre. Si vous avez activé le fractionnement automatique et que vous n'excluez pas explicitement un périphérique USB composite du fractionnement en spécifiant ses ID de fournisseur et de produit, Horizon 7 examine chaque interface du périphérique USB composite afin de décider des interfaces à exclure ou à inclure selon les paramètres de stratégie de filtre. Si vous avez désactivé le fractionnement automatique de périphérique et que vous ne spécifiez pas explicitement les ID de fournisseur et de produit d'un périphérique USB composite que vous souhaitez fractionner, Horizon 7 applique les paramètres de stratégie de filtre à l'ensemble du périphérique.

Si vous activez le fractionnement automatique, vous pouvez utiliser la règle `Exclude Vid/Pid Device From Split` pour spécifier les périphériques USB composites que vous voulez exclure du fractionnement.

Fractionnement manuel de périphérique

Vous pouvez utiliser la règle `Split Vid/Pid Device` pour spécifier les ID de fournisseur et de produit d'un périphérique USB composite que vous voulez fractionner. Vous pouvez également spécifier les interfaces des composants d'un périphérique USB composite que vous voulez exclure de la redirection. Horizon 7 n'applique aucun paramètre de stratégie de filtre aux composants que vous excluez de cette façon.

Important Si vous utilisez la stratégie `Split Vid/Pid Device`, Horizon 7 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.

Tableau 4-5 indique les modificateurs définissant la façon dont Horizon Client gère un paramètre de stratégie de fractionnement de périphérique Horizon Agent si un paramètre de stratégie de fractionnement de périphérique équivalent pour Horizon Client est présent. Ces modificateurs s'appliquent à tous les paramètres de règles de fractionnement de périphérique.

Tableau 4-5. Modificateurs de fractionnement pour des paramètres de règle de fractionnement de périphérique sur Horizon Agent

Modificateur	Description
`m` (fusionner)	Horizon Client applique le paramètre de stratégie de fractionnement de périphérique Horizon Agent en plus du paramètre de stratégie de fractionnement de périphérique Horizon Client.
`o` (remplacer)	Horizon Client utilise le paramètre de stratégie de fractionnement de périphérique Horizon Agent à la place du paramètre de stratégie de fractionnement de périphérique Horizon Client.

Tableau 4-6 montre des exemples de la façon dont Horizon Client traite les paramètres de stratégie `Exclude Device From Split by Vendor/Product ID` lorsque vous spécifiez différents modificateurs de fractionnement.

Tableau 4-6. Exemples d'application de modificateurs de fractionnement sur des paramètres de règle de fractionnement de périphérique

Exclure le périphérique du fractionnement par ID de fournisseur/de produit sur Horizon Agent	Exclure le périphérique du fractionnement par ID de fournisseur/de produit sur Horizon Client	Paramètre effectif de la stratégie Exclure le périphérique du fractionnement par ID de fournisseur/de produit utilisé par Horizon Client
`m:vid-XXXX_pid-XXXX`	`vid-YYYY_pid-YYYY`	`vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY`
`o:vid-XXXX_pid-XXXX`	`vid-YYYY_pid-YYYY`	`vid-XXXX_pid-XXXX`
`m:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY`	`vid-YYYY_pid-YYYY`	`vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY`
`o:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY`	`vid-YYYY_pid-YYYY`	`vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY`

Horizon Agent n'applique pas les paramètres de stratégie de fractionnement de périphérique de son côté de la connexion.

Horizon Client évalue les paramètres de stratégie de fractionnement de périphérique dans l'ordre de priorité suivant.

- `Exclude Vid/Pid Device From Split`
- `Split Vid/Pid Device`

Un paramètre de règle de fractionnement de périphérique qui exclut un périphérique du fractionnement est prioritaire sur tout autre paramètre de règle pour fractionner le périphérique. Si vous définissez des interfaces ou des périphériques à exclure du fractionnement, Horizon Client exclut de la redirection les périphériques de composant correspondants.

Exemples de définition de règles pour fractionner des périphériques USB composites

Définissez des stratégies de fractionnement pour des postes de travail afin d'exclure de la redirection les périphériques avec des ID de fournisseur et de produit spécifiques après le fractionnement automatique, et transmettez ces stratégies aux ordinateurs clients :

- Pour Horizon Agent, définissez la stratégie `Allow Auto Device Splitting` sur `Allow – Override Client Setting`.
- Pour Horizon Agent, définissez la stratégie `Exclude VidPid From Split` sur **`o:vid-`*`xxx`*`_pid-`*`yyyy`***, où *xxx* et *yyyy* sont les ID appropriés.

Autorisez le fractionnement automatique de périphérique pour des postes de travail et spécifiez des stratégies de fractionnement pour des périphériques spécifiques sur des ordinateurs clients :

- Pour Horizon Agent, définissez la stratégie `Allow Auto Device Splitting` sur `Allow – Override Client Setting`.
- Pour le périphérique client, définissez la stratégie de filtre `Include Vid/Pid Device` de façon qu'elle inclue le périphérique spécifique à fractionner, par exemple, **`vid-0781_pid-554c`**.
- Pour le périphérique client, définissez la stratégie `Split Vid/Pid Device` sur **`vid-0781_pid-554c(exintf:00;exintf:01)`**, par exemple, pour fractionner un périphérique USB composite spécifié afin d'exclure de la rediction l'interface 00 et l'interface 01.

Configuration de paramètres de règle de filtre pour des périphériques USB

Les paramètres de stratégie de filtre que vous configurez pour Horizon Agent et Horizon Client déterminent les périphériques USB pouvant être redirigés d'un ordinateur client vers une application ou un poste de travail distant. Le filtrage des périphériques USB est généralement utilisé par les entreprises pour empêcher le recours à des périphériques de stockage de masse sur les postes de travail distants ou pour bloquer le transfert d'un type de périphérique spécifique, comme l'adaptateur USB vers Ethernet qui connecte le périphérique client au poste de travail distant.

Lorsque vous vous connectez à un poste de travail ou une application, Horizon Client télécharge les paramètres de stratégie USB d'Horizon Agent et les utilise avec les paramètres de stratégie USB d'Horizon Client afin de décider quels périphériques USB il vous autorisera à rediriger à partir de l'ordinateur client.

Horizon 7 applique tous les paramètres de stratégie de fractionnement de périphérique avant d'appliquer les paramètres de stratégie de filtre. Si vous avez fractionné un périphérique USB composite, Horizon 7 examine les interfaces de chacun des périphériques pour décider laquelle exclure ou inclure, conformément aux paramètres de stratégie de filtre. Dans le cas contraire, Horizon 7 applique les paramètres de stratégie de filtre à l'ensemble du périphérique.

Les stratégies de fractionnement de périphérique sont incluses dans le fichier de modèle d'administration ADMX pour la configuration d'Horizon Agent (`vdm_agent.adm`).

Interaction des paramètres USB appliqués par l'agent

Le tableau suivant présente les modificateurs qui spécifient de quelle manière Horizon Client gère un paramètre de stratégie de filtre d'Horizon Agent pour un paramètre applicable par l'agent, s'il existe un paramètre de stratégie de filtre équivalent pour Horizon Client.

Tableau 4-7. Modificateurs de filtre pour des paramètres exécutables par un agent

Modificateur	Description
`m` (fusionner)	Horizon Client applique le paramètre de stratégie de filtre d'Horizon Agent en plus du paramètre de stratégie de filtre d'Horizon Client. En cas de paramètres booléens ou vrai/faux, si la stratégie du client n'est pas définie, les paramètres de l'agent sont utilisés. Si la stratégie du client est définie, les paramètres de l'agent sont ignorés, à l'exception du paramètre `Exclude All Devices`. Si la stratégie `Exclude All Devices` est définie du côté de l'agent, elle remplace le paramètre du client.
`o` (remplacer)	Horizon Client utilise le paramètre de stratégie de filtre d'Horizon Agent à la place de celui d'Horizon Client.

Par exemple, la stratégie suivante du côté de l'agent remplace toutes les règles d'inclusion du côté du client, et une règle d'inclusion sera appliquée uniquement au périphérique VID-0911_PID-149a :

```
IncludeVidPid: o:VID-0911_PID-149a
```

Vous pouvez également utiliser des astérisques comme caractères génériques ; par exemple :
`o:vid-0911_pid-****`

Important Si vous configurez le côté agent sans le modificateur **`o`** ou **`m`**, la règle de configuration est considérée comme non valide et sera ignorée.

Interaction des paramètres USB interprétés par le client

Le tableau suivant présente les modificateurs qui spécifient de quelle manière Horizon Client gère un paramètre de stratégie de filtre d'Horizon Agent pour un paramètre interprété par le client.

Tableau 4-8. Modificateurs de filtre pour des paramètres interprétés par un client

Modificateur	Description
`Default` (**`d`** dans le paramètre de registre)	En l'absence de paramètre de stratégie de filtre d'Horizon Client, Horizon Client utilise le paramètre de stratégie de filtre d'Horizon Agent. S'il existe un paramètre de stratégie de filtre d'Horizon Client, Horizon Client applique celui-ci et ignore celui d'Horizon Agent.
`Override` (**`o`** dans le paramètre de registre)	Horizon Client utilise le paramètre de stratégie de filtre d'Horizon Agent à la place d'un paramètre de stratégie de filtre équivalent d'Horizon Client.

Horizon Agent n'applique pas les paramètres de stratégie de filtre pour des paramètres interprétés par un client de son côté de la connexion.

Le tableau suivant montre les différentes manières dont Horizon Client traite les valeurs de l'option `Allow Smart Cards` lorsque vous spécifiez différents modificateurs de filtre.

Tableau 4-9. Exemples d'application de modificateurs de filtre sur des paramètres interprétés par un client

Paramètre Autoriser les cartes à puce dans Horizon Agent	Paramètre Autoriser les cartes à puce dans Horizon Client	Paramètre de stratégie Autoriser les cartes à puce effectif utilisé par Horizon Client
`Disable – Default Client Setting` (**`d:false`** dans le paramètre de registre)	**`true`** (autoriser)	**`true`** (autoriser)
`Disable – Override Client Setting` (**`o:false`** dans le paramètre de registre)	**`true`** (autoriser)	**`false`** (désactiver)

Si vous définissez la stratégie `Disable Remote Configuration Download` sur la valeur **`true`**, Horizon Client ignore les paramètres de stratégie de filtre qu'il reçoit d'Horizon Agent.

Horizon Agent applique toujours les paramètres de stratégie de filtre aux paramètres applicables par l'agent de son côté de la connexion, même si vous configurez Horizon Client afin qu'il utilise un paramètre de stratégie de filtre différent ou qu'il désactive le téléchargement de paramètres de stratégie de filtre par Horizon Client auprès d'Horizon Agent. Horizon Client ne signale pas qu'Horizon Agent empêche le transfert d'un périphérique.

Priorité des paramètres

Horizon Client évalue les paramètres de stratégie de filtre selon un ordre de priorité. Un paramètre de règle de filtre qui exclut la redirection d'un périphérique correspondant est prioritaire sur le paramètre de règle de filtre équivalent qui inclut le périphérique. Si Horizon Client ne rencontre pas de paramètre de stratégie de filtre visant à exclure un périphérique, Horizon Client permet au périphérique d'être redirigé, sauf si vous avez défini la stratégie `Exclude All Devices` sur **`true`**. Toutefois, si vous avez configuré un paramètre de stratégie de filtre sur Horizon Agent afin d'exclure le périphérique, l'application ou le poste de travail bloque toute tentative de redirection du périphérique vers lui.

Horizon Client évalue les paramètres de stratégie de filtre par ordre de priorité, en tenant compte des paramètres d'Horizon Client et de ceux d'Horizon Agent, ainsi que des valeurs de modificateur que vous appliquez aux paramètres d'Horizon Agent. La liste suivante répertorie l'ordre de priorité, l'élément 1 ayant la priorité la plus élevée.

1. `Exclude Path`
2. `Include Path`
3. `Exclude Vid/Pid Device`
4. `Include Vid/Pid Device`
5. `Exclude Device Family`

6 `Include Device Family`

7 `Allow Audio Input Devices`, `Allow Audio Output Devices`, `Allow HIDBootable`, `Allow HID (Non Bootable and Not Mouse Keyboard)`, `Allow Keyboard and Mouse Devices`, `Allow Smart Cards` et `Allow Video Devices`

8 Règle `Exclude All Devices` effective combinée évaluée pour exclure ou inclure tous les périphériques USB

Vous pouvez définir les paramètres de stratégie de filtre `Exclude Path` et `Include Path` uniquement pour Horizon Client. Les paramètres de règle de filtre `Allow` qui font référence à des familles de périphériques séparés ont la même priorité.

Si vous configurez un paramètre de stratégie afin d'exclure les périphériques en fonction des valeurs d'ID de fournisseur et de produit, Horizon Client exclut un périphérique dont les valeurs d'ID de fournisseur et de produit correspondent à cette stratégie, même si vous auriez pu configurer une stratégie `Allow` pour la famille à laquelle appartient le périphérique.

L'ordre de priorité des paramètres de règle résout des conflits entre les paramètres de règle. Si vous configurez `Allow Smart Cards` pour autoriser la redirection de cartes à puce, tout paramètre de règle d'exclusion avec une priorité supérieure remplace ce paramètre. Par exemple, vous pouvez avoir configuré un paramètre de règle `Exclude Vid/Pid Device` pour exclure les périphériques à carte à puce avec un chemin ou des valeurs d'ID de fournisseur et de produit correspondants, ou vous pouvez avoir configuré un paramètre de règle `Exclude Device Family` qui exclut également la famille de périphériques `smart-card` entièrement.

Si vous avez configuré un paramètre de stratégie de filtre d'Horizon Agent, Horizon Agent évalue et applique les paramètres de stratégie de filtre dans l'ordre de priorité suivant sur l'application ou le poste de travail distant, l'élément 1 ayant la priorité la plus élevée.

1 `Exclude Vid/Pid Device`

2 `Include Vid/Pid Device`

3 `Exclude Device Family`

4 `Include Device Family`

5 Règle `Exclude All Devices` appliquée par un agent définie pour exclure ou inclure tous les périphériques USB

Horizon Agent applique cet ensemble limité de paramètres de règle de filtre de son côté de la connexion.

En définissant des paramètres de règle de filtre pour Horizon Agent, vous pouvez créer un paramètre de filtrage pour des ordinateurs client non gérés. Cette fonctionnalité vous permet également de bloquer le transfert des périphériques depuis les ordinateurs clients, même si les paramètres de stratégie de filtre d'Horizon Client autorisent la redirection.

Par exemple, si vous configurez une stratégie permettant à Horizon Client d'autoriser la redirection d'un périphérique, Horizon Agent bloque celui-ci si vous configurez une stratégie pour qu'Horizon Agent l'exclue.

Exemples de définition de règles pour filtrer des périphériques USB

Les ID de fournisseurs et de produits utilisés dans ces exemples sont employés uniquement à titre d'exemple. Pour plus d'informations sur la détermination des ID de fournisseur et de produit d'un périphérique spécifique, reportez-vous à « Utilisation de fichiers journaux pour le dépannage et pour déterminer les ID de périphérique USB », page 84.

- Sur le client, excluez la redirection d'un périphérique particulier :

  ```
  Exclude Vid/Pid Device:     Vid-0341_Pid-1a11
  ```

- Bloquez la redirection de tous les périphériques de stockage vers ce pool d'applications ou de postes de travail. Utilisez un paramètre côté agent :

  ```
  Exclude Device Family:      o:storage
  ```

- Pour tous les utilisateurs d'un pool de postes de travail, bloquez les périphériques audio et vidéo pour vous assurer qu'ils seront toujours disponibles pour la fonctionnalité Audio-vidéo en temps réel. Utilisez un paramètre côté agent :

  ```
  Exclude Device Family:      o:video;audio
  ```

  Notez qu'une autre stratégie consisterait à exclure des périphériques spécifiques par ID de fournisseur et de produit.

- Sur le client, bloquez la redirection de tous les périphériques, à l'exception d'un périphérique particulier :

  ```
  Exclude All Devices:        true
  Include Vid/Pid Device:     Vid-0123_Pid-abcd
  ```

- Excluez tous les périphériques fabriqués par une entreprise spécifique, car ils posent problème à vos utilisateurs finaux. Utilisez un paramètre côté agent :

  ```
  Exclude Vid/Pid Device:     o:Vid-0341_Pid-*
  ```

- Sur le client, incluez deux périphériques spécifiques mais excluez tous les autres :

  ```
  Exclude All Devices:        true
  Include Vid/Pid Device:     Vid-0123_Pid-abcd;Vid-1abc_Pid-0001
  ```

Familles de périphériques USB

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

Remarque Certains périphériques ne lisent pas certaines familles de périphériques.

Tableau 4-10. Familles de périphériques USB

Nom de la famille de périphériques	Description
`audio`	Tout périphérique d'entrée ou de sortie audio.
`audio-in`	Périphériques d'entrée audio, tels que des microphones.
`audio-out`	Périphériques de sortie audio, tels que des haut-parleurs et des écouteurs.
`bluetooth`	Périphériques connectés par Bluetooth.
`comm`	Périphériques de communication, tels que des modems et des adaptateurs réseau filaires.
`hid`	Périphériques d'interface humaine, à l'exclusion des claviers et des pointeurs.
`hid-bootable`	Périphériques d'interface humaine disponibles au démarrage, à l'exclusion des claviers et des pointeurs.
`imaging`	Périphériques graphiques tels que des scanners.
`keyboard`	Périphérique de type clavier.
`mouse`	Périphérique de pointage tel qu'une souris.
`other`	Famille non spécifiée.
`pda`	Assistants numériques personnels.
`physical`	Périphériques à retour de force, tels que les joysticks à retour de force.
`printer`	Périphériques d'impression.

Tableau 4-10. Familles de périphériques USB (suite)

Nom de la famille de périphériques	Description
`security`	Périphériques de sécurité, tels que des lecteurs d'empreintes digitales.
`smart-card`	Périphériques à carte à puce.
`storage`	Périphériques de stockage de masse tels que des disques à mémoire flash et des disques durs externes.
`unknown`	Famille inconnue.
`vendor`	Périphériques disposant de fonctions spécifiques au fournisseur.
`video`	Périphériques d'entrée vidéo.
`wireless`	Adaptateurs réseau sans fil.
`wusb`	Périphériques USB sans fil.

Paramètres USB du modèle d'administration ADMX pour la configuration d' Horizon Agent

Vous pouvez définir des paramètres de stratégie USB pour Horizon Agent et Horizon Client. Lors de la connexion, Horizon Client télécharge les paramètres de stratégie USB depuis Horizon 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 l'ordinateur client.

Le fichier de modèle d'administration ADMX pour la configuration d'Horizon Agent contient des paramètres de stratégie liés aux composants d'authentification et d'environnement d'Horizon Agent, notamment la redirection USB. Le fichier de modèle d'administration ADMX se nomme (`vdm_agent.admx`). Les paramètres s'appliquent au niveau de l'ordinateur. Horizon Agent 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\Agent\USB`.

Paramètres pour la configuration du fractionnement de périphérique USB

Le tableau suivant décrit chaque paramètre de fractionnement de périphériques USB composites situé dans le fichier de modèle d'administration ADMX pour la configuration d'Horizon Agent. Tous ces paramètres se trouvent dans le dossier **Configuration de VMware Horizon Agent > Afficher la configuration USB > Paramètres téléchargeables uniquement par le client** dans l'Éditeur de gestion de stratégie de groupe. Horizon Agent n'applique pas ces paramètres. Horizon Agent transmet les paramètres à Horizon Client pour qu'il les interprète et les applique, selon que vous spécifiez le modificateur de fusion (`m`) ou de remplacement (`o`). Horizon Client utilise les paramètres pour décider s'il faut fractionner des périphériques USB composites en périphériques composants et exclure les périphériques composants de la redirection. Pour voir une description de la façon dont Horizon applique les règles pour le fractionnement de périphériques USB composites, reportez-vous à la section « Configuration de paramètres de règle de fractionnement de périphérique pour des périphériques USB composites », page 86.

Tableau 4-11. Modèle de configuration d' Horizon Agent : paramètres de fractionnement de périphérique

Paramètre	Propriétés
`Allow Auto Device Splitting` Propriété : `AllowAutoDeviceSplitting`	Autorise le fractionnement automatique de périphériques USB composites. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
`Exclude Vid/Pid Device from Split` Propriété : `SplitExcludeVidPid`	Exclut un périphérique USB composite spécifié par des ID de fournisseur et de produit du fractionnement. Le format du paramètre est {`m`|`o`}`: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 : **`o:vid-0781_pid-55**`** La valeur par défaut n'est pas définie.
`Split Vid/Pid Device` Propriété : `SplitVidPid`	Traite les composants d'un périphérique USB composite spécifiés par des ID de fournisseur et de produit en tant que périphériques séparés. Le format du paramètre est {`m`|`o`}`:vid-`*xxxx*`_pid-`*yyyy*`(exintf:`*zz*[`;exintf:`*ww*]) ou {`m`|`o`}`: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 : **`o:vid-0781_pid-554c(exintf:01;exintf:02)`** **Remarque** Horizon 7 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.

Paramètres USB appliqués par Horizon Agent

Le tableau suivant décrit chaque paramètre de stratégie appliqué par un agent pour USB dans le fichier de modèle d'administration ADMX pour la configuration d'Horizon Agent. Tous ces paramètres se trouvent dans le dossier **Configuration de VMware Horizon Agent > Afficher la configuration USB** dans l'Éditeur de gestion de stratégie de groupe. Horizon Agent utilise les paramètres pour décider si un périphérique USB peut être transmis à la machine hôte. Horizon Agent transmet également les paramètres à Horizon Client pour qu'il les interprète et les applique, selon que vous spécifiez le modificateur de fusion (`m`) ou de remplacement (`o`). Horizon Client utilise les paramètres pour décider si un périphérique USB est disponible pour la redirection. Comme Horizon Agent applique toujours un paramètre de stratégie appliqué par un agent que vous spécifiez, l'effet peut être la neutralisation de la stratégie que vous avez définie pour Horizon Client. Pour voir une description de la façon dont Horizon 7 applique les stratégies pour le filtrage de périphériques USB, reportez-vous à la section « Configuration de paramètres de règle de filtre pour des périphériques USB », page 89.

Tableau 4-12. Modèle de configuration d' Horizon Agent : paramètres appliqués par l'agent

Paramètre	Propriétés
`Exclude All Devices` Propriété : `ExcludeAllDevices`	Exclut tous les périphériques USB de la transmission. Si ce paramètre est défini sur **`true`**, vous pouvez utiliser d'autres paramètres de règle pour autoriser la transmission 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 transmission de périphériques spécifiques ou de familles de périphériques. Si ce paramètre est défini sur **`true`** et transmis à Horizon Client, il remplace toujours celui sur Horizon Client. Vous ne pouvez pas utiliser le modificateur de fusion (`m`) ou de remplacement (`o`) avec ce paramètre. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
`Exclude Device Family` Propriété : `ExcludeFamily`	Exclut des familles de périphériques de la transmission. Le format du paramètre est {`m`|`o`}`:`*family_name_1*[`;`*family_name_2*]... Par exemple : **`o:bluetooth;smart-card`** Si vous avez activé le fractionnement automatique de périphérique, Horizon 7 examine la famille de périphériques de chaque interface d'un périphérique USB composite afin de décider des interfaces à exclure. Si vous avez désactivé le fractionnement automatique de périphérique, Horizon 7 examine la famille de périphériques de l'ensemble du périphérique USB composite. La valeur par défaut n'est pas définie.
`Exclude Vid/Pid Device` Propriété : `ExcludeVidPid`	Exclut des périphériques avec des ID de fournisseur et de produit spécifiés de la transmission. Le format du paramètre est {`m`|`o`}`: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 : **`m:vid-0781_pid-****;vid-0561_pid-554c`** La valeur par défaut n'est pas définie.
`Include Device Family` Propriété : `IncludeFamily`	Inclut des familles de périphériques pouvant être transmises. Le format du paramètre est {`m`|`o`}`:`*family_name_1*[`;`*family_name_2*]... Par exemple : **`m:storage`** La valeur par défaut n'est pas définie.
`Include Vid/Pid Device` Propriété : `IncludeVidPid`	Inclut des périphériques avec des ID de fournisseur et de produit spécifiés pouvant être transmis. Le format du paramètre est {`m`|`o`}`: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 : **`o:vid-0561_pid-554c`** La valeur par défaut n'est pas définie.

Paramètres USB interprétés par un client

Le tableau suivant décrit chaque paramètre de stratégie interprété par un client dans le fichier de modèle d'administration ADMX pour la configuration d'Horizon Agent. Tous ces paramètres se trouvent dans le dossier **Configuration de VMware Horizon Agent > Configuration USB de View > Paramètres uniquement téléchargeables par le client** dans l'Éditeur de gestion de stratégie de groupe. Horizon Agent n'applique pas ces paramètres. Horizon Agent transmet les paramètres à Horizon Client pour qu'il les interprète et les applique. Horizon Client utilise les paramètres pour décider si un périphérique USB est disponible pour la redirection.

Tableau 4-13. Modèle de configuration d' Horizon Agent : paramètres interprétés par un client

Paramètre	Propriétés
`Allow Audio Input Devices` Propriété : `AllowAudioIn`	Permet la transmission de périphériques d'entrée audio. La valeur par défaut est indéfinie, ce qui correspond à **`true`**.
`Allow Audio Output Devices` Propriété : `AllowAudioOut`	Permet la transmission de périphériques de sortie audio. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
`Allow HID-Bootable` Propriété : `AllowHIDBootable`	Permet la transmission 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`**.
`Allow Other Input Devices`	Permet la transmission de périphériques d'entrée autres que des périphériques démarrables par HID ou des claviers avec périphériques de pointage intégrés. La valeur par défaut n'est pas définie.
`Allow Keyboard and Mouse Devices` Propriété : `AllowKeyboardMouse`	Permet la transmission de claviers avec périphériques de pointage intégrés (souris, Trackball ou pavé tactile). La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
`Allow Smart Cards` Propriété : `AllowSmartcard`	Permet la transmission de périphériques à carte à puce. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
`Allow Video Devices` Propriété : `AllowVideo`	Permet la transmission de périphériques vidéo. La valeur par défaut est indéfinie, ce qui correspond à **`true`**.

Résolution de problèmes de redirection USB

Plusieurs problèmes peuvent se produire avec la redirection USB dans Horizon Client.

Problème

La redirection USB dans Horizon Client ne parvient pas à rendre disponibles des périphériques locaux sur le poste de travail distant ou certains périphériques ne semblent pas être disponibles pour la redirection dans Horizon Client.

Cause

Voici des causes possibles d'échec du fonctionnement correct ou prévu de la redirection USB.

- Le périphérique est un périphérique USB composite et l'un des périphériques qu'il inclut est bloqué par défaut. Par exemple, un périphérique de dictée qui inclut une souris est bloqué par défaut parce que les souris sont bloquées par défaut. Pour résoudre ce problème, reportez-vous à la section « Configuration de paramètres de stratégie de fractionnement de périphérique pour des périphériques USB composites » dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.
- La redirection USB n'est pas prise en charge sur les hôtes Windows Server 2008 RDS qui déploient des applications et des postes de travail distants. La redirection USB est prise en charge sur les hôtes RDS Windows Server 2012 avec View Agent 6.1 et versions ultérieures, mais uniquement pour les périphériques de stockage USB. La redirection USB est prise en charge sur les systèmes Windows Server 2008 R2 et Windows Server 2012 R2 utilisés comme postes de travail mono-utilisateur.
- Seuls les lecteurs flash et les disques durs USB sont pris en charge sur les postes de travail et applications RDS. Vous ne pouvez pas rediriger d'autres types de périphériques USB (par exemple, d'autres types de périphériques de stockage USB tels que les lecteurs de stockage de sécurité et les CD-ROM USB) vers un poste de travail ou une application RDS.
- Les webcams ne sont pas prises en charge pour la redirection.
- 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.

- La redirection USB n'est pas prise en charge pour les périphériques d'amorçage. Si vous exécutez Horizon Client sur un système Windows qui démarre à partir d'un périphérique USB, et que vous redirigez ce périphérique vers le poste de travail distant, le système d'exploitation local risque de ne plus répondre ou de devenir inutilisable. Reportez-vous à la section http://kb.vmware.com/kb/1021409.
- Par défaut, Horizon Client pour Windows ne vous permet pas de sélectionner des périphériques clavier, souris, carte à puce et sortie audio pour la redirection. Reportez-vous à la section http://kb.vmware.com/kb/1011600.
- RDP ne prend pas en charge la redirection pour les périphériques HID USB pour la session de console, ou pour les lecteurs de cartes à puce. Reportez-vous à la section http://kb.vmware.com/kb/1011600.
- Windows Mobile Device Center peut empêcher la redirection de périphériques USB pour des sessions RDP. Reportez-vous à la section http://kb.vmware.com/kb/1019205.
- Pour certains périphériques HID USB, vous devez configurer la machine virtuelle afin d'actualiser la position du pointeur de la souris. Reportez-vous à la section http://kb.vmware.com/kb/1022076.
- Pour certains périphériques audio, vous devrez éventuellement modifier les paramètres de règle ou de Registre. Reportez-vous à la section http://kb.vmware.com/kb/1023868.
- La latence réseau peut ralentir l'interaction entre périphériques ou rendre les applications figées car elles sont conçues pour interagir avec des périphériques locaux. Les disques durs USB très volumineux peuvent prendre plusieurs minutes pour apparaître dans Windows Explorer.
- Le chargement des cartes flash USB formatées avec le système de fichiers FAT32 est lent. Reportez-vous à la section http://kb.vmware.com/kb/1022836.
- Un processus ou un service sur le système local a ouvert le périphérique avant votre connexion à l'application ou au poste de travail distant.
- Un périphérique USB redirigé arrête de fonctionner si vous reconnectez une session de poste de travail ou d'application, même si le poste de travail ou l'application indique que le périphérique est disponible.
- La redirection USB est désactivée dans Horizon Administrator.
- Des pilotes de redirection USB sont manquants ou désactivés sur le client.

Solution

- S'il est disponible, utilisez PCoIP au lieu de RDP comme protocole.
- Si un périphérique redirigé reste indisponible ou arrête de fonctionner après une déconnexion temporaire, éjectez le périphérique, rebranchez-le et tenter de nouveau l'opération de redirection.
- Dans Horizon Administrator, accédez à **Stratégies > Règles générales**, et vérifiez que l'accès USB est défini sur **Autoriser** sous Stratégies de View.
- Dans le journal de l'invité, recherchez des entrées de la classe `ws_vhub` et, dans le journal du client, recherchez des entrées de la classe `vmware-view-usbd`.

  Les entrées avec ces classes sont inscrites dans les journaux si un utilisateur n'est pas un administrateur, ou si les pilotes de redirection USB ne sont pas installés ou ne fonctionnent pas. Pour voir l'emplacement de ces fichiers journaux, reportez-vous à la section « Utilisation de fichiers journaux pour le dépannage et pour déterminer les ID de périphérique USB » dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.
- Ouvrez le Gestionnaire de périphériques sur l'invité, développez les contrôleurs USB (Universal Serial Bus) et réinstallez les pilotes VMware View Virtual USB Host Controller et VMware View Virtual USB Hub s'ils sont manquants ou réactivez-les s'ils sont désactivés.

Configuration de stratégies pour des pools de postes de travail et d'applications

5

Vous pouvez configurer des stratégies pour contrôler le comportement des pools de postes de travail et d'applications, des machines et des utilisateurs. Vous utilisez Horizon Administrator pour configurer des stratégies pour des sessions clientes. Vous pouvez utiliser les paramètres de stratégie de groupe Active Directory pour contrôler le comportement d'Horizon Agent, d'Horizon Client pour Windows et des fonctionnalités qui affectent les machines mono-utilisateur, les hôtes RDS, PCoIP ou VMware Blast.

Ce chapitre aborde les rubriques suivantes :

Définition de stratégies dans Horizon Administrator

Vous utilisez Horizon Administrator pour configurer des stratégies pour les sessions clientes.

Vous pouvez définir ces règles pour affecter des utilisateurs spécifiques, des pools de postes de travail spécifiques ou tous les utilisateurs de sessions client. Les stratégies qui affectent des utilisateurs et des pools de postes de travail spécifiques sont appelées stratégies au niveau des utilisateurs et stratégies au niveau des pools. Les règles qui affectent toutes les sessions et utilisateurs sont appelées règles générales.

Les stratégies au niveau des utilisateurs héritent des paramètres équivalents des stratégies au niveau des pools de postes de travail. De même, les stratégies au niveau des pools de postes de travail héritent des paramètres équivalents des stratégie globales. Un paramètre de stratégie au niveau des pools de postes de travail a priorité sur le paramètre équivalent de stratégie globale. Un paramètre de stratégie au niveau des utilisateurs a priorité sur les paramètres équivalents de stratégie globale et de stratégie au niveau des pools de postes de travail.

Les paramètres de règle de niveau inférieur peuvent être plus ou moins restrictifs que les paramètres de niveau supérieur équivalents. Par exemple, vous pouvez définir une stratégie globale sur **Refuser** et la stratégie au niveau des pools de postes de travail équivalente sur **Autoriser**, ou l'inverse.

Remarque Seules les stratégies globales sont disponibles pour les pools de postes de travail et d'applications RDS. Vous ne pouvez pas définir des stratégies de niveau utilisateur ou des stratégies de niveau pools pour les pools de postes de travail et d'applications RDS.

Configurer des paramètres de règle générale

Vous pouvez configurer des règles générales pour contrôler le comportement de tous les utilisateurs de sessions client.

Prérequis

Familiarisez-vous avec les descriptions de règles. Reportez-vous à la section « Règles Horizon 7 », page 101.

Procédure

1 Dans Horizon Administrator, sélectionnez **Règles > Règles générales**.

2 Cliquez sur **Modifier les stratégies** dans le volet **Règles de View**.

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

Configurer des règles pour des pools de postes de travail

Vous pouvez configurer des règles de niveau poste de travail pour affecter des pools de postes de travail spécifiques. Les paramètres de règle de niveau poste de travail sont prioritaires par rapport à leurs paramètres de règle générale équivalents.

Prérequis

Familiarisez-vous avec les descriptions de règles. Reportez-vous à la section « Règles Horizon 7 », page 101.

Procédure

1 Dans Horizon Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

2 Double-cliquez sur l'ID du pool de postes de travail et cliquez sur l'onglet **Règles**.

   L'onglet **Règles** montre les paramètres de règle actuels. Lorsqu'un paramètre est hérité de la stratégie générale équivalente, **Hériter** s'affiche dans la colonne **Stratégie de pools de postes de travail**.

3 Cliquez sur **Modifier les stratégies** dans le volet **Règles de View**.

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

Configurer des stratégies pour les utilisateurs

Vous pouvez configurer des règles de niveau utilisateur pour affecter des utilisateurs spécifiques. Les paramètres de stratégie de niveau utilisateur sont toujours prioritaires par rapport aux paramètres de stratégie généraux et de niveau poste de travail équivalents.

Prérequis

Familiarisez-vous avec les descriptions de règles. Reportez-vous à la section « Règles Horizon 7 », page 101.

Procédure

1 Dans Horizon Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

2 Double-cliquez sur l'ID du pool de postes de travail et cliquez sur l'onglet **Règles**.

   L'onglet **Règles** montre les paramètres de règle actuels. Lorsqu'un paramètre est hérité de la stratégie générale équivalente, **Hériter** s'affiche dans la colonne **Stratégie de pools de postes de travail**.

3 Cliquez sur **Remplacements d'utilisateur** et sur **Ajouter un utilisateur**.

4 Pour rechercher un utilisateur, cliquez sur **Ajouter**, saisissez le nom ou la description de l'utilisateur, puis cliquez sur **Rechercher**.

5 Sélectionnez un ou plusieurs utilisateurs dans la liste, cliquez sur **OK**, puis sur **Suivant**.

   La boîte de dialogue Add Individual Policy (Ajouter une règle individuelle) apparaît.

6 Configurez les stratégies Horizon et cliquez sur **Terminer** pour enregistrer vos modifications.

Règles Horizon 7

Vous pouvez configurer des stratégies Horizon 7 pour affecter toutes les sessions clientes, ou vous pouvez les appliquer pour affecter des pools de postes de travail ou des utilisateurs spécifiques.

Tableau 5-1 décrit chaque paramètre de stratégie Horizon 7.

Tableau 5-1. Stratégies Horizon

Règle	Description
Redirection multimédia (MMR)	Détermine si MMR est activé pour les systèmes client. MMR est un filtre de Windows Media Foundation qui permet de transférer des données multimédia de codecs spécifiques sur des postes de travail distants au système client directement via un socket TCP. Les données sont ensuite directement décodées sur le système client, lorsqu'elles sont lues. La valeur par défaut est **Refuser**. Si les systèmes clients disposent de ressources insuffisantes pour gérer le décodage multimédia local, laissez le paramètre défini sur **Refuser**. Les données de redirection multimédia (MMR) sont envoyées sur le réseau sans cryptage basé sur une application et peuvent contenir des données sensibles, selon le contenu redirigé. Pour garantir que les données ne puissent pas être surveillées sur le réseau, utilisez MMR uniquement sur un réseau sécurisé.
USB Access (Accès USB)	Détermine si des postes de travail distants peuvent utiliser des périphériques USB connectés au système client. La valeur par défaut est **Autoriser**. Pour empêcher l'utilisation de périphériques externes pour des raisons de sécurité, passez le paramètre sur **Refuser**.
Accélération matérielle PCoIP	Détermine l'activation de l'accélération matérielle du protocole d'affichage PCoIP et spécifie la priorité d'accélération affectée à la session utilisateur PCoIP. Ce paramètre a un effet uniquement si un périphérique d'accélération matérielle PCoIP est présent sur l'ordinateur physique qui héberge le poste de travail distant. La valeur par défaut est **Autoriser** avec une priorité **Moyenne**.

Utilisation de Stratégies de carte à puce

Vous pouvez utiliser Stratégies de carte à puce pour créer des stratégies qui contrôlent le comportement des fonctionnalités de redirection USB, d'impression virtuelle, de redirection du Presse-papiers, de redirection du lecteur client et de protocole d'affichage PCoIP sur des postes de travail distants spécifiques. Vous pouvez également utiliser Stratégies de carte à puce pour créer des stratégies qui contrôlent le comportement des applications publiées.

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

Configuration requise pour les Stratégies de carte à puce

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

- Vous devez installer Horizon Agent 7.0 ou version ultérieure et VMware User Environment Manager 9.0 ou version ultérieure sur les postes de travail distants que vous voulez gérer avec des Stratégies de carte à puce.
- Les utilisateurs doivent utiliser Horizon Client 4.0 ou version ultérieure pour se connecter à des postes de travail distants que vous gérez avec des Stratégies de carte à puce.

Installation de User Environment Manager

Pour utiliser Stratégies de carte à puce afin de contrôler le comportement des fonctionnalités de poste de travail distant sur un poste de travail distant, vous devez installer User Environment Manager 9.0 ou version ultérieure sur le poste de travail distant.

Vous pouvez télécharger le programme d'installation de User Environment Manager sur la page de téléchargement de VMware. Vous devez installer le composant client VMware UEM FlexEngine sur chaque poste de travail distant que vous voulez gérer avec User Environment Manager. Vous pouvez installer le composant Console de gestion User Environment Manager sur les postes de travail que vous voulez pour gérer l'environnement User Environment Manager.

Pour un pool de clone lié, vous installez User Environment Manager sur la machine virtuelle parente que vous utilisez comme image de base pour les clones liés. Pour un pool de postes de travail RDS, vous installez User Environment Manager sur l'hôte RDS qui fournit les sessions de poste de travail RDS.

Pour voir des instructions sur la configuration système requise et sur l'installation complète de User Environment Manager, consultez le document *Guide de l'administrateur de User Environment Manager*.

Configuration d' User Environment Manager

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

Pour configurer User Environment Manager, suivez les instructions de configuration dans le *Guide de l'administrateur de User Environment Manager*. Les étapes de configuration suivantes complètent les informations dans ce document.

- Lors de la configuration du composant client VMware UEM FlexEngine sur des postes de travail distants, créez des scripts d'ouverture et de fermeture de session FlexEngine. Utilisez le paramètre **`-HorizonViewMultiSession -r`** pour le script d'ouverture de session et le paramètre **`-HorizonViewMultiSession -s`** pour le script de fermeture de session.

  Remarque N'utilisez pas de scripts d'ouverture de session pour démarrer d'autres applications sur un poste de travail distant. Des scripts d'ouverture de session supplémentaires peuvent retarder l'ouverture de session du poste de travail distant de 10 minutes au maximum.

- Activez le paramètre de stratégie de groupe d'utilisateurs `Exécuter les scripts d'ouverture de session simultanément` sur les postes de travail distants. Ce paramètre se trouve dans le dossier `Configuration utilisateur\Stratégies\Modèles d'administration\Système\Scripts`.
- Activez le paramètre de stratégie de groupe d'ordinateurs `Toujours attendre le réseau lors du démarrage de l'ordinateur et de l'ouverture de session` sur les postes de travail distants. Ce paramètre se trouve dans le dossier `Configuration ordinateur\Stratégies\Modèles d'administration\Système\Ouverture de session`.
- Pour les postes de travail distants Windows 8.1, désactivez le paramètre de stratégie de groupe d'ordinateurs `Configurer le délai des scripts d'ouverture de session`. Ce paramètre se trouve dans le dossier `Configuration ordinateur\Stratégies\Modèles d'administration\Système\Stratégie de groupe`.
- Pour s'assurer que les paramètres de stratégie de carte à puce d'Horizon sont actualisés lorsque les utilisateurs se reconnectent à des sessions de poste de travail, utilisez la console de gestion User Environment Manager pour créer une tâche déclenchée. Définissez le déclencheur sur **Reconnecter la session**, définissez l'action sur **Actualiser l'environnement utilisateur** et sélectionnez **Stratégies de carte à puce d'Horizon** pour l'actualisation.

  Remarque Si vous créez la tâche déclenchée alors qu'un utilisateur est connecté au poste de travail distant, l'utilisateur doit se déconnecter du poste de travail pour que la tâche déclenchée prenne effet.

Paramètres de stratégie de carte à puce Horizon

Vous contrôlez le comportement de fonctionnalités de poste de travail distant dans User Environment Manager en créant une stratégie de carte à puce Horizon.

Tableau 5-2 décrit les paramètres que vous pouvez sélectionner lorsque vous définissez une stratégie de carte à puce Horizon dans User Environment Manager.

Tableau 5-2. Paramètres de stratégie de carte à puce Horizon

Paramètre	Description
redirection USB	Détermine si la redirection USB est activée sur le poste de travail distant. La fonctionnalité de redirection USB permet aux utilisateurs d'utiliser des périphériques USB connectés localement, tels que des mémoires Flash, des caméras et des imprimantes, à partir du poste de travail distant.
Impression	Détermine si l'impression virtuelle est activée sur le poste de travail distant. La fonctionnalité d'impression virtuelle permet aux utilisateurs d'imprimer vers une imprimante virtuelle ou USB qui est connectée à l'ordinateur client depuis le poste de travail distant.

Tableau 5-2. Paramètres de stratégie de carte à puce Horizon (suite)

Paramètre	Description
Presse-papiers	Détermine le sens dans lequel la redirection du Presse-papiers est autorisée. Vous pouvez sélectionner l'une des valeurs suivantes : ■ **Désactiver**. La redirection du Presse-papiers est désactivée dans les deux sens. ■ **Autoriser tout**. La redirection du Presse-papiers est activée. Les utilisateurs peuvent copier et coller depuis le système client vers le poste de travail distant, et vice versa. ■ **Autoriser la copie depuis le client vers l'agent**. Les utilisateurs peuvent copier et coller uniquement depuis le système client vers le poste de travail distant. ■ **Autoriser la copie depuis l'agent vers le client**. Les utilisateurs peuvent copier et coller uniquement depuis le poste de travail distant vers le système client.
Redirection de lecteur client	Détermine si la redirection du lecteur client est activée sur le poste de travail distant et si des lecteurs et des dossiers partagés sont accessibles en écriture. Vous pouvez sélectionner l'une des valeurs suivantes : ■ **Désactiver**. La redirection du lecteur client est désactivée sur le poste de travail distant. ■ **Autoriser tout**. Les lecteurs clients et les dossiers sont partagés avec le poste de travail distant et sont accessibles en lecture et en écriture. ■ **Lecture seule**. Les lecteurs clients et les dossiers sont partagés avec le poste de travail distant et sont accessibles en lecture, mais pas en écriture. Si vous ne configurez pas ce paramètre, l'accessibilité en écriture des lecteurs et des dossiers partagés dépend des paramètres de registre locaux. Pour plus d'informations, reportez-vous à la section « Utiliser des paramètres de registre pour configurer la redirection du lecteur client », page 54.
Profil de bande passante	Configure un profil de bande passante pour des sessions PCoIP et Blast sur le poste de travail distant. Vous pouvez sélectionner un profil de bande passante prédéfini, par exemple **Réseau LAN**. La sélection d'un profil de bande passante prédéfini empêche l'agent de tenter de transmettre à un taux supérieur à la capacité de liaison. Si vous sélectionnez le profil par défaut, la bande passante maximale est de 90 000 kilobits par seconde. Pour plus d'informations, reportez-vous à la section « Référence de profil de bande passante », page 104.
Transfert de fichiers HTML Access	Détermine le transfert de fichiers HTML entre le client et l'agent.

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

Référence de profil de bande passante

Avec des stratégies de carte à puce, vous pouvez utiliser le paramètre de stratégie de profil de bande passante pour configurer un profil de bande passante pour des sessions PCoIP ou Blast sur des postes de travail distants.

Tableau 5-3. Profils de bande passante

Profil de bande passante	Bande passante de session max. (Kbit/s)	Bande passante de session min. (Kbit/s)	Activer BTL	Qualité d'image initiale max.	Qualité d'image min.	Image/s max.	Bande passante audio max. (Kbit/s)	Performance de qualité d'image
Réseau LAN haute vitesse	900 000	100	Oui	100	50	60	1 600	50
Réseau LAN	900 000	100	Oui	90	50	30	1 600	50
Réseau WAN dédié	900 000	100	Non	80	40	30	500	50
Réseau WAN à large bande	5 000	100	Non	70	40	20	500	50

Tableau 5-3. Profils de bande passante (suite)

Profil de bande passante	Bande passante de session max. (Kbit/s)	Bande passante de session min. (Kbit/s)	Activer BTL	Qualité d'image initiale max.	Qualité d'image min.	Image/s max.	Bande passante audio max. (Kbit/s)	Performance de qualité d'image
Réseau WAN basse vitesse	2 000	100	Non	70	30	15	200	25
Connexion très basse vitesse	1 000	100	Non	70	30	5	90	0

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

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

Vous pouvez ajouter plusieurs conditions pour la même fonctionnalité de poste de travail distant. Par exemple, vous pouvez ajouter une condition qui active l'impression locale si un utilisateur est membre du groupe RH et une autre condition qui active l'impression locale si le poste de travail distant se trouve dans le pool Win7.

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

Utilisation de la condition de propriété d'Horizon Client

Lorsqu'un utilisateur se connecte ou se reconnecte à un poste de travail distant, Horizon Client recueille des informations sur l'ordinateur client et le Serveur de connexion envoie ces informations au poste de travail distant. Vous pouvez ajouter la condition de propriété d'Horizon Client à une définition de stratégie Horizon pour contrôler quand la stratégie prend effet en fonction des informations que le poste de travail distant reçoit.

Remarque La condition de propriété d'Horizon Client ne prend effet que si un utilisateur lance le poste de travail distant avec le protocole d'affichage PCoIP ou VMware Blast. Si un utilisateur lance le poste de travail distant avec le protocole d'affichage RDP, la condition de propriété d'Horizon Client n'a aucun effet.

Tableau 5-4 décrit les propriétés prédéfinies que vous pouvez sélectionner dans le menu déroulant **Propriétés** lorsque vous utilisez la condition de propriété d'Horizon Client. Chaque propriété prédéfinie correspond à une clé de registre `ViewClient_`.

Tableau 5-4. Propriétés prédéfinies pour la condition de propriété d'Horizon Client

Propriété	Clé de registre correspondante	Description
Emplacement du client	`ViewClient_Broker_GatewayLocation`	Spécifie l'emplacement du système client de l'utilisateur. Les valeurs valides sont les suivantes : ■ Interne : la stratégie prend effet uniquement si un utilisateur se connecte au poste de travail distant à l'intérieur du réseau d'entreprise ■ Externe : la stratégie prend effet uniquement si un utilisateur se connecte au poste de travail distant à l'extérieur du réseau d'entreprise Pour plus d'informations sur la configuration de l'emplacement de passerelle d'un hôte de Serveur de connexion ou de serveur de sécurité, consultez le document *Administration de View*. Pour plus d'informations sur la configuration de l'emplacement de passerelle d'un dispositif Access Point, consultez le document *Déploiement et configuration d'Unified Access Gateway*.
Balise(s) de démarrage	`ViewClient_Launch_Matched_Tags`	Spécifie une ou plusieurs balises. Séparez les balises avec une virgule ou un point-virgule. La stratégie prend effet uniquement si la balise qui activait le démarrage d'applications ou de postes de travail distants correspond à l'une des balises spécifiées. Pour plus d'informations sur l'attribution de balises à des instances du Serveur de connexion et à des pools de postes de travail, consultez votre document Configuration.
Nom de pool	`ViewClient_Launch_ID`	Spécifie un ID de pool de postes de travail ou d'applications. La stratégie prend effet uniquement si l'ID du pool de postes de travail ou d'applications que l'utilisateur a choisi lors du démarrage de l'application ou du poste de travail distant correspond à l'ID du pool de postes de travail ou d'applications spécifié. Par exemple, si l'utilisateur a choisi le pool Win7 et que cette propriété est définie sur Win7, la stratégie prend effet. **Remarque** Si plusieurs pools d'applications sont lancés dans la même session d'hôte RDS, la valeur est l'ID de la première application qui est lancée à partir d'Horizon Client.

Le menu déroulant **Propriétés** est également une zone de texte et vous pouvez entrer manuellement une clé de registre `ViewClient_` dans la zone de texte. N'incluez pas le préfixe `ViewClient_` lorsque vous entrez la clé de registre. Par exemple, pour spécifier `ViewClient_Broker_URL`, entrez `Broker_URL`.

Vous pouvez utiliser l'Éditeur du Registre Windows (`regedit.exe`) sur le poste de travail distant pour voir les clés de registre `ViewClient_`. Horizon Client écrit des informations d'ordinateur client dans le chemin d'accès `HKEY_CURRENT_USER\Volatile Environment` du registre système sur les postes de travail distants qui sont déployés sur des machines mono-utilisateur. Pour les postes de travail distants déployés dans des sessions RDS, Horizon Client écrit les informations de l'ordinateur client dans le chemin d'accès `HKEY_CURRENT_USER\Volatile Environment\`*x* du registre système, où *x* est l'ID de la session sur l'hôte RDS.

Utilisation des autres conditions

La console de gestion User Environment Manager fournit de nombreuses conditions. Les conditions suivantes peuvent être particulièrement utiles lors de la création de stratégies pour des fonctionnalités de poste de travail distant.

Membre de groupe Vous pouvez utiliser cette condition pour configurer la stratégie afin qu'elle ne prenne effet que si un utilisateur est membre d'un groupe spécifique.

Protocole d'affichage distant Vous pouvez utiliser cette condition pour configurer la stratégie afin qu'elle ne prenne effet que si l'utilisateur choisit un protocole d'affichage particulier. Les paramètres de condition incluent RDP, PCoIP et Blast.

Adresse IP Vous pouvez utiliser cette condition pour configurer la stratégie afin qu'elle ne prenne effet que si un utilisateur se connecte à l'intérieur ou à l'extérieur du réseau d'entreprise. Utilisez les paramètres de condition pour spécifier une plage d'adresses IP internes ou une plage d'adresses IP externes.

Remarque Vous pouvez également utiliser la propriété **Emplacement du client** dans la condition de propriété d'Horizon Client.

Pour voir une description de toutes les conditions disponibles, consultez le document *Guide de l'administrateur de User Environment Manager*.

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

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

Prérequis

- Installez et configurez User Environment Manager. Reportez-vous aux sections « Installation de User Environment Manager », page 102 et « Configuration d'User Environment Manager », page 103.
- Familiarisez-vous avec les paramètres de stratégie de carte à puce Horizon. Reportez-vous à la section « Paramètres de stratégie de carte à puce Horizon », page 103.
- Familiarisez-vous avec les conditions que vous pouvez ajouter à des définitions de stratégie de carte à puce Horizon. Reportez-vous à la section « Ajout de conditions à des définitions de stratégie de carte à puce Horizon », page 105.

Pour obtenir des informations complètes sur l'utilisation de la console de gestion User Environment Manager, consultez le document *Guide de l'administrateur de User Environment Manager*.

Procédure

1. Dans la console de gestion User Environment Manager, sélectionnez l'onglet **Environnement utilisateur** et cliquez sur **Stratégies de carte à puce Horizon** dans l'arborescence.

   Les définitions de stratégie de carte à puce Horizon existantes, le cas échéant, apparaissent dans le volet Stratégies de carte à puce Horizon.

2. Cliquez avec le bouton droit de la souris sur **Stratégies de carte à puce Horizon** et sélectionnez **Créer une définition de stratégie de carte à puce Horizon** pour créer une stratégie de carte à puce.

   La boîte de dialogue Stratégie de carte à puce Horizon s'affiche.

3 Sélectionnez l'onglet **Paramètres** et définissez les paramètres de stratégie de carte à puce.

   a Dans la section Paramètres généraux, entrez un nom pour la stratégie de carte à puce dans la zone de texte **Nom**.

      Par exemple, si la stratégie de carte à puce affecte la fonctionnalité de redirection du lecteur client, vous pouvez nommer la stratégie de carte à puce CDR.

   b Dans la section Paramètres de stratégie de carte à puce Horizon, sélectionnez les fonctionnalités et les paramètres de poste de travail distant à inclure dans la stratégie de carte à puce.

      Vous pouvez sélectionner plusieurs fonctionnalités de poste de travail distant.

4 (Facultatif) Pour ajouter une condition à la stratégie de carte à puce, sélectionnez l'onglet **Conditions**, cliquez sur **Ajouter** et sélectionnez une condition.

   Vous pouvez ajouter plusieurs conditions à une définition de stratégie de carte à puce.

5 Cliquez sur **Enregistrer** pour enregistrer la stratégie de carte à puce.

User Environment Manager traite la stratégie de carte à puce Horizon chaque fois qu'un utilisateur se connecte ou se reconnecte au poste de travail distant.

User Environment Manager traite plusieurs stratégies de carte à puce dans l'ordre alphabétique en fonction du nom de la stratégie de carte à puce. Les stratégies de carte à puce Horizon apparaissent dans l'ordre alphabétique dans le volet Stratégies de carte à puce Horizon. En cas de conflit de stratégies de carte à puce, la dernière stratégie de carte à puce traitée est prioritaire. Par exemple, s'il existe une stratégie de carte à puce nommée Sophie qui active la redirection USB pour l'utilisatrice Sophie et une autre stratégie de carte à puce nommée Pool qui désactive la redirection USB pour le pool de postes de travail Win7, la fonctionnalité de redirection USB est activée lorsque Sophie se connecte à un poste de travail distant dans le pool de postes de travail Win7.

Utilisation de stratégies de groupe Active Directory

Vous pouvez utiliser une stratégie de groupe Microsoft Windows pour optimiser et sécuriser des postes de travail distants, contrôler le comportement de composants Horizon 7 et configurer l'impression basée sur l'emplacement.

La stratégie de groupe est une fonction des systèmes d'exploitation Microsoft Windows qui fournit une gestion et une configuration centralisées des ordinateurs et des utilisateurs à distance dans un environnement Active Directory.

Les paramètres de stratégie de groupe sont contenus dans des entités nommées objets de stratégie de groupe (GPO). Des GPO sont associés à des objets Active Directory. Vous pouvez appliquer des GPO à des composants Horizon 7 au niveau d'un domaine pour contrôler diverses zones de l'environnement Horizon 7. Une fois appliqués, les paramètres de GPO sont stockés dans le Registre Windows local du composant spécifié.

Vous utilisez l'Éditeur d'objets de stratégie de groupe de Microsoft Windows pour gérer des paramètres de stratégie de groupe. L'Éditeur d'objets de stratégie de groupe est un composant logiciel enfichable de Microsoft Management Console (MMC). La MMC fait partie de la Console de gestion des stratégies de groupe (GPMC). Pour plus d'informations sur l'installation et l'utilisation de la GPMC, consultez le site Web Microsoft TechNet.

Création d'une UO pour des postes de travail distants

Créez dans Active Directory une unité d'organisation (UO) qui soit propre à vos postes de travail distants.

Pour empêcher l'application des paramètres de stratégie de groupe sur d'autres serveurs ou stations de travail Windows dans le même domaine que vos postes de travail distants, créez un objet de stratégie de groupe (GPO) pour vos stratégies de groupe Horizon 7 et liez-le à l'UO qui contient vos postes de travail distants.

Pour plus d'informations sur la création d'UO et de GPO, consultez la documentation à propos de Microsoft Active Directory sur le site Web Microsoft TechNet.

Activation du traitement en boucle pour des postes de travail distants

Par défaut, les paramètres de stratégie d'un utilisateur viennent de l'ensemble de GPO appliqués à l'objet utilisateur dans Active Directory. Toutefois, dans l'environnement Horizon 7, des GPO s'appliquent à des utilisateurs en fonction de l'ordinateur sur lequel ils ouvrent une session.

Lorsque vous activez le traitement en boucle, un ensemble cohérent de règles s'applique à tous les utilisateurs qui ouvrent une session sur un ordinateur particulier, peu importe l'emplacement de ces règles dans Active Directory.

Pour plus d'informations sur l'activation du traitement en boucle, consultez la documentation à propos de Microsoft Active Directory.

Remarque Le traitement en boucle est seulement une des approches existantes pour gérer les GPO dans Horizon 7. Vous devrez peut-être implémenter une approche différente.

Utilisation des fichiers de modèle d'administration de stratégie de groupe Horizon 7

Horizon 7 fournit plusieurs fichiers de modèle d'administration ADMX de stratégie de groupe propres à un composant. Vous pouvez optimiser et sécuriser des applications et des postes de travail distants en ajoutant les paramètres de stratégie des fichiers de modèle ADMX à un nouveau GPO ou à un GPO existant dans Active Directory.

Tous les fichiers ADMX qui fournissent des paramètres de stratégie de groupe pour Horizon 7 sont disponibles dans un fichier groupé `.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 le fichier 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`.

Les modèles de fichier ADMX d'Horizon 7 contiennent des stratégies de groupe Configuration d'ordinateur et Configuration d'utilisateur.

- Les stratégies Configuration d'ordinateur définissent des stratégies qui s'appliquent à tous les postes de travail distants, quelle que soit la personne qui se connecte au poste de travail.
- Les stratégies Configuration d'utilisateur définissent des stratégies qui s'appliquent à tous les utilisateurs, quel que soit l'application ou le poste de travail distant auquel ils se connectent. Les stratégies Configuration d'utilisateur remplacent les stratégies Configuration d'ordinateur équivalentes.

Microsoft Windows applique les stratégies au démarrage du poste de travail et lorsque les utilisateurs se connectent.

Fichiers de modèle ADMX Horizon 7

Les fichiers de modèle ADMX Horizon 7 fournissent des paramètres de stratégie de groupe qui permettent de contrôler et d'optimiser les composants Horizon 7.

Tableau 5-5. Fichiers de modèle ADMX Horizon

Nom du modèle	Fichier de modèle	Description
Configuration d'Horizon Agent	`vdm_agent.admx`	Contient des paramètres de stratégie liés aux composants d'authentification et d'environnement d'Horizon Agent.
Configuration d'Horizon Client	`vdm_client.admx`	Contient des paramètres de stratégie liés à Horizon Client pour Windows. Les clients qui se connectent de l'extérieur du domaine d'hôte du Serveur de connexion ne sont pas affectés par les stratégies appliquées à Horizon Client. Consultez le document *Utilisation de VMware Horizon Client pour Windows*.
Redirection URL de VMware Horizon	`urlRedirection-enUS.admx`	Contient des paramètres de stratégie liés à la fonctionnalité de redirection de contenu URL. Si vous ajoutez ce modèle à un GPO pour un pool de postes de travail distants ou un pool d'applications, certains liens URL sur lesquels vous cliquez à l'intérieur des applications ou des postes de travail distants peuvent être redirigés vers un client Windows et ouverts dans un navigateur côté client. Si vous ajoutez ce modèle à un GPO côté client, lorsqu'un utilisateur clique sur certains liens URL dans un système client Windows, l'URL peut être ouverte dans une application ou un poste de travail distant. Reportez-vous à la section Chapitre 3, « Configuration de la redirection de contenu URL », page 59 et consultez le document *Utilisation de VMware Horizon Client pour Windows*.
Configuration du Serveur de connexion	`vdm_server.admx`	Contient des paramètres de stratégie liés au Serveur de connexion. Consultez le document *Administration de View*.
configuration commune de View	`vdm_common.admx`	Contient des paramètres de stratégie communs à tous les composants Horizon. Consultez le document *Administration de View*.
variables de session PCoIP	`pcoip.admx`	Contient des paramètres de stratégie liés au protocole d'affichage PCoIP.
Variables de session de client PCoIP	`pcoip.client.admx`	Contient des paramètres de stratégie liés au protocole d'affichage PCoIP qui affectent Horizon Client pour Windows. Consultez le document *Utilisation de VMware Horizon Client pour Windows*.
Configuration d'Horizon Persona Management	`ViewPM.admx`	Contient des paramètres de stratégie liés à Horizon Persona Management. Reportez-vous au document *Configuration des postes de travail virtuels dans Horizon 7*.

Tableau 5-5. Fichiers de modèle ADMX Horizon (suite)

Nom du modèle	Fichier de modèle	Description
Services Bureau à distance	`vmware_rdsh.admx`	Contient des paramètres de stratégie liés aux services Bureau à distance. Reportez-vous à la section « Utilisation de stratégies de groupe des services Bureau à distance », page 144.
Configuration de l'Audio/Vidéo en temps réel	`vdm_agent_rtav.admx`	Contient des paramètres de stratégie liés à des webcams qui sont utilisées avec la fonctionnalité d'Audio/Vidéo en temps réel. Reportez-vous à la section « Paramètres de stratégie de groupe de l'Audio/Vidéo en temps réel », page 34.
Redirection de scanner	`vdm_agent_scanner.admx`	Contient des paramètres de stratégie liés à des périphériques d'analyse qui sont redirigés pour une utilisation dans des applications et des postes de travail publiés. Reportez-vous à la section « Paramètres de stratégie de groupe de redirection de scanner », page 40.
Redirection de port série	`vdm_agent_serialport.admx`	Contient des paramètres de stratégie liés à des ports série (COM) qui sont redirigés pour une utilisation dans des postes de travail virtuels. Reportez-vous à la section « Paramètres de stratégie de groupe de redirection de port série », page 47.

Ajouter les fichiers de modèle d'administration ADMX à Active Directory

Vous pouvez ajouter les paramètres de stratégie pour des fonctionnalités de poste de travail distant spécifiques dans les fichiers ADMX d'Horizon 7 à des objets de stratégie de groupe (GPO) dans Active Directory.

Prérequis

- Vérifiez que l'option d'installation de la fonctionnalité de poste de travail distant pour laquelle vous appliquez la stratégie est installée sur vos postes de travail et vos hôtes RDS. Les paramètres de stratégie de groupe n'ont aucun effet si la fonctionnalité de poste de travail distant n'est pas installée. Consultez le document Configuration pour plus d'informations sur l'installation d'Horizon Agent.
- Créez des GPO pour les fonctionnalités de poste de travail distant auxquelles vous voulez appliquer les paramètres de stratégie de groupe et liez-les à l'UO qui contient vos hôtes RDS.
- Vérifiez le nom du fichier de modèle d'administration ADMX que vous voulez ajouter à Active Directory. Reportez-vous à la section « Fichiers de modèle ADMX Horizon 7 », page 110.
- Vérifiez que la fonctionnalité Gestion de stratégie de groupe est disponible sur votre serveur Active Directory.

  La procédure d'ouverture de la Console de gestion de stratégie de groupe varie entre les versions Windows 2012, Windows 2008 et Windows 2003 d'Active Directory. Reportez-vous à la section « Créer des GPO pour les stratégies de groupe Horizon 7 », page 193.

Procédure

1 Téléchargez le fichier Horizon 7 GPO Bundle `.zip` 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 GPO Bundle.

   Le fichier se nomme `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, où *x.x.x* est la version et *yyyyyyy* le numéro de build. Tous les fichiers ADMX qui fournissent des paramètres de stratégie de groupe pour Horizon 7 sont disponibles dans ce fichier.

2 Décompressez le fichier `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip` et copiez les fichiers ADMX sur votre hôte Active Directory ou RDS.

   a Copiez les fichiers `.admx`, ainsi que le dossier `en-US` dans le dossier `%systemroot%\PolicyDefinitions` sur votre hôte Active Directory ou RDS.

   b Copiez les fichiers de ressources de la langue (`.adml`) dans le sous-dossier correspondant dans `%systemroot%\PolicyDefinitions\` sur votre hôte Active Directory ou RDS.

3 Sur l'hôte Active Directory, ouvrez l'Éditeur de gestion de stratégie de groupe et entrez le chemin vers les fichiers de modèle où ils apparaissent dans l'éditeur après l'installation.

   Sur un hôte RDS individuel, vous pouvez ouvrir l'Éditeur de stratégie de groupe locale avec l'utilitaire `gpedit.msc`.

Suivant

Configurez les paramètres de stratégie de groupe.

Paramètres du modèle d'administration ADMX pour la configuration d' Horizon Agent

Le fichier de modèle d'administration ADMX pour la configuration d'Horizon Agent (`vdm_agent.admx`) contient des paramètres de stratégie liés aux composants d'authentification et d'environnement d'Horizon Agent.

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`.

Le tableau suivant décrit les paramètres de stratégie du fichier de modèle d'administration ADMX pour la configuration d'Horizon Agent qui ne sont pas utilisés avec des périphériques USB. Le modèle contient les paramètres de Configuration d'ordinateur et de Configuration d'utilisateur. Le paramètre de Configuration d'utilisateur remplace le paramètre de Configuration d'ordinateur équivalent.

Tableau 5-6. Paramètres du modèle pour la configuration d' Horizon Agent

Paramètre	Ordinateur	Utilisateur	Propriétés
`AllowDirectRDP`	X		Détermine si les clients qui ne sont pas des périphériques Horizon Client peuvent se connecter directement à des postes de travail distants avec RDP. Lorsque ce paramètre est désactivé, l'agent autorise uniquement les connexions gérées par Horizon via Horizon Client. Lorsque vous vous connectez à un poste de travail distant à partir d'Horizon Client pour Mac, ne désactivez pas le paramètre `AllowDirectRDP`. Si ce paramètre est désactivé, la connexion échoue avec une erreur `Access is denied (Accès refusé)`. Par défaut, lorsqu'un utilisateur a ouvert une session de poste de travail Horizon 7, vous pouvez utiliser RDP pour vous connecter à la machine virtuelle à l'extérieur d'Horizon 7. La connexion RDP met fin à la session de poste de travail Horizon 7 et les données et paramètres non enregistrés de l'utilisateur risquent d'être perdus. L'utilisateur ne peut pas se connecter au poste de travail tant que la connexion RDP externe est fermée. Pour éviter cette situation, désactivez le paramètre `AllowDirectRDP`. **Important** Les services Bureau à distance doivent s'exécuter sur le système d'exploitation invité de chaque poste de travail. Vous pouvez utiliser ce paramètre pour empêcher les utilisateurs de faire des connexions RDP directes sur leurs postes de travail. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration d'agent** dans l'Éditeur de gestion de stratégie de groupe. Ce paramètre est activé par défaut.
`AllowSingleSignon`	X		Détermine si l'authentification unique (Single Sign-On, SSO) est utilisée pour connecter les utilisateurs aux postes de travail et aux applications. Lorsque ce paramètre est activé, les utilisateurs doivent entrer leurs informations d'identification une seule fois, lorsqu'ils se connectent au serveur. Lorsqu'il est désactivé, les utilisateurs doivent s'authentifier de nouveau lorsque la connexion à distance est effectuée. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration d'agent** dans l'Éditeur de gestion de stratégie de groupe. Ce paramètre est activé par défaut.
`CommandsToRunOnConnect`	X		Spécifie une liste de commandes ou de scripts de commande à exécuter lorsqu'une session est connectée pour la première fois. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration d'agent** dans l'Éditeur de gestion de stratégie de groupe. Pour plus d'informations, reportez-vous à « Exécution de commandes sur des postes de travail Horizon », page 123.
`CommandsToRunOnDisconnect`	X		Spécifie la liste des commandes ou des scripts de commande à exécuter lorsqu'une session est déconnectée. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration d'agent** dans l'Éditeur de gestion de stratégie de groupe. Pour plus d'informations, reportez-vous à « Exécution de commandes sur des postes de travail Horizon », page 123.

Tableau 5-6. Paramètres du modèle pour la configuration d' Horizon Agent (suite)

Paramètre	Ordinateur	Utilisateur	Propriétés
`CommandsToRunOnReconnect`	X		Spécifie une liste de commandes ou de scripts de commande à exécuter lorsqu'une session est reconnectée après une déconnexion. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration d'agent** dans l'Éditeur de gestion de stratégie de groupe. Pour plus d'informations, reportez-vous à « Exécution de commandes sur des postes de travail Horizon », page 123.
`ConnectionTicketTimeout`	X		Spécifie la durée en secondes pendant laquelle le ticket de connexion Horizon est valide. Les périphériques Horizon Client utilisent un ticket de connexion pour la vérification et l'authentification unique lorsqu'ils se connectent à l'agent. Pour des raisons de sécurité, un ticket de connexion est valide pendant une durée limitée. Lorsqu'un utilisateur se connecte à un poste de travail distant, l'authentification doit avoir lieu pendant le délai d'expiration du ticket de connexion sinon la session expire. Si ce paramètre n'est pas configuré, le délai d'expiration par défaut est de 900 secondes. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration d'agent** dans l'Éditeur de gestion de stratégie de groupe.
`CredentialFilterExceptions`	X		Spécifie les fichiers exécutables qui ne sont pas autorisés à charger l'agent CredentialFilter. Les noms de fichier ne doivent pas contenir de chemin d'accès ou de suffixe. Utilisez un point-virgule pour séparer plusieurs noms de fichier. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration d'agent** dans l'Éditeur de gestion de stratégie de groupe.
`Disable Time Zone Synchronization`	X	X	Détermine si le fuseau horaire du poste de travail Horizon est synchronisé avec celui du client connecté. Un paramètre activé ne s'applique que si le paramètre `Désactiver le transfert de fuseau horaire` de la stratégie de configuration d'Horizon Client n'est pas définie sur désactivé. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration d'agent** dans l'Éditeur de gestion de stratégie de groupe. Ce paramètre est désactivé par défaut.
`DPI Synchronization`	X	X	Ajuste le paramètre DPI à l'échelle du système de la session distante. Lorsque ce paramètre est activé ou non configuré, le paramètre DPI à l'échelle du système de la session distante est défini pour correspondre au paramètre DPI correspondant sur le système d'exploitation client. Lorsque ce paramètre est désactivé, le paramètre DPI à l'échelle du système de la session distante ne change jamais. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration d'agent** dans l'Éditeur de gestion de stratégie de groupe. Ce paramètre n'est pas configuré par défaut. **Remarque** Ce paramètre s'applique uniquement à la version 7.0.2 ou aux versions ultérieures et aux clients Windows sur lesquels est installé Horizon Client 4.2 ou version ultérieure.

Tableau 5-6. Paramètres du modèle pour la configuration d' Horizon Agent (suite)

Paramètre	Ordinateur	Utilisateur	Propriétés
`Enable multi-media acceleration`	X		Détermine si la redirection multimédia (MMR) est activée sur le poste de travail distant. MMR est un filtre de Windows Media Foundation qui permet de transférer des données multimédia de codecs spécifiques sur le système distant au client directement via un socket TCP. Les données sont ensuite décodées directement sur le client, lorsqu'elles sont lues. Vous pouvez désactiver MMR si le client ne dispose pas de ressources suffisantes pour gérer le décodage multimédia local. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration d'agent** dans l'Éditeur de gestion de stratégie de groupe. Ce paramètre est activé par défaut.
`Force MMR to use software overlay`	X		MMR tente d'utiliser la superposition matérielle pour lire la vidéo afin d'optimiser les performances. Lorsque vous utilisez plusieurs écrans, la superposition matérielle n'existe que sur l'un des écrans, le principal ou celui sur lequel WMP a été démarré. Si WMP est glissé sur un autre écran, la vidéo s'affiche sous la forme d'un rectangle noir. Utilisez cette option pour forcer MMR à utiliser une superposition logicielle qui fonctionne sur tous les écrans. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration d'agent** dans l'Éditeur de gestion de stratégie de groupe. Ce paramètre n'est pas configuré par défaut.
`Single sign-on retry timeout`	X		Spécifie la durée, en millisecondes, après laquelle l'authentification unique est de nouveau tentée. Définissez la valeur sur 0 pour désactiver la nouvelle tentative d'authentification unique. La valeur par défaut est de 5 000 millisecondes. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration d'agent** dans l'Éditeur de gestion de stratégie de groupe. Ce paramètre n'est pas configuré par défaut.
`ShowDiskActivityIcon`	X		Ce paramètre n'est pas pris en charge dans cette version. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration d'agent** dans l'Éditeur de gestion de stratégie de groupe.
`Toggle Display Settings Control`	X		Détermine si l'onglet **Settings (Paramètres)** du panneau de configuration **Display (Affichage)** est désactivé lorsqu'une session client utilise le protocole d'affichage PCoIP. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration d'agent** dans l'Éditeur de gestion de stratégie de groupe. Ce paramètre est activé par défaut.

Tableau 5-6. Paramètres du modèle pour la configuration d' Horizon Agent (suite)

Paramètre	Ordinateur	Utilisateur	Propriétés
`UnAuthenticatedAccessEnabled`			Active ou désactive la fonctionnalité d'accès non authentifié. Lorsque ce paramètre est activé, les utilisateurs ne disposant pas d'un accès authentifié peuvent accéder à des applications publiées à partir d'Horizon Client sans nécessiter d'informations d'identification Active Directory. Lorsque ce paramètre est désactivé, les utilisateurs ne disposant pas d'un accès authentifié ne peuvent pas accéder à des applications publiées à partir d'Horizon Client sans nécessiter d'informations d'identification Active Directory. Vous devez redémarrer l'hôte RDS pour que ce paramètre prenne effet. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Configuration d'agent** dans l'Éditeur de gestion de stratégie de groupe. Ce paramètre est activé par défaut.
`Send updates for empty or offscreen windows`	X		Spécifie si le client reçoit des mises à jour sur les fenêtres vides ou en dehors de l'écran. Lorsque ce paramètre est désactivé, les informations sur les fenêtres inférieures à 2 x 2 pixels ou se trouvant en dehors de l'écran ne sont pas envoyées au client. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Unity Touch et applications hébergées** dans l'Éditeur de gestion de stratégie de groupe. Ce paramètre est désactivé par défaut.
`Enable Unity Touch`	X		Détermine si la fonctionnalité Unity Touch est activée sur le poste de travail distant. Unity Touch prend en charge la livraison d'applications distantes dans Horizon et permet aux utilisateurs d'appareils mobiles d'accéder aux applications dans la barre latérale Unity Touch. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Unity Touch et applications hébergées** dans l'Éditeur de gestion de stratégie de groupe. Ce paramètre est activé par défaut.
`Enable system tray redirection for Hosted Apps`	X		Détermine si la redirection de la barre d'état système est activée pendant qu'un utilisateur exécute des applications distantes. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Unity Touch et applications hébergées** dans l'Éditeur de gestion de stratégie de groupe. Ce paramètre est activé par défaut.

Tableau 5-6. Paramètres du modèle pour la configuration d' Horizon Agent (suite)

Paramètre	Ordinateur	Utilisateur	Propriétés
`Enable user profile customization for Hosted Apps`	X	X	Spécifie s'il faut personnaliser le profil d'utilisateur lorsque des applications distantes sont utilisées. Si ce paramètre est activé, un profil d'utilisateur est généré, le thème Windows est personnalisé et les applications de démarrage sont enregistrées. Ce paramètre Configuration ordinateur se trouve dans le dossier **Configuration de VMware View Agent > Unity Touch et applications hébergées** dans l'Éditeur de gestion de stratégie de groupe. Le paramètre Configuration utilisateur se trouve dans le dossier **Configuration de VMware View Agent > Sécurité d'agent > Unity Touch et applications hébergées** dans l'Éditeur de gestion de stratégie de groupe. Ce paramètre est désactivé par défaut.
`Limit usage of Windows hooks`	X		Désactive la plupart des hooks lorsque des applications distantes ou Unity Touch sont utilisés. Ce paramètre est conçu pour les applications ayant des problèmes de compatibilité lorsque des hooks de niveau système d'exploitation sont définis. Par exemple, l'activation de ce paramètre désactive l'utilisation de la plupart des hooks d'accessibilité et contenus dans un processus actifs de Windows. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Unity Touch et applications hébergées** dans l'Éditeur de gestion de stratégie de groupe. Ce paramètre est désactivé par défaut, ce qui signifie que tous les hooks préférés sont utilisés.
`Accept SSL encrypted framework channel`		X	Active le canal d'infrastructure chiffré SSL. Voici les options disponibles : ■ **Désactiver** : désactivez SSL. ■ **Activer** : activez SSL. Autorisez les clients hérités à se connecter sans SSL. ■ **Appliquer** : activez SSL. Refusez les connexions des clients hérités. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Sécurité d'agent** dans l'Éditeur de gestion de stratégie de groupe. Ce paramètre n'est pas configuré par défaut. La valeur par défaut est **Activer**.
`Default Proxy Server`	X		Paramètres de connexion à Internet Explorer par défaut du serveur proxy. Spécifie le serveur proxy à utiliser dans Options Internet > Paramètres de réseau local. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Transparence IP de VMware Client** dans l'Éditeur de gestion de stratégie de groupe. Ce paramètre n'est pas activé par défaut.

Tableau 5-6. Paramètres du modèle pour la configuration d' Horizon Agent (suite)

Paramètre	Ordinateur	Utilisateur	Propriétés
`Enable`	X		Active Transparence IP de VMware Client. Les connexions à distance à Internet Explorer utilisent l'adresse IP du client au lieu de l'adresse IP de la machine de poste de travail distant. Ce paramètre prend effet lors de la prochaine connexion. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Transparence IP de VMware Client** dans l'Éditeur de gestion de stratégie de groupe. Si l'option de configuration personnalisée Transparence IP de VMware Client est sélectionnée dans le programme d'installation d'Horizon Agent, ce paramètre est activé par défaut.
`Default auto detect proxy`	X		Paramètre de connexion à Internet Explorer par défaut. Active **Détecter automatiquement les paramètres** dans Options Internet > Paramètres de réseau local. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Transparence IP de VMware Client** dans l'Éditeur de gestion de stratégie de groupe. Ce paramètre n'est pas activé par défaut.
`Set proxy for Java applet`	X		Définit le proxy pour les applets Java. Voici les options disponibles : ■ **Utiliser Transparence IP de Client pour le proxy Java** : ordonne à une connexion à distance d'utiliser l'adresse IP du client au lieu de l'adresse IP de la machine de poste de travail distant pour les applets Java. ■ **Utiliser la connexion directe pour le proxy Java** : utilise une connexion directe pour contourner le paramètre de navigateur pour les applets Java. ■ **Utiliser la valeur par défaut pour le proxy Java** : restaure les paramètres du proxy Java d'origine. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Transparence IP de VMware Client** dans l'Éditeur de gestion de stratégie de groupe. Ce paramètre n'est pas activé par défaut.
`Enable flash multi-media redirection`	X		Spécifie si la redirection Flash est activée sur l'agent. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > VMware FlashMMR** dans l'Éditeur de gestion de stratégie de groupe.
`Minimum rect size to enable FlashMMR`	X		Spécifie la taille de rectangle minimale pour activer la redirection Flash. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > VMware FlashMMR** dans l'Éditeur de gestion de stratégie de groupe. La largeur par défaut est de 320 pixels et la hauteur par défaut est de 200 pixels.

Tableau 5-6. Paramètres du modèle pour la configuration d' Horizon Agent (suite)

Paramètre	Ordinateur	Utilisateur	Propriétés
`Definition for FlashMMR url list usage`		X	Définit la règle de liste blanche ou noire qui autorise ou non des URL à utiliser la redirection Flash. Si vous sélectionnez **Activer une liste blanche** dans le menu déroulant **Définition pour l'utilisation de la liste d'URL FlashMMR**, seules les URL dans la liste d'URL sont activées pour utiliser la redirection Flash. Si vous sélectionnez **Activer une liste noire** dans le menu déroulant **Définition pour l'utilisation de la liste d'URL FlashMMR**, les URL dans la liste d'URL ne peuvent pas utiliser la redirection Flash. Spécifiez la liste d'URL dans le paramètre de stratégie de groupe `Hosts Url list to enable FlashMMR`. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > VMware FlashMMR** dans l'Éditeur de gestion de stratégie de groupe. Ce paramètre spécifie une liste blanche par défaut.
`Hosts Url list to enable FlashMMR`		X	Spécifie la liste d'URL autorisées ou non à utiliser la redirection Flash en fonction du paramètre de stratégie de groupe `Definition for FlashMMR url list usage`. Vous devez inclure **http://** ou **https://**. Vous pouvez utiliser des expressions régulières. Par exemple, vous pouvez spécifier **`https://*.google.com`** et **`http://www.cnn.com`**. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > VMware FlashMMR** dans l'Éditeur de gestion de stratégie de groupe.

Remarque Le paramètre `Connect using DNS Name` a été supprimé dans Horizon 6 version 6.1. Vous pouvez définir l'attribut LDAP d'Horizon 7, **pae-PreferDNS**, pour demander au Serveur de connexion Horizon de donner la préférence aux noms DNS lors de l'envoi des adresses de machines de poste de travail et d'hôtes RDS à des clients et des passerelles. Reportez-vous à « Donner la préférence aux noms DNS lorsque le Serveur de connexion Horizon renvoie des informations d'adresse » dans le document *Installation de View*.

Paramètres USB d' Horizon Agent

Reportez-vous à la section « Paramètres USB du modèle d'administration ADMX pour la configuration d'Horizon Agent », page 93.

Envoi d'informations sur le système client à des postes de travail distants

Lorsqu'un utilisateur se connecte ou se reconnecte à un poste de travail distant, Horizon Client recueille des informations sur le système client et le Serveur de connexion envoie ces informations au poste de travail distant.

Horizon Agent écrit les informations d'ordinateur client dans le chemin d'accès `HKCU\Volatile Environment` du registre système sur les postes de travail distants qui sont déployés sur des machines mono-utilisateur. Pour les postes de travail distants déployés dans des sessions RDS, Horizon Agent écrit les informations de l'ordinateur client dans le chemin d'accès `HKCU\Volatile Environment\`*x* du registre système, où *x* est l'ID de la session sur l'hôte RDS.

Si Horizon Client est exécuté dans une session de poste de travail distant, il envoie les informations sur le client physique plutôt que celles sur la machine virtuelle au poste de travail distant. Par exemple, si un utilisateur se connecte depuis son système client à un poste de travail distant, lance Horizon Client dans le poste de travail distant et se connecte à un autre poste de travail distant, l'adresse IP du système client physique est envoyée au deuxième poste de travail distant. On appelle cette fonctionnalité mode imbriqué ou scénario à deux sauts. Horizon Client envoie `ViewClient_Nested_Passthrough`, qui est défini sur 1, avec les informations sur le système client pour indiquer qu'il envoie les informations sur le mode imbriqué.

Remarque Avec Horizon Client 4.1, les informations sur le système client sont transmises au poste de travail de second saut lors de la connexion de protocole initiale. Avec Horizon Client 4.2 et versions ultérieures, les informations sur le système client sont également mises à jour si la connexion de protocole de premier saut se déconnecte et se reconnecte.

Vous pouvez ajouter des commandes aux paramètres de stratégie de groupe `CommandsToRunOnConnect`, `CommandsToRunOnReconnect` et `CommandsToRunOnDisconnect` d'Horizon Agent pour exécuter des commandes ou des scripts de commande qui lisent ces informations dans le registre système lorsque des utilisateurs se connectent et se reconnectent à des postes de travail. Pour plus d'informations, reportez-vous à « Exécution de commandes sur des postes de travail Horizon », page 123.

Tableau 5-7 décrit les clés de Registre qui contiennent des informations sur le système client et répertorie les types de postes de travail et de systèmes clients qui les prennent en charge. Si Oui s'affiche dans la colonne **Prend en charge le mode imbriqué**, cela indique que les informations sur le client physique (plutôt que celles sur la machine virtuelle) sont envoyées à un poste de travail de second saut.

Tableau 5-7. Informations sur le système client

Clé de Registre	Description	Prend en charge le mode imbriqué	Postes de travail pris en charge	Systèmes clients pris en charge
`ViewClient_IP_Address`	Adresse IP du système client.	Oui	VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
`ViewClient_MAC_Address`	Adresse MAC du système client.	Oui	VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac, Android
`ViewClient_Machine_Name`	Nom de machine du système client.	Oui	VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
`ViewClient_Machine_Domain`	Domaine du système client.	Oui	VDI (machine mono-utilisateur) RDS	Windows, Windows Store
`ViewClient_LoggedOn_Username`	Nom d'utilisateur utilisé pour se connecter au système client.		VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac
`ViewClient_LoggedOn_Domainname`	Nom de domaine utilisé pour se connecter au système client.		VDI (machine mono-utilisateur) RDS	Windows, Windows Store Pour les clients Linux et Mac, consultez `ViewClient_Machine_Domain`.`ViewClient_LoggedOn_Domainname` n'est pas donné par le client Linux ou Mac, car les comptes Linux et Mac ne sont pas liés à des domaines Windows.

Tableau 5-7. Informations sur le système client (suite)

Clé de Registre	Description	Prend en charge le mode imbriqué	Postes de travail pris en charge	Systèmes clients pris en charge
`ViewClient_Type`	Nom du client léger ou type de système d'exploitation du système client.	Oui	VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
`ViewClient_Broker_DNS_Name`	Nom DNS de l'instance du Serveur de connexion View.		VDI (machine mono-utilisateur) RDS	La valeur est envoyée directement par le Serveur de connexion View, elle n'est pas recueillie par Horizon Client.
`ViewClient_Broker_URL`	URL de l'instance du Serveur de connexion View.		VDI (machine mono-utilisateur) RDS	La valeur est envoyée directement par le Serveur de connexion View, elle n'est pas recueillie par Horizon Client.
`ViewClient_Broker_Tunneled`	État de la connexion tunnel du Serveur de connexion View qui peut être `true` (activé) ou `false` (désactivé).		VDI (machine mono-utilisateur) RDS	La valeur est envoyée directement par le Serveur de connexion View, elle n'est pas recueillie par Horizon Client.
`ViewClient_Broker_Tunnel_URL`	URL de la connexion tunnel du Serveur de connexion View, si la connexion tunnel est activée.		VDI (machine mono-utilisateur) RDS	La valeur est envoyée directement par le Serveur de connexion View, elle n'est pas recueillie par Horizon Client.
`ViewClient_Broker_Remote_IP_Address`	Adresse IP du système client qui est vue par l'instance de Serveur de connexion View.		VDI (machine mono-utilisateur) RDS	La valeur est envoyée directement par le Serveur de connexion View, elle n'est pas recueillie par Horizon Client.
`ViewClient_TZID`	ID du fuseau horaire Olson. Pour désactiver la synchronisation du fuseau horaire, activez le paramètre de stratégie de groupe `Disable Time Zone Synchronization` d'Horizon Agent.		VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac, Android, iOS
`ViewClient_Windows_Timezone`	Heure GMT standard. Pour désactiver la synchronisation du fuseau horaire, activez le paramètre de stratégie de groupe `Disable Time Zone Synchronization` d'Horizon Agent.		VDI (machine mono-utilisateur) RDS	Windows, Windows Store

Tableau 5-7. Informations sur le système client (suite)

Clé de Registre	Description	Prend en charge le mode imbriqué	Postes de travail pris en charge	Systèmes clients pris en charge
`ViewClient_Broker_DomainName`	Nom de domaine utilisé pour s'authentifier auprès du Serveur de connexion View.		VDI (machine mono-utilisateur) RDS	La valeur est envoyée directement par le Serveur de connexion View, elle n'est pas recueillie par Horizon Client.
`ViewClient_Broker_UserName`	Nom d'utilisateur utilisé pour s'authentifier auprès du Serveur de connexion View.		VDI (machine mono-utilisateur) RDS	La valeur est envoyée directement par le Serveur de connexion View, elle n'est pas recueillie par Horizon Client.
`ViewClient_Client_ID`	Spécifie l'`Unique Client HardwareId` utilisé comme lien vers la clé de licence.		VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
`ViewClient_Displays.Number`	Spécifie le nombre de moniteurs utilisés actuellement par le client.		VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
`ViewClient_Displays.Topology`	Spécifie la disposition, la résolution et les dimensions d'affichage du client.		VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
`ViewClient_Keyboard.Type`	Spécifie le type de clavier utilisé actuellement par le client. Par exemple : japonais, coréen.		VDI (machine mono-utilisateur) RDS	Windows
`ViewClient_Launch_SessionType`	Spécifie le type de session. Il peut s'agir d'un poste de travail ou d'une application.		VDI (machine mono-utilisateur) RDS	La valeur est envoyée directement par le Serveur de connexion View, elle n'est pas recueillie par Horizon Client.
`ViewClient_Mouse.Identifier`	Spécifie le type de souris.		VDI (machine mono-utilisateur) RDS	Windows
`ViewClient_Mouse.NumButtons`	Spécifie le nombre de boutons pris en charge par la souris.		VDI (machine mono-utilisateur) RDS	Windows
`ViewClient_Mouse.SampleRate`	Spécifie le taux, en rapports par seconde, auquel l'entrée d'une souris PS/2 est échantillonnée.		VDI (machine mono-utilisateur) RDS	Windows
`ViewClient_Protocol`	Spécifie le protocole en cours d'utilisation.		VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
`ViewClient_Language`	Spécifie la langue du système d'exploitation.		VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac, Android, iOS, Windows Store

Tableau 5-7. Informations sur le système client (suite)

Clé de Registre	Description	Prend en charge le mode imbriqué	Postes de travail pris en charge	Systèmes clients pris en charge
`ViewClient_Launch_Matched_Tags`	Spécifie une ou plusieurs balises.		VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
`ViewClient_Launch_ID`	Spécifie l'ID unique du pool de postes de travail ou d'applications.		VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
`ViewClient_Broker_Farm_ID`	Spécifie l'ID de batterie de serveurs du pool de postes de travail ou d'applications sur un hôte RDS.		RDS	Windows, Linux, Mac, Android, iOS, Windows Store

Remarque Les définitions de `ViewClient_LoggedOn_Username` et de `ViewClient_LoggedOn_Domainname` dans Tableau 5-7 s'appliquent à Horizon Client 2.2 pour Windows ou version ultérieure.

Pour Horizon Client 5.4 pour Windows ou version antérieure, `ViewClient_LoggedOn_Username` envoie le nom d'utilisateur entré dans Horizon Client, et `ViewClient_LoggedOn_Domainname` envoie le nom de domaine entré dans Horizon Client.

Horizon Client 2.2 pour Windows est une version postérieure à Horizon Client 5.4 pour Windows. À partir d'Horizon Client 2.2, les numéros de versions pour Windows correspondent aux versions d'Horizon Client sur d'autres systèmes d'exploitation et périphériques.

Exécution de commandes sur des postes de travail Horizon

Vous pouvez utiliser les paramètres de stratégie de groupe `CommandsToRunOnConnect`, `CommandsToRunOnReconnect` et `CommandsToRunOnDisconnect` d'Horizon Agent pour exécuter des commandes et des scripts de commande sur des postes de travail Horizon lorsque les utilisateurs se connectent, se reconnectent et se déconnectent.

Pour exécuter une commande ou un script de commande, ajoutez le nom de commande ou le chemin de fichier du script à la liste de commandes du paramètre de stratégie de groupe. Par exemple :

```
date
```

```
C:\Scripts\myscript.cmd
```

Pour exécuter des scripts qui requièrent un accès à la console, ajoutez en préfixe l'option `-C` ou `-c` suivie d'un espace. Par exemple :

```
-c C:\Scripts\Cli_clip.cmd
```

```
-C e:\procexp.exe
```

Les types de fichiers pris en charge sont `.CMD`, `.BAT` et `.EXE`. Les fichiers `.VBS` ne sont pas exécutés sauf s'ils sont analysés avec `cscript.exe` ou `wscript.exe`. Par exemple :

```
-C C:\WINDOWS\system32\wscript.exe C:\Scripts\checking.vbs
```

La longueur totale de la chaîne, y compris l'option `-C` ou `-c`, ne doit pas dépasser 260 caractères.

Paramètres de stratégie PCoIP

Le fichier de modèle d'administration ADMX PCoIP contient des paramètres de stratégie liés au protocole d'affichage PCoIP. Le fichier de modèle d'administration ADMX se nomme (`pcoip.admx`). Vous pouvez configurer des paramètres sur des valeurs par défaut, qui peuvent être remplacées par un administrateur, ou vous pouvez configurer des paramètres sur des valeurs ne pouvant pas être remplacées.

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`.

Le fichier de modèle d'administration ADMX pour les variables de session PCoIP contient deux sous-catégories :

Valeurs par défaut remplaçables par l'administrateur

Spécifie les valeurs par défaut du paramètre de stratégie PCoIP. Ces paramètres peuvent être remplacés par un administrateur. Ces paramètres inscrivent des valeurs de clé de Registre sur `HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin_defaults`. Tous ces paramètres se trouvent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Variables de session PCoIP > Valeurs par défaut remplaçables par l'administrateur** dans l'Éditeur de gestion des stratégies de groupe.

Paramètres non remplaçables par l'administrateur

Contient les mêmes paramètres que Valeurs par défaut remplaçables par l'administrateur, mais ces paramètres ne peuvent pas être remplacés par un administrateur. Ces paramètres inscrivent des valeurs de clé de Registre sur `HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin`. Tous ces paramètres se trouvent dans le dossier **Configuration utilisateur > Stratégies > Modèles d'administration > Variables de session PCoIP > Paramètres non remplaçables par l'administrateur** dans l'Éditeur de gestion des stratégies de groupe.

Le modèle contient les paramètres de Configuration d'ordinateur et de Configuration d'utilisateur.

Clés de Registre non liées à des stratégies

Si un paramètre de machine locale doit être appliqué et ne peut pas être placé sous `HKLM\Software\Policies\Teradici`, des paramètres de machine locale peuvent être placés dans des clés de Registre dans `HKLM\Software\Teradici`. Les mêmes clés de Registre peuvent être placées dans `HKLM\Software\Teradici` comme dans `HKLM\Software\Policies\Teradici`. Si la même clé de Registre est présente dans les deux emplacements, le paramètre dans `HKLM\Software\Policies\Teradici` remplace la valeur de machine locale.

Paramètres généraux PCoIP

Le fichier de modèle d'administration ADMX PCoIP contient des paramètres de stratégie de groupe qui configurent des paramètres généraux, tels que la qualité d'image PCoIP, les périphériques USB et les ports réseau.

Tous ces paramètres se trouvent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Variables de session PCoIP > Valeurs par défaut remplaçables par l'administrateur** dans l'Éditeur de gestion des stratégies de groupe.

Tous ces paramètres se trouvent également dans le dossier **Configuration utilisateur > Stratégies > Modèles d'administration > Variables de session PCoIP > Paramètres non remplaçables par l'administrateur** dans l'Éditeur de gestion des stratégies de groupe.

Tableau 5-8. Paramètres de stratégie généraux PCoIP

Paramètre	Description
`Configure PCoIP event log cleanup by size in MB`	Active la configuration du nettoyage du journal des événements PCoIP par taille en Mo. Lorsque cette stratégie est configurée, le paramètre contrôle la taille que peut prendre un fichier journal avant d'être nettoyé. Pour une valeur de *m* différente de zéro, les fichiers journaux dont la taille est supérieure à *m* Mo sont supprimés automatiquement et de manière silencieuse. La valeur 0 indique qu'aucun nettoyage de fichier par taille n'est effectué. Lorsque cette stratégie est désactivée ou non configurée, la valeur par défaut du nettoyage du journal des événements par taille est de 100 Mo. Le nettoyage du fichier journal s'effectue une seule fois au démarrage d'une session. Tout changement apporté au paramètre ne sera appliqué qu'à l'ouverture de la prochaine session.
`Configure PCoIP event log cleanup by time in days`	Active la configuration du nettoyage du journal des événements PCoIP par durée en jours. Lorsque cette stratégie est configurée, le paramètre contrôle le nombre de jours qui peuvent s'écouler avant que le fichier journal soit nettoyé. Pour une valeur de *n* différente de zéro, les fichiers journaux antérieurs à *n* jours sont supprimés automatiquement et de manière silencieuse. La valeur 0 indique qu'aucun nettoyage de fichier par durée n'est effectué. Lorsque cette stratégie est désactivée ou non configurée, la valeur par défaut du nettoyage du journal des événements est de 7 jours. Le nettoyage du fichier journal s'effectue une seule fois au démarrage d'une session. Tout changement apporté au paramètre ne sera appliqué qu'à l'ouverture de la prochaine session.
`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 5-8. Paramètres de stratégie généraux PCoIP (suite)

Paramètre	Description
`Configure PCoIP image quality levels`	Contrôle comment PCoIP rend les images lors de périodes de surcharge du réseau. Les valeurs **Qualité d'image minimale**, **Qualité d'image initiale maximale** et **Fréquence d'image maximale** interagissent pour contrôler précisément des environnements contraints en termes de bande passante réseau. Utilisez la valeur **Qualité d'image minimale** pour équilibrer la qualité d'image et la fréquence d'image lorsque la bande passante est limitée. Vous pouvez spécifier une valeur comprise entre 30 et 100. La valeur par défaut est 40. Une valeur inférieure permet d'utiliser des fréquences d'image élevées, mais avec un affichage d'une qualité potentiellement inférieure. Une valeur supérieure fournit une qualité d'image supérieure, mais avec des fréquences d'image potentiellement inférieures lorsque la bande passante réseau est contrainte. Lorsque la bande passante réseau n'est pas contrainte, PCoIP conserve la qualité maximale quelle que soit cette valeur. Utilisez la valeur **Qualité d'image initiale maximale** pour réduire les pics de bande passante réseau requis par PCoIP en limitant la qualité initiale des régions modifiées de l'image affichée. Vous pouvez spécifier une valeur comprise entre 30 et 100. La valeur par défaut est 80. Une valeur inférieure réduit la qualité d'image des modifications de contenu et diminue les exigences de bande passante maximale. Une valeur supérieure augmente la qualité d'image des modifications de contenu et augmente les exigences de bande passante maximale. Les régions non modifiées de l'image entraînent progressivement une qualité sans perte (parfaite) quelle que soit cette valeur. Une valeur de 80 ou moins permet d'utiliser au mieux la bande passante disponible. La valeur **Qualité d'image minimale** ne peut pas dépasser la valeur **Qualité d'image initiale maximale**. Utilisez la valeur **Fréquence d'image maximale** pour gérer la bande passante moyenne consommée par utilisateur en limitant le nombre d'actualisations d'écran par seconde. Vous pouvez spécifier une valeur comprise entre 1 et 120 images par seconde. La valeur par défaut est 30. Une valeur supérieure peut utiliser plus de bande passante mais fournit moins de gigue, ce qui permet des transitions plus homogènes entre les images, comme dans une vidéo. Une valeur inférieure utilise moins de bande passante mais entraîne plus de gigue. Ces valeurs de qualité d'image ne s'appliquent qu'à l'hôte léger et n'ont aucun effet sur un client léger. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les valeurs par défaut sont utilisées. Lorsque ce paramètre est modifié lors d'une session PCoIP active, le nouveau paramètre prend effet immédiatement.
`Configure frame rate vs image quality preference`	Configurez la préférence pour la fréquence d'images et la qualité d'image entre 0 (fréquence d'images la plus élevée) et 100 (qualité d'image la plus élevée). Si cette stratégie est désactivée ou non configurée, la valeur par défaut est 50. Une valeur supérieure (max : 100) signifie que vous préférez une qualité d'image élevée même si la fréquence d'images est hachée. Une valeur inférieure (min : 0) signifie que vous préférez une expérience fluide avec une qualité d'image agressive. Ce paramètre peut fonctionner avec le GPO `Configure PCoIP image quality levels`, qui détermine le niveau de qualité d'image initial maximal et le niveau de qualité d'image minimal. Alors que la `Frame rate and image quality preference` peut ajuster le niveau de qualité d'image de chaque image, elle ne peut pas dépasser le seuil de niveau de qualité maximal/minimal configuré par le GPO `Configure PCoIP image quality levels`. Lorsque cette stratégie est modifiée au cours de l'exécution, elle peut prendre effet immédiatement.

Tableau 5-8. Paramètres de stratégie généraux 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 **Disable AES-128-GCM encryption (Désactiver le cryptage AES-128-GCM)** est toujours remplacée pour que le cryptage AES-128-GCM soit activé. 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. Si les deux points de terminaison sont configurés pour prendre en charge ces trois algorithmes et que la connexion n'utilise pas de passerelle de sécurité (Security Gateway, SG), l'algorithme SALSA20 est négocié et utilisé. En revanche, si la connexion utilise une passerelle de sécurité (SG), l'algorithme SALSA20 est désactivé automatiquement et c'est l'algorithme AES128 qui est négocié et utilisé. Si l'un des points de terminaison ou la passerelle de sécurité désactive l'algorithme SALSA20 et que l'un des points de terminaison désactive l'algorithme AES128, c'est l'algorithme AES256 qui est alors négocié et utilisé.

Tableau 5-8. Paramètres de stratégie généraux PCoIP (suite)

Paramètre	Description
`Configure PCoIP USB allowed and unallowed device rules`	Spécifie les périphériques USB autorisés et interdits pour les sessions PCoIP qui utilisent un client zéro exécutant le microprogramme Teradici. Les périphériques USB utilisés dans des sessions PCoIP doivent apparaître dans la table d'autorisation USB. Les périphériques USB qui apparaissent dans la table d'interdiction USB ne peuvent pas être utilisés dans des sessions PCoIP. Vous pouvez définir un maximum de 10 règles d'autorisation USB et un maximum de 10 règles d'interdiction USB. Séparez les valeurs avec le caractère de barre verticale (|). Chaque règle peut être une combinaison d'un ID de fournisseur (VID) et d'un ID de produit (PID), ou une règle peut décrire une classe de périphériques USB. Une règle de classe peut autoriser ou interdire une classe de périphériques entière, une seule sous-classe ou un protocole dans une sous-classe. Le format d'une combinaison de règle VID/PID est **`1xxxxyyyy`**, où **`xxxx`** est le VID au format hexadécimal et **`yyyy`** le PID au format hexadécimal. Par exemple, la règle pour autoriser ou bloquer un périphérique avec le VID **`0x1a2b`** et le PID **`0x3c4d`** est **`11a2b3c4d`**. Pour des règles de classe, utilisez l'un des formats suivants : **Autoriser tous les périphériques USB** — Format : **`23XXXXXX`** Exemple : **`23XXXXXX`** **Autoriser tous les périphériques USB avec un ID de classe spécifique** — Format : **`22`*`class`*`XXXX`** Exemple : **`22aaXXXX`** **Autoriser une sous-classe spécifique** — Format : **`21`*`class-subclass`*`XX`** Exemple : **`21aabbXX`** **Autoriser un protocole spécifique** — Format : **`20`*`class-subclass-protocol`*** Exemple : **`20aabbcc`** Par exemple, la chaîne d'autorisation USB pour autoriser les périphériques HID USB (souris et clavier) (ID de classe 0x03) et les webcams (ID de classe 0x0e) est **`2203XXXX|220eXXXX`**. La chaîne d'interdiction USB pour interdire les périphériques de stockage de masse USB (ID de classe 0x08) est **`2208XXXX`**. Une chaîne d'autorisation USB vide signifie qu'aucun périphérique USB n'est autorisé. Une chaîne d'interdiction USB vide signifie qu'aucun périphérique USB n'est interdit. Ce paramètre s'applique à Horizon Agent uniquement et seulement lorsque le poste de travail distant est dans une session avec un client ultra léger qui exécute le micrologiciel Teradici. L'utilisation de périphérique est négociée entre les points de terminaison. Par défaut, tous les périphériques sont autorisés et aucun n'est interdit.

Tableau 5-8. Paramètres de stratégie généraux PCoIP (suite)

Paramètre	Description
`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_vdpvcbridge`**. 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 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**.

Tableau 5-8. Paramètres de stratégie généraux PCoIP (suite)

Paramètre	Description
`Configure the TCP port to which the PCoIP host binds and listens`	Spécifie le port TCP de l'agent lié par des hôtes PCoIP logiciels. La valeur du port TCP spécifie le port TCP de base auquel l'agent tente de se lier. La valeur de plage du port TCP détermine le nombre de ports supplémentaires à essayer si le port de base n'est pas disponible. La plage du port doit être comprise entre 1 et 10. 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 4172 et que la plage du port est 10, la plage s'étend de 4172 à 4182. Ne définissez pas la taille de la plage de ports sur 0, car cela entraînera un échec de connexion lorsque l'utilisateur se connectera au poste de travail avec le protocole d'affichage PCoIP. Horizon Client renvoie le message d'erreur `Le protocole d'affichage de ce poste de travail n'est pas actuellement disponible. Contactez votre administrateur système`. Ce paramètre s'applique à Horizon Agent uniquement. Sur des machines mono-utilisateur, le port TCP de base par défaut est 4172 dans View 4.5 et version ultérieure. Le port de base par défaut est 50002 dans View 4.0.*x* et version antérieure. Par défaut, la plage de port est 1. Sur des hôtes RDS, le port TCP de base par défaut est 4173. Lorsque PCoIP est utilisé avec des hôtes RDS, un port PCoIP distinct est utilisé pour chaque connexion utilisateur. La plage de ports par défaut qui est utilisée par le service Bureau à distance est suffisamment étendue pour gérer le nombre maximal de connexions utilisateurs simultanées prévu. **Important** Nous vous recommandons de ne pas utiliser ce paramètre de stratégie pour modifier la plage de ports par défaut sur des hôtes RDS ou pour changer la valeur du port TCP par défaut qui est de 4173. Mais surtout, ne définissez pas la valeur du port TCP sur 4172. La réinitialisation de cette valeur à 4172 affecterait les performances PCoIP dans les session RDS.
`Configure the UDP port to which the PCoIP host binds and listens`	Spécifie le port UDP de l'agent lié par des hôtes PCoIP logiciels. La valeur du port UDP spécifie le port UDP de base auquel l'agent tente de se lier. 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 du port doit être comprise entre 1 et 10. Ne définissez pas la taille de la plage de ports sur 0, car cela entraînera un échec de connexion lorsque l'utilisateur se connectera au poste de travail avec le protocole d'affichage PCoIP. Horizon Client renvoie le message d'erreur `Le protocole d'affichage de ce poste de travail n'est pas actuellement disponible. Contactez votre administrateur système`. 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 4172 et que la plage du port est 10, la plage s'étend de 4172 à 4182. Ce paramètre s'applique à Horizon Agent uniquement. Sur des machines mono-utilisateur, le port UDP de base par défaut est 4172 pour View 4.5 et versions ultérieures, et 50002 pour View 4.0.*x* et version antérieure. Par défaut, la plage de port est 10. Sur des hôtes RDS, le port UDP de base par défaut est 4173. Lorsque PCoIP est utilisé avec des hôtes RDS, un port PCoIP distinct est utilisé pour chaque connexion utilisateur. La plage de ports par défaut qui est utilisée par le service Bureau à distance est suffisamment étendue pour gérer le nombre maximal de connexions utilisateurs simultanées prévu. **Important** Nous vous recommandons de ne pas utiliser ce paramètre de stratégie pour modifier la plage de ports par défaut sur des hôtes RDS ou pour changer la valeur du port UDP par défaut qui est de 4173. Mais surtout, ne définissez pas la valeur du port UDP sur 4172. La réinitialisation de cette valeur à 4172 affecterait les performances PCoIP dans les session RDS.

Tableau 5-8. Paramètres de stratégie généraux PCoIP (suite)

Paramètre	Description
`Enable access to a PCoIP session from a vSphere console`	Détermine s'il est nécessaire d'autoriser une console vSphere Client à afficher une session PCoIP active et à envoyer l'entrée au poste de travail. Par défaut, lorsqu'un client est attaché via PCoIP, l'écran de la console vSphere Client est vide et la console ne peut pas envoyer l'entrée. Le paramètre par défaut garantit qu'un utilisateur malveillant ne peut pas voir le poste de travail de l'utilisateur ou fournir d'entrées sur l'hôte localement lorsqu'une session distante PCoIP est active. Ce paramètre s'applique à Horizon Agent uniquement. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, l'accès à la console n'est pas autorisé. Lorsque ce paramètre est activé, la console affiche la session PCoIP et l'entrée de console est autorisée. Lorsque ce paramètre est activé, la console peut afficher une session PCoIP exécutée sur un système Windows 7 uniquement lorsque la machine virtuelle Windows 7 est le matériel version v8. La version matérielle v8 est disponible uniquement sur ESXi 5.0 et version ultérieure. A contrario, l'entrée de console sur un système Windows 7 est autorisée quelle que soit la version matérielle de la machine virtuelle.
`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.
`Enable/disable microphone noise and DC offset filter in PCoIP session`	Détermine s'il est nécessaire d'activer le bruit microphonique et le filtre de tension de décalage continue pour l'entrée de microphone lors de sessions PCoIP. Ce paramètre ne s'applique qu'à Horizon Agent et au pilote audio Teradici. Lorsque ce paramètre n'est pas configuré, le pilote audio Teradici utilise le bruit microphonique et le filtre de tension de décalage continue par défaut.
`Turn on PCoIP user default input language synchronization`	Détermine si la langue d'entrée par défaut pour l'utilisateur dans la session PCoIP est synchronisée avec la langue d'entrée par défaut du point de terminaison du client PCoIP. Lorsque ce paramètre est activé, la synchronisation est autorisée. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, la synchronisation est interdite. Ce paramètre s'applique à Horizon Agent uniquement.

Tableau 5-8. Paramètres de stratégie généraux PCoIP (suite)

Paramètre	Description
`Configure SSL Connections to satisfy Security Tools`	Spécifie comment les connexions de négociation de session SSL sont établies. Afin de satisfaire les scanners de port, activez ce paramètre « Configurer les connexions SSL » et, sur Horizon Agent, réalisez les tâches suivantes : 1 Dans Microsoft Management Console, stockez un certificat correctement nommé et signé dans le magasin Personnel pour le compte d'ordinateur de la machine locale et marquez-le comme exportable. 2 Stockez le certificat pour l'autorité de certification qui l'a signé dans le magasin de certificats racine approuvés. 3 Désactivez les connexions à VMware View 5.1 et versions antérieures. 4 Configurez Horizon Agent pour qu'il charge les certificats provenant uniquement du magasin de certificats. Si le magasin Personnel pour la machine locale est utilisé, ne modifiez pas les noms MY et ROOT des magasins de certificats, sauf si un emplacement de magasin différent a été utilisé dans les étapes 1 et 2. Le serveur PCoIP Server résultant satisfait les outils de sécurité, tels que les scanners de port.
`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 deux-points. Notez que toutes les chaînes de chiffrement ne sont pas sensibles à la casse. La valeur par défaut est « TLS1.1:TLS1.2 ». Cela signifie que TLS v1.1 et TLS v1.2 sont activés (SSL v2.0, SSL v3.0 et TLS v1.0 sont désactivés). Ce paramètre s'applique à la fois à Horizon Agent et à Horizon Client. S'il est défini des deux côtés, la règle de négociation du protocole OpenSSL est suivie.

Paramètres de Presse-papiers PCoIP

Le fichier de modèle d'administration ADMX PCoIP d'Horizon contient des paramètres de stratégie de groupe qui configurent des paramètres de Presse-papiers pour les opérations de copier-coller.

Tous ces paramètres se trouvent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Variables de session PCoIP > Valeurs par défaut remplaçables par l'administrateur** dans l'Éditeur de gestion des stratégies de groupe.

Tous ces paramètres se trouvent également dans le dossier **Configuration utilisateur > Stratégies > Modèles d'administration > Variables de session PCoIP > Paramètres non remplaçables par l'administrateur** dans l'Éditeur de gestion des stratégies de groupe.

Tableau 5-9. Paramètres de stratégie de Presse-papiers PCoIP

Paramètre	Description
`Configure clipboard memory size on server (in kilobytes)`	Spécifie la valeur de la taille de la mémoire du Presse-papiers du serveur, en kilo-octets. Le client possède également une valeur pour la taille de la mémoire du Presse-papiers. Après la configuration de la session, le serveur envoie sa valeur de la taille de la mémoire du Presse-papiers au client. La valeur de 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. Vous pouvez spécifier une valeur minimale de 512 kilo-octets et une valeur maximale de 16 384 kilo-octets. Si vous spécifiez 0 ou si vous ne spécifiez aucune valeur, la taille par défaut de la mémoire du Presse-papiers du serveur est de 1 024 kilo-octets. Ce paramètre s'applique uniquement à la version 7.0.1 ou ultérieure et aux clients Windows, Linux et Mac sur lesquels est installé Horizon Client 4.1 ou version ultérieure. Sur les versions antérieures, la taille de la mémoire du Presse-papiers est de 1 Mo. **Remarque** En fonction de votre réseau, une taille importante de la mémoire du Presse-papiers peut avoir une incidence négative sur les performances. VMware recommande de ne pas définir la taille de la mémoire du Presse-papiers à une valeur supérieure à 16 Mo.
`Configure clipboard redirection`	Détermine le sens dans lequel la redirection du Presse-papiers est autorisée. Vous pouvez sélectionner l'une des valeurs suivantes : ■ **Activé uniquement de client vers agent** (C'est-à-dire, autoriser le copier-coller uniquement depuis le système client vers le poste de travail distant.) ■ **Désactivé dans les deux sens** ■ **Activé dans les deux sens** ■ **Activé uniquement d'agent vers client** (C'est-à-dire, autoriser le copier-coller uniquement depuis le poste de travail distant vers le système client.) La redirection du presse-papier est implémentée sous forme de canal virtuel. Si des canaux virtuels sont désactivés, la redirection du presse-papier ne fonctionne pas. Ce paramètre s'applique à Horizon Agent uniquement. Lorsque ce paramètre est désactivé ou non configuré, la valeur par défaut est **Activé uniquement de client vers agent**.
`Filter text out of the incoming clipboard data`	Spécifie si les données textuelles sont filtrées dans les données de Presse-papiers provenant du client vers l'agent. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Filter Rich Text Format data out of the incoming clipboard data`	Spécifie si les données RTF sont filtrées dans les données de Presse-papiers provenant du client vers l'agent. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Filter images out of the incoming clipboard data`	Spécifie si les données image sont filtrées dans les données de Presse-papiers provenant du client vers l'agent. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Filter Microsoft Office text data out of the incoming clipboard data`	Spécifie si les données au format de texte Microsoft Office (format BIFF12) sont filtrées dans les données de Presse-papiers provenant du client vers l'agent. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.

Tableau 5-9. Paramètres de stratégie de Presse-papiers PCoIP (suite)

Paramètre	Description
`Filter Microsoft Chart and Smart Art data out of the incoming clipboard data`	Spécifie si les données de Graphique Microsoft Office et de graphique Smart Graphique (Art::GVML ClipFormat) sont filtrées dans les données de Presse-papiers provenant du client vers l'agent. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Filter Microsoft Text Effects data out of the incoming clipboard data`	Spécifie si les données d'effets de texte Microsoft Office (format HTML) sont filtrées dans les données de Presse-papiers provenant du client vers l'agent. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Filter text out of the outgoing clipboard data`	Spécifie si les données textuelles sont filtrées dans les données de Presse-papiers envoyées de l'agent vers le client. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Filter Rich Text Format data out of the outgoing clipboard data`	Spécifie si les données RTF sont filtrées dans les données de Presse-papiers envoyées à l'agent vers le client. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Filter images out of the outgoing clipboard data`	Spécifie si les données image sont filtrées dans les données de Presse-papiers envoyées de l'agent vers le client. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Filter Microsoft Office text data out of the outgoing clipboard data`	Spécifie si les données au format de texte Microsoft Office (format BIFF12) sont filtrées dans les données de Presse-papiers envoyées de l'agent vers le client. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data`	Spécifie si les données de Graphique Microsoft Office et de graphique Smart Graphique (Art::GVML ClipFormat) sont filtrées dans les données de Presse-papiers envoyées de l'agent vers le client. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Filter Microsoft Text Effects data out of the outgoing clipboard data`	Spécifie si les données d'effets de texte Microsoft Office (format HTML) sont filtrées dans les données de Presse-papiers envoyées de l'agent vers le client. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.

Paramètres de bande passante PCoIP

Le fichier de modèle d'administration ADMX PCoIP d'Horizon contient des paramètres de stratégie de groupe qui configurent des caractéristiques de bande passante PCoIP.

Tous ces paramètres se trouvent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Variables de session PCoIP > Valeurs par défaut remplaçables par l'administrateur** dans l'Éditeur de gestion des stratégies de groupe.

Tous ces paramètres se trouvent également dans le dossier **Configuration utilisateur > Stratégies > Modèles d'administration > Variables de session PCoIP > Paramètres non remplaçables par l'administrateur** dans l'Éditeur de gestion des stratégies de groupe.

Tableau 5-10. Variables de bande passante de la session PCoIP d'Horizon

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 Horizon Agent et au client. Si les deux points de terminaison ont des paramètres différents, la valeur la plus faible est utilisée.
`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 Horizon 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.

Tableau 5-10. Variables de bande passante de la session PCoIP d'Horizon (suite)

Paramètre	Description
`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 Horizon 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 Horizon Agent.

Tableau 5-10. Variables de bande passante de la session PCoIP d'Horizon (suite)

Paramètre	Description
`Configure the PCoIP session audio bandwidth limit`	Spécifie la bande passante maximale pouvant être utilisée pour le son (lecture audio) dans une session PCoIP. Le traitement audio surveille la bande passante utilisée pour le son. Le traitement sélectionne l'algorithme de compression audio qui fournit le meilleur son possible, en fonction de l'utilisation actuelle de la bande passante. Si une limite de bande passante est définie, le traitement réduit la qualité en modifiant la sélection de l'algorithme de compression jusqu'à ce que la limite de bande passante soit atteinte. S'il n'est pas possible d'atteindre un son de qualité minimale dans la limite de bande passante spécifiée, le son est désactivé. Pour un son stéréo non compressé de haute qualité, définissez cette valeur sur plus de 1 600 kbit/s. Une valeur de 450 kbit/s et plus permet d'obtenir un son stéréo compressé de haute qualité. Une valeur comprise entre 50 kbit/s et 450 kbit/s donne un son dont la qualité va de celle d'une radio FM à celle d'un appel téléphonique. Une valeur inférieure à 50 kbit/s peut entraîner une lecture sans son. Ce paramètre s'applique à Horizon Agent uniquement. Vous devez activer le son sur les deux points de terminaison avant que ce paramètre ne prenne effet. En outre, ce paramètre n'a pas d'effet sur l'audio USB. Si ce paramètre est désactivé ou qu'il n'est pas configuré, une limite de bande passante audio par défaut de 500 kilobits par seconde est configurée pour contraindre l'algorithme de compression audio sélectionné. Si le paramètre est configuré, la valeur est mesurée en kilobits par seconde, avec une limite de bande passante audio par défaut de 500 kilobits par seconde. Ce paramètre s'applique à View 4.6 et supérieur. Il n'a aucun effet sur les versions antérieures de View. Lorsque ce paramètre est modifié lors d'une session PCoIP active, la modification prend effet immédiatement.
`Turn off Build-to-Lossless feature`	Ce paramètre spécifie s'il convient de désactiver ou non la fonctionnalité de développement sans perte du protocole PCoIP. Cette fonctionnalité est désactivée par défaut. Si ce paramètre est activé ou qu'il n'est pas configuré, la fonctionnalité de développement sans perte est désactivée, et les images et autre contenu de poste de travail et d'application ne sont jamais développés pour un état sans perte. Dans les environnements réseau dans lesquels la bande passante est limitée, la désactivation de la fonctionnalité de développement sans perte peut permettre d'économiser de la bande passante. Si ce paramètre est désactivé, la fonctionnalité de développement sans perte est activée. L'activation de la fonctionnalité de développement sans perte est recommandée dans les environnements nécessitant que les images et autre contenu de poste de travail et d'application soient développés pour un état sans perte. Lorsque ce paramètre est modifié lors d'une session PCoIP active, la modification prend effet immédiatement. Pour plus d'informations sur la fonction de développement sans perte PCoIP, reportez-vous à la section « Fonction de développement sans perte PCoIP », page 139.

Paramètres de clavier PCoIP

Le fichier de modèle d'administration ADMX PCoIP de View contient des paramètres de stratégie de groupe qui configurent des paramètres PCoIP affectant l'utilisation du clavier.

Tous ces paramètres se trouvent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Variables de session PCoIP > Valeurs par défaut remplaçables par l'administrateur** dans l'Éditeur de gestion des stratégies de groupe.

Tous ces paramètres se trouvent également dans le dossier **Configuration utilisateur > Stratégies > Modèles d'administration > Variables de session PCoIP > Paramètres non remplaçables par l'administrateur** dans l'Éditeur de gestion des stratégies de groupe.

Tableau 5-11. Variables de la session PCoIP d'Horizon pour le clavier

Paramètre	Description
`Disable sending CAD when users press Ctrl+Alt+Del`	Lorsque cette stratégie est activée, les utilisateurs doivent appuyer sur Ctrl+Alt+Inser plutôt que sur Ctrl+Alt+Suppr pour envoyer une séquence de touches de sécurité (SAS, Secure Attention Sequence) au poste de travail distant pendant une session PCoIP. Vous voulez peut-être activer ce paramètre si des utilisateurs sont confus lorsqu'ils appuient sur Ctrl+Alt+Suppr pour verrouiller le point de terminaison du client et qu'une SAS est envoyée à l'hôte et au client. Ce paramètre s'applique à Horizon Agent uniquement et n'a aucun effet sur un client. Lorsque cette stratégie n'est pas configurée ou est désactivée, les utilisateurs peuvent appuyer sur Ctrl+Alt+Suppr ou sur Ctrl+Alt+Inser pour envoyer une SAS au poste de travail distant.
`Use alternate key for sending Secure Attention Sequence`	Spécifie une touche alternative, à la place de la touche Inser, pour l'envoi d'une séquence de touches de sécurité (SAS, Secure Attention Sequence). Vous pouvez utiliser ce paramètre pour conserver la séquence de touches Ctrl+Alt+Inser sur les machines virtuelles lancées de l'intérieur d'un poste de travail distant pendant une session PCoIP. Par exemple, un utilisateur peut démarrer un vSphere Client depuis un poste de travail PCoIP et ouvrir une console sur une machine virtuelle dans vCenter Server. Si la séquence Ctrl+Alt+Inser est utilisée dans le système d'exploitation client sur la machine virtuelle vCenter Server, une SAS Ctrl+Alt+Suppr est envoyée à la machine virtuelle. Ce paramètre permet à la séquence Ctrl+Alt+*Alternate Key* d'envoyer une SAS Ctrl+Alt+Suppr au poste de travail PCoIP. Lorsque ce paramètre est activé, vous devez sélectionner une autre touche depuis un menu déroulant. Vous ne pouvez pas activer ce paramètre et laisser la valeur non spécifiée. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, la séquence de touches Ctrl+Alt+Inser est utilisée comme SAS. Ce paramètre s'applique à Horizon Agent uniquement et n'a aucun effet sur un client.

Fonction de développement sans perte PCoIP

Vous pouvez configurer le protocole d'affichage PCoIP afin qu'il utilise approche de codage nommée développement progressif ou développement sans perte qui permet de fournir une expérience utilisateur globale optimale, même dans des conditions de réseau contraintes. Cette fonctionnalité est désactivée par défaut.

La fonctionnalité de développement sans perte fournit une image initiale hautement compressée, appelée image avec perte, qui est ensuite progressivement développée vers un état sans perte complet. Un état sans perte signifie que l'image apparaît avec la haute fidélité prévue.

Sur un réseau LAN, PCoIP affiche toujours le texte à l'aide de la compression sans perte. Si la fonctionnalité de développement sans perte est activée, et si la bande passante disponible par session passe en dessous de 1 Mbits/s, le protocole PCoIP affiche initialement une image texte avec perte et développe rapidement l'image vers un état sans perte. Cette approche permet au poste de travail de rester réactif et d'afficher la meilleure image possible lorsque les conditions de réseau changent, ce qui offre aux utilisateurs une expérience optimale.

La fonction de développement sans perte fournit les caractéristiques suivantes :

- règle dynamiquement la qualité d'image ;
- réduit la qualité d'image sur les réseaux encombrés ;
- maintient la réactivité en réduisant la latence de mise à jour de l'écran ;
- reprend la qualité d'image maximale lorsque le réseau n'est plus encombré.

Vous pouvez activer la fonctionnalité le développement sans perte en désactivant le paramètre de stratégie de groupe `Turn off Build-to-Lossless feature`. Reportez-vous à la section « Paramètres de bande passante PCoIP », page 135.

Paramètres de stratégie VMware Blast

Le fichier de modèle d'administration ADMX de stratégie de groupe VMware Blast `vdm_blast.admx` contient des paramètres de stratégie pour le protocole d'affichage VMware Blast. Une fois la stratégie appliquée, les paramètres sont stockés dans la clé de registre `HKLM\Software\Policies\VMware, Inc.\VMware Blast\config`.

Ces paramètres s'appliquent à HTML Access et toutes les instances d'Horizon Client.

Tableau 5-12. Paramètres de stratégie VMware Blast

Paramètre	Description
`Max Session Bandwidth`	Spécifie la bande passante maximale, en kilobits par seconde (Kbit/s), pour une session VMware Blast. La bande passante inclut la création d'images, le son, le canal virtuel, USB et le trafic de contrôle VMware Blast. La valeur par défaut est de 1 Gbit/s.
`Min Session Bandwidth`	Spécifie la bande passante minimale, en kilobits par seconde (Kbit/s), qui est réservée pour une session VMware Blast. La valeur par défaut est de 256 Kbit/s.
`Max Bandwidth Slope for the Kbps Per Megapixel`	Spécifie la pente de bande passante maximale, en kilobits par seconde (Kbit/s), qui est réservée pour une session VMware Blast. La valeur minimale est de 100. La valeur maximale est de 100 000. La valeur par défaut est de 6 200.
`Max Frame Rate`	Spécifie le nombre maximal d'actualisations d'écran. Utilisez ce paramètre pour gérer la bande passante moyenne que les utilisateurs consomment. La valeur par défaut est de 30 actualisations par seconde.
`UDP Protocol`	Spécifie si vous voulez utiliser le protocole UDP ou TCP. Le protocole UDP est utilisé par défaut. Ce paramètre requiert un redémarrage de la machine Horizon Agent sur laquelle la clé de registre existe. Ce paramètre ne s'applique pas à HTML Access, qui utilise toujours le protocole TCP.
`H264`	Spécifie si vous voulez utiliser le codage H.264 ou JPEG/PNG. L'option par défaut est d'utiliser le codage H.264.
`PNG`	Si vous activez ou ne configurez pas ce paramètre, le codage PNG est disponible pour les sessions distantes. Si vous désactivez ce paramètre, seul le codage JPEG est utilisé pour le codage en mode JPEG/PNG. Cette stratégie ne s'applique pas lorsque le codeur H.264 est actif. Ce paramètre n'est pas configuré par défaut. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Screen Blanking`	Spécifie si vous voulez que la console de la machine virtuelle de poste de travail affiche le poste de travail réel que l'utilisateur voit ou si vous voulez afficher un écran vide lorsque le poste de travail a une session active. L'option par défaut est d'afficher un écran vide.
`Cookie Cleanup Interval`	Détermine la fréquence, en millisecondes, à laquelle les cookies associés à des sessions inactives sont supprimés. La valeur par défaut est de 100 ms.

Tableau 5-12. Paramètres de stratégie VMware Blast (suite)

Paramètre	Description
`Image Quality`	Spécifie la qualité d'image de l'écran distant. Vous pouvez spécifier deux paramètres de qualité faible, deux paramètres de qualité élevée et un paramètre de qualité moyenne. Les paramètres de qualité faible sont destinés aux zones de l'écran qui changent souvent, par exemple, lors du défilement. Les paramètres de qualité élevée sont destinés aux zones de l'écran qui sont plus statiques, ce qui se traduit par une meilleure qualité d'image. Vous pouvez spécifier les paramètres suivants : ■ **Qualité JPEG faible** (plage de valeurs disponible : 1 - 100, valeur par défaut : 25) ■ **Sous-échantillonnage chromatique JPEG faible** (plage de valeurs disponible : 4:1:0 (le plus faible), 4:1:1, 4:2:0, 4:2:2 et 4:4:4 (le plus élevé), valeur par défaut : 4:1:0) ■ **Qualité JPEG moyenne** (plage de valeurs disponible : 1 - 100, valeur par défaut : 35) ■ **Qualité JPEG élevée** (plage de valeurs disponible : 1 - 100, valeur par défaut : 90) ■ **Sous-échantillonnage chromatique JPEG élevé** (plage de valeurs disponible : 4:1:0 (le plus faible), 4:1:1, 4:2:0, 4:2:2 et 4:4:4 (le plus élevé), valeur par défaut : 4:4:4)
`H.264 Quality`	Spécifie la qualité d'image de l'écran distant configuré pour utiliser le codage H.264. Vous pouvez spécifier les valeurs de quantification minimale et maximale qui déterminent le degré de contrôle d'une image pour la compression sans perte. Vous pouvez spécifier une valeur de quantification minimale pour la meilleure qualité d'image. Vous pouvez spécifier une valeur de quantification maximale pour la qualité d'image la plus faible. Vous pouvez spécifier les paramètres suivants : ■ **H264maxQP** (plage de valeurs disponible : 0 à 51, valeur par défaut : 36) ■ **H264minQP** (plage de valeurs disponible : 0 à 51, valeur par défaut : 10) Pour la meilleure qualité d'image, définissez les valeurs de quantification à plus ou moins 5 de la plage de valeurs disponible.
`HTTP Service`	Spécifie le port utilisé pour la communication sécurisée (HTTPS) entre le serveur de sécurité ou un dispositif Access Point et un poste de travail. Le pare-feu doit être configuré pour que ce port soit ouvert. La valeur par défaut est 22443.
`Audio playback`	Spécifie si vous voulez que la lecture audio soit activée pour les postes de travail distants. Ce paramètre permet d'activer la lecture audio.
`Configure clipboard redirection`	Spécifie le comportement autorisé de la redirection du Presse-papiers. Les options sont : ■ **Activé dans les deux sens** ■ **Désactivé dans les deux sens** ■ **Activé du client vers le serveur uniquement** (Les utilisateurs peuvent copier/coller uniquement depuis le client vers le poste de travail.) ■ **Activé du serveur vers le client uniquement** (Les utilisateurs peuvent copier/coller uniquement depuis le poste de travail vers le client.) La valeur par défaut est **Activé du client vers le serveur uniquement**.
`Clipboard memory size on server(in kilobytes)`	Spécifie la valeur de la taille de la mémoire du Presse-papiers du serveur, en kilo-octets. Le client possède également une valeur pour la taille de la mémoire du Presse-papiers. Après la configuration de la session, le serveur envoie sa valeur de la taille de la mémoire du Presse-papiers au client. La valeur de 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. Vous pouvez spécifier une valeur minimale de 512 kilo-octets et une valeur maximale de 16 384 kilo-octets. Si vous spécifiez 0 ou si vous ne spécifiez aucune valeur, la taille par défaut de la mémoire du Presse-papiers du serveur est de 1 024 kilo-octets. Ce paramètre s'applique uniquement à la version 7.0.1 et aux versions ultérieures et aux clients Windows, Linux et Mac sur lesquels est installé Horizon Client 4.1 ou version ultérieure. Sur les versions antérieures, la taille de la mémoire du Presse-papiers est de 1 Mo. **Remarque** En fonction de votre réseau, une taille importante de la mémoire du Presse-papiers peut avoir une incidence négative sur les performances. VMware recommande de ne pas définir la taille de la mémoire du Presse-papiers à une valeur supérieure à 16 Mo.

Tableau 5-12. Paramètres de stratégie VMware Blast (suite)

Paramètre	Description
`Keyboard locale synchronization`	Spécifie s'il faut synchroniser la liste des paramètres régionaux du clavier et les paramètres régionaux du clavier par défaut d'un client avec l'application ou le poste de travail distant. Si ce paramètre est activé, la synchronisation a lieu. Ce paramètre s'applique uniquement à Horizon Agent. **Remarque** Cette fonctionnalité est prise en charge uniquement pour Horizon Client pour Windows.
`Configure file transfer`	Spécifie le comportement autorisé du transfert de fichiers entre un poste de travail distant et le client HTML Access. Vous pouvez sélectionner l'une des valeurs suivantes : ■ **Désactiver le chargement et le téléchargement** ■ **Activer le chargement et le téléchargement** ■ **Activer le chargement de fichiers uniquement** (Les utilisateurs peuvent charger des fichiers depuis le système client vers le poste de travail distant uniquement.) ■ **Activer le téléchargement de fichiers uniquement** (Les utilisateurs peuvent télécharger des fichiers depuis le poste de travail distant vers le système client uniquement.) La valeur par défaut est **Activer le chargement de fichiers uniquement**. Ce paramètre ne s'applique qu'à la version 7.0.1 et aux versions ultérieures et à HTML Access 4.1 et versions ultérieures.
`Filter text out of the incoming clipboard data`	Spécifie si les données textuelles sont filtrées dans les données de Presse-papiers provenant du client vers l'agent. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Filter Rich Text Format data out of the incoming clipboard data`	Spécifie si les données RTF sont filtrées dans les données de Presse-papiers provenant du client vers l'agent. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Filter images out of the incoming clipboard data`	Spécifie si les données image sont filtrées dans les données de Presse-papiers provenant du client vers l'agent. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Filter Microsoft Office text data out of the incoming clipboard data`	Spécifie si les données au format de texte Microsoft Office (format BIFF12) sont filtrées dans les données de Presse-papiers provenant du client vers l'agent. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Filter Microsoft Chart and Smart Art data out of the incoming clipboard data`	Spécifie si les données de Graphique Microsoft Office et de graphique Smart Graphique (Art::GVML ClipFormat) sont filtrées dans les données de Presse-papiers provenant du client vers l'agent. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Filter Microsoft Text Effects data out of the incoming clipboard data`	Spécifie si les données d'effets de texte Microsoft Office (format HTML) sont filtrées dans les données de Presse-papiers provenant du client vers l'agent. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Filter text out of the outgoing clipboard data`	Spécifie si les données textuelles sont filtrées dans les données de Presse-papiers envoyées de l'agent vers le client. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.

Tableau 5-12. Paramètres de stratégie VMware Blast (suite)

Paramètre	Description
`Filter Rich Text Format data out of the outgoing clipboard data`	Spécifie si les données RTF sont filtrées dans les données de Presse-papiers envoyées à l'agent vers le client. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Filter images out of the outgoing clipboard data`	Spécifie si les données image sont filtrées dans les données de Presse-papiers envoyées de l'agent vers le client. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Filter Microsoft Office text data out of the outgoing clipboard data`	Spécifie si les données au format de texte Microsoft Office (format BIFF12) sont filtrées dans les données de Presse-papiers envoyées de l'agent vers le client. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data`	Spécifie si les données de Graphique Microsoft Office et de graphique Smart Graphique (Art::GVML ClipFormat) sont filtrées dans les données de Presse-papiers envoyées de l'agent vers le client. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.
`Filter Microsoft Text Effects data out of the outgoing clipboard data`	Spécifie si les données d'effets de texte Microsoft Office (format HTML) sont filtrées dans les données de Presse-papiers envoyées de l'agent vers le client. Lorsque ce paramètre est activé et que la case est cochée, les données sont filtrées. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les données sont autorisées. Ce paramètre s'applique à la version 7.0.2 et aux versions ultérieures.

Appliquer les paramètres de stratégie VMware Blast

Si les stratégies VMware Blast suivantes changent au cours d'une session de client, Horizon Client détecte le changement et applique immédiatement le nouveau paramètre.

- `H264`
- `Audio Playback`
- `Max Session Bandwidth`
- `Min Session Bandwidth`
- `Max Frame Rate`
- `Image Quality`

Pour toutes les autres stratégies VMware Blast, les règles de mise à jour de stratégies de groupe Microsoft s'appliquent. Les stratégies de groupe peuvent être mises à jour manuellement ou en redémarrant la machine Horizon Agent. Pour plus d'informations, reportez-vous à la documentation de Microsoft.

Activation de la compression sans perte pour VMware Blast

Vous pouvez activer le protocole d'affichage VMware Blast pour utiliser une approche de codage appelée « développement progressif » ou « développement sans perte ». Cette fonctionnalité fournit une image initiale hautement compressée, appelée « image avec perte », qui est ensuite progressivement développée vers un état sans perte complet. Un état sans perte signifie que l'image apparaît avec la haute fidélité prévue.

Pour activer la compression sans perte de VMware Blast, définissez la clé `EncoderBuildToPNG` sur `1` dans le dossier `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config` du registre Windows de la machine agent. La valeur par défaut est `0` (désactivé), ce qui signifie que le codec ne développe pas en PNG, qui est un format sans perte.

Les modifications apportées à la configuration de la clé `EncoderBuildToPNG` s'appliquent immédiatement.

Remarque L'activation de la compression sans perte pour VMware Blast provoque une augmentation de l'utilisation du CPU et de la bande passante. VMware recommande d'utiliser le protocole d'affichage PCoIP au lieu de VMware Blast si vous avez besoin d'une compression sans perte. Pour plus d'informations sur la configuration de la compression sans perte pour PCoIP, consultez « Fonction de développement sans perte PCoIP », page 139.

Utilisation de stratégies de groupe des services Bureau à distance

Vous pouvez utiliser les stratégies de groupe des services Bureau à distance (Remote Desktop Services, RDS) pour contrôler la configuration et les performances des hôtes RDS, ainsi que des sessions de poste de travail et d'application RDS. Horizon 7 fournit des fichiers ADMX contenant les stratégies de groupe Microsoft RDS prises en charge dans Horizon 7.

Nous vous recommandons de configurer les stratégies de groupe fournies dans les fichiers ADMX de Horizon 7 plutôt que les stratégies de groupe Microsoft correspondantes. En effet, les stratégies de groupe de Horizon 7 sont certifiées pour la prise en charge de déploiements de Horizon 7.

Configurer le stockage de la licence d'accès utilisateur des services Bureau à distance par périphérique

Vous pouvez configurer les options de stockage de la licence d'accès utilisateur des services Bureau à distance par périphérique afin de spécifier l'emplacement des licences d'accès utilisateur à stocker. Cette fonctionnalité vous permet de choisir si vous voulez stocker les licences d'accès utilisateur ou pas.

Parfois, il peut exister une surutilisation potentielle des licences d'accès utilisateur par périphérique, par exemple les déploiements d'Horizon RDS peuvent disposer des deux systèmes Windows Server 2008 et Windows Server 2012. L'activation de cette fonctionnalité rend l'utilisation des licences d'accès utilisateur efficace dans les déploiements d'Horizon RDS. Pour cela, la licence émise est stockée, elle est fournie lorsque le client tente de se connecter à l'hôte RDS, puis elle est stockée de nouveau en cas d'éventuelle mise à niveau de licence.

Vous pouvez configurer la licence d'accès utilisateur des services Bureau à distance par périphérique dans Horizon Administrator ou manuellement dans la base de données Horizon LDAP.

Procédure

1 Dans Horizon Administrator, cliquez sur **Configuration de View** > **Paramètres généraux**.

2 Dans le volet Général, cliquez sur **Modifier**.

3 Sélectionnez l'une des configurations suivantes dans le menu déroulant **Options de stockage de la licence d'accès utilisateur des services Bureau à distance par périphérique**.

Option	Description
Enregistrer uniquement sur le broker	Les licences d'accès utilisateur par périphérique sont enregistrées uniquement sur le broker. **Remarque** L'entrée LDAP, `cs-enablerdslicensing=true` et `sendRdsLicense=false`.
Enregistrer sur les clients et sur le broker	Les licences d'accès utilisateur par périphérique sont stockées sur les clients et sur le broker. **Remarque** Les entrées LDAP `cs-enablerdslicensing=true` et `sendRdsLicense=true`.
Ne pas enregistrer la licence d'accès utilisateur par périphérique	Les licences d'accès utilisateur par périphérique ne sont stockées nulle part. **Remarque** Les entrées LDAP, `cs-enablerdslicensing=false` et `sendRdsLicense=false`.

4 Cliquez sur **OK**.

Ajouter les fichiers ADMX des services Bureau à distance à Active Directory

Vous pouvez ajouter les paramètres de stratégie dans les fichiers RDS ADMX de Horizon 7 pour les objets de stratégie de groupe (GPO) dans Active Directory. Vous pouvez également installer les fichiers RDS ADMX sur des hôtes RDS individuels.

Prérequis

- Créez des objets de stratégie de groupe pour les paramètres de stratégie de groupe et liez-les à l'UO qui contient vos hôtes RDS.
- Vérifiez que la fonctionnalité Gestion de stratégie de groupe est disponible sur votre serveur Active Directory.

  La procédure d'ouverture de la Console de gestion de stratégie de groupe varie entre les versions Windows 2012, Windows 2008 et Windows 2003 d'Active Directory. Reportez-vous à la section « Créer des GPO pour les stratégies de groupe Horizon 7 », page 193.

Procédure

1 Téléchargez le fichier Horizon 7 GPO Bundle `.zip` 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 GPO Bundle.

  Le fichier se nomme `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, où *x.x.x* est la version et *yyyyyyy* le numéro de build. Tous les fichiers ADMX qui fournissent des paramètres de stratégie de groupe pour Horizon 7 sont disponibles dans ce fichier.

2 Décompressez le fichier `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip` et copiez les fichiers RDS ADMX sur votre hôte Active Directory ou RDS.

  a Copiez les fichiers `vmware_rdsh.admx` et `vmware_rdsh_server.admx`, ainsi que le dossier `en-US` dans le dossier `C:\Windows\PolicyDefinitions` sur votre hôte Active Directory ou RDS.

  b (Facultatif) Copiez les fichiers ressources de la langue `vmware_rdsh.adml` et `vmware_rdsh_server.adml` dans le sous-dossier correspondant dans `C:\Windows\PolicyDefinitions\` sur votre hôte Active Directory ou RDS.

3 Sur l'hôte Active Directory, ouvrez l'Éditeur de gestion des stratégies de groupe.

   Sur un hôte RDS individuel, vous pouvez ouvrir l'Éditeur de stratégie de groupe locale avec l'utilitaire `gpedit.msc`.

   Les paramètres de la stratégie de groupe RDS d'Horizon 7 sont installés dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance**.

   Certains paramètres de la stratégie de groupe RDS d'Horizon 7 sont également installés dans le dossier **Configuration utilisateur > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance**.

4 (Facultatif) Configurez les paramètres de stratégie de groupe dans le dossier **Services Bureau à distance > Hôte de session Bureau à distance**.

Paramètres de compatibilité des applications RDS

Les paramètres de la stratégie de groupe Compatibilité des applications des services Bureau à distance (RDS) contrôlent la compatibilité de Windows Installer, la virtualisation IP des services Bureau à distance, la sélection de l'adaptateur réseau et l'utilisation de l'adresse IP de l'hôte RDS.

Tableau 5-13. Paramètres de la stratégie de groupe Compatibilité des applications RDS

Paramètre	Description
`Turn off Windows Installer RDS Compatibility`	Ce paramètre de stratégie indique si la compatibilité des services Bureau à distance de Windows Installer est exécutée en fonction d'une stratégie par utilisateur pour les applications entièrement installées. Windows Installer ne permet qu'à une seule instance du processus `msiexec` de s'exécuter à la fois. Par défaut, la compatibilité RDS de Windows Installer est activée. Si vous activez ce paramètre de stratégie, la compatibilité RDS de Windows Installer est désactivée et une seule instance du processus `msiexec` peut s'exécuter à la fois. Si vous ne désactivez pas ou si vous ne configurez pas ce paramètre de stratégie, la compatibilité RDS de Windows Installer est activée et plusieurs demandes d'installation d'application par utilisateur sont placées en file d'attente et gérées par le processus `msiexec` selon leur ordre de réception.

`Turn on Remote Desktop IP Virtualization`	Ce paramètre de stratégie spécifie si la virtualisation des adresses IP des services Bureau à distance est activée.
	Par défaut, la virtualisation IP des services Bureau à distance est désactivée.
	Si vous activez ce paramètre de stratégie, la virtualisation IP des services Bureau à distance est activée. Vous pouvez sélectionner le mode d'application de ce paramètre. Si vous utilisez le mode Par programme, vous devez entrer la liste des programmes pour utiliser des adresses IP virtuelles. Répertoriez chaque programme sur une ligne distincte (n'insérez pas de ligne vierge entre les programmes). Par exemple :
	`explorer.exe`
	`mstsc.exe`
	Si vous désactivez ou si vous ne configurez pas ce paramètre de stratégie, la virtualisation IP des services Bureau à distance est désactivée.

Tableau 5-13. Paramètres de la stratégie de groupe Compatibilité des applications RDS (suite)

Paramètre	Description
`Select the network adapter to be used for Remote Desktop IP Virtualization`	Ce paramètre de stratégie spécifie l'adresse IP et le masque réseau correspondant à l'adaptateur réseau utilisé pour les adresses IP virtuelles. L'adresse IP et le masque réseau doivent être entrés conformément à la notation CIDR (Classless Inter-Domain Routing). Par exemple : 192.0.2.96/24. Si vous activez ce paramètre de stratégie, l'adresse IP et le masque réseau spécifiés sont utilisés pour sélectionner l'adaptateur réseau employé pour les adresses IP virtuelles. Si vous désactivez ou si vous ne configurez pas ce paramètre de stratégie, la virtualisation IP des services Bureau à distance est désactivée. Un adaptateur réseau doit être configuré pour que la virtualisation IP des services Bureau à distance fonctionne.
`Do not use Remote Desktop Session Host server IP address when virtual IP address is not available`	Ce paramètre de stratégie spécifie si une session utilise l'adresse IP de l'hôte RDS si aucune adresse IP virtuelle n'est disponible. Si vous activez ce paramètre de stratégie, l'adresse IP de l'hôte RDS n'est pas utilisée si aucune adresse IP virtuelle n'est disponible. La session ne disposera pas de connectivité réseau. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, l'adresse IP de l'hôte RDS est utilisée si aucune adresse IP virtuelle n'est disponible.

Paramètres de connexion RDS

Les paramètres de la stratégie de groupe Connexions RDS permettent aux utilisateurs de définir des stratégies pour les connexions à des sessions sur des hôtes RDS.

Les paramètres de la stratégie de groupe RDS d'Horizon 7 sont installés dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Connexions**.

Les paramètres de la stratégie de groupe RDS d'Horizon 7 sont également installés dans le dossier **Configuration utilisateur > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Connexions**.

Tableau 5-14. Paramètres de la stratégie de groupe Connexions RDS

Paramètre	Description
`Automatic reconnection`	Spécifie s'il faut autoriser les clients Connexion Bureau à distance à se reconnecter automatiquement aux sessions d'un hôte RDS si leur liaison réseau est temporairement perdue. Par défaut, vingt tentatives de reconnexion au maximum sont effectuées à intervalles de cinq secondes. Si vous activez ce paramètre de stratégie, la reconnexion automatique est tentée pour tous les clients qui exécutent Connexion Bureau à distance chaque fois que la connexion réseau est perdue. Si vous désactivez ce paramètre de stratégie, une reconnexion automatique des clients est interdite. Si vous ne configurez pas ce paramètre de stratégie, la reconnexion automatique n'est pas spécifiée au niveau de la stratégie de groupe. Toutefois, les utilisateurs peuvent configurer la reconnexion automatique à l'aide de la case à cocher **Reconnecter si la connexion est abandonnée** dans l'onglet **Expérience** de Connexion Bureau à distance.
`Allow users to connect remotely using Remote Desktop Services`	Ce paramètre de stratégie configure l'accès à distance à des ordinateurs à l'aide des services Bureau à distance. Si vous activez ce paramètre de stratégie, les utilisateurs membres du groupe Utilisateurs du Bureau à distance sur l'ordinateur cible peuvent se connecter à distance à l'ordinateur cible à l'aide des services Bureau à distance. Si vous désactivez ce paramètre de stratégie, les utilisateurs ne peuvent pas se connecter à distance à l'ordinateur cible à l'aide des services Bureau à distance. L'ordinateur cible conservera toutes les connexions en cours, mais il n'acceptera plus de nouvelles connexions entrantes. Si vous ne configurez pas ce paramètre de stratégie, les services Bureau à distance utilisent le paramètre Bureau à distance sur l'ordinateur cible pour déterminer si la connexion à distance est autorisée. Ce paramètre se trouve dans l'onglet **Utilisation à distance** dans **Propriétés du système**. Par défaut, la connexion à distance n'est pas autorisée. **Remarque** Vous pouvez limiter les clients susceptibles de se connecter à distance à l'aide des services Bureau à distance en configurant le paramètre de stratégie « Requérir l'authentification utilisateur pour les connexions à distance à l'aide de l'authentification au niveau du réseau » se trouvant dans le dossier **Configuration ordinateur > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Sécurité**. Vous pouvez limiter le nombre d'utilisateurs qui peuvent se connecter simultanément en configurant l'option Nombre maximal de connexions dans l'onglet **Carte réseau** de l'outil Configuration d'hôte de session Bureau à distance ou en configurant le paramètre de stratégie « Limiter le nombre de connexions » se trouvant dans le dossier **Configuration ordinateur > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Connexions**.

Tableau 5-14. Paramètres de la stratégie de groupe Connexions RDS (suite)

Paramètre	Description
`Deny logoff of an administrator logged in to the console session`	Ce paramètre de stratégie détermine si un administrateur tentant de se connecter à distance à la console d'un serveur peut déconnecter un administrateur actuellement connecté à la console. Cette stratégie est utile lorsque l'administrateur actuellement connecté ne veut pas être déconnecté par un autre administrateur. Si l'administrateur connecté est déconnecté, les données n'ayant pas été enregistrées auparavant sont perdues. Si vous activez ce paramètre de stratégie, la déconnexion de l'administrateur connecté n'est pas autorisée. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, la déconnexion de l'administrateur connecté est autorisée. **Remarque** La session de la console est également appelée Session 0. L'accès à la console peut être obtenu en utilisant le commutateur `/console` de la connexion Bureau à distance dans le nom du champ d'ordinateur ou à partir de la ligne de commande.
`Configure keep-alive connection interval`	Ce paramètre de stratégie vous permet d'entrer un intervalle de conservation pour garantir que l'état de la session sur l'hôte RDS est cohérent avec l'état du client. Après la perte de la connexion à un hôte RDS, la session sur l'hôte RDS peut rester active au lieu de passer à un état déconnecté, même si le client est physiquement déconnecté de l'hôte RDS. Si le client se connecte à nouveau au même hôte RDS, une nouvelle session est susceptible d'être établie (si l'hôte RDS est configuré pour autoriser plusieurs sessions) et la session d'origine peut être encore active. Si vous activez ce paramètre de stratégie, vous devez entrer un intervalle de conservation. L'intervalle de conservation détermine la fréquence, en minutes, à laquelle le serveur vérifie l'état de la session. La plage des valeurs que vous pouvez entrer est comprise entre 1 et 999 999. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, aucun intervalle de conservation n'est défini et le serveur ne vérifie pas l'état de la session.

Tableau 5-14. Paramètres de la stratégie de groupe Connexions RDS (suite)

Paramètre	Description
`Limit number of connections`	Spécifie si les services Bureau à distance limitent le nombre de connexions simultanées au serveur. Vous pouvez utiliser ce paramètre pour limiter le nombre de sessions des services Bureau à distance qui peuvent être actives sur un serveur. Si ce nombre est dépassé, les utilisateurs supplémentaires qui tentent de se connecter reçoivent un message d'erreur leur indiquant que le serveur est occupé et de réessayer plus tard. La limitation du nombre de sessions améliore les performances, car un nombre moins élevé de sessions nécessite moins de ressources système. Par défaut, les hôtes RDS autorisent un nombre illimité de sessions des services Bureau à distance et le Bureau à distance pour administration autorise deux sessions des services Bureau à distance. Pour utiliser ce paramètre, entrez le nombre maximal de connexions que vous voulez spécifier pour le serveur. Pour spécifier un nombre illimité de connexions, tapez 999999. Si vous activez ce paramètre de stratégie, le nombre maximal de connexions est limité au nombre spécifié cohérent avec la version de Windows et le mode des services Bureau à distance qui s'exécutent sur le serveur. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les limites du nombre de connexions ne sont pas appliquées au niveau de la stratégie de groupe. **Remarque** Ce paramètre est destiné à être utilisé sur des hôtes RDS, qui sont des serveurs exécutant le système d'exploitation Windows et où le service de rôle Hôte de session Bureau à distance est installé.
`Set rules for remote control of Remote Desktop Services user sessions`	Utilisez ce paramètre de stratégie pour spécifier le niveau de contrôle à distance autorisé dans une session des services Bureau à distance. Vous pouvez utiliser ce paramètre de stratégie pour sélectionner l'un des deux niveaux de contrôle à distance : Afficher la session ou Contrôle total. Afficher la session permet à l'utilisateur du contrôle à distance de consulter une session. Contrôle total permet à l'administrateur d'interagir avec la session. Le contrôle à distance peut être établi avec ou sans autorisation de l'utilisateur. Si vous activez ce paramètre de stratégie, les administrateurs peuvent interagir à distance avec la session des services Bureau à distance d'un utilisateur selon les règles spécifiées. Pour définir ces règles, sélectionnez le niveau de contrôle et l'autorisation souhaités dans la liste Options. Pour désactiver le contrôle à distance, sélectionnez « Aucun contrôle à distance autorisé ». Si vous désactivez ou ne configurez pas ce paramètre de stratégie, des règles de contrôle à distance sont déterminées par le paramètre dans l'onglet **Contrôle à distance** de l'outil Configuration d'hôte de session Bureau à distance. Par défaut, les utilisateurs du contrôle à distance disposent du contrôle total de la session avec l'autorisation de l'utilisateur. **Remarque** Ce paramètre de stratégie s'affiche à la fois dans Configuration ordinateur et dans Configuration utilisateur. Si les deux paramètres de stratégie sont configurés, le paramètre de stratégie Configuration ordinateur est prioritaire.

Tableau 5-14. Paramètres de la stratégie de groupe Connexions RDS (suite)

Paramètre	Description
`Restrict Remote Desktop Services users to a single Remote Desktop Services session`	Utilisez ce paramètre de stratégie pour limiter les utilisateurs à une seule session des services Bureau à distance. Si vous activez ce paramètre de stratégie, les utilisateurs qui ouvrent une session à distance via les services Bureau à distance sont limités à une seule session (active ou déconnectée) sur ce serveur. Si l'utilisateur quitte la session dans un état déconnecté, il se reconnecte automatiquement à cette session lors de la prochaine ouverture de session. Si vous désactivez ce paramètre de stratégie, les utilisateurs sont autorisés à établir un nombre illimité de connexions simultanées à distance à l'aide des services Bureau à distance. Si vous ne configurez pas ce paramètre de stratégie, le paramètre « Limiter les utilisateurs à une seule session » de l'outil Configuration d'hôte de session Bureau à distance détermine si les utilisateurs sont limités à une seule session des services Bureau à distance.
`Allow remote start of unlisted programs`	Utilisez ce paramètre de stratégie pour spécifier si des utilisateurs distants peuvent démarrer tout programme sur l'hôte RDS lorsqu'ils démarrent une session des services Bureau à distance ou s'ils peuvent uniquement démarrer des programmes répertoriés dans la liste Programmes RemoteApp. Vous pouvez contrôler quels programmes sur un hôte RDS peuvent être démarrés à distance en utilisant le Gestionnaire RemoteApp pour créer une liste des programmes RemoteApp. Par défaut, seuls les programmes figurant dans la liste Programmes RemoteApp peuvent être démarrés lorsqu'un utilisateur démarre une session des services Bureau à distance. Si vous activez ce paramètre de stratégie, les utilisateurs distants peuvent démarrer n'importe quel programme sur l'hôte RDS lorsqu'ils démarrent une session des services Bureau à distance. Par exemple, un utilisateur distant peut le faire en spécifiant le chemin de l'exécutable du programme au moment de la connexion à l'aide du client Connexion Bureau à distance. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les utilisateurs distants peuvent uniquement démarrer des programmes répertoriés dans la liste Programmes RemoteApp dans le Gestionnaire RemoteApp lorsqu'ils démarrent une session des services Bureau à distance.
`Turn off Fair Share CPU Scheduling`	La planification de la répartition de charge équilibrée du temps processeur répartit de façon dynamique le temps processeur entre toutes les sessions des services Bureau à distance sur le même hôte RDS, en fonction du nombre de sessions et de la demande en temps processeur de chaque session. Si vous activez ce paramètre de stratégie, la planification de répartition de charge équilibrée du temps processeur est désactivée. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, la planification de répartition de charge équilibrée du temps processeur est activée.

Paramètres de redirection de ressources et de périphériques RDS

Les paramètres de stratégie de groupe de redirection des ressources et des périphériques RDS contrôlent l'accès aux périphériques et aux ressources sur un ordinateur client dans des sessions des services Bureau à distance.

Les paramètres de la stratégie de groupe RDS d'Horizon 7 sont installés dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Redirection de périphérique et de ressource**.

Les paramètres de la stratégie de groupe RDS d'Horizon 7 sont également installés dans le dossier **Configuration utilisateur > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Redirection de périphérique et de ressource**.

Tableau 5-15. Paramètres de stratégie de groupe de redirection des ressources et des périphériques RDS

Paramètre	Description
`Allow audio and video playback redirection`	Utilisez ce paramètre de stratégie pour spécifier si les utilisateurs peuvent rediriger la sortie audio et vidéo de l'ordinateur distant lors d'une session des services Bureau à distance. Les utilisateurs peuvent définir l'emplacement de lecture de la sortie audio de l'ordinateur distant en configurant les paramètres audio de l'ordinateur distant dans l'onglet Ressources locales de Connexion Bureau à distance. Ils peuvent choisir de lire la sortie audio de l'ordinateur distant à distance ou en local. Les utilisateurs peuvent également choisir de ne pas lire la sortie audio. La lecture vidéo peut être configurée à l'aide du paramètre videoplayback dans un fichier de protocole RDP (Remote Desktop Protocol) (.rdp). Par défaut, la lecture vidéo est activée. Par défaut, la redirection de la lecture audio et vidéo n'est pas autorisée lors de la connexion à un ordinateur exécutant Windows Server 2008 R2, Windows Server 2008 ou Windows Server 2003. La redirection de la lecture audio et vidéo est autorisée par défaut lors de la connexion à un ordinateur exécutant Windows 7, Windows Vista ou Windows XP Professionnel. Si vous activez ce paramètre de stratégie, la redirection de la lecture audio et vidéo est autorisée. Si vous désactivez ce paramètre de stratégie, la redirection de la lecture audio et vidéo n'est pas autorisée, même si la redirection de la lecture audio est spécifiée dans Connexion Bureau à distance ou si la lecture vidéo est spécifiée dans le fichier .rdp. Si vous ne configurez pas ce paramètre de stratégie, le paramètre Lecture audio/vidéo dans l'onglet Paramètres du client de l'outil Configuration d'hôte de session Bureau à distance détermine si la redirection de la lecture audio et vidéo est autorisée.
`Allow audio recording redirection`	Utilisez ce paramètre de stratégie pour spécifier si les utilisateurs peuvent effectuer des enregistrements audio sur l'ordinateur distant lors d'une session des services Bureau à distance. Les utilisateurs peuvent spécifier s'ils veulent effectuer des enregistrements audio sur l'ordinateur distant en configurant les paramètres audio de l'ordinateur distant dans l'onglet Ressources locales de Connexion Bureau à distance. Ils peuvent effectuer des enregistrements audio en utilisant un périphérique d'entrée audio sur l'ordinateur local, tel qu'un microphone intégré. Par défaut, la redirection de l'enregistrement audio n'est pas autorisée lors de la connexion à un ordinateur exécutant Windows Server 2008 R2. La redirection de l'enregistrement audio est autorisée par défaut lors de la connexion à un ordinateur exécutant Windows 7. Si vous activez ce paramètre de stratégie, la redirection de l'enregistrement audio est autorisée. Si vous désactivez ce paramètre de stratégie, la redirection de l'enregistrement audio n'est pas autorisée, même si elle est spécifiée dans Connexion Bureau à distance. Si vous ne configurez pas ce paramètre de stratégie, le paramètre Enregistrement audio dans l'onglet Paramètres du client de l'outil Configuration d'hôte de session Bureau à distance détermine si la redirection de l'enregistrement audio est autorisée.

Tableau 5-15. Paramètres de stratégie de groupe de redirection des ressources et des périphériques RDS (suite)

Paramètre	Description
`Limit audio playback quality`	Utilisez ce paramètre de stratégie pour limiter la qualité de la lecture audio lors d'une session des services Bureau à distance. La limitation de la qualité de la lecture audio peut améliorer les performances de connexion, en particulier en cas de liaisons lentes. Si vous activez ce paramètre de stratégie, vous devez sélectionner une des valeurs suivantes : Élevée, Moyenne ou Dynamique. Si vous sélectionnez Élevée, la sortie audio sera envoyée sans compression et avec une latence minimale. Cette option nécessite une grande quantité de bande passante. Si vous sélectionnez Moyenne, la sortie audio sera envoyée avec une certaine compression et une latence minimale déterminées par le codec utilisé. Si vous sélectionnez Dynamique, la sortie audio sera envoyée avec un niveau de compression déterminé par la bande passante de la connexion à distance. La qualité de la lecture audio que vous spécifiez sur l'ordinateur distant à l'aide de ce paramètre de stratégie correspond à la qualité maximale pouvant être utilisée pour une session des services Bureau à distance, quelle que soit la qualité de la lecture audio configurée sur l'ordinateur client. Par exemple, si la qualité de la lecture audio configurée sur l'ordinateur client est supérieure à celle configurée sur l'ordinateur distant, le niveau de qualité de lecture audio le plus faible est utilisé. La qualité de la lecture audio peut être configurée sur l'ordinateur client à l'aide du paramètre audioqualitymode dans un fichier de protocole RDP (Remote Desktop Protocol) (.rdp). Par défaut, la qualité de la lecture audio est définie sur Dynamique.
`Do not allow clipboard redirection`	Spécifie s'il faut empêcher le partage de contenu du Presse-papiers (redirection du Presse-papiers) entre un ordinateur distant et un ordinateur client au cours d'une session des services Bureau à distance. Vous pouvez utiliser ce paramètre pour empêcher les utilisateurs de rediriger les données du Presse-papiers de l'ordinateur distant vers l'ordinateur local et inversement. Par défaut, les services Bureau à distance autorisent la redirection du Presse-papiers. Si vous activez ce paramètre, les utilisateurs ne peuvent pas rediriger les données du Presse-papiers. Si vous désactivez ce paramètre, les services Bureau à distance autorisent toujours la redirection du Presse-papiers. Si vous ne configurez pas ce paramètre, la redirection du Presse-papiers n'est pas spécifiée au niveau de la stratégie de groupe. Toutefois, un administrateur peut toujours désactiver la redirection du Presse-papiers à l'aide de l'outil Configuration d'hôte de session Bureau à distance.

Tableau 5-15. Paramètres de stratégie de groupe de redirection des ressources et des périphériques RDS (suite)

Paramètre	Description
`Do not allow COM port redirection`	Spécifie s'il faut empêcher la redirection de données vers les ports COM client à partir de l'ordinateur distant lors d'une session des services Bureau à distance. Vous pouvez utiliser ce paramètre pour empêcher les utilisateurs de rediriger les données vers les périphériques de port COM ou de mapper les ports COM locaux lorsqu'ils sont connectés à une session des services Bureau à distance. Par défaut, les services Bureau à distance autorisent cette redirection de port COM. Si vous activez ce paramètre, les utilisateurs ne peuvent pas rediriger les données du serveur vers le port COM local. Si vous désactivez ce paramètre, les services Bureau à distance autorisent toujours la redirection de port COM. Si vous ne configurez pas ce paramètre, la redirection de port COM n'est pas spécifiée au niveau de la stratégie de groupe. Toutefois, un administrateur peut toujours désactiver la redirection de port COM à l'aide de l'outil Configuration d'hôte de session Bureau à distance.
`Do not allow drive redirection`	Spécifie s'il faut empêcher le mappage des lecteurs client dans une session des services Bureau à distance (redirection de lecteur). Par défaut, un serveur Hôte de session Bureau à distance mappe automatiquement les lecteurs du client lors de la connexion. Les lecteurs mappés apparaissent dans l'arborescence des dossiers de la session dans l'Explorateur Windows ou dans Poste de travail, au format <lettre_lecteur> sur <nom_ordinateur>. Vous pouvez utiliser ce paramètre pour modifier ce comportement. Si vous activez ce paramètre, la redirection du lecteur client n'est pas autorisée dans les sessions des services Bureau à distance. Si vous désactivez ce paramètre, la redirection du lecteur client est toujours autorisée. Si vous ne configurez pas ce paramètre, la redirection du lecteur client n'est pas spécifiée au niveau de la stratégie de groupe. Toutefois, un administrateur peut toujours désactiver la redirection du lecteur client à l'aide de l'outil Configuration d'hôte de session Bureau à distance.
`Do not allow LTP Port redirection`	Spécifie s'il faut empêcher la redirection de données vers les ports LPT clients lors d'une session des services Bureau à distance. Vous pouvez utiliser ce paramètre pour empêcher les utilisateurs de mapper les ports LPT locaux et de rediriger les données à partir de l'ordinateur distant vers les périphériques de port LPT locaux. Par défaut, les services Bureau à distance autorisent cette redirection de ports LPT. Si vous activez ce paramètre, les utilisateurs d'une session des services Bureau à distance ne peuvent pas rediriger les données du serveur vers le port LPT local. Si vous désactivez ce paramètre, la redirection de ports LPT est toujours autorisée. Si vous ne configurez pas ce paramètre, la redirection de ports LPT n'est pas spécifiée au niveau de la stratégie de groupe. Toutefois, un administrateur peut toujours désactiver la redirection de ports LPT locaux à l'aide de l'outil Configuration d'hôte de session Bureau à distance.

Tableau 5-15. Paramètres de stratégie de groupe de redirection des ressources et des périphériques RDS (suite)

Paramètre	Description
`Do not allow supported Plug and Play device redirection`	Utilisez ce paramètre de stratégie pour contrôler la redirection de périphériques Plug-and-Play pris en charge, tels que les appareils mobiles Windows, vers l'ordinateur distant lors d'une session des services Bureau à distance. Par défaut, les services Bureau à distance autorisent la redirection de périphériques Plug-and-Play pris en charge. Les utilisateurs peuvent utiliser l'option « Autres » de l'onglet Ressources locales de Connexion Bureau à distance pour choisir les périphériques Plug-and-Play pris en charge à rediriger vers l'ordinateur distant. Si vous activez ce paramètre de stratégie, les utilisateurs ne peuvent pas rediriger leurs périphériques Plug-and-Play pris en charge vers l'ordinateur distant. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les utilisateurs peuvent rediriger leurs périphériques Plug-and-Play pris en charge vers l'ordinateur distant. **Remarque** Vous pouvez également interdire la redirection des périphériques Plug-and-Play pris en charge dans l'onglet Paramètres du client de l'outil Configuration d'hôte de session Bureau à distance. Vous pouvez interdire la redirection de types de périphériques Plug-and-Play pris en charge spécifiques à l'aide des paramètres de stratégie dans le dossier **Configuration ordinateur > Modèles d'administration > Système > Installation de périphériques > Restrictions d'installation de périphériques**.
`Do not allow smart card device redirection`	Utilisez ce paramètre de stratégie pour contrôler la redirection des périphériques à carte à puce dans une session des services Bureau à distance. Si vous activez ce paramètre de stratégie, les utilisateurs des services Bureau à distance ne peuvent pas utiliser de carte à puce pour se connecter à une session des services Bureau à distance. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, la redirection des périphériques à carte à puce est autorisée. Par défaut, les services Bureau à distance redirigent automatiquement les périphériques à carte à puce dès la connexion. **Remarque** L'ordinateur client doit exécuter au minimum Microsoft Windows 2000 Server ou Microsoft Windows XP Professionnel et le serveur cible doit être joint à un domaine.
`Allow time zone redirection`	Ce paramètre de stratégie détermine si l'ordinateur client redirige ses paramètres de fuseau horaire vers la session des services Bureau à distance. Si vous activez ce paramètre de stratégie, les clients capables de rediriger un fuseau horaire envoient leurs informations de fuseau horaire au serveur. L'heure de base du serveur est alors utilisée pour calculer l'heure de la session actuelle (heure de la session actuelle = heure de base du serveur + fuseau horaire du client). Si vous désactivez ou ne configurez pas ce paramètre de stratégie, l'ordinateur client ne redirige pas ses informations de fuseau horaire et le fuseau horaire de la session est identique à celui du serveur.

Paramètres d'attribution de licence RDS

Les paramètres de stratégie de groupe Licences RDS contrôlent l'ordre dans lequel les serveurs de licences RDS sont localisés, si des notifications de problèmes s'affichent et si des licences par utilisateur ou par périphérique sont utilisées pour les licences d'accès client RDS.

Les paramètres de la stratégie de groupe RDS d'Horizon 7 sont installés dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Licences**.

Tableau 5-16. Paramètre de stratégie de groupe de licences RDS

Paramètre	Description
`Use the specified Remote Desktop license servers`	Ce paramètre de stratégie vous permet de spécifier l'ordre dans lequel un serveur d'hôte RDS tente de localiser les serveurs de licences Bureau à distance. Si vous activez ce paramètre de stratégie, un serveur d'hôte RDS tente d'abord de localiser les serveurs de licences spécifiés. Si les serveurs de licences spécifiés ne peuvent pas être localisés, le serveur d'hôte RDS tentera une découverte automatique des serveurs de licences. Dans le processus de découverte automatique des serveurs de licences, un serveur d'hôte RDS dans un domaine Windows Server tente de contacter un serveur de licences dans l'ordre suivant : 1 Serveurs de licences spécifiés dans l'outil Configuration d'hôte de session Bureau à distance. 2 Serveurs de licences publiés dans les services de domaine Active Directory. 3 Serveurs de licences installés sur des contrôleurs du même domaine que le serveur d'hôte RDS. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, l'hôte RDS utilise le mode de découverte des serveurs de licences spécifié dans l'outil Configuration d'hôte de session Bureau à distance.
`Hide notifications about RD Licensing problems that affect the RD Session Host server`	Ce paramètre de stratégie détermine si des notifications s'affichent sur un hôte RDS lorsque celui-ci connaît des problèmes de licence RD. Par défaut, des notifications sont affichées sur un hôte RDS une fois que vous avez ouvert une session en tant qu'administrateur local, en cas de problèmes de licence RD touchant l'hôte RDS. Le cas échéant, une notification s'affiche également pour indiquer le nombre de jours restant avant l'expiration de la période de grâce de la licence de l'hôte RDS. Si vous activez ce paramètre de stratégie, ces notifications ne s'affichent pas sur l'hôte RDS. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, ces notifications s'affichent sur l'hôte RDS une fois que vous avez ouvert une session en tant qu'administrateur local.
`Set the Remote Desktop licensing mode`	Ce paramètre de stratégie vous permet de spécifier le type de licence d'accès client (CAL) des services Bureau à distance (RDS) nécessaire à la connexion à cet hôte RDS. Vous pouvez utiliser ce paramètre de stratégie pour sélectionner l'un des deux modes d'octroi de licence : par utilisateur ou par périphérique. Le mode de licence par utilisateur impose que chaque compte d'utilisateur qui se connecte à cet hôte RDS dispose d'une CAL RDS par utilisateur. Le mode de licence par périphérique impose que chaque périphérique qui se connecte à cet hôte RDS dispose d'une CAL RDS par périphérique. Si vous activez ce paramètre de stratégie, le mode de licence que vous spécifiez a priorité sur le mode de licence qui est spécifié lors de l'installation de l'Hôte de session Bureau à distance ou spécifié dans l'outil Configuration d'hôte de session Bureau à distance.

Tableau 5-16. Paramètre de stratégie de groupe de licences RDS (suite)

Paramètre	Description
	Si vous désactivez ou ne configurez pas ce paramètre de stratégie, le mode de licence qui est spécifié lors de l'installation du service de rôle Hôte de session Bureau à distance ou spécifié dans l'outil Configuration d'hôte de session Bureau à distance est utilisé.

Paramètres de redirection de l'imprimante RDS

Les paramètres de stratégie de groupe Redirection de l'imprimante RDS permettent aux utilisateurs de configurer des stratégies pour la redirection de l'imprimante.

Les paramètres de la stratégie de groupe RDS d'Horizon 7 sont installés dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Redirection de l'imprimante**.

Les paramètres de la stratégie de groupe RDS d'Horizon 7 sont également installés dans le dossier **Configuration utilisateur > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Redirection de l'imprimante**.

Tableau 5-17. Paramètres de stratégie de groupe Redirection de l'imprimante RDS

Paramètre	Description
`Do not set default client printer to be default printer in a session`	Utilisez ce paramètre de stratégie pour spécifier si l'imprimante par défaut du client est automatiquement définie en tant qu'imprimante par défaut d'une session sur un hôte RDS. Par défaut, les services Bureau à distance désignent automatiquement l'imprimante par défaut du client comme imprimante par défaut d'une session sur un hôte RDS. Vous pouvez utiliser ce paramètre de stratégie pour modifier ce comportement. Si vous activez ce paramètre de stratégie, l'imprimante par défaut est l'imprimante spécifiée sur l'ordinateur distant. Si vous désactivez ce paramètre de stratégie, l'hôte RDS mappe automatiquement l'imprimante par défaut du client et la définit comme imprimante par défaut au moment de la connexion. Si vous ne configurez pas ce paramètre de stratégie, l'imprimante par défaut n'est pas spécifiée au niveau de la stratégie de groupe. Toutefois, un administrateur peut configurer l'imprimante par défaut des sessions client à l'aide de l'outil Configuration d'hôte de session Bureau à distance.
`Do not allow client printer redirection`	Utilisez ce paramètre de stratégie pour spécifier s'il faut empêcher le mappage d'imprimantes du client dans des sessions des services Bureau à distance. Vous pouvez utiliser ce paramètre de stratégie pour empêcher les utilisateurs de rediriger les travaux d'impression de l'ordinateur distant vers une imprimante connectée à leur ordinateur local (client). Par défaut, les services Bureau à distance autorisent ce mappage des imprimantes du client. Si vous activez ce paramètre de stratégie, les utilisateurs ne peuvent pas rediriger les travaux d'impression de l'ordinateur distant vers une imprimante locale du client durant les sessions des services Bureau à distance. Si vous désactivez ce paramètre de stratégie, les utilisateurs peuvent rediriger les travaux d'impression avec le mappage des imprimantes du client. Si vous ne configurez pas ce paramètre de stratégie, le mappage des imprimantes du client n'est pas spécifié au niveau de la stratégie de groupe. Toutefois, un administrateur peut toujours désactiver le mappage des imprimantes du client à l'aide de l'outil Configuration d'hôte de session Bureau à distance.

Tableau 5-17. Paramètres de stratégie de groupe Redirection de l'imprimante RDS (suite)

Paramètre	Description
`Use Remote Desktop Easy Print printer driver first`	Utilisez ce paramètre de stratégie pour spécifier si le pilote d'imprimante Easy Print des services Bureau à distance est d'abord utilisé pour installer toutes les imprimantes client. Si vous activez ou ne configurez pas ce paramètre de stratégie, l'hôte RDS tente d'abord d'utiliser le pilote d'imprimante Easy Print des services Bureau à distance pour installer toutes les imprimantes client. Si pour une raison quelconque le pilote d'imprimante Easy Print des services Bureau à distance ne peut pas être utilisé, un pilote d'imprimante de l'hôte RDS correspondant à l'imprimante client est utilisé. Si l'hôte RDS ne dispose d'aucun pilote d'imprimante correspondant à l'imprimante client, celle-ci n'est pas disponible pour la session Bureau à distance. Si vous désactivez ce paramètre de stratégie, l'hôte RDS tente de trouver un pilote d'imprimante adéquat pour installer l'imprimante client. Si l'hôte RDS ne dispose d'aucun pilote d'imprimante correspondant à l'imprimante client, il tente d'utiliser le pilote d'imprimante Easy Print des services Bureau à distance pour installer l'imprimante client. Si pour une raison quelconque le pilote d'imprimante Easy Print des services Bureau à distance ne peut pas être utilisé, l'imprimante client n'est pas disponible pour la session des services Bureau à distance. **Remarque** Si le paramètre de stratégie « Ne pas autoriser la redirection de l'imprimante client » est activé, le paramètre de stratégie « Utiliser d'abord le pilote d'imprimante Easy Print des services Bureau à distance » est ignoré.

Tableau 5-17. Paramètres de stratégie de groupe Redirection de l'imprimante RDS (suite)

Paramètre	Description
`Specify RD Session Host Server fallback printer driver behavior`	Utilisez ce paramètre de stratégie pour spécifier le comportement du pilote d'imprimante de secours de l'hôte RDS. Par défaut, le pilote d'imprimante de secours de l'hôte RDS est désactivé. Si l'hôte RDS ne dispose d'aucun pilote d'imprimante correspondant à l'imprimante du client, aucune imprimante n'est disponible pour la session des services Bureau à distance. Si vous activez ce paramètre de stratégie, le pilote d'imprimante de secours est activé et, par défaut, l'hôte RDS recherche un pilote d'imprimante adéquat. S'il n'en trouve pas, l'imprimante du client n'est pas disponible. Vous pouvez choisir de modifier ce comportement par défaut. Les options disponibles sont les suivantes : ■ `Do nothing if one is not found`. Si les pilotes d'imprimante ne correspondent pas, l'hôte RDS tente de trouver un pilote adéquat. S'il n'en trouve pas, l'imprimante du client n'est pas disponible. Il s'agit du comportement par défaut. ■ `Default to PCL if one is not found`. Si aucun pilote adéquat n’est trouvé, le pilote d’imprimante de secours PCL (Printer Control Language) est utilisé par défaut. ■ `Default to PS if one is not found`. Si aucun pilote adéquat n’est trouvé, le pilote d’imprimante de secours PS (PostScript) est utilisé par défaut. ■ `Show both PCL and PS if one is not found`. Si aucun pilote adéquat n’est trouvé, les pilotes d’imprimante de secours PS et PCL sont affichés. Si vous désactivez ce paramètre de stratégie, le pilote d'imprimante de secours de l'hôte RDS est désactivé et celui-ci ne tentera pas d'utiliser le pilote d'imprimante de secours. Si vous ne configurez pas ce paramètre de stratégie, le pilote d'imprimante de secours est désactivé par défaut. **Remarque** Si le paramètre « Ne pas autoriser la redirection de l’imprimante client » est activé, ce paramètre de stratégie est ignoré et le pilote d’imprimante de secours est désactivé.
`Redirect only the default client printer`	Utilisez ce paramètre de stratégie pour spécifier si l’imprimante cliente par défaut est la seule imprimante redirigée dans les sessions des services Bureau à distance. Si vous activez ce paramètre de stratégie, seule l’imprimante cliente par défaut est redirigée dans les sessions des services Bureau à distance. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, toutes les imprimantes clientes sont redirigées dans les sessions des services Bureau à distance.

Paramètres de profils RDS

Les paramètres de stratégie de groupe des profils RDS contrôlent les paramètres de profil itinérant et de répertoire de base des sessions des services Bureau à distance.

Tableau 5-18. Paramètres de stratégie de groupe des profils RDS

Paramètre	Description
`Limit the size of the entire roaming user profile cache`	Ce paramètre de stratégie vous permet de limiter la taille de l'ensemble du cache de profils d'utilisateur itinérant sur le disque local. Il s'applique uniquement à un ordinateur sur lequel le service du rôle Hôte de session Bureau à distance est installé. **Remarque** Si vous souhaitez limiter la taille d'un profil d'utilisateur individuel, utilisez le paramètre de stratégie `Limit profile size` situé dans **Configuration utilisateur\Stratégies\Modèles d'administration\Système\Profils d'utilisateur**. Si vous activez ce paramètre de stratégie, vous devez spécifier un intervalle de surveillance (en minutes) et une taille maximale (en giga-octets) pour l'ensemble du cache de profils d'utilisateur itinérant. L'intervalle de surveillance détermine la fréquence de vérification de la taille de l'ensemble du cache de profils d'utilisateur itinérant. Lorsque la taille de l'ensemble du cache de profils d'utilisateur itinérant dépasse la taille maximale que vous avez spécifiée, les profils d'utilisateur itinérant les plus anciens (utilisés le moins récemment) sont supprimés jusqu'à ce que la taille de l'ensemble du cache de profils d'utilisateur itinérant soit inférieure à la taille maximale spécifiée. Si vous désactivez ou si vous ne configurez pas ce paramètre de stratégie, aucune limitation n'est imposée à la taille de l'ensemble du cache de profils d'utilisateur itinérant sur le lecteur local. Remarque : ce paramètre de stratégie est ignoré si le paramètre de stratégie `Prevent Roaming Profile changes from propagating to the server` situé dans **Configuration ordinateur\Stratégies\Modèles d'administration\Système\Profils d'utilisateur** est activé.
`Set Remote Desktop Services User Home Directory`	Spécifie si les services Bureau à distance utilisent le partage réseau spécifié ou un chemin de répertoire local en tant que racine du répertoire de base de l'utilisateur pour une session des services Bureau à distance. Pour utiliser ce paramètre, sélectionnez l'emplacement du répertoire de base (réseau ou local) dans la liste déroulante Emplacement. Si vous choisissez de placer le répertoire sur un partage réseau, tapez le chemin racine du répertoire de base sous la forme `\\NomOrdinateur\NomPartage`, puis sélectionnez la lettre du lecteur auquel vous souhaitez mapper le partage réseau.

Tableau 5-18. Paramètres de stratégie de groupe des profils RDS (suite)

Paramètre	Description
	Si vous choisissez de conserver le répertoire de base sur l'ordinateur local, tapez le chemin d'accès racine au répertoire de base sous la forme `Lecteur:\Chemin`, sans variables d'environnement, ni ellipses. Ne spécifiez pas d'espace réservé pour l'alias de l'utilisateur, car les services Bureau à distance l'ajoutent automatiquement à l'ouverture de session. **Remarque** Le champ Lettre du lecteur est ignoré si vous choisissez de spécifier un chemin local. Si vous choisissez de spécifier un chemin local, mais que vous tapez ensuite le nom d'un partage réseau dans le chemin d'accès racine au répertoire de base, les services Bureau à distance placent les répertoires de base des utilisateurs dans l'emplacement réseau. Si l'état est défini sur Activé, les services Bureau à distance créent le répertoire de base de l'utilisateur dans l'emplacement spécifié sur l'ordinateur local ou le réseau. Le chemin d'accès au répertoire de base de chaque utilisateur correspond au chemin d'accès racine au répertoire de base et à l'alias de l'utilisateur. Si l'état est défini sur Désactivé ou Non configuré, le répertoire de base de l'utilisateur est celui qui est spécifié au niveau du serveur.

Tableau 5-18. Paramètres de stratégie de groupe des profils RDS (suite)

Paramètre	Description
`Use mandatory profiles on the RD Session Host server`	Ce paramètre de stratégie vous permet de spécifier si les services Bureau à distance utilisent un profil obligatoire pour tous les utilisateurs se connectant à distance à l'hôte RDS. Si vous activez ce paramètre de stratégie, les services Bureau à distance utilisent le chemin d'accès spécifié dans le paramètre de stratégie `Set path for Remote Desktop Services Roaming User Profile` en tant que dossier racine du profil d'utilisateur obligatoire. Tous les utilisateurs se connectant à distance à l'hôte RDS utilisent le même profil d'utilisateur. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les profils d'utilisateur obligatoires ne sont pas employés par les utilisateurs qui se connectent à distance à l'hôte RDS. **Remarque** Pour que ce paramètre de stratégie entre en vigueur, vous devez également activer et configurer le paramètre de stratégie `Set path for Remote Desktop Services Roaming User Profile`.
`Set path for Remote Desktop Services Roaming User Profile`	Ce paramètre de stratégie vous permet de spécifier le chemin d'accès réseau que les services Bureau à distance utilisent pour les profils d'utilisateur itinérant. Par défaut, les services Bureau à distance stockent tous les profils d'utilisateur localement sur l'hôte RDS. Vous pouvez utiliser ce paramètre de stratégie pour spécifier un partage réseau sur lequel les profils d'utilisateur peuvent être centralisés, ce qui permet aux utilisateurs d'accéder au même profil lors de sessions sur tous les hôtes RDS configurés pour utiliser le partage réseau pour les profils d'utilisateur. Si vous activez ce paramètre de stratégie, les services Bureau à distance utilisent le chemin d'accès spécifié en tant que répertoire de base pour tous les profils utilisateurs. Les profils sont situés dans des sous-dossiers portant le nom de compte de chaque utilisateur. Pour configurer ce paramètre de stratégie, tapez le chemin d'accès au partage réseau sous la forme `\\NomOrdinateur\NomPartage`. Ne spécifiez pas d'espace réservé pour le nom de compte de l'utilisateur, car les services Bureau à distance l'ajoutent automatiquement lors de l'ouverture de session de l'utilisateur et de la création du profil. Si le partage réseau spécifié n'existe pas, les services Bureau à distance affichent un message d'erreur sur l'hôte RDS et stockent les profils d'utilisateur localement sur l'hôte RDS. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les profils d'utilisateur sont stockés localement sur l'hôte RDS. Vous pouvez configurer le chemin d'accès au profil d'un utilisateur dans l'onglet Profil des services Bureau à distance de la boîte de dialogue Propriétés du compte de l'utilisateur. Remarques : 1 Les profils utilisateurs itinérants activés par le paramètre de stratégie s'appliquent uniquement aux connexions des services Bureau à distance. Un utilisateur peut également posséder un profil d'utilisateur itinérant Windows configuré. Le profil d'utilisateur itinérant des services Bureau à distance est toujours prioritaire dans une session des services Bureau à distance. 2 Pour configurer un profil d'utilisateur itinérant des services Bureau à distance obligatoire pour tous les utilisateurs se connectant à distance à l'hôte RDS, utilisez ce paramètre de stratégie conjointement avec le paramètre

Tableau 5-18. Paramètres de stratégie de groupe des profils RDS (suite)

Paramètre	Description
	de stratégie `Use mandatory profiles on the RD Session Host server` situé dans **Configuration ordinateur\Modèles d'administration\Composants Windows\Services Bureau à distance\Hôte session Bureau à distance\Profils**. Le chemin d'accès défini dans le paramètre de stratégie `Set path for Remote Desktop Services Roaming User Profile` doit contenir le profil obligatoire.

Paramètres du Serveur de connexion RDS

Les paramètres de la stratégie de groupe Serveur de connexion RDS permettent aux utilisateurs de définir des stratégies pour le Serveur de connexion.

Les paramètres de la stratégie de groupe RDS d'Horizon 7 sont installés dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Service Broker pour les connexions Bureau à distance**.

Tableau 5-19. Paramètres de la stratégie de groupe du Serveur de connexion RDS

Paramètre	Description
`Join RD Connection Broker`	Utilisez ce paramètre de stratégie pour spécifier si l'hôte RDS doit se joindre à une batterie de serveurs du Serveur de connexion installé sur un hôte RDS. Le Serveur de connexion sur un hôte RDS assure le suivi des sessions utilisateur et permet à un utilisateur de se reconnecter à sa session existante dans une batterie de serveurs RDS à charge équilibrée. Pour rejoindre le Serveur de connexion sur un hôte RDS, le service de rôle Hôte de session Bureau à distance doit être installé sur l'hôte RDS. Si le paramètre de stratégie est activé, l'hôte RDS se joint à la batterie de serveurs spécifiée dans le paramètre « Configurer le nom de la batterie de serveurs du service Broker pour les connexions Bureau à distance ». La batterie de serveurs existe sur le Serveur de connexion spécifié dans le paramètre de stratégie « Configurer le nom du serveur du service Broker pour les connexions Bureau à distance ». Si vous désactivez ce paramètre de stratégie, l'hôte RDS ne se joint à aucune batterie de serveurs du Serveur de connexion et le suivi des sessions utilisateur n'a pas lieu. Si le paramètre est désactivé, vous ne pouvez pas utiliser l'outil Configuration d'hôte de session Bureau à distance ou le fournisseur WMI des services Terminal Server pour joindre l'hôte RDS au Serveur de connexion. Si le paramètre de stratégie n'est pas configuré, il n'est pas spécifié au niveau de la stratégie de groupe. Dans ce cas, vous pouvez configurer l'hôte RDS pour qu'il se joigne au Serveur de connexion sur l'hôte RDS à l'aide de l'outil Configuration d'hôte de session Bureau à distance ou du fournisseur WMI des services Terminal Server. **Remarque** 1 Si vous activez ce paramètre, vous devez également activer les paramètres de stratégie « Configurer le nom de la batterie de serveurs du service Broker pour les connexions Bureau à distance » et « Configurer le nom du serveur du service Broker pour les connexions Bureau à distance » ou les configurer à l'aide de l'outil Configuration d'hôte de session Bureau à distance ou du fournisseur WMI des services Terminal Server. 2 Pour Windows Server 2008, ce paramètre de stratégie est pris en charge par Windows Server 2008 Standard et éditions ultérieures.
`Configure RD Connection Broker farm name`	Utilisez ce paramètre de stratégie pour spécifier le nom d'une batterie de serveurs à joindre au Serveur de connexion pour un hôte RDS. Le Serveur de connexion utilise le nom de la batterie de serveurs pour déterminer quels hôtes RDS appartiennent à la même batterie de serveurs RDS. Vous devez donc utiliser le même nom de batterie de serveurs pour tous les hôtes RDS qui appartiennent à la même batterie de serveurs à charge équilibrée. Le nom de la batterie ne doit pas nécessairement correspondre à un nom des services de domaine Active Directory. Si vous donnez un autre nom à la batterie de serveurs, une batterie de serveurs est créée dans le Serveur de connexion pour l'hôte RDS. Si vous indiquez le nom d'une batterie de serveurs existante, l'hôte RDS se joint à cette batterie de serveurs dans le Serveur de connexion sur l'hôte RDS. Si vous activez ce paramètre de stratégie, vous devez spécifier le nom d'une batterie de serveurs dans le Serveur de connexion pour l'hôte RDS.

Tableau 5-19. Paramètres de la stratégie de groupe du Serveur de connexion RDS (suite)

Paramètre	Description
	Si vous désactivez ou ne configurez pas ce paramètre de stratégie, le nom de la batterie de serveurs n'est pas spécifié dans la stratégie de groupe. Dans ce cas, vous pouvez définir le nom de la batterie de serveurs à l'aide de l'outil Configuration d'hôte de session Bureau à distance ou du fournisseur WMI des services Terminal Server. **Remarque** Pour Windows Server 2008, ce paramètre de stratégie est pris en charge par Windows Server 2008 Standard et éditions ultérieures. Ce paramètre est effectif uniquement lorsque les paramètres « Joindre le service Broker pour les connexions Bureau à distance » et « Configurer le nom du serveur du service Broker pour les connexions Bureau à distance » sont tous deux activés et configurés à l'aide de la stratégie de groupe, de l'outil Configuration d'hôte de session Bureau à distance ou du fournisseur WMI des services Terminal Server.
`Use IP Address Redirection`	Utilisez ce paramètre de stratégie pour spécifier la méthode de redirection à utiliser lorsqu'un périphérique client se reconnecte à une session existante des services Bureau à distance dans une batterie de serveurs RDS à charge équilibrée. Ce paramètre s'applique à un hôte RDS configuré pour utiliser le Serveur de connexion sur un hôte RDS, et non au Serveur de connexion sur un poste de travail distant. Si vous activez ce paramètre de stratégie, un client des services Bureau à distance interroge le Serveur de connexion sur l'hôte RDS, puis il est redirigé vers une session existante à l'aide de l'adresse IP de l'hôte RDS de la session où elle se trouve. Pour utiliser cette méthode de redirection, les ordinateurs clients doivent être capables de se connecter directement par adresse IP à l'hôte RDS de la batterie de serveurs. Si vous désactivez ce paramètre de stratégie, l'adresse IP de l'hôte RDS n'est pas envoyée au client. Au lieu de cela, l'adresse IP est intégrée dans un jeton. Lorsqu'un client se reconnecte à l'équilibrage de charge, le jeton de routage est utilisé pour rediriger le client vers la session existante sur l'hôte RDS correct de la batterie de serveurs. Désactivez ce paramètre uniquement lorsque votre solution d'équilibrage de charge réseau prend en charge l'utilisation des jetons de routage du Serveur de connexion de l'hôte RDS et lorsque vous ne voulez pas que les clients se connectent directement par adresse IP à l'hôte RDS de la batterie de serveurs à charge équilibrée. Si vous ne configurez pas ce paramètre de stratégie, le paramètre « Utiliser la redirection d'adresse IP » de l'outil Configuration d'hôte de session Bureau à distance est utilisé. Par défaut, ce paramètre est activé dans l'outil Configuration d'hôte de session Bureau à distance. **Remarque** Pour Windows Server 2008, ce paramètre de stratégie est pris en charge par Windows Server 2008 Standard et éditions ultérieures.

Tableau 5-19. Paramètres de la stratégie de groupe du Serveur de connexion RDS (suite)

Paramètre	Description
`Configure RD Connection Broker Server name`	Utilisez ce paramètre de stratégie pour spécifier le Serveur de connexion utilisé par l'hôte RDS pour suivre et rediriger les sessions utilisateur d'une batterie de serveurs RDS à charge équilibrée. L'hôte RDS spécifié doit exécuter le service Serveur de connexion. Tous les hôtes RDS d'une batterie de serveurs à charge équilibrée doivent utiliser le même Serveur de connexion. Si vous activez ce paramètre de stratégie, vous devez spécifier le Serveur de connexion pour l'hôte RDS par son nom d'hôte, son adresse IP ou son nom de domaine complet. Si vous spécifiez un nom ou une adresse IP non valide pour le Serveur de connexion, un message d'erreur est enregistré dans l'Observateur d'événements sur l'hôte RDS. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, vous pouvez définir le nom ou l'adresse IP du Serveur de connexion de l'hôte RDS à l'aide de l'outil Configuration d'hôte de session Bureau à distance ou du fournisseur WMI des services Terminal Server. **Remarque** ■ Pour Windows Server 2008, ce paramètre de stratégie est pris en charge par Windows Server 2008 Standard. ■ Ce paramètre de stratégie est effectif uniquement lorsque le paramètre de stratégie « Joindre le service Broker pour les connexions Bureau à distance » est activé ou lorsque l'hôte RDS est configuré pour se joindre au Serveur de connexion sur l'hôte RDS à l'aide de l'outil Configuration d'hôte de session Bureau à distance ou du fournisseur WMI des services Terminal Server. ■ Pour être membre actif d'une session compatible avec le Serveur de connexion sur une batterie de serveurs RDS, le compte d'ordinateur de chaque hôte RDS de la batterie de serveurs doit être membre du groupe local « Ordinateurs annuaire de sessions » sur le Serveur de connexion pour l'hôte RDS.
`Use RD Connection Broker load balancing`	Utilisez ce paramètre de stratégie pour spécifier s'il convient d'utiliser la fonctionnalité d'équilibrage de charge du Serveur de connexion sur un hôte RDS pour équilibrer la charge entre des serveurs d'une batterie de serveurs RDS. Si vous activez ce paramètre de stratégie, le Serveur de connexion sur un hôte RDS redirige les utilisateurs qui n'ont pas de session en cours vers l'hôte RDS dans la batterie de serveurs ayant le moins de sessions. Le comportement de redirection pour les utilisateurs ayant des sessions en cours n'est pas affecté. Si le serveur est configuré de façon à utiliser le Serveur de connexion sur un hôte RDS, les utilisateurs ayant une session en cours sont redirigés vers l'hôte RDS où réside leur session. Si vous désactivez ce paramètre de stratégie, les utilisateurs qui n'ont pas de session en cours se connectent au premier hôte RDS auquel ils se sont initialement connectés.

Tableau 5-19. Paramètres de la stratégie de groupe du Serveur de connexion RDS (suite)

Paramètre	Description
	Si vous ne configurez pas ce paramètre de stratégie, vous pouvez configurer l'hôte RDS pour qu'il participe à l'équilibrage de charge du Serveur de connexion pour l'hôte RDS à l'aide de l'outil Configuration d'hôte de session Bureau à distance ou du fournisseur WMI des services Terminal Server. **Remarque** Si vous activez ce paramètre de stratégie, vous devez également activer les paramètres de stratégie « Joindre le service Broker pour les connexions Bureau à distance », « Configurer le nom de la batterie de serveurs du service Broker pour les connexions Bureau à distance » et « Configurer le nom du serveur du service Broker pour les connexions Bureau à distance ».

Paramètres d'environnement de session distante RDS

Les paramètres de la stratégie de groupe Environnement de session à distance RDS contrôlent la configuration de l'interface utilisateur dans les sessions des services Bureau à distance.

Les paramètres de la stratégie de groupe RDS d'Horizon 7 sont installés dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Environnement de session à distance**.

Les paramètres de la stratégie de groupe RDS d'Horizon 7 sont également installés dans le dossier **Configuration utilisateur > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Environnement de session à distance**.

Tableau 5-20. Paramètres de la stratégie de groupe de l'environnement de session distante RDS

Paramètre	Description
`Limit maximum color depth`	Utilisez ce paramètre de stratégie pour spécifier la résolution de couleur maximale (intensité de couleur) pour les connexions des services Bureau à distance. Vous pouvez utiliser ce paramètre de stratégie pour définir une limite au nombre de couleurs de toute connexion à l'aide du protocole RDP. La limitation de l'intensité de couleur peut améliorer les performances des connexions, en particulier en présence de liaisons lentes, et réduire la charge du serveur. Si vous activez ce paramètre de stratégie, le nombre de couleurs que vous spécifiez correspond au nombre maximal de couleurs autorisé pour la connexion d'un utilisateur via le protocole RDP. L'intensité de couleur réelle de la connexion est déterminée par la prise en charge des couleurs disponible sur l'ordinateur client. Si vous sélectionnez « Compatible client », l'intensité de couleur la plus élevée prise en charge par le client est utilisée. **Remarque** Le nombre de couleurs 24 bits n'est pris en charge que sur Windows XP Professionnel et Windows Server 2003. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, le nombre de couleurs des connexions est déterminé par le paramètre « Limiter le nombre maximal de couleurs » dans l'onglet Paramètres client de l'outil Configuration d'hôte de session Bureau à distance, à moins qu'un niveau inférieur soit spécifié par l'utilisateur au moment de la connexion.
`Enforce Removal of Remote Desktop Wallpaper`	Spécifie si le papier peint du Bureau s'affiche pour les clients distants qui se connectent via les services Bureau à distance. Vous pouvez utiliser ce paramètre pour appliquer la suppression du papier peint lors d'une session des services Bureau à distance. Par défaut, Windows XP Professionnel affiche le papier peint pour les clients distants qui se connectent par l'intermédiaire du Bureau à distance, en fonction de la configuration du client. Pour plus d'informations, consultez l'onglet Avancé dans les options de Connexion Bureau à distance. Par défaut, les serveurs qui exécutent Windows Server 2003 n'affichent pas le papier peint pour les sessions de services Bureau à distance. Si vous activez ce paramètre, le papier peint ne s'affiche jamais dans une session des services Bureau à distance. Si vous désactivez ce paramètre, le papier peint peut s'afficher dans une session des services Bureau à distance, en fonction de la configuration du client. Si vous ne configurez pas ce paramètre, le comportement par défaut s'applique.

Tableau 5-20. Paramètres de la stratégie de groupe de l'environnement de session distante RDS (suite)

Paramètre	Description
`Configure RemoteFX`	Utilisez ce paramètre de stratégie pour contrôler la disponibilité de RemoteFX sur un hôte de virtualisation des services Bureau à distance et un hôte RDS. Lorsque RemoteFX est déployé sur un hôte de virtualisation des services Bureau à distance, il enrichit l'expérience utilisateur en assurant le rendu du contenu sur le serveur via des unités de traitement graphique (GPU) ou du matériel. Par défaut, RemoteFX pour hôte de virtualisation des services Bureau à distance utilise les GPU côté serveur ou le matériel pour assurer une expérience utilisateur enrichie via des connexions au réseau local et RDP 7.1. Lorsque RemoteFX est déployé sur un hôte RDS, il assure une expérience utilisateur enrichie via un schéma de compression à accélération matérielle. Si vous activez ce paramètre de stratégie, RemoteFX assure une expérience utilisateur enrichie via des connexions au réseau local et RDP 7.1. Si vous désactivez ce paramètre de stratégie, RemoteFX est désactivé. Si vous ne configurez pas ce paramètre de stratégie, le comportement par défaut est utilisé. Par défaut, RemoteFX pour hôte de virtualisation des services Bureau à distance est activé et RemoteFX pour hôte RDS est désactivé.
`Limit maximum display resolution`	Utilisez ce paramètre de stratégie pour spécifier la résolution d'affichage maximale pouvant être utilisée par chaque moniteur servant à afficher une session des services Bureau à distance. La limitation de la résolution utilisée pour afficher une session à distance peut améliorer les performances de connexion, en particulier en cas de liaisons lentes, et réduire la charge de travail du serveur. Si vous activez ce paramètre de stratégie, vous devez spécifier une largeur et une hauteur de résolution. La résolution spécifiée sera la résolution maximale pouvant être appliquée à chaque moniteur utilisé pour afficher une session des services Bureau à distance. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, la résolution maximale pouvant être utilisée par chaque moniteur pour afficher une session des services Bureau à distance sera déterminée par les valeurs spécifiées dans l'onglet Paramètres d'affichage de l'outil Configuration d'hôte de session Bureau à distance.
`Limit maximum number of monitors`	Utilisez ce paramètre de stratégie pour limiter le nombre de moniteurs qu'un utilisateur peut utiliser pour afficher une session des services Bureau à distance. La limitation du nombre de moniteurs permettant d'afficher une session des services Bureau à distance peut améliorer les performances de connexion, en particulier en cas de liaisons lentes, et réduire la charge de travail du serveur. Si vous activez ce paramètre de stratégie, vous pouvez spécifier le nombre de moniteurs pouvant être utilisés pour afficher une session des services Bureau à distance. Vous pouvez spécifier un nombre compris entre 1 et 10. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, le nombre de moniteurs pouvant être utilisés pour afficher une session des services Bureau à distance est déterminé par la valeur spécifiée dans la zone « Nombre maximal de moniteurs par session » dans l'onglet Paramètres d'affichage de l'outil Configuration d'hôte de session Bureau à distance.

Tableau 5-20. Paramètres de la stratégie de groupe de l'environnement de session distante RDS (suite)

Paramètre	Description
`Remove "Disconnect" option from Shut Down dialog`	Utilisez ce paramètre de stratégie pour supprimer l'option « Déconnecter » de la boîte de dialogue Arrêt de Windows dans les sessions des services Bureau à distance. Vous pouvez utiliser ce paramètre de stratégie pour empêcher les utilisateurs d'employer cette méthode courante pour déconnecter leur client d'un hôte RDS. Si vous activez ce paramètre de stratégie, « Déconnecter » ne s'affiche pas parmi les options de la liste déroulante de la boîte de dialogue Arrêt de Windows. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, l'option « Déconnecter » n'est pas supprimée de la liste de la boîte de dialogue Arrêt de Windows. **Remarque** Ce paramètre de stratégie concerne seulement la boîte de dialogue Arrêt de Windows. Il n'empêche pas les utilisateurs d'employer d'autres méthodes pour se déconnecter d'une session des services Bureau à distance. Il n'empêche pas non plus les sessions déconnectées au niveau du serveur. Vous pouvez contrôler combien de temps une session déconnectée reste active sur le serveur en configurant le paramètre de stratégie « Définir le délai d'expiration des sessions déconnectées » dans le dossier **Configuration ordinateur > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Délais d'expiration des sessions**.
`Optimize visual experience when using RemoteFX`	Utilisez ce paramètre de stratégie pour spécifier l'expérience visuelle des utilisateurs distants via des connexions RDC qui utilisent RemoteFX. Vous pouvez utiliser cette stratégie pour équilibrer l'utilisation de la bande passante réseau et l'expérience graphique proposée. Selon les besoins des utilisateurs, vous pouvez limiter l'utilisation de la bande passante réseau en réduisant le taux de capture d'écran. Vous pouvez également limiter l'utilisation de la bande passante réseau en réduisant la qualité de l'image (augmentation du taux de compression d'images). Si votre réseau présente une bande passante supérieure à la moyenne, vous pouvez en optimiser l'exploitation en sélectionnant le paramètre le plus élevé de taux de capture d'écran et de qualité de l'image. Par défaut les sessions Connexion Bureau à distance qui utilisent RemoteFX sont optimisées pour assurer une expérience utilisateur équilibrée sur un réseau local. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les sessions Connexion Bureau à distance qui utilisent RemoteFX adoptent des paramètres moyens de taux de capture d'écran et de compression d'images (comportement par défaut).

Tableau 5-20. Paramètres de la stratégie de groupe de l'environnement de session distante RDS (suite)

Paramètre	Description
`Set compression algorithm for RDP data`	Utilisez ce paramètre de stratégie pour spécifier l'algorithme de compression RDP (Remote Desktop Protocol) à utiliser. Par défaut, les serveurs utilisent un algorithme de compression RDP qui dépend de la configuration matérielle du serveur. Si vous activez ce paramètre de stratégie, vous pouvez spécifier l'algorithme de compression RDP à utiliser. Si vous sélectionnez l'algorithme optimisé pour consommer moins de mémoire, cette option sollicite moins de mémoire, mais la bande passante réseau utilisée est supérieure. Si vous sélectionnez l'algorithme optimisé pour utiliser moins de bande passante réseau, cette option restreint l'utilisation de la bande passante réseau, mais sollicite davantage de mémoire. Une troisième option est disponible pour utiliser la mémoire et la bande passante réseau de façon équilibrée. Vous pouvez également décider de ne pas utiliser d'algorithme de compression RDP. Si vous décidez de ne pas utiliser d'algorithme de compression RDP, vous utilisez davantage de bande passante réseau et cela n'est recommandé que si vous utilisez un périphérique matériel conçu pour optimiser le trafic sur le réseau. Même si vous décidez de ne pas recourir à un algorithme de compression RDP, certaines données graphiques sont compressées. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, l'algorithme de compression RDP par défaut est utilisé.
`Optimize visual experience for Remote Desktop Services sessions`	Utilisez ce paramètre de stratégie pour spécifier l'expérience visuelle des utilisateurs distants lors des sessions des services Bureau à distance. Les sessions à distance exécutées sur l'ordinateur distant sont ensuite optimisées pour assurer cette expérience visuelle. Par défaut, les sessions des services Bureau à distance sont optimisées pour un contenu multimédia riche (applications ayant recours à Silverlight ou Windows Presentation Foundation, par exemple). Si vous activez ce paramètre de stratégie, vous devez sélectionner l'expérience visuelle pour laquelle vous souhaitez optimiser des sessions des services Bureau à distance. Vous avez le choix entre Contenu multimédia et Texte. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les sessions des services Bureau à distance sont optimisées pour un contenu multimédia riche.

Tableau 5-20. Paramètres de la stratégie de groupe de l'environnement de session distante RDS (suite)

Paramètre	Description
`Start a program on connection`	Configure les services Bureau à distance pour qu'ils exécutent automatiquement un programme spécifié lors de la connexion. Vous pouvez utiliser ce paramètre pour spécifier un programme à exécuter automatiquement lorsqu'un utilisateur se connecte à un ordinateur distant. Par défaut, les sessions des services Bureau à distance fournissent un accès à la totalité du Bureau Windows, sauf si l'administrateur du serveur ou l'utilisateur, lors de la configuration de la connexion client, spécifie le contraire à l'aide de ce paramètre. L'activation de ce paramètre annule les paramètres « Démarrer le programme » définis par l'administrateur du serveur ou l'utilisateur. Le menu Démarrer et le Bureau Windows ne sont pas affichés et, quand l'utilisateur quitte le programme, la session est automatiquement déconnectée. Pour utiliser ce paramètre, dans Chemin d'accès au programme et nom du fichier, tapez le chemin d'accès et le nom de fichier complets du fichier à exécuter quand l'utilisateur ouvre une session. Si nécessaire, dans Répertoire de travail, entrez le chemin complet du répertoire de démarrage du programme. Si vous n'indiquez rien dans Répertoire de travail, le programme est exécuté à partir de son répertoire de travail par défaut. Si le répertoire de travail, le nom de fichier ou le chemin du programme spécifié n'est pas le nom d'un répertoire valide, la connexion de l'hôte RDS échoue en affichant un message d'erreur. Si vous activez ce paramètre, les sessions des services Bureau à distance exécutent automatiquement le programme spécifié et utilisent le répertoire de travail indiqué (ou, à défaut, le répertoire par défaut du programme). Si vous désactivez ou ne configurez pas ce paramètre, les sessions des services Bureau à distance démarrent avec l'intégralité du Bureau, sauf si l'administrateur du serveur ou l'utilisateur en décident autrement. Pour plus d'informations, consultez le paramètre de stratégie « Exécuter ces programmes à l'ouverture de session utilisateur » dans le dossier **Configuration ordinateur > Modèles d'administration > Système > Ouverture de session**. **Remarque** Ce paramètre apparaît dans Configuration ordinateur et Configuration utilisateur. Si les deux paramètres sont configurés, le paramètre Configuration ordinateur remplace le paramètre Configuration utilisateur.

Tableau 5-20. Paramètres de la stratégie de groupe de l'environnement de session distante RDS (suite)

Paramètre	Description
`Always show desktop on connection`	Ce paramètre de stratégie permet de spécifier, lors de la connexion d'un client à un ordinateur distant, soit l'affichage systématique du Bureau, soit le démarrage initial d'un programme. Utilisez ce paramètre pour imposer l'affichage du Bureau lors de la connexion d'un client à un ordinateur distant, même si le profil d'utilisateur par défaut, les paramètres de Connexion Bureau à distance, le client des services Bureau à distance ou la stratégie de groupe prévoient déjà un programme de démarrage initial. Si vous activez ce paramètre de stratégie, le Bureau s'affiche toujours lors de la connexion d'un client à un ordinateur distant. Ce paramètre de stratégie remplace tout autre paramètre de stratégie relatif au démarrage du programme initial. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, un programme initial peut être spécifié pour s'exécuter sur l'ordinateur distant après la connexion du client à ce dernier. Si aucun programme initial n'est spécifié, le Bureau est toujours affiché sur l'ordinateur distant après la connexion du client à cet ordinateur. **Remarque** Si ce paramètre de stratégie est activé, le paramètre de stratégie « Démarrer un programme à la connexion » est ignoré.
`Allow desktop composition for remote desktop sessions`	Utilisez ce paramètre de stratégie pour spécifier si la composition du Bureau est autorisée pour les sessions Bureau à distance. Il ne s'applique pas aux sessions RemoteApp. La composition du Bureau fournit les éléments de l'interface utilisateur de Windows Aero, telles que des fenêtres translucides, pour les sessions Bureau à distance. Windows Aero nécessitant des ressources système et de bande passante supplémentaires, le fait d'autoriser la composition du Bureau pour les sessions Bureau à distance peut réduire les performances de connexion, particulièrement dans le contexte de liaisons lentes, et augmenter la charge sur l'ordinateur distant. Si vous activez ce paramètre de stratégie, la composition du Bureau sera autorisée pour les sessions Bureau à distance. Sur l'ordinateur client, vous pouvez configurer la composition du Bureau dans l'onglet Avancé de la Connexion Bureau à distance (RDC, Remote Desktop Connection) ou à l'aide du paramètre d'autorisation de la composition du Bureau dans un fichier .rdp (Remote Desktop Protocol). L'ordinateur client doit être doté du matériel nécessaire à la prise en charge des fonctionnalités Windows Aero. **Remarque** Il peut être nécessaire de procéder à une configuration supplémentaire sur l'ordinateur distant afin que les sessions Bureau à distance puissent bénéficier des fonctionnalités Windows Aero. Par exemple, la fonctionnalité Expérience utilisateur doit être installée sur l'ordinateur distant et le nombre maximal de couleurs sur cet ordinateur doit être de 32 bits par pixel. Le service Thèmes doit également être démarré sur l'ordinateur distant. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, la composition du Bureau n'est pas autorisée pour les sessions Bureau à distance, même si elle est activée pour RDC ou dans le fichier .rdp.

Tableau 5-20. Paramètres de la stratégie de groupe de l'environnement de session distante RDS (suite)

Paramètre	Description
`Do not allow font smoothing`	Utilisez ce paramètre de stratégie pour spécifier si le lissage des polices est autorisé pour les connexions à distance. Le lissage des polices permet aux connexions à distance de bénéficier de la fonctionnalité ClearType. ClearType est une technologie permettant d'afficher les polices de façon très nette, tout particulièrement sur les écrans LCD. Dans la mesure où le lissage des polices requiert des ressources supplémentaires en matière de bande passante, la désactivation de ce paramètre peut améliorer les performances de connexion, en particulier dans le cas de liaisons lentes. Par défaut, le lissage des polices est autorisé pour les connexions à distance. Vous pouvez configurer le lissage des polices dans l'onglet Avancé de la Connexion Bureau à distance (RDC, Remote Desktop Connection) ou à l'aide du paramètre Autoriser le lissage des polices dans un fichier .rdp (Remote Desktop Protocol). Si vous activez ce paramètre, le lissage des polices ne sera pas autorisé pour les connexions à distance, même s'il est activé dans RDC ou dans le fichier .rdp. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, le lissage des polices est autorisé pour les connexions à distance.
`Remove Windows Security item from Start menu`	Spécifie s'il convient de supprimer l'élément Sécurité de Windows du menu Paramètres sur les clients Bureau à distance. Vous pouvez utiliser ce paramètre pour empêcher les utilisateurs inexpérimentés de se déconnecter accidentellement des services Bureau à distance. Si l'état est défini sur Activé, Sécurité de Windows ne s'affiche pas sous Paramètres dans le menu Démarrer. Par conséquent, les utilisateurs doivent taper une séquence d'attention de sécurité, telle que CTRL+ALT+FIN, pour ouvrir la boîte de dialogue Sécurité de Windows sur l'ordinateur client. Si l'état est défini sur Désactivé ou Non configuré, Sécurité de Windows figure toujours dans le menu Paramètre.

Paramètres de sécurité RDS

Le paramètre de stratégie de groupe de sécurité RDS contrôle si les administrateurs locaux peuvent personnaliser les autorisations.

Les paramètres de la stratégie de groupe RDS d'Horizon 7 sont installés dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Sécurité**.

Tableau 5-21. Paramètres de la stratégie de groupe de sécurité RDS

Paramètre	Description
`Server Authentication Certificate Template`	Utilisez ce paramètre de stratégie pour spécifier le nom du modèle de certificat qui détermine le certificat sélectionné automatiquement pour authentifier un hôte RDS. Un certificat est nécessaire pour authentifier un hôte RDS lorsque SSL (TLS 1.0) est utilisé pour sécuriser les communications entre un client et un hôte RDS pendant des connexions RDP (Remote Desktop Protocol). Si vous activez ce paramètre de stratégie, vous devez spécifier un nom de modèle de certificat. Seuls les certificats créés à l'aide du modèle de certificat spécifié sont pris en compte lors de la sélection automatique d'un certificat pour authentifier l'hôte RDS. Un certificat est sélectionné automatiquement uniquement si aucun certificat n'a été spécifié. S'il n'existe aucun certificat créé à l'aide du modèle de certificat spécifié, l'hôte RDS émet une demande d'inscription de certificat et utilise le certificat actif jusqu'à ce que la demande soit traitée. S'il existe plusieurs certificats créés à l'aide du modèle de certificat spécifié, le certificat dont la date d'expiration est la plus éloignée et qui correspond au nom actuel de l'hôte RDS est sélectionné. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, un certificat auto-signé est utilisé par défaut pour authentifier l'hôte RDS. Vous pouvez sélectionner un certificat à utiliser pour authentifier l'hôte RDS dans l'onglet Général de l'outil Configuration d'hôte de session Bureau à distance. **Remarque** Si vous sélectionnez un certificat à utiliser pour authentifier l'hôte RDS, ce certificat est prioritaire sur ce paramètre de stratégie.
`Set client connection encryption level`	Spécifie s'il faut requérir l'utilisation d'un niveau de chiffrement spécifique pour sécuriser les communications entre les clients et les hôtes RDS lors des connexions RDP (Remote Desktop Protocol). Si vous activez ce paramètre, toutes les communications entre les clients et les hôtes RDS doivent utiliser la méthode de chiffrement spécifiée dans ce paramètre lors des connexions à distance. Par défaut, le niveau de chiffrement est défini sur Élevé. Les méthodes de chiffrement suivantes sont disponibles : ■ `High`. Le paramètre Élevé chiffre les données envoyées du client au serveur et du serveur au client à l'aide d'un chiffrement renforcé sur 128 bits. Utilisez ce niveau de chiffrement dans les environnements comportant

Tableau 5-21. Paramètres de la stratégie de groupe de sécurité RDS (suite)

Paramètre	Description
	seulement des clients 128 bits (par exemple, des clients qui exécutent une connexion Bureau à distance). Les clients qui ne prennent pas en charge ce niveau de chiffrement ne peuvent pas se connecter aux serveurs d'hôte RDS. ■ `Client Compatible`. Le paramètre Compatible avec le client chiffre les données envoyées entre le client et le serveur avec la puissance de clé maximale prise en charge par le client. Utilisez ce niveau de chiffrement dans les environnements comportant des clients qui ne prennent pas en charge le chiffrement sur 128 bits. ■ `Low`. Le paramètre Faible chiffre seulement les données envoyées du client au serveur à l'aide d'un chiffrement sur 56 bits. Si vous désactivez ou ne configurez pas ce paramètre, le niveau de chiffrement à utiliser pour les connexions à distance à l'hôte RDS n'est pas appliqué via la stratégie de groupe. Vous pouvez cependant configurer un niveau de chiffrement obligatoire pour ces connexions à l'aide de l'outil Configuration d'hôte de session Bureau à distance. **Important** La conformité FIPS peut être configurée via le paramètre de stratégie « Chiffrement système : utiliser des algorithmes compatibles FIPS pour le chiffrement, le hachage et la signature » dans le dossier **Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité** ou via le paramètre « Compatible FIPS » de l'outil Configuration d'hôte de session Bureau à distance. Le paramètre Compatible FIPS chiffre et déchiffre les données envoyées du client vers le serveur et du serveur vers le client, avec les algorithmes de chiffrement FIPS (Federal Information Processing Standard) 140-1, à l'aide des modules de chiffrement Microsoft. Utilisez ce niveau de chiffrement quand les communications entre les clients et les hôtes RDS nécessitent un niveau de chiffrement élevé. Si la compatibilité FIPS est déjà activée via le paramètre de stratégie de groupe « Chiffrement système : utiliser des algorithmes compatibles FIPS pour le chiffrement, le hachage et la signature », ce paramètre remplace le niveau de chiffrement spécifié dans ce paramètre de stratégie de groupe ou dans l'outil Configuration d'hôte de session Bureau à distance.

Tableau 5-21. Paramètres de la stratégie de groupe de sécurité RDS (suite)

Paramètre	Description
`Always prompt for password upon connection`	Spécifie si les services Bureau à distance demandent toujours un mot de passe au client lors de la connexion. Vous pouvez utiliser ce paramètre pour forcer la demande de mot de passe aux utilisateurs se connectant aux services Bureau à distance, même s'ils ont déjà fourni le mot de passe dans le client Connexion Bureau à distance. Par défaut, les services Bureau à distance autorisent les utilisateurs à se connecter automatiquement en entrant un mot de passe dans le client Connexion Bureau à distance. Si vous activez ce paramètre de stratégie, les utilisateurs ne peuvent pas se connecter automatiquement aux services Bureau à distance en fournissant leurs mots de passe dans le client Connexion Bureau à distance. Un mot de passe leur est demandé pour ouvrir une session. Si vous désactivez ce paramètre, les utilisateurs peuvent toujours se connecter automatiquement aux services Bureau à distance en fournissant leurs mots de passe dans le client Connexion Bureau à distance. Si vous ne configurez pas ce paramètre, l'ouverture de session automatique n'est pas spécifiée au niveau de la stratégie de groupe. Toutefois, un administrateur peut toujours forcer la demande d'un mot de passe en utilisant l'outil Configuration d'hôte de session Bureau à distance.
`Require secure RPC communication`	Spécifie si un hôte RDS requiert des communications RPC sécurisées avec tous les clients ou bien autorise des communications non sécurisées. Vous pouvez utiliser ce paramètre pour renforcer la sécurité des communications RPC avec les clients en autorisant seulement les demandes authentifiées et chiffrées. Si vous activez ce paramètre, les services Bureau à distance acceptent les demandes des clients RPC qui prennent en charge les demandes sécurisées et n'autorisent pas les communications non sécurisées avec les clients non approuvés. Si vous désactivez ce paramètre, les services Bureau à distance requièrent toujours la sécurité pour tout le trafic RPC. Cependant, les communications non sécurisées sont autorisées pour les clients RPC qui ne répondent pas à la demande. Si vous ne configurez pas ce paramètre, les communications non sécurisées sont autorisées. **Remarque** L'interface RPC sert à administrer et configurer les services Bureau à distance.

Tableau 5-21. Paramètres de la stratégie de groupe de sécurité RDS (suite)

Paramètre	Description
`Require use of specific security layer for remote (RDP) connections`	Spécifie s'il faut requérir l'utilisation d'une couche de sécurité spécifique pour sécuriser les communications entre les clients et les hôtes RDS lors des connexions RDP (Remote Desktop Protocol). Si vous activez ce paramètre, toutes les communications entre les clients et les hôtes RDS doivent utiliser la méthode de sécurité spécifiée dans ce paramètre lors des connexions à distance. Les méthodes de sécurité suivantes sont disponibles : ■ `Negotiate`. La méthode Négocier applique la méthode la plus sécurisée qui est prise en charge par le client. Si TLS (Transport Layer Security) version 1.0 est pris en charge, il est utilisé pour authentifier l'hôte RDS. Si TLS n'est pas pris en charge, le chiffrement RDP (Remote Desktop Protocol) natif est utilisé pour sécuriser les communications, mais l'hôte RDS n'est pas authentifié. ■ `RDP`. La méthode RDP utilise le chiffrement RDP natif pour sécuriser les communications entre le client et l'hôte RDS. Si vous sélectionnez cette valeur, l'hôte RDS n'est pas authentifié. ■ `SSL (TLS 1.0)`. La méthode SSL nécessite l'utilisation de TLS 1.0 pour authentifier l'hôte RDS. Si TLS n'est pas pris en charge, la connexion échoue. Si vous désactivez ou ne configurez pas ce paramètre, la méthode de sécurité à utiliser pour les connexions à distance aux hôtes RDS n'est pas appliquée via la stratégie de groupe. Vous pouvez cependant configurer une méthode de sécurité obligatoire pour ces connexions à l'aide de l'outil Configuration d'hôte de session Bureau à distance.

Tableau 5-21. Paramètres de la stratégie de groupe de sécurité RDS (suite)

Paramètre	Description
`Require user authentication for remote connections by using Network`	Utilisez ce paramètre de stratégie pour spécifier s'il faut requérir l'authentification utilisateur pour les connexions à distance à l'hôte RDS en utilisant l'authentification au niveau du réseau. Ce paramètre de stratégie renforce la sécurité en imposant l'authentification utilisateur plus tôt dans le processus de connexion à distance. Si vous activez ce paramètre de stratégie, seuls les ordinateurs client qui prennent en charge l'authentification au niveau du réseau peuvent se connecter à l'hôte RDS. Pour déterminer si un ordinateur client prend en charge l'authentification au niveau du réseau, démarrez Connexion Bureau à distance sur l'ordinateur client, cliquez sur l'icône dans le coin supérieur gauche de la boîte de dialogue Connexion Bureau à distance, puis cliquez sur À propos de. Dans la boîte de dialogue À propos de la Connexion Bureau à distance, recherchez l'expression « Authentification au niveau du réseau prise en charge ». Si vous désactivez ou ne configurez pas ce paramètre de stratégie, l'authentification au niveau du réseau n'est pas nécessaire pour l'authentification utilisateur avant d'autoriser les connexions à distance à l'hôte RDS. Vous pouvez spécifier que l'authentification au niveau du réseau soit requise pour l'authentification utilisateur à l'aide de l'outil Configuration d'hôte de session Bureau à distance ou de l'onglet Utilisation à distance dans Propriétés système. **Important** La désactivation ou la non-configuration de ce paramètre de stratégie offre moins de sécurité, car l'authentification utilisateur est effectuée plus tard dans le processus de connexion à distance.
`Do not allow local administrators to customize permissions`	Spécifie si vous devez désactiver les droits de l'administrateur à personnaliser des autorisations de sécurité dans l'outil de configuration de l'hôte RDS. Vous pouvez utiliser ce paramètre pour empêcher les administrateurs d'apporter des changements aux groupes d'utilisateurs sur l'onglet Autorisations de l'outil de configuration de l'hôte de session Bureau à distance. Par défaut, les administrateurs peuvent apporter ces changements. Si l'état est défini sur Activé, l'onglet Autorisations de l'outil de configuration de l'hôte de session Bureau à distance ne peut pas servir à personnaliser les descripteurs de sécurité par connexion ou à modifier les descripteurs de sécurité par défaut d'un groupe existant. Tous les descripteurs de sécurité sont en lecture seule. Si l'état est défini sur Désactivé ou Non configuré, les administrateurs du serveur disposent de privilèges de lecture/écriture complets sur les descripteurs de sécurité de l'utilisateur de l'onglet Autorisations dans l'outil de configuration de l'hôte de session Bureau à distance. **Remarque** Le mode de gestion préféré de l'accès utilisateur consiste à ajouter un utilisateur au groupe Utilisateurs de poste de travail distant.

Délais d'expiration des sessions RDS

Les paramètres de la stratégie de groupe Délais d'expiration des sessions RDS permettent aux utilisateurs de définir des stratégies pour les délais d'expiration des sessions sur des hôtes RDS.

Les paramètres de la stratégie de groupe RDS d'Horizon 7 sont installés dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Délais d'expiration des sessions**.

Les paramètres de la stratégie de groupe RDS d'Horizon 7 sont également installés dans le dossier **Configuration utilisateur > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Délais d'expiration des sessions**.

Tableau 5-22. Paramètres de la stratégie de groupe Délais d'expiration des sessions RDS

Paramètre	Description
`Set time limit for disconnected sessions`	Utilisez ce paramètre de stratégie pour configurer un délai d'expiration pour les sessions des services Bureau à distance déconnectées. Vous pouvez utiliser ce paramètre de stratégie pour spécifier la durée maximale pendant laquelle une session déconnectée est maintenue active sur le serveur. Par défaut, les services Bureau à distance permettent aux utilisateurs de se déconnecter d'une session des services Bureau à distance sans se déconnecter et mettre fin à la session. Quand une session est dans un état déconnecté, les programmes en cours d'exécution sont maintenus actifs même si l'utilisateur n'est plus connecté de façon active. Par défaut, ces sessions déconnectées sont conservées pendant une durée illimitée sur le serveur. Si vous activez ce paramètre de stratégie, les sessions déconnectées sont supprimées du serveur après une durée spécifiée. Pour appliquer le comportement par défaut consistant à conserver les sessions déconnectées pendant une durée illimitée, sélectionnez « Jamais ». Si vous avez une session de console, les limites de durée des sessions déconnectées ne s'appliquent pas. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les sessions déconnectées sont conservées pendant une durée illimitée. Vous pouvez spécifier des limites de durée pour les sessions déconnectées dans l'onglet Sessions de l'outil Configuration d'hôte de session Bureau à distance. **Remarque** Ce paramètre de stratégie s'affiche à la fois dans Configuration ordinateur et dans Configuration utilisateur. Si les deux paramètres de stratégie sont configurés, le paramètre de stratégie Configuration ordinateur est prioritaire.
`Set time limit for active but idle Remote Desktop Services sessions`	Utilisez ce paramètre de stratégie pour spécifier la durée maximale pendant laquelle une session des services Bureau à distance active peut demeurer inactive (sans saisie de données de la part de l'utilisateur) avant d'être automatiquement déconnectée. Pour activer ce paramètre de stratégie, vous devez sélectionner le délai souhaité dans la liste déroulante Limite de session inactive. Les services Bureau à distance déconnecteront automatiquement les sessions ouvertes mais inactives après la période de temps spécifiée. L'utilisateur reçoit un avertissement deux minutes avant la déconnexion de la session, ce qui lui permet d'appuyer sur une touche ou de déplacer la souris pour maintenir la session active. Si vous avez une session de console, les limites de durée des sessions inactives ne s'appliquent pas. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les services Bureau à distance autorisent les sessions à rester ouvertes, mais inactives pendant une durée illimitée. Vous pouvez spécifier des limites de durée pour les sessions ouvertes, mais inactives dans l'onglet Sessions de l'outil Configuration d'hôte de session Bureau à distance. Si vous voulez que les services Bureau à distance mettent fin à une session au lieu de la déconnecter quand le délai d'expiration est atteint, vous pouvez configurer le paramètre de stratégie « Mettre fin à la session quand les délais d'expiration ont été atteints » dans le dossier

Tableau 5-22. Paramètres de la stratégie de groupe Délais d'expiration des sessions RDS (suite)

Paramètre	Description
	Configuration ordinateur > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Délais d'expiration des sessions. **Remarque** Ce paramètre de stratégie s'affiche à la fois dans Configuration ordinateur et dans Configuration utilisateur. Si les deux paramètres de stratégie sont configurés, le paramètre de stratégie Configuration ordinateur est prioritaire.
`Set time limit for active Remote Desktop Services sessions`	Utilisez ce paramètre de stratégie pour spécifier la durée maximale pendant laquelle une session des services Bureau à distance peut être active avant d'être automatiquement déconnectée. Pour activer ce paramètre de stratégie, vous devez sélectionner le délai souhaité dans la liste déroulante Limite de session active. Les services Bureau à distance déconnecteront automatiquement les sessions actives après la durée spécifiée. L'utilisateur reçoit un avertissement deux minutes avant la déconnexion de la session des services Bureau à distance, ce qui lui permet d'enregistrer les fichiers ouverts et de fermer les programmes. Si vous avez une session de console, les limites de durée des sessions actives ne s'appliquent pas. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les services Bureau à distance autorisent les sessions à rester actives pendant une durée illimitée. Vous pouvez spécifier des limites de durée pour les sessions actives dans l'onglet Sessions de l'outil Configuration d'hôte de session Bureau à distance. Si vous voulez que les services Bureau à distance mettent fin à une session au lieu de la déconnecter quand le délai d'expiration est atteint, vous pouvez configurer le paramètre de stratégie « Mettre fin à la session quand les délais d'expiration ont été atteints » dans le dossier **Configuration ordinateur > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Délais d'expiration des sessions**. **Remarque** Ce paramètre de stratégie s'affiche à la fois dans Configuration ordinateur et dans Configuration utilisateur. Si les deux paramètres de stratégie sont configurés, le paramètre de stratégie Configuration ordinateur est prioritaire.

Tableau 5-22. Paramètres de la stratégie de groupe Délais d'expiration des sessions RDS (suite)

Paramètre	Description
`Terminate session when time limits are reached`	Spécifie si une session des services Bureau à distance ayant expiré doit être terminée plutôt que déconnectée. Vous pouvez utiliser ce paramètre pour indiquer aux services Bureau à distance de mettre fin à une session (autrement dit, l'utilisateur a fermé sa session et la session est supprimée du serveur) une fois les délais d'expiration des sessions actives ou inactives atteints. Par défaut, les services Bureau à distance déconnectent les sessions qui atteignent leurs délais d'expiration. Les délais d'expiration sont définis localement par l'administrateur du serveur ou dans la stratégie de groupe. Voir les paramètres « Définir le délai d'expiration des sessions de services Bureau à distance actives » et « Définir le délai d'expiration des sessions de services Bureau à distance ouvertes, mais inactives ». Si vous activez ce paramètre, les services Bureau à distance mettent fin à toute session qui atteint son délai d'expiration. Si vous désactivez ce paramètre, les services Bureau à distance déconnectent toujours une session ayant expiré, même si l'administrateur en décide autrement. Si vous ne configurez pas ce paramètre, les services Bureau à distance déconnectent une session ayant expiré, à moins que cela ne soit autrement spécifié dans les paramètres locaux. **Remarque** Ce paramètre ne s'applique qu'aux délais d'expiration délibérément définis dans l'outil Configuration d'hôte de session Bureau à distance ou dans la Console de gestion des stratégies de groupe, et non aux événements de délai d'expiration qui se produisent en raison de problèmes de réseau ou de connexion. Notez également que ce paramètre s'affiche à la fois dans Configuration ordinateur et dans Configuration utilisateur. Si les deux paramètres sont configurés, le paramètre Configuration ordinateur est prioritaire.
`Set time limit for logoff of RemoteApp sessions`	Utilisez ce paramètre de stratégie pour spécifier combien de temps une session d'application distante d'un utilisateur restera dans un état déconnecté avant que la session de l'hôte RDS soit fermée. Par défaut, si un utilisateur ferme une application distante, la session est déconnectée de l'hôte RDS. Si vous activez ce paramètre de stratégie, lorsqu'un utilisateur ferme une application distante, la session d'application distante reste dans un état déconnecté jusqu'à ce que la limite de temps que vous avez spécifiée soit atteinte. Lorsque cette limite est atteinte, la session d'application distante est fermée sur l'hôte RDS. Si l'utilisateur démarre une application distante avant que la limite de temps ne soit atteinte, l'utilisateur se reconnecte à la session déconnectée sur l'hôte RDS. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, lorsqu'un utilisateur ferme une application distante, la session est déconnectée de l'hôte RDS. **Remarque** Ce paramètre de stratégie s'affiche à la fois dans Configuration ordinateur et dans Configuration utilisateur. Si les deux paramètres de stratégie sont configurés, le paramètre de stratégie Configuration ordinateur est prioritaire.

Paramètres de dossiers temporaires RDS

Les paramètres de stratégie du groupe Connexion RDS contrôlent la création et la suppression de dossiers temporaires pour les sessions des services Bureau à distance.

Tableau 5-23. Paramètres de stratégie de groupe de dossiers temporaires

Paramètre	Description
`Do not delete temp folder upon exit`	Spécifie si les services Bureau à distance conservent les dossiers temporaires par session d'un utilisateur à la fermeture de la session. Vous pouvez utiliser ce paramètre pour conserver les dossier temporaires spécifiques à la session d'un utilisateur, même si celui-ci ferme une session. Par défaut, les services Bureau à distance suppriment les dossiers temporaires d'un utilisateur quand celui-ci se déconnecte. Si l'état est défini sur Activé, les dossiers temporaires par session de l'utilisateur sont conservés lorsque celui ferme une session. Si l'état est défini sur Désactivé, les dossiers temporaires sont supprimés lorsqu'un utilisateur se déconnecte, même si l'administrateur spécifie autre chose dans l'outil Configuration de l'hôte de session Bureau à distance. Si l'état est défini sur Non configuré, les services Bureau à distance suppriment les dossiers temporaires de l'ordinateur distant à la fermeture de la session, sauf si l'administrateur du serveur a spécifié autre chose. **Remarque** Ce paramètre n'est appliqué que si les dossiers temporaires par session sont utilisés sur le serveur. Cela signifie que si vous activez le paramètre « Ne pas utiliser les dossiers temporaires par session », celui-ci n'est pas appliqué.
`Do not use temporary folders per session`	Ce paramètre vous permet d'empêcher les services Bureau à distance de créer des dossiers temporaires spécifiques à la session. Vous pouvez utiliser ce paramètre de stratégie pour désactiver la création de dossiers temporaires distincts sur un ordinateur distant pour chaque session. Par défaut, les services Bureau à distance créent un dossier temporaire distinct pour chaque session active qu'un utilisateur conserve sur un ordinateur distant. Ces dossiers temporaires sont créés sur l'ordinateur distant dans un dossier Temp situé dans le dossier du profil de l'utilisateur et portent le nom de `sessionid`. Si vous activez ce paramètre de stratégie, les dossiers temporaires par session ne sont pas créés. À la place, les dossiers temporaires de toutes les sessions d'un utilisateur sur l'ordinateur distant sont stockés dans un dossier Temp commun dans le dossier du profil de l'utilisateur sur l'ordinateur distant. Si vous désactivez ce paramètre de stratégie, les dossiers temporaires par session sont toujours créés, même si vous spécifiez autre chose dans l'outil Configuration de l'hôte de session Bureau à distance. Si vous ne configurez pas ce paramètre de stratégie, les dossiers temporaires par session sont toujours créés, sauf si vous spécifiez autre chose dans l'outil Configuration de l'hôte de session Bureau à distance.

Configuration de l'impression basée sur l'emplacement

La fonction d'impression basée sur l'emplacement mappe les imprimantes physiquement proches des systèmes client vers des postes de travail View, ce qui permet aux utilisateurs d'imprimer sur leurs imprimantes locales et en réseau depuis leurs postes de travail View.

L'impression basée sur l'emplacement permet aux services informatiques de mapper des postes de travail View vers l'imprimante la plus proche du périphérique client de point de terminaison. Par exemple, lorsqu'un médecin passe de chambre en chambre dans un hôpital, chaque fois qu'il imprime un document, le travail d'impression est envoyé à l'imprimante la plus proche.

La fonctionnalité d'impression basée sur l'emplacement est disponible pour Windows, Mac, Linux, et pour les périphériques clients mobiles.

Dans Horizon 6.0.1 et version ultérieure, l'impression basée sur l'emplacement est prise en charge sur les applications et les postes de travail distants suivants :

- Postes de travail qui sont déployés sur des machines mono-utilisateur, notamment les machines postes de travail Windows et Windows Server
- Postes de travail qui sont déployées sur des hôtes RDS, où les hôtes RDS sont des machines virtuelles
- applications hébergées ;
- Applications hébergées qui sont lancées à partir d'Horizon Client à l'intérieur de postes de travail distants

Dans Horizon 6.0 et version antérieure, l'impression basée sur l'emplacement est prise en charge sur les postes de travail qui sont déployés sur des machines postes de travail Windows mono-utilisateur.

Pour utiliser la fonctionnalité d'impression basée sur l'emplacement, vous devez installer l'option de configuration Impression virtuelle avec Horizon Agent et les pilotes d'imprimante correspondants sur le poste de travail.

Vous réglez l'impression basée sur l'emplacement en configurant le paramètre de stratégie de groupe Active Directory `AutoConnect Map Additional Printers for VMware View`, situé dans l'Éditeur d'objets de stratégie de groupe de Microsoft dans le dossier **Paramètres du logiciel** sous **Configuration ordinateur**.

Remarque `AutoConnect Map Additional Printers for VMware View` est une stratégie spécifique à l'ordinateur. Les stratégies spécifiques à l'ordinateur s'appliquent à tous les postes de travail View, quelle que soit la personne se connectant au poste de travail.

`AutoConnect Map Additional Printers for VMware View` est un tableau de traduction de noms. Vous utilisez chaque ligne du tableau pour identifier une imprimante spécifique et définir un ensemble de règles de traduction pour cette imprimante. Les règles de traduction déterminent si l'imprimante est mappée vers le poste de travail View pour un système client particulier.

Lorsqu'un utilisateur se connecte à un poste de travail View, View compare le système client avec les règles de traduction associées à chaque imprimante du tableau. Si le système client satisfait toutes les règles de traduction définies pour l'imprimante, ou si une imprimante n'a pas de règle de traduction associée, View mappe l'imprimante vers le poste de travail View au cours de la session de l'utilisateur.

Vous pouvez définir des règles de traduction basées sur l'adresse IP, le nom et l'adresse MAC du système client, et sur le nom et le groupe de l'utilisateur. Vous pouvez spécifier une règle de traduction, ou une combinaison de plusieurs règles de traduction, pour une imprimante spécifique.

Les informations utilisées pour mapper l'imprimante vers le poste de travail View sont stockées dans une entrée de registre sur le poste de travail View dans `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\thinprint\tpautoconnect`.

Paramètres d'imprimante pour impression basée sur l'emplacement

Dans Horizon 6.0.2 et versions ultérieures, les réglages d'imprimante des imprimantes basées sur l'emplacement sont conservés après la déconnexion des utilisateurs de leur poste de travail. Par exemple, un utilisateur peut choisir d'utiliser une imprimante basée sur l'emplacement en mode monochrome. Après que l'utilisateur se déconnecte et reconnecte au poste de travail, l'imprimante basée sur l'emplacement continue de fonctionner en mode monochrome.

Pour enregistrer les paramètres de l'imprimante à travers les sessions dans une application hébergée, l'utilisateur doit sélectionner une imprimante basée sur l'emplacement dans la boîte de dialogue d'impression de l'application, cliquer avec le bouton droit sur l'imprimante sélectionnée, puis sélectionner **Préférences d'impression**. Les paramètres de l'imprimante ne sont pas enregistrés si l'utilisateur sélectionne une imprimante et clique sur le bouton **Préférences** dans la boîte de dialogue d'impression de l'application.

Les paramètres persistants d'imprimantes basées sur l'emplacement ne sont pas pris en charge si les paramètres sont enregistrés dans l'espace privé du pilote plutôt que dans sa partie étendue DEVMODE, comme le recommande Microsoft. Pour prendre en charge les paramètres persistants, déployez les imprimantes dont les paramètres sont enregistrés dans la partie DEVMODE du pilote de l'imprimante.

Enregistrer le fichier DLL de la stratégie de groupe de l'impression basée sur l'emplacement

Avant de pouvoir configurer le paramètre de stratégie de groupe pour l'impression basée sur l'emplacement, vous devez enregistrer le fichier DLL `TPVMGPoACmap.dll`.

Les versions 32 bits et 64 bits de `TPVMGPoACmap.dll` sont disponibles dans un fichier `.zip` groupé 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 le fichier sur le site de téléchargement de VMware Horizon 6 à l'adresse http://www.vmware.com/go/downloadview.

Les versions de View antérieures fournissent les versions 32 bits et 64 bits de `TPVMGPoACmap.dll` dans le répertoire *`install_directory`*`\VMware\VMware View\Server\extras\GroupPolicyFiles\ThinPrint` sur votre hôte du Serveur de connexion View.

Procédure

1 Copiez la version appropriée de `TPVMGPoACmap.dll` sur votre serveur Active Directory ou sur l'ordinateur de domaine que vous utilisez pour configurer des stratégies de groupe.

2 Utilisez l'utilitaire `regsvr32` pour enregistrer le fichier `TPVMGPoACmap.dll`.

   Par exemple : `regsvr32 "C:\TPVMGPoACmap.dll"`

Suivant

Configurez le paramètre de stratégie de groupe pour l'impression basée sur l'emplacement.

Configurer la stratégie de groupe de l'impression basée sur l'emplacement

Pour régler l'impression basée sur l'emplacement, vous configurez le paramètre de stratégie de groupe `AutoConnect Map Additional Printers for VMware View`. Le paramètre de stratégie de groupe est un tableau de traduction de noms qui mappe des imprimantes à des postes de travail Horizon.

Prérequis

- Vérifiez que les composants logiciels enfichables Microsoft MMC et que l'Éditeur d'objets de stratégie de groupe sont disponibles sur votre serveur Active Directory ou sur l'ordinateur de domaine que vous utilisez pour configurer des stratégies de groupe.

- Enregistrez le fichier DLL `TPVMGPoACmap.dll` sur votre serveur Active Directory ou sur l'ordinateur de domaine que vous utilisez pour configurer des stratégies de groupe. Reportez-vous à la section « Enregistrer le fichier DLL de la stratégie de groupe de l'impression basée sur l'emplacement », page 189.
- Familiarisez-vous avec la syntaxe du paramètre de stratégie de groupe `AutoConnect Map Additional Printers for VMware View`. Reportez-vous à la section « Syntaxe de paramètre de stratégie de groupe de l'impression basée sur l'emplacement », page 191.
- Créez un GPO pour le paramètre de stratégie de groupe basé sur l'emplacement et liez-le à l'unité d'organisation qui contient vos postes de travail Horizon. Reportez-vous à « Créer des GPO pour les stratégies de groupe Horizon 7 », page 193 pour obtenir un exemple de création de GPO pour des stratégies de groupe Horizon.
- Vérifiez que l'option de configuration Impression virtuelle a été installée avec Horizon Agent sur vos postes de travail. Pour cela, vérifiez si les services TP AutoConnect et TP VC Gateway sont installés sur le système d'exploitation du poste de travail.
- Comme les travaux d'impression sont envoyés directement du poste de travail Horizon vers l'imprimante, vérifiez que les pilotes d'imprimante requis sont installés sur vos postes de travail.

Procédure

1 Sur le serveur Active Directory, modifiez les GPO.

Version d'AD	Chemin de navigation
Windows 2003	a Sélectionnez **Démarrer > Tous les programmes > Outils d'administration > Utilisateurs et ordinateurs Active Directory**. b Cliquez avec le bouton droit sur l'unité d'organisation qui contient vos postes de travail Horizon et sélectionnez **Propriétés**. c Sous l'onglet **Stratégie de groupe**, cliquez sur **Ouvrir** pour ouvrir le plug-in Gestion de stratégie de groupe. d Dans le volet de droite, cliquez avec le bouton droit sur le GPO que vous avez créé pour le paramètre de stratégie de groupe d'impression basée sur l'emplacement et sélectionnez **Modifier**.
Windows 2008	a Sélectionnez **Démarrer > Outils d'administration > Gestion de stratégie de groupe**. b Développez votre domaine, cliquez avec le bouton droit sur le GPO que vous avez créé pour le paramètre de stratégie de groupe d'impression basée sur l'emplacement et sélectionnez **Modifier**.

La fenêtre de l'Éditeur d'objets de stratégie de groupe apparaît.

2 Développez **Configuration ordinateur**, ouvrez le dossier **Paramètres du logiciel** et sélectionnez **Imprimantes supplémentaires de mappage de connexion automatique pour VMware View**.

3 Dans le volet Règle, double-cliquez sur **Configurer des imprimantes supplémentaires de mappage de connexion automatique**.

La fenêtre AutoConnect Map Additional Printers for VMware View (Imprimantes supplémentaires de mappage de connexion automatique pour VMware View) apparaît.

4 Sélectionnez **Activé** pour activer le paramètre de stratégie de groupe.

Les titres et les boutons du tableau de traduction apparaissent dans la fenêtre de stratégie de groupe.

Important Cliquer sur **Désactivé** supprime toutes les entrées du tableau. Par précaution, enregistrez votre configuration pour pouvoir l'importer ultérieurement.

5 Ajoutez les imprimantes que vous voulez mapper à des postes de travail Horizon et définissez leurs règles de traduction associées.

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

Syntaxe de paramètre de stratégie de groupe de l'impression basée sur l'emplacement

Vous utilisez le paramètre de stratégie de groupe `AutoConnect Map Additional Printers for VMware View` pour mapper des imprimantes à des postes de travail distants.

`AutoConnect Map Additional Printers for VMware View` est une table de traductions de noms qui identifie des imprimantes et définit les règles de traduction associées. Tableau 5-24 décrit la syntaxe de la table de traductions.

L'impression basée sur l'emplacement mappe les imprimantes locales à des postes de travail distants, mais ne prend pas en charge le mappage d'imprimantes réseau qui sont configurées à l'aide de chemins UNC.

Tableau 5-24. Colonnes et valeurs contenues dans le tableau de traduction

Colonne	Description
`IP Range`	Règle de traduction spécifiant une plage d'adresses IP pour des systèmes client. Pour spécifier des adresses IP dans une plage spécifique, utilisez la notation suivante : ***ip_address–ip_address*** Par exemple : **`10.112.116.0–10.112.119.255`** Pour spécifier toutes les adresses IP dans un sous-réseau spécifique, utilisez la notation suivante : *ip_address/subnet_mask_bits* Par exemple : **`10.112.4.0/22`** Cette notation spécifie les adresses IPv4 utilisables comprises entre 10.112.4.1 et 10.112.7.254. Saisissez un astérisque pour inclure toutes les adresses IP.
`Client Name`	Règle de traduction spécifiant un nom d'ordinateur. Par exemple : **`Ordinateur de Marie`** Saisissez un astérisque pour inclure tous les noms d'ordinateur.
`Mac Address`	Règle de traduction spécifiant une adresse MAC. Dans l'éditeur de GPO, vous devez voir le même format que celui utilisé par le système client. Par exemple : ■ Les clients Windows utilisent des traits d'union : **`01–23–45–67–89–ab`** ■ Les clients Linux utilisent des deux-points : **`01:23:45:67:89:ab`** Saisissez un astérisque pour inclure toutes les adresses MAC.
`User/Group`	Règle de traduction spécifiant un nom d'utilisateur ou de groupe. Pour spécifier un utilisateur ou un groupe particulier, utilisez la notation suivante : *\\domain\user_or_group* Par exemple : **`\\mondomaine\Marie`** Le nom de domaine complet n'est pas une notation prise en charge pour le nom de domaine. Tapez un astérisque pour inclure tous les noms d'utilisateurs ou de groupes.
`Printer Name`	Nom de l'imprimante lorsqu'elle est mappée au poste de travail distant. Par exemple : **`PRINTER–2–CLR`** Le nom mappé n'a pas à correspondre au nom de l'imprimante sur le système client. L'imprimante doit être locale par rapport au périphérique client. Le mappage d'une imprimante réseau dans un chemin UNC n'est pas pris en charge.

Tableau 5-24. Colonnes et valeurs contenues dans le tableau de traduction (suite)

Colonne	Description
`Printer Driver`	Nom du pilote qu'utilise l'imprimante. Par exemple : **`HP Color LaserJet 4700 PS`** **Important** Comme les travaux d'impression sont envoyés directement du poste de travail vers l'imprimante, le pilote d'imprimante doit être installé sur le poste de travail.
`IP Port/ThinPrint Port`	Pour les imprimantes en réseau, adresses IP de l'imprimante avec le préfixe **`IP_`**. Par exemple : **`IP_10.114.24.1`** Le port par défaut est 9100. Vous pouvez spécifier un port différent du port par défaut en ajoutant le numéro de port à l'adresse IP. Par exemple : **`IP_10.114.24.1:9104`**
`Default`	Indique si l'imprimante est l'imprimante par défaut.

Vous utilisez les boutons qui apparaissent au-dessus des titres de colonne pour ajouter, supprimer et déplacer des lignes et pour enregistrer et importer des entrées de tableau. Chaque bouton a un raccourci clavier équivalent. Passez la souris sur chaque bouton pour en voir une description et son raccourci clavier. Par exemple, pour insérer une ligne à la fin du tableau, cliquez sur le premier bouton du tableau ou appuyez sur Alt+A. Cliquez sur les deux derniers boutons pour importer et enregistrer des entrées de tableau.

Tableau 5-25 montre un exemple de deux lignes de tableau de traduction.

Tableau 5-25. Exemple de paramètre de stratégie de groupe de l'impression basée sur l'emplacement

Plage IP	Nom du client	Adresse Mac	Utilisateur/ Groupe	Nom de l'imprimante	Pilote d'imprimante	IP Port/ThinPrint Port (Port IP/Port ThinPrint)	Valeur par défaut
*	*	*	*	PRINTER-1-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.1	
10.112.116.140-10.112.116.145	*	*	*	PRINTER-2-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.2	X

L'imprimante réseau spécifiée sur la première ligne sera mappée à un poste de travail distant de n'importe quel système client, car des astérisques figurent dans toutes les colonnes de la règle de traduction. L'imprimante réseau spécifiée sur la deuxième ligne sera mappée à un poste de travail distant uniquement si l'adresse IP du système client est comprise dans la plage 10.112.116.140 à 10.112.116.145.

Exemple de stratégie de groupe Active Directory

L'une des méthodes de mise en œuvre des stratégies de groupe Active Directory dans Horizon 7 consiste à créer une unité d'organisation (UO) pour les machines Horizon 7 qui fournissent des sessions de postes de travail distants et à lier un ou plusieurs objets de stratégie de groupe (GPO) à cette UO. Vous pouvez utiliser ces GPO pour appliquer des paramètres de stratégie de groupe à vos machines Horizon 7.

Vous pouvez lier les GPO directement à un domaine si les paramètres de stratégie s'appliquent à tous les ordinateurs du domaine. Pour la plupart des déploiements, nous recommandons toutefois de lier des GPO à des UO individuelles, afin d'éviter le traitement de la stratégie sur tous les ordinateurs du domaine.

Vous pouvez configurer des stratégies sur votre serveur Active Directory ou sur n'importe quel ordinateur de votre domaine. Cet exemple montre comment configurer des stratégies directement sur votre serveur Active Directory.

Remarque Chaque environnement Horizon 7 étant différent, il vous faudra peut-être effectuer différentes étapes pour répondre aux besoins spécifiques de votre organisation.

Créer une unité d'organisation (UO) pour des machines Horizon 7

Pour appliquer des stratégies de groupe aux machines Horizon 7 qui fournissent des sessions de poste de travail distant sans affecter d'autres ordinateurs Windows du même domaine Active Directory, vous devez créer une UO propre à vos machines Horizon 7. Vous pouvez créer une UO pour l'ensemble de votre déploiement de Horizon 7 ou des UO distinctes pour des machines mono-utilisateur et des hôtes RDS.

Procédure

1. Sur votre serveur Active Directory, sélectionnez **Démarrer > Tous les programmes > Outils d'administration > Utilisateurs et ordinateurs Active Directory**.
2. Cliquez avec le bouton droit sur le domaine qui contient vos machines Horizon 7 et sélectionnez **Nouveau > Unité d'organisation**.
3. Saisissez un nom pour l'UO et cliquez sur **OK**.

   La nouvelle UO apparaît dans le volet de gauche.
4. Pour ajouter des machines Horizon 7 à la nouvelle UO :
   a. Cliquez sur **Ordinateurs** dans le volet de gauche.

      Tous les objets ordinateur dans le domaine apparaissent dans le volet de droite.
   b. Cliquez avec le bouton droit sur le nom de l'objet ordinateur qui représente la machine Horizon 7 dans le volet de droite et sélectionnez **Déplacer**.
   c. Sélectionnez l'UO et cliquez sur **OK**.

      La machine Horizon 7 s'affiche dans le volet de droite lorsque vous sélectionnez l'UO.

Suivant

Créez des GPO pour les stratégies de groupe Horizon 7.

Créer des GPO pour les stratégies de groupe Horizon 7

Créez des GPO contenant des stratégies de groupe pour des composants Horizon 7 et l'impression basée sur l'emplacement et liez-les à l'unité d'organisation de vos machines Horizon 7.

Prérequis

- Créez une unité d'organisation pour vos machines Horizon 7.
- Vérifiez que la fonctionnalité Gestion de stratégie de groupe est disponible sur votre serveur Active Directory.

Procédure

1 Sur le serveur Active Directory, ouvrez la Console de gestion de stratégie de groupe.

Version d'AD	Chemin de navigation
Windows 2012	Sélectionnez **Gestionnaire de serveur > Outils > Gestion des stratégies de groupe**.
Windows 2008	Sélectionnez **Démarrer > Outils d'administration > Gestion de stratégie de groupe**.
Windows 2003	a Sélectionnez **Démarrer > Tous les programmes > Outils d'administration > Utilisateurs et ordinateurs Active Directory**. b Cliquez avec le bouton droit sur l'unité d'organisation qui contient vos machines Horizon 7 et sélectionnez **Propriétés**. c Sous l'onglet **Stratégie de groupe**, cliquez sur **Ouvrir** pour ouvrir le plug-in Gestion de stratégie de groupe.

2 Développez votre domaine, cliquez avec le bouton droit sur l'unité d'organisation qui contient vos machines Horizon 7 et sélectionnez **Créer un objet GPO dans ce domaine, et le lier ici**.

   Dans Windows 2003 Active Directory, cette option se nomme **Créer et lier un objet GPO ici**.

3 Saisissez un nom pour le GPO et cliquez sur **OK**.

   Le nouveau GPO apparaît sous l'UO dans le volet de gauche.

4 (Facultatif) Pour appliquer le GPO uniquement à des postes de travail Horizon 7 spécifiques de l'unité d'organisation :

   a Sélectionnez le GPO dans le volet de gauche.

   b Sélectionnez **Filtrage de sécurité > Ajouter**.

   c Entrez les noms d'ordinateur des machines Horizon 7 et cliquez sur **OK**.

      Les machines Horizon 7 s'affichent dans le volet Filtrage de sécurité. Les paramètres du GPO ne s'appliquent qu'à ces machines.

Suivant

Ajoutez les modèles d'administration ADMX d'Horizon au GPO pour des stratégies de groupe.

Ajouter le fichier de modèle d'administration ADMX Horizon 7 à un GPO

Pour appliquer des paramètres de stratégie de groupe de composant Horizon 7 à vos postes de travail et applications publiés, ajoutez leurs fichiers de modèle d'administration ADMX à des GPO.

Prérequis

- Créez des GPO pour les paramètres de stratégie de groupe du composant Horizon 7 et liez-les à l'UO qui contient vos machines Horizon 7.
- Vérifiez que la fonctionnalité Gestion de stratégie de groupe est disponible sur votre serveur Active Directory.

  La procédure d'ouverture de la Console de gestion de stratégie de groupe varie entre les versions Windows 2012, Windows 2008 et Windows 2003 d'Active Directory. Reportez-vous à la section « Créer des GPO pour les stratégies de groupe Horizon 7 », page 193.

Procédure

1 Téléchargez le fichier Horizon 7 GPO Bundle `.zip` 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 GPO Bundle.

   Le fichier se nomme `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, où *x.x.x* est la version et *yyyyyyy* le numéro de build. Tous les fichiers ADMX qui fournissent des paramètres de stratégie de groupe pour Horizon 7 sont disponibles dans ce fichier.

2 Décompressez le fichier `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip` et copiez les fichiers ADMX sur votre hôte Active Directory ou RDS.

   a Copiez les fichiers `.admx`, ainsi que le dossier `en-US` dans le dossier `%systemroot%\PolicyDefinitions` sur votre hôte Active Directory ou RDS.

   b Copiez les fichiers de ressources de la langue (`.adml`) dans le sous-dossier correspondant dans `%systemroot%\PolicyDefinitions\` sur votre hôte Active Directory ou RDS.

3 Sur l'hôte Active Directory, ouvrez l'Éditeur de gestion de stratégie de groupe et entrez le chemin vers les fichiers de modèle où ils apparaissent dans l'éditeur après l'installation.

   Sur un hôte RDS individuel, vous pouvez ouvrir l'Éditeur de stratégie de groupe locale avec l'utilitaire `gpedit.msc`.

Suivant

Configurez les paramètres de stratégie de groupe et activez le traitement en boucle pour vos machines Horizon 7.

Activer le traitement en boucle des postes de travail distants

Pour appliquer des paramètres de Configuration d'utilisateur qui s'appliquent généralement à un ordinateur à tous les utilisateurs qui ouvrent une session sur cet ordinateur, activez le traitement en boucle.

Prérequis

- Créez des GPO pour les paramètres de stratégie de groupe du composant Horizon 7 et liez-les à l'UO qui contient vos machines Horizon 7.
- Vérifiez que la fonctionnalité Gestion de stratégie de groupe est disponible sur votre serveur Active Directory.

  La procédure d'ouverture de la Console de gestion de stratégie de groupe varie entre les versions Windows 2012, Windows 2008 et Windows 2003 d'Active Directory. Reportez-vous à la section « Créer des GPO pour les stratégies de groupe Horizon 7 », page 193.

Procédure

1 Sur le serveur Active Directory, ouvrez la Console de gestion de stratégie de groupe.

2 Développez votre domaine, cliquez avec le bouton droit sur le GPO que vous avez créé pour les paramètres de stratégie de groupe et sélectionnez **Modifier**.

3 Dans l'Éditeur de gestion de stratégie de groupe, accédez à **Configuration de l'ordinateur > Stratégies > Modèles administratifs : définitions de stratégies > Système > Stratégie de groupe**.

4 Dans le volet de droite, double-cliquez sur **Mode de traitement en boucle de la stratégie de groupe d'utilisateurs**.

5 Sélectionnez **Activé**, puis sélectionnez un mode de traitement en boucle dans le menu déroulant **Mode**.

Option	Action
Merge (Fusionner)	Les paramètres de règle utilisateur appliqués sont la combinaison de ceux inclus dans les GPO ordinateur et utilisateur. En cas de conflit, les GPO ordinateur sont prioritaires.
Replace (Remplacer)	La règle utilisateur est définie entièrement depuis les GPO associés à l'ordinateur. Tous les GPO associés à l'utilisateur sont ignorés.

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

Exemple de stratégie de groupe Active Directory

6

L'une des méthodes de mise en œuvre des stratégies de groupe Active Directory dans Horizon 7 consiste à créer une unité d'organisation (UO) pour les machines Horizon 7 qui fournissent des sessions de postes de travail distants et à lier un ou plusieurs objets de stratégie de groupe (GPO) à cette UO. Vous pouvez utiliser ces GPO pour appliquer des paramètres de stratégie de groupe à vos machines Horizon 7.

Vous pouvez lier les GPO directement à un domaine si les paramètres de stratégie s'appliquent à tous les ordinateurs du domaine. Pour la plupart des déploiements, nous recommandons toutefois de lier des GPO à des UO individuelles, afin d'éviter le traitement de la stratégie sur tous les ordinateurs du domaine.

Vous pouvez configurer des stratégies sur votre serveur Active Directory ou sur n'importe quel ordinateur de votre domaine. Cet exemple montre comment configurer des stratégies directement sur votre serveur Active Directory.

Remarque Chaque environnement Horizon 7 étant différent, il vous faudra peut-être effectuer différentes étapes pour répondre aux besoins spécifiques de votre organisation.

Ce chapitre aborde les rubriques suivantes :

Créer une unité d'organisation (UO) pour des machines Horizon 7

Pour appliquer des stratégies de groupe aux machines Horizon 7 qui fournissent des sessions de poste de travail distant sans affecter d'autres ordinateurs Windows du même domaine Active Directory, vous devez créer une UO propre à vos machines Horizon 7. Vous pouvez créer une UO pour l'ensemble de votre déploiement de Horizon 7 ou des UO distinctes pour des machines mono-utilisateur et des hôtes RDS.

Procédure

1. Sur votre serveur Active Directory, sélectionnez **Démarrer > Tous les programmes > Outils d'administration > Utilisateurs et ordinateurs Active Directory**.
2. Cliquez avec le bouton droit sur le domaine qui contient vos machines Horizon 7 et sélectionnez **Nouveau > Unité d'organisation**.
3. Saisissez un nom pour l'UO et cliquez sur **OK**.

   La nouvelle UO apparaît dans le volet de gauche.

4 Pour ajouter des machines Horizon 7 à la nouvelle UO :

   a Cliquez sur **Ordinateurs** dans le volet de gauche.

     Tous les objets ordinateur dans le domaine apparaissent dans le volet de droite.

   b Cliquez avec le bouton droit sur le nom de l'objet ordinateur qui représente la machine Horizon 7 dans le volet de droite et sélectionnez **Déplacer**.

   c Sélectionnez l'UO et cliquez sur **OK**.

     La machine Horizon 7 s'affiche dans le volet de droite lorsque vous sélectionnez l'UO.

Suivant

Créez des GPO pour les stratégies de groupe Horizon 7.

Créer des GPO pour les stratégies de groupe Horizon 7

Créez des GPO contenant des stratégies de groupe pour des composants Horizon 7 et l'impression basée sur l'emplacement et liez-les à l'unité d'organisation de vos machines Horizon 7.

Prérequis

- Créez une unité d'organisation pour vos machines Horizon 7.
- Vérifiez que la fonctionnalité Gestion de stratégie de groupe est disponible sur votre serveur Active Directory.

Procédure

1 Sur le serveur Active Directory, ouvrez la Console de gestion de stratégie de groupe.

Version d'AD	Chemin de navigation
Windows 2012	Sélectionnez **Gestionnaire de serveur > Outils > Gestion des stratégies de groupe**.
Windows 2008	Sélectionnez **Démarrer > Outils d'administration > Gestion de stratégie de groupe**.
Windows 2003	a Sélectionnez **Démarrer > Tous les programmes > Outils d'administration > Utilisateurs et ordinateurs Active Directory**. b Cliquez avec le bouton droit sur l'unité d'organisation qui contient vos machines Horizon 7 et sélectionnez **Propriétés**. c Sous l'onglet **Stratégie de groupe**, cliquez sur **Ouvrir** pour ouvrir le plug-in Gestion de stratégie de groupe.

2 Développez votre domaine, cliquez avec le bouton droit sur l'unité d'organisation qui contient vos machines Horizon 7 et sélectionnez **Créer un objet GPO dans ce domaine, et le lier ici**.

   Dans Windows 2003 Active Directory, cette option se nomme **Créer et lier un objet GPO ici**.

3 Saisissez un nom pour le GPO et cliquez sur **OK**.

   Le nouveau GPO apparaît sous l'UO dans le volet de gauche.

4 (Facultatif) Pour appliquer le GPO uniquement à des postes de travail Horizon 7 spécifiques de l'unité d'organisation :

   a Sélectionnez le GPO dans le volet de gauche.

   b Sélectionnez **Filtrage de sécurité > Ajouter**.

   c Entrez les noms d'ordinateur des machines Horizon 7 et cliquez sur **OK**.

   Les machines Horizon 7 s'affichent dans le volet Filtrage de sécurité. Les paramètres du GPO ne s'appliquent qu'à ces machines.

Suivant

Ajoutez les modèles d'administration ADMX d'Horizon au GPO pour des stratégies de groupe.

Ajouter le fichier de modèle d'administration ADMX Horizon 7 à un GPO

Pour appliquer des paramètres de stratégie de groupe de composant Horizon 7 à vos postes de travail et applications publiés, ajoutez leurs fichiers de modèle d'administration ADMX à des GPO.

Prérequis

- Créez des GPO pour les paramètres de stratégie de groupe du composant Horizon 7 et liez-les à l'UO qui contient vos machines Horizon 7.
- Vérifiez que la fonctionnalité Gestion de stratégie de groupe est disponible sur votre serveur Active Directory.

  La procédure d'ouverture de la Console de gestion de stratégie de groupe varie entre les versions Windows 2012, Windows 2008 et Windows 2003 d'Active Directory. Reportez-vous à la section « Créer des GPO pour les stratégies de groupe Horizon 7 », page 193.

Procédure

1 Téléchargez le fichier Horizon 7 GPO Bundle `.zip` 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 GPO Bundle.

   Le fichier se nomme `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, où *x.x.x* est la version et *yyyyyyy* le numéro de build. Tous les fichiers ADMX qui fournissent des paramètres de stratégie de groupe pour Horizon 7 sont disponibles dans ce fichier.

2 Décompressez le fichier `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip` et copiez les fichiers ADMX sur votre hôte Active Directory ou RDS.

   a Copiez les fichiers `.admx`, ainsi que le dossier `en-US` dans le dossier `%systemroot%\PolicyDefinitions` sur votre hôte Active Directory ou RDS.

   b Copiez les fichiers de ressources de la langue (`.adml`) dans le sous-dossier correspondant dans `%systemroot%\PolicyDefinitions\` sur votre hôte Active Directory ou RDS.

3 Sur l'hôte Active Directory, ouvrez l'Éditeur de gestion de stratégie de groupe et entrez le chemin vers les fichiers de modèle où ils apparaissent dans l'éditeur après l'installation.

   Sur un hôte RDS individuel, vous pouvez ouvrir l'Éditeur de stratégie de groupe locale avec l'utilitaire `gpedit.msc`.

Suivant

Configurez les paramètres de stratégie de groupe et activez le traitement en boucle pour vos machines Horizon 7.

Activer le traitement en boucle des postes de travail distants

Pour appliquer des paramètres de Configuration d'utilisateur qui s'appliquent généralement à un ordinateur à tous les utilisateurs qui ouvrent une session sur cet ordinateur, activez le traitement en boucle.

Prérequis

- Créez des GPO pour les paramètres de stratégie de groupe du composant Horizon 7 et liez-les à l'UO qui contient vos machines Horizon 7.
- Vérifiez que la fonctionnalité Gestion de stratégie de groupe est disponible sur votre serveur Active Directory.

  La procédure d'ouverture de la Console de gestion de stratégie de groupe varie entre les versions Windows 2012, Windows 2008 et Windows 2003 d'Active Directory. Reportez-vous à la section « Créer des GPO pour les stratégies de groupe Horizon 7 », page 193.

Procédure

1. Sur le serveur Active Directory, ouvrez la Console de gestion de stratégie de groupe.
2. Développez votre domaine, cliquez avec le bouton droit sur le GPO que vous avez créé pour les paramètres de stratégie de groupe et sélectionnez **Modifier**.
3. Dans l'Éditeur de gestion de stratégie de groupe, accédez à **Configuration de l'ordinateur > Stratégies > Modèles administratifs : définitions de stratégies > Système > Stratégie de groupe**.
4. Dans le volet de droite, double-cliquez sur **Mode de traitement en boucle de la stratégie de groupe d'utilisateurs**.
5. Sélectionnez **Activé**, puis sélectionnez un mode de traitement en boucle dans le menu déroulant **Mode**.

Option	Action
Merge (Fusionner)	Les paramètres de règle utilisateur appliqués sont la combinaison de ceux inclus dans les GPO ordinateur et utilisateur. En cas de conflit, les GPO ordinateur sont prioritaires.
Replace (Remplacer)	La règle utilisateur est définie entièrement depuis les GPO associés à l'ordinateur. Tous les GPO associés à l'utilisateur sont ignorés.

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

Index

O

P

R

S

T

U

V

W