Configuration des fonctionnalités de poste de travail distant dans Horizon

VMware Horizon 2103

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

https://docs.vmware.com/fr/

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

VMware France SAS.
Tour Franklin
100-101 Terrasse Boieldieu
92042 Paris La Défense 8 Cedex
France
www.vmware.com/fr

Copyright © 2021 VMware, Inc. Tous droits réservés. Informations relatives aux copyrights et marques commerciales.

Table des matières

Configuration des fonctionnalités de poste de travail distant dans Horizon

1

Configuration des fonctionnalités de poste de travail distant dans Horizon décrit comment configurer des fonctionnalités de poste de travail distant qui sont installées avec Horizon Agent sur des postes de travail virtuels 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 virtuels 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 les versions d'VMware Horizon. Vous pouvez configurer ces fonctionnalités afin d'améliorer l'expérience de vos utilisateurs finaux sur les postes de travail distants.

Ces fonctionnalités incluent HTML Access, Unity Touch, la redirection, la redirection multimédia HTML5, la redirection de géolocalisation, l'Audio/Vidéo en temps réel, la redirection multimédia Windows Media (MMR), la redirection USB, la redirection de scanner, la redirection de port série, la redirection de scanner d'empreintes digitales, la collaboration de session, Skype Entreprise et la redirection de contenu URL.

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. Pour plus d'informations sur la redirection de contenu URL, reportez-vous au document Chapitre 3 Configuration de la redirection de contenu URL.

Ce chapitre contient 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 l'installation d'Horizon Agent en configurant le paramètre de stratégie de groupe **Activer Unity Touch** dans le fichier de modèle d'administration ADMX pour la configuration d'Horizon Agent (`vdm_agent.admx`).

Pour plus d'informations sur les fonctionnalités pour l'utilisateur final fournies par Unity Touch, reportez-vous à la documentation d'Horizon Client pour les périphériques iOS et Android.

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 distant

- Installez la fonctionnalité Unity Touch dans Horizon Agent. Pour plus d'informations, consultez le document *Configuration d'applications et de postes de travail publiés dans Horizon*.
- Les systèmes d'exploitation pris en charge incluent Windows 10 64 bits, Windows Server 2012 R2, Windows Server 2016 et Windows Server 2019.

Logiciel Horizon Client

- Unity Touch est pris en charge dans Horizon Client pour iOS et Horizon Client pour Android.
- Pour les versions de système d'exploitation prises en charge, reportez-vous à la documentation d'Horizon Client pour les périphériques iOS et Android.

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 un poste de travail distant, une application ou un fichier 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 final se connecte pour la première fois à un poste de travail sur lequel Unity Touch est activé. Toutefois, si l'utilisateur configure sa propre liste d'applications préférées, la liste par défaut est 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 distant, 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 principale 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

Note 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"`.

Conditions préalables

- 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-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /a /v"/qn TARGETDIR=""a network
  share to store the admin install package"" UNITY_DEFAULT_APPS=""the list of default
  favorite apps that should be set in the registry"""
  ```

  Par exemple :

  ```
  VMware-Horizon-Agent-x86-YYMM-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-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn UNITY_DEFAULT_APPS=""the list of
  default favorite apps that should be set in the registry"""
  ```

  Note 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.

Étape suivante

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 multimédia HTML5

Avec la redirection multimédia HTML5, si un utilisateur final utilise le navigateur Google Chrome ou Microsoft Edge dans un poste de travail distant, le contenu multimédia HTML5 est transmis au

système client, ce qui réduit la charge sur l'hôte ESXi. Le système client lit le contenu multimédia, et l'utilisateur peut profiter d'une meilleure expérience audio et vidéo.

Configuration système requise pour la redirection multimédia HTML5

Horizon Agent et Horizon Client, ainsi que les postes de travail distants et les systèmes clients sur lesquels vous installez les logiciels agent et client doivent respecter la configuration système requise pour la prise en charge de la fonctionnalité de redirection multimedia HTML5.

Poste de travail distant

- Les paramètres de stratégie de groupe de redirection multimédia HTML5 doivent être configurés sur le serveur Active Directory. Reportez-vous à la section Installer et configurer la redirection multimédia HTML5.
- Le navigateur Chrome ou Edge doit être installé.
- L'extension de redirection multimédia HTML5 de VMware Horizon doit être installée dans le navigateur Chrome ou Edge. Reportez-vous à la section Installer l'extension de redirection HTML5 de VMware Horizon pour Chrome ou Installer l'extension de redirection HTML5 de VMware Horizon pour Edge.

Système client

- Pour les systèmes clients Windows, vous devez installer Horizon Client pour Windows avec la prise en charge de la redirection multimédia HTML5 et l'option de configuration personnalisée de redirection de navigateur sélectionnée. Cette option est sélectionnée par défaut. Consultez les rubriques sur l'installation d'Horizon Client dans le document *Guide d'installation et de configuration de VMware Horizon Client pour Windows*.
- Pour les systèmes clients Linux, vous devez installer Horizon Client pour Linux avec la prise en charge de la redirection multimédia HTML5 et l'option de configuration personnalisée sélectionnée. Cette option est sélectionnée par défaut. Consultez les rubriques sur l'installation d'Horizon Client dans le *Guide d'installation et de configuration de VMware Horizon Client pour Linux*.

Protocole d'affichage de la session distante

- PCoIP
- VMware Blast

Port TCP

La redirection multimédia HTML5 utilise le port 9427.

Limites

La fonctionnalité de redirection multimédia HTML5 présente les limitations suivantes.

- La fonctionnalité de souris relative Horizon Client n'est pas prise en charge.

- Vous ne pouvez pas utiliser **Couper le son du site** (navigateur Chrome) ou **Couper le son de l'onglet** (navigateur Edge) pour désactiver le contenu vidéo redirigé.
- Pour utiliser la redirection multimédia HTML5 à partir de Chrome sur un système client Linux, ouvrez au plus un navigateur Chrome publié par un hôte RDS. La redirection multimédia HTML5 ne fonctionne pas correctement si vous ouvrez un navigateur Chrome supplémentaire publié par un autre hôte RDS.
- Si vous rencontrez un ralentissement des performances lors de la lecture d'un contenu multimédia redirigé sur un système client Linux qui utilise du matériel client léger de faible capacité, vous pouvez optimiser les performances du système comme décrit ici. Ajoutez l'entrée `disableGPU.html5mmr=true` à l'un des trois fichiers de configuration suivants. Les fichiers de configuration sont traités dans l'ordre suivant :

  a `/usr/lib/vmware/config`

  b `/etc/vmware/config`

  c `~/.vmware/config`

Installer et configurer la redirection multimédia HTML5

Pour rediriger du contenu multimédia HTML5 à partir d'un poste de travail distant vers le système client local, vous devez installer la fonctionnalité de redirection multimédia HTML5 et le navigateur Chrome ou Edge sur le poste de travail distant, activer la fonctionnalité de redirection multimédia HTML5 et spécifier les sites Web qui utilisent cette fonctionnalité.

Pour activer la redirection multimédia HTML5 et spécifier les sites Web pouvant utiliser cette fonctionnalité, configurez les paramètres de stratégie de groupe de votre serveur Active Directory. Vous devez compiler une liste d'URL de sites Web pouvant rediriger le contenu multimédia HTML5. Incluez le préfixe `http://` ou `https://` dans les URL. Vous pouvez utiliser des modèles de correspondance dans les URL.

Par exemple, pour rediriger toutes les vidéos sur YouTube, spécifiez `https://www.youtube.com/*`. Pour rediriger toutes les vidéos sur Vimeo, spécifiez `https://www.vimeo.com/*`. Pour plus d'informations, consultez la page https://developer.chrome.com/extensions/match_patterns.

Conditions préalables

- Installez Horizon Client sur le système client et Horizon Agent sur le poste de travail distant avec la fonctionnalité de redirection multimédia HTML5 activée. Pour connaître les versions, les options d'installation et la configuration système requises, reportez-vous à la section Configuration système requise pour la redirection multimédia HTML5.
- 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.

- Ajoutez le fichier de modèle ADMX de configuration de VMware View Agent `vdm_agent.admx` à un GPO lié à l'UO pour le poste de travail virtuel ou à l'hôte RDS pour le poste de travail publié. Pour obtenir des instructions d'installation, reportez-vous à la section Ajouter les fichiers de modèle d'administration ADMX à Active Directory.
- Compilez une liste d'URL de sites Web pouvant rediriger le contenu multimédia HTML5.

Procédure

1. Installez le navigateur Chrome ou Edge sur le poste de travail distant.
2. Sur votre serveur Active Directory, ouvrez l'Éditeur de gestion de stratégie de groupe.
3. Accédez au dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Configuration de VMware View Agent > Fonctionnalités HTML5 de VMware**.
4. Ouvrez le paramètre **Activer les fonctionnalités VMware HTML5**, sélectionnez **Activée**, puis cliquez sur **OK**.
5. Accédez au dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Configuration de VMware View Agent > Fonctionnalités VMware HTML5 > Redirection multimédia VMware HTML5**.
6. Ouvrez le paramètre **Activer la redirection multimédia HTML5 de VMware**, sélectionnez **Activée**, puis cliquez sur **OK**.
7. Pour utiliser le navigateur Chrome, procédez comme suit.
   a. Accédez au dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Configuration de VMware View Agent > Fonctionnalités VMware HTML5 > Redirection multimédia VMware HTML5**.
   b. Ouvrez le paramètre **Activer le navigateur Chrome pour la redirection multimédia HTML5 de VMware**, sélectionnez **Activé** et cliquez sur **OK**.
8. Pour utiliser le navigateur Edge, procédez comme suit.
   a. Accédez au dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Configuration de VMware View Agent > Fonctionnalités VMware HTML5 > Redirection multimédia VMware HTML5**.
   b. Ouvrez le paramètre **Activer le navigateur Edge pour la redirection multimédia HTML5 de VMware**, sélectionnez **Activé** et cliquez sur **OK**.
   c. Accédez au dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Configuration de VMware View Agent > Fonctionnalités HTML5 de VMware**.
   d. Ouvrez le paramètre **Désactiver la détection automatique du réseau intranet**, sélectionnez **Activé** et cliquez sur **OK**.

9 Spécifiez quels sites Web utiliseront la fonctionnalité de redirection multimédia HTML5.

a Accédez au dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Configuration de VMware View Agent > Fonctionnalités VMware HTML5 > Redirection multimédia VMware HTML5**.

b Ouvrez le paramètre **Activer la liste d'URL pour la redirection multimédia HTML5 de VMware**, puis sélectionnez **Activée**.

c Cliquez sur **Afficher** et entrez les URL que vous avez compilées dans la colonne Nom de la valeur.

Seules les URL que vous spécifiez peuvent rediriger le contenu multimédia HTML5. Aucune URL n'est ajoutée par défaut. Laissez vide la colonne Valeur.

d Cliquez sur **OK** pour enregistrer la liste d'URL, puis cliquez sur **OK** pour enregistrer le paramètre de stratégie.

Étape suivante

Pour utiliser le navigateur Chrome, installez l'extension de redirection HTML5 de VMware Horizon pour Chrome dans le navigateur Chrome sur le poste de travail distant. Reportez-vous à la section Installer l'extension de redirection HTML5 de VMware Horizon pour Chrome.

Pour utiliser le navigateur Edge, installez l'extension de redirection HTML5 de VMware Horizon pour Edge dans le navigateur Edge sur le poste de travail distant. Reportez-vous à la section Installer l'extension de redirection HTML5 de VMware Horizon pour Edge.

Installer l'extension de redirection HTML5 de VMware Horizon pour Chrome

Pour utiliser la fonctionnalité de redirection multimédia HTML5 avec le navigateur Chrome, vous devez forcer l'installation de l'extension de redirection HTML5 de VMware Horizon sur le poste de travail distant. Pour forcer l'installation de l'extension, vous devez configurer un paramètre de stratégie de groupe Google Chrome sur votre serveur Active Directory.

Pour appliquer le paramètre de stratégie de groupe Chrome au poste de travail distant, vous devez ajouter le fichier de modèle d'administration ADMX à un GPO sur votre serveur Active Directory. Pour un poste de travail virtuel, le GPO doit être lié à l'UO qui contient le poste de travail virtuel. Pour un poste de travail publié, le GPO doit être lié à l'UO qui contient l'hôte RDS.

Conditions préalables

- Configurez la fonctionnalité de redirection multimédia HTML5. Reportez-vous à la section Installer et configurer la redirection multimédia HTML5.
- 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.

Procédure

1. Téléchargez le fichier `policy_templates.zip` de Google Chrome sur https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip.
2. Décompressez le fichier `policy_templates.zip`, puis copiez les fichiers `chrome.admx` et `chrome.adml` sur votre serveur Active Directory.

   Le fichier `chrome.admx` se trouve dans le dossier `\windows\admx` et le fichier `chrome.adml` se trouve dans le dossier `\windows\admx\`*`language`* dans le fichier `policy_templates.zip`.

   a. Copiez le fichier `chrome.admx` dans le dossier `%systemroot%\PolicyDefinitions` sur votre serveur Active Directory.

   b. Copiez le fichier de ressources de la langue `chrome.adml` dans le sous-dossier de langue correspondant dans `%systemroot%\PolicyDefinitions` sur votre serveur Active Directory.

      Par exemple, copiez la version `fr_fr` du fichier `chrome.adml` dans le sous-dossier `%systemroot%\PolicyDefinitions\fr_fr` sur votre serveur Active Directory.
3. Toujours sur votre serveur Active Directory, ouvrez l'Éditeur de gestion de stratégie de groupe et accédez au dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Google Chrome > Extensions**.
4. Ouvrez le paramètre de stratégie **Configurer la liste des applications et des extensions installées de force**, puis cliquez sur **Activées**.
5. Cliquez sur **Afficher** et tapez **`ljmaegmnepbgjekghdfkgegbckolmcok;https://clients2.google.com/service/update2/crx`** dans la colonne Valeur.
6. Cliquez sur **OK** pour enregistrer l'ID d'extension/URL de mise à jour, puis cliquez sur **OK** pour enregistrer le paramètre de stratégie.
7. Vérifiez que l'extension de redirection multimédia HTML5 est installée sur le poste de travail distant.

   a. Connectez-vous au poste de travail distant et démarrez Chrome.

   b. Tapez **`chrome://extensions`** dans la barre d'adresses de Chrome.

      Extension de redirection HTML5 de VMware Horizon s'affiche dans la liste des extensions.

Installer l'extension de redirection HTML5 de VMware Horizon pour Edge

Pour utiliser la fonctionnalité de redirection multimédia HTML5 avec le navigateur Edge, vous devez installer l'extension de redirection HTML5 de VMware Horizon pour Edge à partir de Microsoft Store sur le poste de travail distant.

Conditions préalables

Configurez la fonctionnalité de redirection multimédia HTML5. Reportez-vous à la section Installer et configurer la redirection multimédia HTML5.

Procédure

1. Connectez-vous au poste de travail distant.
2. Téléchargez et installez l'extension **Extension de redirection HTML5 de VMware Horizon pour Edge** à partir de Microsoft Store.

Résultats

Une fois l'extension installée, l'icône **Redirection multimédia HTML5 de VMware** s'affiche dans le coin supérieur droit de la fenêtre du navigateur Edge. Lorsque la redirection multimédia HTML5 fonctionne, les lettres REDR s'affichent sur l'icône.

Limitations de la redirection multimédia HTML5

La fonctionnalité de redirection multimédia HTML5 présente certaines limitations.

- La redirection multimédia HTML5 ne prend pas en charge les vidéos à 360°. L'icône d'extension de la redirection multimédia HTML5 est marquée du badge REDR, même si la vidéo n'est pas prise en charge.
- La fonctionnalité de redirection multimédia HTML5 ne peut pas rediriger le contenu multimédia HTML de l'adresse `http://huffingtonpost.com`. La fonctionnalité de redirection multimédia HTML5 peut rediriger le contenu multimédia HTML5 de l'adresse `http://www.yahoo.com`, mais un message « La page ne répond pas » peut s'afficher.
- Si vous incluez l'URL d'un site de confiance Microsoft Edge dans la liste de sites Web dans le paramètre de stratégie de groupe **Activer la liste d'URL pour la redirection multimédia HTML5 de VMware**, la redirection multimédia HTML5 ne fonctionne pas pour cette URL. Vous pouvez éviter cette limitation en rendant l'hôte moins sécurisé via l'exécution de la commande **`CheckNetIsolation LoopbackExempt -a -n="Microsoft.MicrosoftEdge_8wekyb3d8bbwe"`**.
- Avec le navigateur Microsoft Edge, la fonctionnalité de redirection multimédia HTML5 ne peut pas rediriger du contenu multimédia HTML à partir de sites Web qui utilisent le format vidéo m3u8, tels que `ted.com`.
- Lorsque l'option d'installation de **Redirection de scanner** est activée dans Horizon Agent sur un poste de travail distant, l'extension Extension de redirection HTML5 de VMware Horizon pour Edge se bloque parfois lorsque le navigateur Microsoft Edge est lancé sur le poste de travail distant. Ce problème se produit généralement dans les grands environnements de moniteur et sous contrainte.
- Si un utilisateur lit une vidéo HTML5 qui utilise une URL vidéo statique sur un poste de travail distant, sa machine cliente n'a pas accès à l'URL statique et la lecture se fait sur le poste de travail distant.

- Les commentaires marqués par une puce dans la vidéo ne sont pas pris en charge lors de l'utilisation de la fonctionnalité de redirection multimédia HTML5.

Configuration de la redirection de navigateur

Grâce à la redirection de navigateur, lorsqu'un utilisateur final utilise le navigateur Google Chrome sur un poste de travail distant, le site Web est restitué sur le système client plutôt que sur le système agent, et il est affiché sur la fenêtre d'affichage du navigateur distant. La fenêtre d'affichage est la partie de la fenêtre du navigateur qui affiche le contenu d'une page Web.

Configuration système requise pour la redirection de navigateur

Les postes de travail distants et les systèmes clients sur lesquels vous installez les logiciels agent et client doivent respecter la configuration requise pour la prise en charge de la fonctionnalité Redirection de navigateur.

Postes de travail distants

- Les paramètres de stratégie de groupe de Redirection de VMware Browser doivent être configurés sur le serveur Active Directory.
- Le navigateur Chrome doit être installé.
- L'extension de redirection de navigateur VMware Horizon doit être installée dans le navigateur Chrome.

Système client

Seuls les systèmes clients Windows sont pris en charge.

Vous devez installer Horizon Client pour Windows avec la prise en charge de la redirection multimédia HTML5 et l'option de configuration personnalisée de redirection de navigateur sélectionnée. Cette option est sélectionnée par défaut. Consultez les rubriques sur l'installation d'Horizon Client dans le document *Guide d'installation et de configuration de VMware Horizon Client pour Windows*.

Protocole d'affichage de la session distante

- PCoIP
- VMware Blast

Installer et configurer la redirection de navigateur

L'installation et la configuration de la fonctionnalité Redirection de navigateur implique l'installation du navigateur Chrome, l'activation de la fonctionnalité Redirection de navigateur sur la machine agent et la spécification des URL de redirection.

Vous pouvez éventuellement spécifier les URL auxquelles les utilisateurs peuvent accéder à partir des URL redirigées et personnaliser le comportement de basculement pour les violations de la liste verte. Vous pouvez également configurer des paramètres de stratégie de groupe côté client pour l'utilisation du microphone et de l'appareil photo, la gestion des erreurs de certificat et le stockage du cache de navigateur.

Pour activer la redirection de navigateur et spécifier les URL de redirection, vous devez configurer les paramètres de stratégie de groupe côté agent sur votre serveur Active Directory. Compilez une liste des URL pour les sites Web qui peuvent être redirigés et, éventuellement, pour les sites Web auxquels les utilisateurs peuvent accéder à partir des URL redirigées. Incluez le préfixe **`http://`** ou **`https://`** dans les URL. Vous pouvez utiliser des modèles de correspondance dans les URL. Par exemple, pour rediriger tout le contenu Yahoo, entrez **`https://www.yahoo.com/*`**. Pour plus d'informations, reportez-vous à la section https://developer.chrome.com/extensions/match_patterns.

Conditions préalables

- 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.
- Ajoutez le fichier de modèle ADMX de configuration de VMware View Agent `vdm_agent.admx` à un GPO lié à l'UO pour le poste de travail virtuel ou à l'hôte RDS pour le poste de travail publié. Si vous prévoyez de configurer l'un des paramètres facultatifs de stratégie de groupe côté client, ajoutez également le modèle de fichier Horizon Client Configuration ADMX pour la configuration de Horizon Client (`vdm_client. admx`). Pour obtenir des instructions d'installation, consultez le document Ajouter les fichiers de modèle d'administration ADMX à Active Directory.
- Compilez une liste d'URL pour les sites Web qui peuvent utiliser la fonction Redirection de navigateur.

Procédure

1. Installez le navigateur Chrome sur le poste de travail distant.
2. Sur votre serveur Active Directory, ouvrez l'Éditeur de gestion de stratégie de groupe.
3. Accédez au dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Configuration de VMware View Agent > Fonctionnalités HTML5 de VMware**.
4. Ouvrez le paramètre **Activer les fonctionnalités VMware HTML5**, sélectionnez **Activée**, puis cliquez sur **OK**.
5. Accédez au dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Configuration de VMware View Agent > Fonctionnalités HTML5 de VMware > Redirection de VMware Browser**.

6 Ouvrez le paramètre **Activer la Redirection de VMware Browser**, sélectionnez **Activée**, puis cliquez sur **OK**.

7 Spécifie les URL de la fonctionnalité de redirection de navigateur.

Les utilisateurs peuvent accéder à ces URL en les entrant dans la barre d'adresse Chrome ou dans la barre d'adresse personnalisée. Ils peuvent également consulter ces URL en y accédant à partir d'une autre URL de la liste ou à partir de toute page rendue du côté agent. Seules les URL que vous avez spécifiées sont redirigées. Aucune URL n'est ajoutée par défaut.

a Ouvrez le paramètre **Activer la liste d'URL pour la Redirection de VMware Browser**, puis sélectionnez **Activée**.

b Cliquez sur **Afficher**, entrez les URL dans la colonne Nom de la valeur, puis cliquez sur **OK**.

Laissez vide la colonne Valeur.

c Pour enregistrer le paramètre de stratégie, cliquez sur **OK**.

8 (Facultatif) Configurez un ou plusieurs des paramètres de stratégie de groupe facultatifs du côté agent.

Le tableau suivant décrit les paramètres facultatifs de stratégie de groupe côté agent.

Option	Description
Activer la liste d'URL de navigation pour la redirection de VMware Browser	Vous pouvez utiliser ce paramètre pour spécifier les URL auxquelles un utilisateur est autorisé à accéder depuis une URL spécifiée dans la liste verte **Activer la liste d'URL pour la redirection de VMware Browser**, soit en entrant l'URL directement dans la barre d'adresse personnalisée, soit en accédant à l'URL commençant à partir d'une URL spécifiée dans la liste verte. Les utilisateurs ne peuvent pas accéder directement à ces URL en les tapant dans la barre d'adresse Chrome ou en y accédant à partir d'une page rendue du côté agent. Pour spécifier les URL, cliquez sur **Afficher**, entrez les URL dans la colonne Nom de la valeur, puis cliquez sur **OK**. Laissez vide la colonne Valeur.
`Enable automatic fallback after a whitelist violation`	Lorsque vous activez ce paramètre, si un utilisateur accède à une URL qui n'est pas spécifiée dans l'une des listes blanches de redirection de navigateur, en l'entrant dans la barre d'adresse personnalisée ou en y accédant à partir d'une URL dans une liste blanche, la redirection s'arrête pour cet onglet et l'URL est extraite et s'affiche plutôt sur l'agent. **Note** Si un utilisateur tente d'accéder à une URL qui n'est pas spécifiée dans le paramètre **Activer la liste d'URL pour la redirection de VMware Browser**, l'onglet revient toujours à l'extraction et au rendu de l'URL sur l'agent, que ce paramètre soit ou non activé.
`Show a page with error information before automatic fallback`	Lorsque vous activez ce paramètre et qu'une violation de la liste verte se produit, une page s'affiche et indique un compte à rebours de cinq secondes. Lorsque la période de cinq secondes s'est écoulée, l'onglet revient à l'extraction et au rendu de l'URL qui a provoqué la violation sur l'agent. Si ce paramètre est désactivé, la page d'avertissement de cinq secondes ne s'affiche pas. Ce paramètre ne prend effet que si le paramètre **Activer le secours automatique après une violation de la liste blanche** est également activé.

9 (Facultatif) Pour configurer un ou plusieurs des paramètres facultatifs de stratégie de groupe du côté client, accédez au dossier **Configuration de l'ordinateur > Stratégies > Modèles d'administration > Configuration de VMware Horizon Client > Redirection de VMware Browser**.

Le tableau suivant décrit les paramètres de stratégie de groupe côté client.

Option	Description
Activer l'accès à la caméra WebRTC et au microphone pour la redirection de navigateur	Lorsque vous activez ce paramètre, les pages redirigées qui utilisent WebRTC ont accès à la caméra et au microphone du système client. Ce paramètre est activé par défaut.
Ignorer les erreurs de certificat pour la redirection de navigateur	Lorsque vous activez ce paramètre, les erreurs de certificat qui se produisent dans une page redirigée sont ignorées et la navigation se poursuit. Ce paramètre est désactivé par défaut.
Activer le cache pour la redirection de navigateur	Lorsque vous activez ce paramètre, l'historique de navigation, y compris les cookies, est stocké sur le système client. Ce paramètre est activé par défaut. **Note** La désactivation de ce paramètre n'engendre pas d'effacement du cache. Si vous désactivez, puis réactivez ce paramètre, le cache est réutilisé.

Exemple

`https://play.google.com` et `https://news.google.com` disposent d'une page de connexion commune, `https://accounts.google.com`.

Dans l'exemple suivant, `https://play.google.com/*` et `https://accounts.google.com/*` sont inclus dans **Activer la liste d'URL pour la redirection de VMware Browser**. Le tableau suivant décrit le comportement qui se produit dans ce scénario.

Un utilisateur accède à `https://play.google.com`	■ `https://play.google.com` est redirigé vers la machine cliente. ■ Lorsque l'utilisateur se connecte, `https://accounts.google.com` s'ouvre sur la machine cliente et l'utilisateur s'authentifie sur la machine cliente. ■ Une fois l'authentification réussie, le site Web est redirigé vers `https://play.google.com` sur la machine cliente et l'utilisateur est connecté correctement.
Un utilisateur accède à `https://news.google.com`	■ `https://news.google.com` est rendu sur la machine agent. ■ Lorsque l'utilisateur se connecte, `https://accounts.google.com` est redirigé vers la machine cliente et l'utilisateur s'authentifie sur la machine cliente. ■ Une fois l'authentification réussie, l'utilisateur n'est pas connecté correctement, car `https://news.google.com` est rendu sur la machine agent, mais l'authentification s'est produite sur la machine cliente.
Un utilisateur ouvre `https://accounts.google.com` directement dans la barre d'adresse	`https://accounts.google.com` est redirigé vers la machine cliente.

Dans l'exemple suivant, `https://play.google.com/*` est inclus dans **Activer la liste d'URL pour la redirection de VMware Browser** et `https://accounts.google.com/*` est inclus dans **Activer la liste d'URL de navigation pour la redirection de VMware Browser**. Le tableau suivant décrit le comportement qui se produit dans ce scénario.

Un utilisateur accède à `https://play.google.com`	■ `https://play.google.com` est redirigé vers la machine cliente. ■ Lorsque l'utilisateur se connecte, `https://accounts.google.com` s'ouvre sur la machine cliente et l'utilisateur s'authentifie sur la machine cliente. ■ Une fois l'authentification réussie, le site Web est redirigé vers `https://play.google.com` sur la machine cliente et l'utilisateur est connecté correctement.
Un utilisateur accède à `https://news.google.com`	■ `https://news.google.com` est rendu sur la machine agent. ■ Lorsque l'utilisateur se connecte, `https://accounts.google.com` est rendu sur la machine agent et l'utilisateur s'authentifie sur la machine agent. ■ Une fois l'authentification réussie, le site Web est redirigé vers `https://news.google.com` sur la machine agent et l'utilisateur est connecté correctement.
Un utilisateur ouvre `https://accounts.google.com` directement dans la barre d'adresse	`https://accounts.google.com` est rendu sur la machine agent.

Étape suivante

Installer l'extension de redirection de navigateur de VMware Horizon pour Chrome.

Installer l'extension de redirection de navigateur de VMware Horizon pour Chrome

Pour utiliser la fonctionnalité de redirection de navigateur avec le navigateur Chrome, vous devez forcer l'installation de l'extension de redirection de navigateur de VMware Horizon sur le poste de travail distant. Pour forcer l'installation de l'extension, vous devez configurer un paramètre de stratégie de groupe Google Chrome sur votre serveur Active Directory.

Pour appliquer le paramètre de stratégie de groupe Chrome au poste de travail distant, vous devez ajouter le fichier de modèle d'administration ADMX à un GPO sur votre serveur Active Directory. Pour un poste de travail virtuel, le GPO doit être lié à l'UO qui contient le poste de travail virtuel. Pour un poste de travail publié, le GPO doit être lié à l'UO qui contient l'hôte RDS.

Conditions préalables

- Configurez la fonctionnalité de redirection de navigateur. Reportez-vous à la section Installer et configurer la redirection de navigateur.
- 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.

Procédure

1. Téléchargez le fichier `policy_templates.zip` de Google Chrome sur https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip.
2. Décompressez le fichier `policy_templates.zip`, puis copiez les fichiers `chrome.admx` et `chrome.adml` sur votre serveur Active Directory.

   Le fichier `chrome.admx` se trouve dans le dossier `\windows\admx` et le fichier `chrome.adml` se trouve dans le dossier `\windows\admx\language` dans le fichier `policy_templates.zip`.

   a. Copiez le fichier `chrome.admx` dans le dossier `%systemroot%\PolicyDefinitions` sur votre serveur Active Directory.

   b. Copiez le fichier de ressources de la langue `chrome.adml` dans le sous-dossier de langue correspondant dans `%systemroot%\PolicyDefinitions` sur votre serveur Active Directory.

      Par exemple, copiez la version `fr_fr` du fichier `chrome.adml` dans le sous-dossier `%systemroot%\PolicyDefinitions\fr_fr` sur votre serveur Active Directory.
3. Toujours sur votre serveur Active Directory, ouvrez l'Éditeur de gestion de stratégie de groupe et accédez au dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Google Chrome > Extensions**.
4. Ouvrez le paramètre de stratégie **Configurer la liste des applications et des extensions installées de force**, puis cliquez sur **Activées**.
5. Cliquez sur **Afficher** et tapez **`demgbalbngngkkgjcofhdiiipjblblob;https://clients2.google.com/service/update2/crx`** dans la colonne Valeur.
6. Cliquez sur **OK** pour enregistrer l'ID d'extension/URL de mise à jour, puis cliquez sur **OK** pour enregistrer le paramètre de stratégie.
7. Vérifiez que l'extension de redirection de navigateur de VMware Horizon est installée sur le poste de travail distant.

   a. Connectez-vous au poste de travail distant et démarrez Chrome.

   b. Tapez **`chrome://extensions`** dans la barre d'adresses de Chrome.

      Extension de navigateur VMware Horizon s'affiche dans la liste des extensions.

Limitations de la redirection de navigateur

La fonctionnalité Redirection de navigateur comporte certaines limitations.

- La fonctionnalité de redirection de navigateur est prise en charge uniquement avec les clients Windows.

- Seuls les protocoles d'affichage VMware Blast et PCoIP sont pris en charge avec la fonctionnalité de redirection de navigateur. Le protocole RDP n'est pas pris en charge.
- La fonctionnalité de redirection de navigateur ne fonctionne pas avec les autres fonctionnalités de redirection VMware Horizon suivantes :
  - Redirection de contenu URL.
  - Fonctionnalité de redirection multimédia HTML5 dans Chrome. Si l'extension de redirection de navigateur VMware Horizon et l'extension de redirection multimédia HTML5 sont toutes les deux installées dans Chrome et que les paramètres de stratégie de groupe sont configurés correctement pour les deux fonctionnalités, seule la redirection de navigateur fonctionne.
  - Redirection de géolocalisation. Si les deux fonctionnalités sont configurées, la redirection de navigateur est prioritaire.
- La fonctionnalité de redirection de navigateur est prise en charge uniquement avec un navigateur Chrome.
- La fonctionnalité de redirection de navigateur ne fonctionne pas si vous démarrez Chrome à l'aide d'une commande d'exécution, comme **`Chrome url`**, cliquez sur une URL dans un éditeur, ou faites glisser un élément de favori du menu **Favoris** de Chrome sur le poste de travail distant et double-cliquez sur l'icône de raccourci.
- Les protocoles autres que http et https, comme mailto, ne sont pas pris en charge avec la fonctionnalité de redirection de navigateur.
- Lorsque vous utilisez la fonctionnalité de redirection de navigateur dans le navigateur Chrome, vous pouvez rencontrer les limitations suivantes liées au navigateur.
  - Les fenêtres contextuelles s'ouvrent toujours dans un nouvel onglet.
  - Les fenêtres contextuelles liées aux autorisations ne s'affichent pas.
  - Il n'est pas possible de faire glisser un lien sur la fenêtre d'affichage redirigée vers la barre d'adresses.
  - Il n'est pas possible de télécharger un fichier ou d'enregistrer une image.
  - Il n'est pas possible d'enregistrer des mots de passe pour des sites Web qui nécessitent une authentification.
  - Pour fermer un onglet, déplacez le focus vers l'onglet du navigateur. Si vous appuyez sur Alt+F4, Ctrl+F4 ou Ctrl+W alors que le focus se trouve sur la fenêtre d'affichage, un comportement inattendu peut en résulter.
  - L'effacement des données du navigateur, notamment des cookies, n'a aucun effet.
  - Parfois, vous ne pouvez pas revenir en arrière ou avancer à la page précédente.
- Le partage d'écran n'est pas pris en charge avec la fonctionnalité de redirection de navigateur.

Configuration de la redirection de géolocalisation

Avec la fonctionnalité de redirection de géolocalisation, les postes de travail distants et les applications publiées peuvent utiliser les informations de géolocalisation du terminal client.

Configuration système requise pour la redirection de géolocalisation

Horizon Agent et Horizon Client, ainsi que le poste de travail virtuel ou l'hôte RDS et la machine cliente sur lesquels vous installez les logiciels agent et client doivent respecter la configuration requise pour la prise en charge de la fonctionnalité de redirection de géolocalisation.

Poste de travail virtuel ou hôte RDS

- Le paramètre **Service d'emplacement** de Windows doit être **activé** dans **Paramètres > Confidentialité > Emplacement**.
- La fonctionnalité de redirection de géolocalisation prend en charge les applications de poste de travail distant suivantes.

Application	Plate-forme
Google Chrome (dernière version)	Tous les postes de travail virtuels ou hôtes RDS
Internet Explorer 11	Tous les postes de travail virtuels ou hôtes RDS
Edge, Maps, Météo et autres applications Win32 et UWP	Windows 10

  Le paramètre d'autorisation **Emplacement**, le cas échéant, doit être activé individuellement dans chaque navigateur pris en charge.
- Vous devez installer Horizon Agent avec l'option de configuration personnalisée de redirection de géolocalisation sélectionnée. Cette option n'est pas sélectionnée par défaut. Consultez les rubriques sur l'installation Horizon Agent dans les documents *Configuration des postes de travail virtuels dans Horizon* et *Configuration d'applications et de postes de travail publiés dans Horizon*.
- Les paramètres de stratégie de groupe de redirection de géolocalisation VMware doivent être configurés sur le serveur Active Directory. Reportez-vous à la section Installer et configurer la redirection de géolocalisation.
- Pour Internet Explorer 11, vous devez activer le plug-in IE de redirection de géolocalisation VMware Horizon pour les hôtes RDS. Reportez-vous à Activer le plug-in IE de redirection de géolocalisation VMware Horizon. Il n'est pas nécessaire d'activer le plug-in IE de redirection de géolocalisation VMware Horizon pour les postes de travail virtuels Windows 10. Internet Explorer est pris en charge sur les postes de travail virtuels Windows 10 avec le pilote de redirection de géolocalisation de VMware.

- Pour Chrome, le plug-in Chrome de redirection de géolocalisation VMware Horizon doit être activé. Reportez-vous à la section Activer le plug-in Chrome de redirection de géolocalisation VMware Horizon.

Système client

- Installez Horizon Client pour Windows sur un système client Windows. Les clients non-Windows ne sont pas pris en charge. Pour plus d'informations, consultez le document *Guide d'installation et de configuration de VMware Horizon Client pour Windows*.
- Pour partager les informations d'emplacement du système client, configurez les paramètres de **Géolocalisation** dans Horizon Client pour Windows.
- Pour les systèmes clients Windows 10, le paramètre de service **Emplacement** Windows doit être **activé** dans **Paramètres > Confidentialité > Emplacement** pour qu'Horizon accède à votre emplacement.

Protocole d'affichage de la session distante

- PCoIP
- VMware Blast

Installer et configurer la redirection de géolocalisation

Rediriger les informations de géolocalisation du périphérique client vers des postes de travail distants ou des applications publiées nécessite d'activer la fonctionnalité de redirection de géolocalisation sur la machine agent, de configurer des paramètres de stratégie de groupe sur votre serveur Active Directory et de spécifier les sites Web qui utilisent cette fonctionnalité.

Pour activer la redirection de géolocalisation et spécifier les sites Web pouvant utiliser cette fonctionnalité, configurez les paramètres de stratégie de groupe de votre serveur Active Directory. Vous devez compiler une liste d'URL pour les sites Web qui peuvent utiliser les informations de géolocalisation redirigées. Incluez le préfixe `http://` ou `https://` dans les URL. Vous pouvez utiliser des modèles de correspondance dans les URL.

Conditions préalables

- Installez Horizon Client sur le système client et Horizon Agent sur le poste de travail virtuel ou l'hôte RDS avec la fonctionnalité de redirection de géolocalisation activée. Pour connaître les versions, les options d'installation et la configuration système requises, reportez-vous à la section Configuration système requise pour la redirection de géolocalisation.
- 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 Éditeur d'objets de stratégie de groupe sont disponibles sur votre serveur Active Directory.

- Ajoutez le fichier de modèle VMware View Agent Configuration ADMX (`vdm_agent.admx`) à un GPO lié à l'UO pour le poste de travail virtuel ou à l'hôte RDS. Pour obtenir des instructions d'installation, consultez le document Ajouter les fichiers de modèle d'administration ADMX à Active Directory.
- Compilez une liste d'URL pour les sites Web qui peuvent utiliser les informations de géolocalisation redirigées.
- Installez Internet Explorer 11 ou Chrome sur la machine agent.

Procédure

1. Sur votre serveur Active Directory, ouvrez l'Éditeur de gestion de stratégie de groupe.
2. Accédez au dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Configuration de VMware View Agent > Fonctionnalités HTML5 de VMware**.
3. Ouvrez le paramètre **Désactiver la détection automatique du réseau intranet**, sélectionnez **Activé** et cliquez sur **OK**.
4. Ouvrez le paramètre **Activer les fonctionnalités VMware HTML5**, sélectionnez **Activée**, puis cliquez sur **OK**.
5. Accédez au dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Configuration de VMware View Agent > Fonctionnalités HTML5 de VMware > Redirection de géolocalisation VMware**.
6. Ouvrez le paramètre **Activer la redirection de géolocalisation VMware**, sélectionnez **Activée**, puis cliquez sur **OK**.
7. Spécifiez quels sites Web peuvent utiliser la fonctionnalité de redirection de géolocalisation.

   Le plug-in Chrome de redirection de géolocalisation VMware Horizon utilise cette liste de sites Web dans tous les environnements d'hôte RDS et de poste de travail virtuel. Le plug-in IE de redirection de géolocalisation VMware Horizon utilise cette liste de sites Web dans les environnements d'hôte RDS et de poste de travail virtuel Windows 7.

   a. Ouvrez le paramètre **Activer la liste d'URL pour la redirection de géolocalisation de VMware**, puis sélectionnez **Activée**.

   b. Cliquez sur **Afficher** et entrez les URL que vous avez compilées dans la colonne Nom de la valeur.

      Seules les URL que vous spécifiez peuvent utiliser les informations de géolocalisation redirigée. Aucune URL n'est ajoutée par défaut. Laissez vide la colonne Valeur.

   c. Cliquez sur **OK** pour enregistrer la liste d'URL, puis cliquez sur **OK** pour enregistrer le paramètre de stratégie.

8 Ouvrez le paramètre **Définir la distance minimale pour laquelle signaler des mises à jour d'emplacement**, cliquez sur **Activé** et spécifiez la distance minimale (en mètres), entre une mise à jour d'emplacement dans le client et la dernière mise à jour signalée à l'agent. dont le nouvel emplacement doit être mis à jour.

   Par défaut, la distance minimale est de 75 mètres.

Étape suivante

Si vous avez installé Internet Explorer sur une machine agent d'hôte RDS, vous devez également activer le plug-in IE de redirection de géolocalisation VMware Horizon. Pour plus d'informations, reportez-vous à la section Activer le plug-in IE de redirection de géolocalisation VMware Horizon.

Note Internet Explorer est pris en charge sur les postes de travail virtuels Windows 10 avec le pilote de redirection de géolocalisation VMware. Vous n'avez pas besoin d'activer le plug-in IE de redirection de géolocalisation VMware Horizon pour les postes de travail virtuels Windows 10.

Si vous avez installé Chrome sur la machine agent, vous devez également activer le plug-in Chrome de redirection de géolocalisation VMware Horizon. Pour plus d'informations, consultez Activer le plug-in Chrome de redirection de géolocalisation VMware Horizon.

Activer le plug-in IE de redirection de géolocalisation VMware Horizon

Pour utiliser Internet Explorer sur un poste de travail publié avec la fonctionnalité de redirection de géolocalisation, vous devez activer le plug-in IE de redirection de géolocalisation VMware Horizon sur l'hôte RDS.

Internet Explorer est pris en charge sur les postes de travail virtuels Windows 10 avec le pilote de redirection de géolocalisation VMware. Vous n'avez pas besoin d'activer le plug-in IE de redirection de géolocalisation VMware Horizon pour les postes de travail virtuels Windows 10.

Conditions préalables

- Installer et configurer la redirection de géolocalisation.
- Vérifiez que l'option **Mode de protection amélioré** est désactivée dans Internet Explorer 11. Le plug-in ne fonctionne pas avec cette fonctionnalité.
- Pour les systèmes d'exploitation Windows Server, vérifiez que la **configuration de sécurité renforcée d'Internet Explorer** est désactivée. Le plug-in ne fonctionne pas avec cette fonctionnalité.

Procédure

1 Sur l'hôte RDS sur lequel la fonctionnalité de redirection de géolocalisation est activée, ouvrez Internet Explorer 11.

2 Cliquez sur l'icône **Outils** dans le coin supérieur droit de la fenêtre du navigateur et sélectionnez **Gérer les modules complémentaires**.

3 Faites défiler l'affichage vers le bas jusqu'à la section VMware, Inc., sélectionnez **Plug-in IE de redirection de géolocalisation VMware Horizon**, puis cliquez sur **Activer**.

4 Redémarrez Internet Explorer 11.

Activer le plug-in Chrome de redirection de géolocalisation VMware Horizon

Pour utiliser la fonctionnalité de redirection de géolocalisation avec Chrome, vous devez activer le plug-in Chrome de redirection de géolocalisation VMware Horizon.

Conditions préalables

Installer et configurer la redirection de géolocalisation.

Procédure

1 Sur votre serveur Active Directory, téléchargez le fichier `https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip`.

2 Décompressez le fichier `chrome.admx` et copiez-le dans le dossier `%systemroot%\PolicyDefinitions` sur votre serveur Active Directory.

3 Décompressez le fichier de ressources de la langue `chrome.adml` et copiez-le dans le sous-dossier de langue correspondant dans le dossier `%systemroot%\PolicyDefinitions` sur votre serveur Active Directory.

   Par exemple, copiez la version `fr_fr` du fichier `chrome.adml` dans le sous-dossier `%systemroot%\PolicyDefinitions\fr_fr` sur votre serveur Active Directory.

4 Toujours sur votre serveur Active Directory, ouvrez l'Éditeur de gestion de stratégie de groupe et accédez au dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Google Chrome > Extensions**.

5 Ouvrez le paramètre de stratégie de groupe **Configurer la liste des applications et des extensions installées de force**, puis cliquez sur **Activées**.

6 Cliquez sur **Afficher**, tapez **`lndponbebpocehnoblfgdfeiegeaokcf;https://clients2.google.com/service/update2/crx`** dans la zone de texte **Valeur** et cliquez sur **OK**.

7 Cliquez sur **OK** pour enregistrer les modifications.

8 Pour vérifier que l'extension de redirection de géolocalisation VMware Horizon est installée sur le poste de travail distant, procédez comme suit.

   a Connectez-vous au poste de travail distant et démarrez Chrome.

   b Tapez **`chrome://extensions`** dans la barre d'adresses de Chrome.

   c Vérifiez que la redirection de géolocalisation de VMware Horizon s'affiche dans la liste Extensions.

Configuration de l'Audio/Vidéo en temps réel

L'Audio/Vidéo en temps réel permet aux utilisateurs d'Horizon d'exécuter Skype, Webex, Google Hangouts, Microsoft Teams et d'autres applications de conférence en ligne dans leurs sessions distantes. Avec l'Audio/Vidéo en temps réel, les webcams et les périphériques audio qui sont connectés localement au système client sont redirigés vers les sessions distantes. Cette fonctionnalité redirige les données vidéo et audio 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.

Lors de l'installation d'une application telle que Skype, Webex, Google Hangouts ou Microsoft Teams, les utilisateurs peuvent choisir des périphériques d'entrée et de sortie dans les menus de l'application.

- Pour les postes de travail virtuels, la fonctionnalité Audio/Vidéo en temps réel peut rediriger plusieurs périphériques audio et vidéo. Les noms de périphériques redirigés dans le poste de travail virtuel sont les noms de périphériques réels, mais avec l'ajout de (VDI), par exemple, C670i FHD Webcam (VDI).
- Pour les postes de travail publiés et les applications publiées, la fonction Audio/Vidéo en temps réel ne peut rediriger qu'un seul périphérique audio et un seul périphérique vidéo. Les noms de périphériques sont le périphérique audio distant et la Webcam virtuelle VMware dans les sessions distantes.

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.

Les pilotes des webcams et des périphériques audio doivent être installés sur les 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 sessions distantes 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 votre serveur 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 .

Si vous disposez de plusieurs webcams et périphériques d'entrée audio intégrés ou connectés à vos ordinateurs clients, vous devrez peut-être configurer des webcams et des périphériques d'entrée audio préférés à rediriger. Reportez-vous à la section Sélection de webcams et microphones préférés.

Note 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 une session distante, 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 la session distante.

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

La fonctionnalité Audio/Vidéo en temps réel fonctionne avec des webcams standard, audio USB et des périphériques audio analogiques. La fonctionnalité fonctionne également avec les applications de conférence standard. Pour prendre en charge l'Audio/Vidéo en temps réel, votre déploiement d'Horizon doit satisfaire certaines exigences matérielles et logicielles.

Postes de travail virtuels

Lorsque vous utilisez Microsoft Teams avec la fonctionnalité d'Audio/Vidéo en temps réel, les postes de travail virtuels doivent disposer d'au moins 4 vCPU et 4 Go de RAM.

Logiciel Horizon Client

Horizon Client pour Windows, Linux, Mac, iOS ou Android.

Ordinateur Horizon Client ou périphérique d'accès client

- Tous les systèmes d'exploitation qui exécutent Horizon Client pour Windows, Mac, iOS et Android.
- Tous les systèmes d'exploitation exécutant Horizon Client pour Linux sur des périphériques x64. Cette fonctionnalité n'est pas prise en charge par les processeurs ARM.
- Pour plus d'informations sur les systèmes d'exploitation clients pris en charge, reportez-vous au document d'installation et de configuration d'Horizon Client concernant le système ou le 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. Vous n'avez pas besoin d'installer les pilotes de périphérique sur la machine sur laquelle l'agent est installé.

Protocoles d'affichage

- PCoIP
- VMware Blast

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 stratégies pour contrôler la redirection USB.

Attention 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 préférés que la fonctionnalité audio/vidéo en temps réel redirige vers le poste de travail distant ou l'application publiée. Ces périphériques peuvent être intégrés ou connectés à l'ordinateur client.

La fonctionnalité audio/vidéo en temps réel redirige la webcam préférée si elle est disponible. Si la webcam préférée n'est pas disponible, la fonction audio/vidéo en temps réel utilise la première webcam qui est fournie par l'énumération du système.

Ordinateur client Windows

Pour un poste de travail publié ou une application publiée, vous sélectionnez une webcam ou un microphone préféré en configurant les paramètres audio/vidéo en temps réel dans la boîte de dialogue Paramètres d'Horizon Client.

Pour un poste de travail virtuel, la fonctionnalité Audio/Vidéo en temps réel peut rediriger plusieurs webcams et microphones vers un poste de travail virtuel et vous n'avez pas à sélectionner une webcam ou un microphone préféré.

Pour plus d'informations, reportez-vous au document *Guide d'installation et de configuration de VMware Horizon Client pour Windows*.

Ordinateur client Mac

Vous spécifiez une webcam ou un microphone préféré à l'aide du système de valeurs par défaut de Mac. Pour plus d'informations, reportez-vous au document *Guide d'installation et de configuration de VMware Horizon Client pour Mac*.

Ordinateur client Linux

Vous spécifiez 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. Pour plus d'informations, reportez-vous au document *Guide d'installation et de configuration de VMware Horizon Client pour Linux*.

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 distants. 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.

Ces paramètres de stratégie affectent vos postes de travail distants et non les systèmes clients 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.

Conditions préalables

- Vérifiez que l'option de configuration RTAV est installée sur vos postes de travail de machine virtuelle et vos hôtes RDS. 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 GPO doivent être liés à l'unité d'organisation (UO) qui contient vos postes de travail de machine virtuelle ou vos hôtes RDS. Reportez-vous à la section Exemple de stratégie de groupe Active Directory.
- 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 .

Procédure

1. Téléchargez le fichier VMware Horizon 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, qui inclut GPO Bundle.

   Le fichier est nommé `VMware-Horizon-Extras-Bundle-`*`YYMM`*`-`*`x.x.x`*`-`*`yyyyyyyy`*`.zip`, où *YYMM* est la version marketing, *x.x.x* est la version interne et *yyyyyyyy* est le numéro de build. Tous les fichiers ADMX qui fournissent des paramètres de stratégie de groupe pour VMware Horizon sont disponibles dans ce fichier.
2. Décompressez le fichier `VMware-Horizon-Extras-Bundle-`*`YYMM`*`-`*`x.x.x`*`-`*`yyyyyyyy`*`.zip` et copiez les fichiers ADMX sur votre serveur Active Directory.
   a. Copiez le fichier `vdm_agent_rtav.admx`, ainsi que le dossier `en-US` dans le dossier `C:\Windows\PolicyDefinitions` sur votre serveur Active Directory.
   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 serveur Active Directory.
3. Sur le serveur Active Directory, ouvrez l'Éditeur de gestion de stratégie de groupe et entrez le chemin vers le fichier de modèle dans l'éditeur.

   Les paramètres se trouvent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Configuration de VMware View Agent > Afficher la configuration RTAV**.

Étape suivante

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 > Afficher la configuration RTAV > Afficher les paramètres de webcam RTAV** 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 > Afficher la configuration RTAV > Afficher les paramètres de webcam RTAV** 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 > Afficher la configuration RTAV > Afficher les paramètres de webcam RTAV** 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. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Afficher la configuration RTAV > Afficher les paramètres de webcam RTAV** 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. Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Afficher la configuration RTAV > Afficher les paramètres de webcam RTAV** 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 2-1. Résultats de l'exemple de bande passante pour envoyer des données Audio/Vidéo en temps réel d'Horizon Client à Horizon Agent mesurent la bande passante que la fonctionnalité Audio/Vidéo en temps réel utilise dans un environnement Horizon 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 2-1. 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 Microsoft Teams avec Audio/Vidéo en temps réel

Grâce à la fonction Audio/Vidéo en temps réel, les utilisateurs peuvent exécuter Microsoft Teams dans leurs sessions distantes.

Les webcams et les périphériques audio qui sont connectés localement au système client sont redirigés vers les sessions distantes et utilisent une bande passante nettement inférieure à celle de la redirection USB.

Lorsque vous lancez l'application Microsoft Teams à l'intérieur d'un poste de travail distant, vous sélectionnez des périphériques d'entrée et de sortie virtuels VMware dans les menus de l'application. Les périphériques virtuels VMware redirigent les périphériques audio et vidéo qui sont connectés à la machine cliente.

- Pour les postes de travail virtuels, la fonctionnalité Audio/Vidéo en temps réel peut rediriger plusieurs périphériques audio et vidéo. Les noms de périphériques redirigés dans le poste de travail virtuel sont les noms de périphériques réels, mais avec l'ajout de (VDI), par exemple, C670i FHD Webcam (VDI).
- Pour les postes de travail publiés et les applications publiées, la fonction Audio/Vidéo en temps réel ne peut rediriger qu'un seul périphérique audio et un seul périphérique vidéo. Les noms de périphériques sont le périphérique audio distant et la Webcam virtuelle VMware dans les sessions distantes.

Pour utiliser Audio/Vidéo en temps réel avec Microsoft Teams, vous devez installer les pilotes de périphérique audio et webcam sur vos systèmes Horizon Client.

Lorsque vous installez Horizon Agent avec la fonction Audio/Vidéo en temps réel, Microsoft Teams s'utilise sur vos sessions distantes sans autre configuration. Reportez-vous à Configuration de l'Audio/Vidéo en temps réel.

Recommandation d'utilisation de Microsoft Teams avec Audio/Vidéo en temps réel

Pour utiliser Microsoft Teams avec Audio/Vidéo en temps réel, suivez ces recommandations :

- Microsoft Teams avec Audio/Vidéo en temps réel est pris en charge sur Horizon Agent 7.9 et versions ultérieures sur les clients Windows, Linux et Mac.

- Microsoft Teams avec Audio/Vidéo en temps réel nécessite un minimum de 4 vCPU, une configuration de RAM de 4 Go avec une résolution vidéo maximale de 640 x 480 pixels. D'autres configurations de vCPU et de mémoire offrent une expérience supérieure.
- La résolution vidéo par défaut pour Audio/Vidéo en temps réel est de 320 x 240 pixels. Vous pouvez modifier la résolution en modifiant le paramètre dans le dossier **Configuration de VMware View Agent > Afficher la configuration RTAV** de l'Éditeur de gestion de stratégie de groupe.

Configuration de l'optimisation des supports pour Microsoft Teams

L'optimisation des supports pour Microsoft Teams redirige les appels audio, les appels vidéo et l'affichage des partages de postes de travail pour une expérience transparente entre le système client et la session distante sans avoir de conséquences négatives sur l'infrastructure virtuelle et surcharger le réseau. Le traitement multimédia de Teams a lieu sur la machine cliente plutôt que sur le poste de travail virtuel.

Fonctionnalités de l'optimisation des supports pour Microsoft Teams

L'optimisation des supports pour Microsoft Teams offre les fonctionnalités suivantes :

- Accepter et effectuer des appels audio et vidéo
- Conférence audio et vidéo à plusieurs
- Transfert, coupure du son, mise en attente et reprise d'un appel
- Appels PSTN via un pavé de numérotation
- Partage d'écran de postes de travail
- Partage d'écran de plusieurs moniteurs et sélecteur d'écran pour le partage d'écran
- Contrôle de volume à partir du poste de travail distant
- Identification de haut-parleur actif
- Vue Galerie dans les réunions (2x2) – Contactez Microsoft pour activer la vue Galerie.

Configuration système requise pour l'optimisation des supports pour Microsoft Teams

L'optimisation des supports pour Microsoft Teams prend en charge ces configurations.

Tableau 2-2. Configuration système requise pour l'optimisation des supports pour Microsoft Teams

Système	Configuration requise
Microsoft Server	Microsoft 365
Client Microsoft Teams (Optimisé)	■ Client de poste de travail Microsoft Teams x64 ■ Client de poste de travail Microsoft Teams x86 **Note** Le client du navigateur Web est pris en charge avec la redirection de navigateur. Reportez-vous à la section Configuration de la redirection de navigateur.
Systèmes d'exploitation de postes de travail virtuels	La configuration minimale requise est de 2 vCPU pour les systèmes d'exploitation pris en charge pour Horizon Agent.
Systèmes d'exploitation de machines clients	Windows : l'optimisation des supports pour Microsoft Teams prend en charge les mêmes systèmes d'exploitation Windows que ceux pris en charge par Horizon Client. Configuration matérielle minimale requise : processeur double cœur 2,4 GHz. Mac : l'optimisation des supports pour Microsoft Teams prend en charge les mêmes systèmes d'exploitation Mac que ceux pris en charge par Horizon Client. L'optimisation des supports pour Microsoft Teams avec un client Mac n'est pas prise en charge avec les versions antérieures à Horizon Client 2103.
Déploiements	■ VDI (sur site et cloud) ■ Postes de travail non persistants ■ Déploiements de postes de travail publiés par RDS ■ Déploiements d'applications publiées RDS (non prises en charge avec les versions antérieures à Horizon Client 2012 ou Horizon Client 5.5)
Protocoles d'affichage	VMware Blast et PCoIP (non RDP)
Port TCP	9427
Réseau	IPv4
Microphones et webcams	Les mêmes périphériques qui sont certifiés pour fonctionner avec Microsoft Teams
Codecs audio	Pour plus d'informations, reportez-vous à la section https://developer.mozilla.org/en-US/docs/Web/Media/Formats/WebRTC_codecs. ■ SILK ■ Opus ■ G.722
Codecs vidéo	Pour plus d'informations, reportez-vous à la section https://developer.mozilla.org/en-US/docs/Web/Media/Formats/WebRTC_codecs. ■ AVC/H.264 ■ VP8 ■ VP9
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.

Installation et configuration de l'optimisation des supports pour Microsoft Teams

La fonctionnalité Optimisation des supports pour Microsoft Teams est installée par défaut avec Horizon Client pour Windows lors de l'utilisation de l'assistant d'installation interactive. Pour plus d'informations, reportez-vous au *Guide d'installation et de configuration de VMware Horizon Client pour Windows*.

La fonctionnalité Optimisation des supports pour Microsoft Teams est installée par défaut avec Horizon Client pour Mac.

Vous devez installer Horizon Agent avant Microsoft Teams. Si vous installez Microsoft Teams avant Horizon Agent, supprimez le dossier `%APPDATA%\Microsoft\Teams` et relancez Teams.

Vous devez activer le paramètre de stratégie de groupe d'optimisation des supports pour Microsoft Teams pour utiliser la fonctionnalité. Reportez-vous aux Fonctionnalités de redirection de VMware WebRTC dans Paramètres de stratégie de fonctionnalité HTML5 de VMware.

Pour obtenir les conditions requises d'installation, de configuration et de déploiement, les directives sur les postes de travail persistants et non persistants et les limitations d'utilisation de Teams sur un poste de travail distant, consultez la documentation Teams pour l'infrastructure de poste de travail virtualisé de Microsoft.

Microsoft met à jour périodiquement la version recommandée de Teams. Recherchez les mises à jour de Microsoft et installez la dernière version recommandée pour accéder aux nouvelles fonctionnalités sans mettre à jour Horizon Client ou Horizon Agent.

Note L'optimisation des supports pour Microsoft Teams n'est pas prise en charge dans Horizon Agent 7.12 ou version antérieure et Horizon Client versions 5.4.3, 5.4.2, 5.4.1, 5.4 et 5.3 ou antérieures en raison des problèmes d'UX. Ces problèmes d'UX ont été corrigés dans la dernière version d'Horizon Agent et d'Horizon Client.

Limitations de l'optimisation des supports pour Microsoft Teams

L'optimisation des supports pour Microsoft Teams présente les limitations suivantes. Pour obtenir les limitations décrites comme dépendance de Teams, contactez Microsoft.

Limitation	Commentaires
Les boutons HID pour répondre aux appels et les terminer ne sont pas pris en charge.	Limitation de VMware
Le partage de fenêtres d'applications sortantes n'est pas pris en charge.	Limitation de VMware
Les arrière-plans virtuels ne sont pas pris en charge.	Limitation de Microsoft et de VMware
Les événements en direct ne sont pas pris en charge.	Limitation de Microsoft et de VMware
La fonctionnalité Donner ou prendre le contrôle du partage d'écran de postes de travail n'est pas prise en charge.	Dépendance de Teams

Limitation	Commentaires
Fenêtre de chat, d'appel ou de réunion.	Limitation de Microsoft. À partir de Horizon Client version 2103, la fenêtre de chat, d'appel ou de réunion n'est pas prise en charge par Microsoft pour VDI.
Le voyant de la caméra reste allumé si l'utilisateur met l'appel vidéo en attente (mais la vidéo n'est pas envoyée).	Dépendance de Teams
Lors d'un appel vidéo, la vidéo de l'utilisateur s'arrête automatiquement lorsqu'un utilisateur de poste de travail distant démarre un partage de poste de travail. Après avoir terminé le partage de poste de travail, l'utilisateur du poste de travail distant peut cliquer sur le bouton de la vidéo pour réactiver cette dernière.	Dépendance de Teams
Un seul flux vidéo d'un flux de caméra ou de partage d'écran entrant est pris en charge. Lors d'un partage d'écran entrant, ce dernier s'affiche à la place de la vidéo du haut-parleur dominant.	Dépendance de Teams
Lors de la réduction d'une fenêtre d'appel vidéo Teams, la petite fenêtre Teams dans le coin inférieur droit n'affiche aucune vidéo active.	Limitation de Microsoft
Lors de l'utilisation du module d'optimisation de Microsoft Teams avec l'application distante du client Mac, le partage d'écran n'est pas pris en charge.	Limitation de VMware

Modes de couplage d'une session

Un utilisateur peut vérifier si Teams s'exécute en mode optimisé, de secours ou natif sur le poste de travail virtuel (aucune optimisation). Dans le coin supérieur droit de l'interface de Teams, cliquez sur l'icône de l'utilisateur et accédez à **À propos de -> Version** pour afficher une bannière sous l'icône de l'utilisateur décrivant la version et les modes de couplage de Microsoft Teams :

- Optimisé : si la bannière affiche **Supports VMware optimisés**, Teams s'exécute en mode optimisé. Dans ce mode, le GPO **Activer l'optimisation des supports pour Microsoft Teams** est activé, Teams s'exécute dans le poste de travail virtuel. L'audio et la vidéo ont été alors déchargés sur la machine cliente.
- De secours : si la bannière affiche **Supports VMware non connectés**, Teams s'exécute en mode de secours. Dans ce mode, le GPO **Activer l'optimisation des supports pour Microsoft Teams** est activé et Teams a tenté de démarrer en mode optimisé, mais l'instance d'Horizon Client utilisée ne prend pas en charge l'optimisation de Teams. L'audio et la vidéo de Teams ne sont pas déchargés sur la machine cliente. Les limitations du mode de secours et du mode optimisé sont identiques. Lorsque vous effectuez un appel en mode de secours, un avertissement s'affiche lors de l'appel :

  Votre périphérique ne prend pas en charge l'optimisation de VMware. La qualité audio et vidéo peut être réduite. Contactez votre administrateur informatique.

- Aucune optimisation : si la bannière n'affiche pas le texte **VMware** dans le message, le GPO **Activer l'optimisation des supports pour Microsoft Teams** n'est pas activé. L'audio et la vidéo de Teams ne sont pas déchargés sur la machine cliente.

Configuration de la redirection de scanner

La redirection de scanner permet aux utilisateurs finaux 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 prend en charge les périphériques d'analyse et d'acquisition d'images standard compatibles avec les formats TWAIN et WIA, ainsi que le format SANE sur les clients Linux.

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.

Pour garantir la consolidation d'hôte optimale, assurez-vous que l'option de configuration Redirection de scanner est uniquement sélectionnée pour les utilisateurs qui en ont besoin. (Par défaut, l'option Redirection de scanner n'est pas sélectionnée lorsque vous installez Horizon Agent.) Pour les utilisateurs ayant besoin de la fonctionnalité de redirection de scanner, configurez un pool de postes de travail distinct et sélectionnez l'option de configuration uniquement dans ce pool.

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 sur votre serveur 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.

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 VMware Horizon doit répondre à certaines exigences matérielles et logicielles.

Poste de travail distant ou application publiée

Vous devez installer Horizon Agent avec l'option de configuration de la redirection de scanner activée sur le poste de travail virtuel ou l'hôte RDS pour les postes de travail publiés et les applications publiées. L'option de configuration de la redirection de scanner d'Horizon Agent est désélectionnée par défaut.

Cette fonctionnalité est prise en charge sur les postes de travail virtuels et les hôtes RDS suivants.

- Windows 10 1903 64 bits
- Windows Server 2012 R2 configuré en tant que poste de travail ou hôte RDS
- Windows Server 2016 configuré en tant que poste de travail avec Expérience utilisateur installée
- Windows Server 2016 configuré en tant qu'hôte RDS
- Windows Server 2019 configuré en tant que poste de travail ou hôte 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 pour Windows

Ordinateur Horizon Client ou périphérique d'accès client

Les pilotes du scanner doivent être installés, et ce dernier doit être opérationnel sur l'ordinateur client.

Les systèmes d'exploitation client suivants sont pris en charge.

- Windows 10 32 ou 64 bits
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Norme de scanner

TWAIN ou WIA

Protocole d'affichage

PCoIP

VMware Blast

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 publiées, l'icône de barre d'état système 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 Configuration des paramètres de stratégie de groupe de redirection de scanner.

- 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 **Forcer la boîte de dialogue des propriétés de numérisation TWAIN** 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 s'affiche toujours, que l'option **Forcer la boîte de dialogue des propriétés de numérisation TWAIN** soit sélectionnée ou non.

Note Si vous exécutez deux applications publiées hébergées sur différentes batteries de serveurs, deux icônes de barre d'état système 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 publiées 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 publiée.

Pour obtenir des instructions d'utilisateur final relatives à l'utilisation des scanners redirigés, consultez le document *Guide d'installation et de configuration 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 distants. 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.

Conditions préalables

- Vérifiez que l'option de configuration Redirection de scanner est installée sur vos postes de travail de machine virtuelle ou sur vos hôtes RDS. 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 GPO doivent être liés à l'UO qui contient vos postes de travail de machine virtuelle ou vos hôtes RDS. Reportez-vous à la section Exemple de stratégie de groupe 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.
- Familiarisez-vous avec les paramètres de stratégie de groupe de redirection de scanner. Reportez-vous à la section Paramètres du modèle d'administration ADMX pour la configuration de VMware View Agent.

Procédure

1 Téléchargez le fichier VMware Horizon 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, qui inclut GPO Bundle.

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

2 Décompressez le fichier `VMware-Horizon-Extras-Bundle-`*`YYMM`*`-`*`x.x.x`*`-`*`yyyyyyyy`*`.zip` et copiez les fichiers ADMX sur votre serveur Active Directory.

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

   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 serveur Active Directory.

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

   Les paramètres se trouvent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Configuration de VMware View Agent > Redirection de scanner**.

   La plupart des paramètres sont également ajoutés au dossier **Configuration utilisateur**, situé dans le dossier **Configuration utilisateur > Stratégies > Modèles d'administration > Configuration de VMware View Agent > Redirection de 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 et les applications publiées.

Après avoir installé Horizon Agent et configuré la fonctionnalité de redirection de port série, cette dernière peut fonctionner sur vos postes de travail distants et vos applications publiées 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 se connecte au poste de travail distant ou à l'application publiée. Reportez-vous à la section Opération utilisateur de la redirection de port série.

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 machines individuelles. Reportez-vous à la section Configuration des paramètres de stratégie de groupe de redirection de port série.

Dans VMware Horizon version 2103 et ultérieures, vous pouvez exécuter un utilitaire de console `vmwsprrdctl.exe` sur Horizon Agent pour afficher la liste des ports COM redirigés. Pour chaque port COM virtuel sur l'agent où le port source (port COM distant) sur le client est créé à partir d'un périphérique USB, l'utilitaire fournit les informations suivantes :

- ID du matériel
  - ID de fournisseur du périphérique USB
  - ID de produit du périphérique USB
  - Révision du périphérique USB (révision du produit)
- Description du périphérique du port COM telle qu'elle s'affiche dans le gestionnaire de périphériques

Pour tous les ports, l'utilitaire fournit les informations supplémentaires suivantes :

- Numéro de port COM source côté client
- État de la redirection du port COM

L'utilitaire sur Horizon Agent se trouve dans `C:\Program Files\Common Files\VMware\SerialPortRedirection\Agent\vmwsprrdctl.exe`.

Pour obtenir de l'aide sur l'utilisation de la ligne de commande pour l'utilitaire, lancez une session de poste de travail dans Horizon Client, puis tapez :

`# cd "C:\Program Files\Common Files\VMware\SerialPortRedirection\Agent\"` (Si le chemin se trouve dans la variable d'environnement OS PATH de l'agent, ignorez cette étape.)

```
# vmwsprrdctl.exe -h
```

Cet utilitaire est pris en charge sur les postes de travail distants et les sessions en mode imbriqué sur les systèmes clients Windows.

Lorsqu'un port COM redirigé est ouvert et utilisé sur un poste de travail distant ou une application publiée, 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 ou l'application publiée.

Configuration système requise pour la redirection de port série

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

Postes de travail virtuels

Vous devez installer Horizon Agent avec l'option de configuration de redirection de port série sélectionnée. Cette option d'installation n'est pas sélectionnée par défaut.

Les systèmes d'exploitation suivants sont pris en charge sur les postes de travail virtuels.

- Windows 10 64 bits
- Windows Server 2016
- Windows Server 2019

Il n'est pas nécessaire d'installer les pilotes de périphériques de port série sur le poste de travail virtuel.

Postes de travail publiés et applications publiées

Horizon Agent doit être installé sur les hôtes RDS avec l'option de configuration de redirection de port série sélectionnée. Cette option d'installation n'est pas sélectionnée par défaut.

Les systèmes d'exploitation suivants sont pris en charge pour les postes de travail publiés et les applications publiées.

- Windows Server 2016
- Windows Server 2019

Il n'est pas nécessaire d'installer les pilotes de périphériques de port série sur l'hôte RDS.

La redirection de port série est disponible avec des postes de travail complets et n'est pas prise en charge sur les applications publiées sur les hôtes RDS.

Ordinateur Horizon Client ou périphérique d'accès client

Pour Horizon Client pour Windows, la redirection de port série est prise en charge sur les systèmes clients Windows 10. Tous les pilotes de périphérique de port série nécessaires doivent être installés et le port série doit être opérationnel.

Protocoles d'affichage

- PCoIP
- VMware Blast

La redirection de port série 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), autoriser le port comme port permanent et mapper le port local sur le client vers un port COM différent sur le poste de travail distant en sélectionnant un port dans le menu déroulant **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, reportez-vous au document *Guide d'installation et de configuration 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 la section Paramètres du modèle d'administration ADMX pour la configuration de VMware View Agent.

- 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 sessions distantes. 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 distants.

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 sessions distantes et les systèmes clients.

Ces paramètres de stratégie affectent vos sessions distantes, et non les systèmes clients sur lesquels les périphériques de port COM physiques sont connectés. Pour configurer ces paramètres sur des postes de travail distants et des applications publiées, ajoutez le fichier de modèle d'administration (ADMX) de stratégie de groupe de 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 COM série (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.

Conditions préalables

- Vérifiez que l'option de configuration Redirection de port série est installée sur vos postes de travail virtuels ou vos hôtes RDS. Les paramètres de stratégie de groupe n'ont aucun effet si la redirection de port série n'est pas installée. Pour plus d'informations sur l'installation d'Horizon Agent, consultez le document *Configuration des postes de travail virtuels dans Horizon* ou *Configuration d'applications et de postes de travail publiés dans Horizon*.
- 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 GPO doivent être liés à l'UO qui contient vos postes de travail de machine virtuelle ou vos hôtes RDS. Reportez-vous à la section Exemple de stratégie de groupe 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.
- Familiarisez-vous avec les paramètres de stratégie de groupe de la redirection de port série. Reportez-vous à la section Paramètres du modèle d'administration ADMX pour la configuration de VMware View Agent.

Procédure

1. Téléchargez le fichier VMware Horizon 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, qui inclut GPO Bundle.

   Le fichier est nommé `VMware-Horizon-Extras-Bundle-`*`YYMM-x.x.x-yyyyyyyy`*`.zip`, où *YYMM* est la version marketing, *x.x.x* est la version interne et *yyyyyyyy* est le numéro de build. Tous les fichiers ADMX qui fournissent des paramètres de stratégie de groupe pour VMware Horizon sont disponibles dans ce fichier.
2. Décompressez le fichier `VMware-Horizon-Extras-Bundle-`*`YYMM-x.x.x-yyyyyyyy`*`.zip` et copiez les fichiers ADMX sur votre serveur Active Directory.
   a. Copiez le fichier `vdm_agent_serialport.admx`, ainsi que le dossier `en-US` dans le dossier `C:\Windows\PolicyDefinitions` sur votre serveur Active Directory.
   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 serveur Active Directory.

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

   Les paramètres se trouvent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Configuration de VMware View Agent > COM série**.

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

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 sessions distantes 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 un poste de travail de machine virtuelle individuel ou un hôte RDS.

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.

Conditions préalables

- Vérifiez que l'option de configuration Redirection de port série est installée sur vos postes de travail de machine virtuelle ou sur vos hôtes RDS. Les paramètres de stratégie de groupe n'ont aucun effet si la redirection de port série n'est pas installée. Pour plus d'informations sur l'installation d'Horizon Agent, consultez le document *Configuration des postes de travail virtuels dans Horizon* ou *Configuration d'applications et de postes de travail publiés dans Horizon*.
- Vérifiez que le fichier de modèle d'administration ADMX de redirection de port série est ajouté dans Active Directory.
- Familiarisez-vous avec l'élément **Serial2USBModeChangeEnabled** dans le paramètre de stratégie de groupe **PortSettings**. Reportez-vous à la section Paramètres du modèle d'administration ADMX pour la configuration de VMware View Agent.

Procédure

1 Sur le serveur Active Directory, ouvrez l'Éditeur d'objets de gestion de stratégie de groupe.

2 Accédez au dossier **Configuration ordinateur > Stratégies > Modèles d'administration > 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 gestion de stratégie de groupe.

Résultats

Les adaptateurs USB-série peuvent être redirigés vers des sessions distantes. Ils peuvent recevoir des données lorsque les utilisateurs démarrent leurs prochaines sessions.

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

VMware Horizon fournit la fonctionnalité Windows Media MMR pour les postes de travail virtuels exécutés sur des machines mono-utilisateur et pour les postes de travail publiés sur des hôtes RDS. MMR n'est pas disponible sur les applications publiées sur les hôtes 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 des clients 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 MMR entre les clients et les machines de poste de travail ne sont pas chiffrées.

Activation de la redirection multimédia dans Horizon

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 sur un réseau sécurisé.

Par défaut, la stratégie générale **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 sur la définition de stratégies générales, reportez-vous à la section Stratégies Horizon.

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

Pour prendre en charge la redirection multimédia (MMR) Windows Media, le déploiement de VMware Horizon doit répondre à certaines exigences matérielles et logicielles.

Poste de travail distant

- Cette fonctionnalité est prise en charge sur les postes de travail virtuels et les hôtes RDS pour les postes de travail publiés.
- Les systèmes d'exploitation invités suivants sont pris en charge.
  - Windows 10 64 bits. Le Lecteur Windows Media est pris en charge. Le lecteur par défaut TV & Movies n'est pas pris en charge.
  - Windows Server 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).

Logiciel Horizon Client

Horizon Client pour Windows.

Ordinateur Horizon Client ou périphérique d'accès client

Les clients doivent exécuter un système d'exploitation Windows 10 64 bits ou 32 bits.

Formats multimédias pris en charge

Les formats multimédias pris en charge par le lecteur Windows Media, par exemple : M4V ; MOV ; MP4 ; WMP ; MPEG-4 Part 2 ; WMV 7, 8 et 9 ; WMA ; AVI ; ACE ; MP3 ; WAV.

MP3 n'est pas pris en charge lors de l'utilisation de MMS et de RTSP.

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

Stratégies Horizon

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

Pare-feu principal

Si votre déploiement VMware Horizon inclut un pare-feu principal, vérifiez que celui-ci autorise le trafic vers le port 9427 sur vos postes de travail.

Utiliser la redirection multimédia (MMR) Windows Media en fonction de la latence réseau

Par défaut, la redirection multimédia (MMR) Windows Media s'adapte aux conditions du réseau sur les postes de travail mono-utilisateur qui s'exécutent sur des postes de travail publiés et Windows.

Si la latence réseau entre Horizon Client et le poste de travail distant est de 29 millisecondes ou moins, la vidéo est redirigée avec la redirection multimédia (MMR) Windows Media. 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.

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 et Horizon Agent avec la redirection du lecteur client, les fichiers et dossiers sont chiffrés avant d'être transmis sur le réseau.

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. Si VMware Blast est activé, les fichiers et dossiers sont chiffrés avant d'être transférés sur un canal virtuel.

Des connexions TCP sur le port 9427 sont requises pour prendre en charge la redirection du lecteur client. Si votre déploiement d'Horizon inclut un pare-feu principal entre vos serveurs de sécurité de la zone DMZ et votre réseau interne, le pare-feu principal doit autoriser le trafic vers le port 9427 de vos postes de travail distants. Si VMware Blast est activé, vous n'avez pas besoin d'ouvrir le port TCP 9427, car la redirection du lecteur client transfère les données via le canal virtuel.

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

Si vous désélectionnez l'option d'installation personnalisée **Redirection du lecteur client**, les fonctionnalités suivantes ne fonctionnent pas.

- Glisser-déposer des fichiers et des dossiers entre les clients et les postes de travail distants et les applications publiées.
- Glisser-déposer du contenu des fichiers (par exemple, les pièces jointes Outlook et les éléments de fichier ZIP) entre des postes de travail distants et des applications publiées.
- Copie de fichiers et de dossiers entre les clients et les postes de travail distants et les applications publiées.
- Ouverture de fichiers locaux avec des applications publiées à partir d'un poste de travail distant ne disposant pas de la fonctionnalité de redirection du lecteur client.

Lorsque la redirection du lecteur client est installée, vous pouvez glisser et déposer des fichiers et des dossiers, et les copier-coller entre des systèmes client et des postes de travail distants et des applications publiées. Reportez-vous aux sections Configuration de la fonctionnalité de glisser-déposer et Configuration de la fonctionnalité de redirection du Presse-papiers.

Utilisation de la redirection du lecteur client dans une implémentation d'Unified Access Gateway

Si votre mise en œuvre d'Horizon utilise un dispositif Unified Access Gateway, si les utilisateurs utilisent la redirection du lecteur client avec le protocole d'affichage PCoIP et si les machines Horizon Client et Horizon Agent se trouvent sur des réseaux différents, le serveur de tunnel UDP doit être activé pour le dispositif Unified Access Gateway.

Pour activer le serveur de tunnel UDP, dans l'interface utilisateur d'administration d'Unified Access Gateway, définissez le paramètre **Serveur de tunnel UDP activé** sur **Oui**.

Si vous n'activez pas le serveur de tunnel UDP, les utilisateurs ne peuvent pas utiliser la fonctionnalité de redirection du lecteur client avec le protocole d'affichage PCoIP. La redirection du lecteur client fonctionne avec le protocole d'affichage VMware Blast, que le serveur de tunnel UDP soit activé ou non.

Pour plus d'informations, consultez la documentation Unified Access Gateway.

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 pour vos postes de travail distants sur votre serveur Active Directory.

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

Conditions préalables

- 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.
- Ajoutez le fichier de modèle d'administration ADMX RDS `vmware_rdsh_server.admx` à un GPO lié à l'UO pour vos postes de travail virtuels, ou à l'hôte RDS pour vos postes de travail publiés. Pour obtenir des instructions d'installation, consultez le document Ajouter les fichiers de modèle d'administration ADMX à Active Directory.

Procédure

1. Sur votre serveur Active Directory, ouvrez l'Éditeur de gestion de stratégie de groupe et accédez à **Configuration ordinateur\Stratégies\Modèles d'administration\Composants Windows\Services Bureau à distance\Hôte de session Bureau à distance\Redirection de périphérique et de ressource**.
2. Ouvrez le paramètre de stratégie de groupe **Ne pas autoriser la redirection du lecteur**, sélectionnez **Activé**, puis cliquez sur **OK**.

Utiliser une stratégie de groupe pour configurer le comportement de la lettre de lecteur

Vous pouvez utiliser les paramètres de stratégie de groupe de l'agent pour configurer le comportement de la lettre de lecteur pour les lecteurs redirigés à l'aide de la fonctionnalité de redirection du lecteur client.

Lorsque le mappage de lettre de lecteur est configuré, les dossiers configurés dans la liste de partages de redirection du lecteur client ne sont pas redirigés. Cette limitation ne s'applique qu'à Horizon Client pour Windows. Pour plus d'informations sur le partage de fichiers et de lecteurs locaux dans Horizon Client pour Windows, reportez-vous au document *Guide d'installation et de configuration de VMware Horizon Client pour Windows*.

Conditions préalables

- 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.
- Ajoutez le fichier de modèle d'administration ADMX de Redirection du lecteur de VMware Horizon Client (`vdm_agent_cdr.admx`) à un GPO lié à l'UO pour vos postes de travail virtuels, ou à l'hôte RDS pour vos postes de travail publiés. Pour obtenir des instructions d'installation, consultez le document Ajouter les fichiers de modèle d'administration ADMX à Active Directory.

Procédure

1. Dans votre serveur Active Directory, ouvrez l'Éditeur de gestion de stratégie de groupe et accédez au dossier **Configuration ordinateur > Modèles d'administration > Configuration de VMware View Agent > Redirection du lecteur de VMware Horizon Client**.
2. Pour configurer l'affichage d'une lettre de lecteur pour les lecteurs redirigés, configurez le paramètre de stratégie de groupe **Afficher le périphérique redirigé avec la lettre de lecteur**.

   Ce paramètre est activé par défaut.
3. Pour spécifier le délai d'attente, en millisecondes, pour que l'Explorateur Windows initialise et affiche une lettre de lecteur pour les lecteurs redirigés, définissez le paramètre de stratégie de groupe **Délai d'expiration pour la configuration de la lettre de lecteur**.

   Si ce paramètre est désactivé ou n'est pas configuré, la valeur par défaut est 5 000 millisecondes.
4. Pour définir le mode de mappage des lettres de lecteur, configurez le paramètre de stratégie de groupe **Configurer le mode de mappage de lettre de lecteur**.

   Vous pouvez sélectionner l'une des options suivantes.

Option	Description
Mappage un à un	Mappe la lettre de lecteur sur la machine cliente à la même lettre de lecteur sur la machine agent. Par exemple, le lecteur X sur la machine cliente est mappé au lecteur X sur la machine agent.
Mappage défini	Mappe les lettres de lecteur sur la machine cliente à certaines lettres de lecteur sur la machine agent en fonction d'une table de mappage définie dans le paramètre de stratégie de groupe **Définir la table de mappage de lettre de lecteur**.

5 Pour mapper des lettres de lecteur, configurez le paramètre de stratégie de groupe **Définir la table de mappage de lettre de lecteur**.

   Vous cliquez sur **Afficher** pour définir une table de mappage des lettres de lecteur. La colonne **Nom de valeur** spécifie la lettre de lecteur sur la machine cliente et la colonne **Valeur** correspondante spécifie la lettre de lecteur à utiliser sur la machine agent.

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.

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.

Note 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 ou en lecture 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
```

Pour empêcher l'accès en lecture, définissez la valeur `permissions` sur toute chaîne qui commence par `w`.

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

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
```

Note 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`.

Configuration de la fonctionnalité de glisser-déposer

Les utilisateurs peuvent glisser-déposer des données entre des systèmes clients et des postes de travail distants et des applications publiées.

Configuration requise du client pour le glisser-déposer

- Seuls les systèmes clients Windows et Mac sont pris en charge. Les autres types de systèmes clients ne sont pas pris en charge.

- Pour glisser-déposer des fichiers et des dossiers, la fonctionnalité de redirection du lecteur client doit être activée dans Horizon Client pour Windows.

Pour plus d'informations sur l'utilisation de la fonctionnalité de glisser-déposer sur un client Windows, consultez le document *Guide d'installation et de configuration de VMware Horizon Client pour Windows*. Pour plus d'informations sur l'utilisation de la fonctionnalité de glisser-déposer sur un client Mac, consultez le document *Guide d'installation et de configuration de VMware Horizon Client pour Mac*.

Configuration requise de l'agent pour le glisser-déposer

Pour utiliser la fonctionnalité de glisser-déposer avec des fichiers, des dossiers et le contenu des fichiers, vous devez activer l'option **Redirection du lecteur client** lorsque vous installez Horizon Agent.

Utilisation des paramètres de stratégie de groupe pour configurer le glisser-déposer

Vous pouvez configurer la direction du glisser-déposer, ses formats autorisés et sa limite de taille en modifiant les paramètres de stratégie de groupe du fichier de modèle ADMX `vdm_agent_dnd.admx`. Les paramètres du glisser-déposer se trouvent dans le dossier **Configuration de VMware View Agent > Glisser-déposer** dans l'Éditeur de gestion de stratégie de groupe. Reportez-vous à la section Paramètres du modèle d'administration ADMX pour la configuration de VMware View Agent.

Utilisation d'Dynamic Environment Manager pour configurer le glisser-déposer

Avec Dynamic Environment Manager 9.8 ou version ultérieure, vous pouvez utiliser Stratégies de carte à puce pour configurer le comportement du glisser-déposer, et également désactiver l'intégralité de la fonctionnalité de glisser-déposer. Reportez-vous à la section Paramètres de stratégie de carte à puce Horizon.

Configuration de la fonctionnalité de redirection du Presse-papiers

Les utilisateurs peuvent copier et coller des données entre des systèmes clients et des postes de travail distants et des applications publiées.

Configuration requise du client pour la redirection du Presse-papiers

- Pour copier et coller des fichiers et des dossiers, seuls les systèmes clients Windows sont pris en charge. Les autres types de systèmes clients ne sont pas pris en charge.
- Pour copier et coller des fichiers et des dossiers, la fonctionnalité de redirection du lecteur client doit être activée dans Horizon Client pour Windows.

Pour plus d'informations sur la copie et le collage de fichiers et de dossiers sur un client Windows, reportez-vous au document *Guide d'installation et de configuration de VMware Horizon Client pour Windows*.

Configuration requise de l'agent pour la redirection du Presse-papiers

Pour utiliser la fonctionnalité de copier et coller avec des fichiers, des dossiers et le contenu des fichiers, vous devez activer l'option **Redirection du lecteur client** lorsque vous installez Horizon Agent.

Utilisation de paramètres de stratégie de groupe pour configurer la redirection du Presse-papiers

Vous pouvez configurer le sens du copier et coller, ses formats autorisés et sa limite de taille en modifiant les paramètres de stratégie de groupe du fichier de modèle ADMX `vdm_agent_clipboard.admx`. Les paramètres de redirection du Presse-papiers se trouvent dans le dossier **Configuration de VMware View Agent > Redirection du Presse-papiers** dans l'Éditeur de gestion de stratégie de groupe. Reportez-vous à la section Paramètres du modèle d'administration ADMX pour la configuration de VMware View Agent.

Utilisation de Dynamic Environment Manager pour configurer la redirection du Presse-papiers

Avec Dynamic Environment Manager 9.8 ou version ultérieure, vous pouvez utiliser Stratégies de carte à puce pour configurer le comportement du copier-coller, et également désactiver la fonctionnalité complète de redirection du Presse-papiers. Reportez-vous à la section Paramètres de stratégie de carte à puce Horizon.

Limitation des formats de Presse-papiers pour les opérations de copier-coller

Vous pouvez configurer des paramètres de stratégie de groupe pour contrôler quels formats de Presse-papiers sont autorisés lorsque des utilisateurs copient et collent des données au cours de sessions PCoIP et VMware Blast. Cette fonctionnalité est utile si vous devez limiter les opérations de copier-coller pour des raisons de sécurité.

Vous pouvez configurer des limites du format de Presse-papiers en fonction du sens de l'opération de copier-coller. Par exemple, vous pouvez configurer un ensemble de stratégies pour les données copiées depuis des systèmes clients vers des postes de travail distants et un autre ensemble de stratégies pour les données copiées depuis des postes de travail distants vers des systèmes clients.

Les paramètres de stratégie de groupe pour le filtrage des formats de redirection du Presse-papiers se trouvent dans le fichier de modèle ADMX `vdm_agent_clipboard.admx`. Vous pouvez modifier les paramètres dans **Configuration de VMware View Agent > Redirection du Presse-papiers > Configurer les formats de redirection du Presse-papiers** dans l'Éditeur de gestion de stratégie de groupe. Reportez-vous à la section Paramètres du modèle d'administration ADMX pour la configuration de VMware View Agent.

Exemples de filtrage de format de Presse-papiers

Les exemples suivants indiquent comment vous pouvez utiliser des paramètres de stratégie de groupe pour filtrer des formats de Presse-papiers lors d'opérations de copier-coller.

- Pour filtrer des images pour des applications non-Microsoft Office, telles que Wordpad, lorsque les utilisateurs copient des données depuis leurs systèmes clients vers des postes de travail distants, activez le paramètre de stratégie de groupe `Filter images out of the incoming clipboard data`.
- Pour filtrer des images pour des applications non-Microsoft Office et des applications Microsoft Office lorsque les utilisateurs copient des données depuis leurs systèmes clients vers des postes de travail distants, activez les paramètres de stratégie de groupe `Filter Microsoft Chart and Smart Art data out of the incoming clipboard data` et `Filter images out of the incoming clipboard data`. Le paramètre de stratégie de groupe `Filter Microsoft Chart and Smart Art data out of the incoming clipboard data` filtre les données de Graphique Microsoft Office et de graphique Smart Graphique, qui peuvent inclure des images.
- Pour filtrer uniquement des données de Graphique Microsoft Office et de graphique Smart Graphique lorsque les utilisateurs copient des données depuis leur système client vers des postes de travail distants, activez uniquement le paramètre de stratégie de groupe `Filter Microsoft Chart and Smart Art data out of the incoming clipboard data`.
- Pour filtrer le formatage de texte lié à Microsoft Word lorsque les utilisateurs copient des données depuis leurs systèmes clients vers des postes de travail distants et depuis des postes de travail distants vers leurs systèmes clients, activez les paramètres de stratégie de groupe entrants `Filter Microsoft Text Effects data out of the incoming clipboard data` et `Filter Rich Text Format data out of the incoming clipboard data`, ainsi que les paramètres de stratégie de groupe sortants `Filter Microsoft Text Effects data out of the outgoing clipboard data` et `Filter Rich Text Format data out of the outgoing clipboard data`.
- Pour filtrer des images pour Microsoft Word lorsque les utilisateurs copient des données depuis leurs systèmes clients vers des postes de travail distants et depuis des postes de travail distants vers leurs systèmes clients, activez le paramètre de stratégie de groupe entrant `Filter Rich Text Format data out of the incoming clipboard data` et le paramètre de stratégie de groupe sortant `Filter Rich Text Format data out of the outgoing clipboard data`. Les images dans Microsoft Word sont stockées au format RTF composé.

Configuration de la redirection du capteur d'orientation de périphérique simple

La fonctionnalité de redirection du capteur d'orientation de périphérique simple peut capter les changements d'orientation de l'écran d'un périphérique client et ainsi afficher une vue différente sur le périphérique.

La redirection du capteur d'orientation de périphérique simple s'intègre à votre application logicielle sur Horizon Agent. Si votre application utilise la classe SimpleOrientationSensor https://docs.microsoft.com/en-us/uwp/api/windows.devices.sensors.simpleorientationsensor, l'application peut afficher des contenus basés sur l'orientation de quadrant actuelle du périphérique client.

Configuration système requise pour la redirection du capteur d'orientation de périphérique simple

Les périphériques suivants sont pris en charge :

Tableau 2-3. Périphériques prenant en charge la redirection du capteur d'orientation de périphérique simple

Périphérique	Système d'exploitation du client	Serveurs de système d'exploitation Windows	Protocoles
Surface Book	Windows 10 1709	Windows 10 1709 (64 bits, 32 bits)	PCoIP, Blast
Surface Pro	Windows 10 1709	Windows 10 1709 (64 bits, 32 bits)	PCoIP, Blast

Pour les systèmes d'exploitation Horizon Agent, seul Windows 10 64 bits est pris en charge.

Installation du capteur d'orientation de périphérique simple

La redirection du capteur d'orientation de périphérique simple est une option d'installation personnalisée du programme d'installation d'Horizon Agent. Cette option n'est pas sélectionnée par défaut. Vous devez sélectionner Redirection du capteur d'orientation de périphérique simple pour l'installer. Pour les propriétés d'installation silencieuse de la redirection du capteur d'orientation de périphérique simple, reportez-vous au document *Configuration des postes de travail virtuels dans Horizon*.

Le Service de capteur sur le système local doit être activé pour que le pilote du capteur d'orientation de périphérique simple fonctionne. Le capteur d'orientation de périphérique simple doit être activé sur le périphérique client.

Journaux

Les journaux Horizon Client pour la redirection du capteur d'orientation de périphérique simple sont enregistrés dans le fichier journal rdeSvc `%TEMP%\vmware-%USERNAME%\vmware-rdeSvc-x-xxxxx.log`.

Les journaux Horizon Agent pour la redirection du capteur d'orientation de périphérique simple sont enregistrés dans le fichier journal rdeSvc `C:\Windows\Temp\vmware-SYSTEM*\vmware-rdeSvc-x-xxxx.log`.

Configuration de la redirection de stylet

Comme extension de la souris et de la fonctionnalité tactile, vous pouvez utiliser un stylet intégré sur une tablette Windows, telle que Microsoft Surface Book 2.

L'entrée de stylet inclut le pointage, la pression pour créer des épaisseurs de traits différentes, une inclinaison, une rotation et un effacement. Vous pouvez aposer une signature sur un PDF avec Microsoft Edge ou dessiner dans OneNote ou une autre application à encre dans les environnements LAN et WAN. La fonctionnalité de stylet est activée par défaut si votre système prend en charge le stylet.

Configuration système requise pour la redirection de stylet

Système	Configuration requise
Périphérique	Surface Book 2 et son stylet intégré
Système d'exploitation de machine cliente	Windows 10
Système d'exploitation de machine agent	Windows 10 1809 ou version ultérieure
Logiciel	Applications d'espace de travail Windows Ink Sketchpad, Screen Sketch Applications basées sur Windows Ink OneNote, Edge
Protocole d'affichage	Blast

Configuration d'un filigrane numérique

Vous pouvez créer un filigrane numérique unique comme solution pour l'authenticité, l'intégrité du contenu et la protection de votre propriété intellectuelle. Un filigrane affiche des informations traçables qui peuvent empêcher des personnes de voler des données potentielles.

Fonctionnalités et limitations du filigrane

Le filigrane peut être affiché sur les sessions distantes suivantes :

- Applications publiées et applications exécutées sur un pool de postes de travail
- Postes de travail virtuels et hôtes RDS
- Mode imbriqué
- Plusieurs écrans
- Session principale dans une session de collaboration

La fonctionnalité de filigrane présente les limites suivantes :

- Le protocole RDP n'est pas pris en charge.
- La redirection multimédia HTML5 n'est pas prise en charge.
- Les sessions enregistrées dans les applications Zoom ou WebEx n'incluent pas le filigrane.
- Les applications de capture d'écran et la touche Impr. écran n'incluent pas le filigrane.
- L'assistance à distance Windows n'affiche pas le filigrane.
- Si vous utilisez une ancienne version de client avec la dernière version de l'agent, le filigrane s'affiche côté agent, mais certaines fonctionnalités de redirection de poste de travail distant, telles que Skype et Microsoft Teams, ne fonctionnent pas.
- Si vous utilisez la dernière version du client avec une ancienne version de l'agent, le filigrane ne s'affiche pas.
- Une session de copie dans une session de collaboration ne peut pas afficher le filigrane.

Utilisation de paramètres de stratégie de groupe pour configurer le filigrane

Vous pouvez configurer des fonctions de filigrane, telles que le contenu du texte, la disposition, la rotation et l'opacité, en modifiant les paramètres de stratégie de groupe. Reportez-vous à la section Paramètres du modèle d'administration ADMX pour la configuration de VMware View Agent. Les modifications sont appliquées lors de la prochaine connexion.

Configuration de la collaboration de session

Avec la fonctionnalité de collaboration de session, les utilisateurs peuvent inviter d'autres utilisateurs à rejoindre une session de poste de travail distant Windows ou Linux existante.

Configuration système requise pour la collaboration de session

Pour prendre en charge la fonctionnalité de collaboration de session, votre déploiement de VMware Horizon doit satisfaire certaines exigences.

Composant	Configuration requise
Système client	Les propriétaires de session et les collaborateurs doivent disposer d'Horizon Client pour Windows, Mac ou Linux installé sur le système client, ou ils doivent utiliser HTML Access.
Postes de travail distants Windows	Horizon Agent doit être installé sur le poste de travail virtuel, ou sur l'hôte RDS pour les applications publiées. La fonctionnalité de collaboration de session doit être activée au niveau du pool de postes de travail ou de la batterie de serveurs. Pour plus d'informations sur l'activation de la fonctionnalité de collaboration de session pour des pools de postes de travail, consultez le document *Configuration des postes de travail virtuels dans Horizon*. Pour plus d'informations sur l'activation de la fonctionnalité de collaboration de session pour une batterie de serveurs, consultez le document *Configuration d'applications et de postes de travail publiés dans Horizon*.

Composant	Configuration requise
Postes de travail à distance Linux	Pour connaître les exigences des postes de travail distants Linux, consultez le document *Configuration des postes de travail Linux dans Horizon*.
Serveur de connexion	L'instance du Serveur de connexion utilise une licence d'entreprise.
Protocole d'affichage	VMware Blast

Pour plus d'informations sur l'utilisation de la fonctionnalité de collaboration de session, consultez la documentation d'Horizon Client.

Configuration des paramètres de stratégie de groupe de collaboration de session

Utilisez les paramètres de stratégie de groupe Collaboration dans le fichier de modèle d'administration ADMX Configuration de VMware View Agent (`vdm_agent.admx`) pour configurer la collaboration de session. Reportez-vous à la section Paramètres du modèle d'administration ADMX pour la configuration de VMware View Agent.

Limites de la fonctionnalités de collaboration de session

Les utilisateurs ne peuvent pas utiliser les fonctionnalités suivantes de poste de travail distant dans une session de collaboration.

- Redirection USB
- Audio/Vidéo en temps réel (RTAV)
- Redirection multimédia
- Redirection du lecteur client
- Redirection de carte à puce
- Redirection de Microsoft Lync
- Redirection de fichier et fonctionnalité Conserver dans le Dock
- Redirection du Presse-papiers

Les utilisateurs ne peuvent pas modifier la résolution du poste de travail distant dans une session de collaboration.

Les utilisateurs ne peuvent pas disposer de plusieurs sessions de collaboration sur la même machine cliente.

Configuration du pack de virtualisation VMware pour 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.

Fonctionnalités du pack de virtualisation VMware pour Skype Entreprise

Le pack de virtualisation VMware pour Skype Entreprise offre les fonctionnalités suivantes :

- Exécuter des appels et des conférences à l'aide d'un serveur proxy HTTPS
- Groupes de réponse
- Intégration de Microsoft Office : démarrer un appel Skype Entreprise à partir de Word, Outlook, SharePoint, etc.
- Quality-of-Experience permet aux clients Skype Entreprise de communiquer des mesures d'appel au serveur Skype Entreprise pour générer des rapports
- Gérer des appels au nom d'une autre personne en tant que délégué
- Identification de haut-parleur actif
- Appeler via X (domicile, travail, etc.)
- Contrôler le volume à partir du poste de travail distant
- Appels E911
- Parcage d'appel et prise d'appel
- Participer à des réunions externes de manière anonyme
- Rediriger les appels vers des périphériques mobiles
- Statistiques d'appels
- Authentification par carte à puce
- 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
- Sonneries personnalisées
- Intégration de la messagerie vocale
- Téléphones USB

- Prise en charge des applications publiées
- Correction d'erreur de transmission (FEC) avec l'audio et la vidéo
- Réunion en ligne Skype Entreprise
- Conférence maintenant
- Tableau blanc et partage d'écran

Configuration système requise du pack de virtualisation VMware pour Skype Entreprise

Le pack de virtualisation VMware pour Skype Entreprise prend en charge ces configurations.

Tableau 2-4. Configuration système requise du pack de virtualisation VMware pour Skype Entreprise

Système	Configuration requise
Microsoft Server	Lync Server 2013, Skype Entreprise Server 2015, Skype Entreprise Server 2019, Office 365 Pour les déploiements de serveurs sur site Skype Entreprise, le serveur Edge Skype Entreprise est nécessaire pour la communication avec les utilisateurs externes.
Client Microsoft	VMware recommande fortement d'utiliser les toutes dernières mises à jour du client Skype Entreprise. ■ Client Skype Entreprise 2015 : 15.0.4933.100 ou version ultérieure ■ 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 : 16.0.4561.1000 ou version ultérieure **Note** Les clients Skype Entreprise 2015 ou 2016 basique ne sont pas pris en charge.
Systèmes d'exploitation de postes de travail virtuels	Au minimum, 2 vCPU
Systèmes d'exploitation de machines clients	Configuration matérielle minimale : processeur double cœur 2,4 GHz Le Pack de virtualisation VMware pour Skype Entreprise prend en charge les mêmes systèmes d'exploitation Windows, Mac et Linux que ceux pris en charge par Horizon Client.
Déploiements	■ VDI (sur site et cloud) ■ Postes de travail persistants et non persistants ■ Déploiements RDS (applications et postes de travail publiés)
Protocoles d'affichage	VMware Blast et PCoIP
Ports réseau	Les mêmes ports que ceux utilisés par le client Skype Entreprise natif. Reportez-vous aux ports clients dans https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/ports-and-protocols. Reportez-vous également à la section https://kb.vmware.com/s/article/52558.

Tableau 2-4. Configuration système requise du pack de virtualisation VMware pour Skype Entreprise (suite)

Système	Configuration requise
Microphones et webcams	Les mêmes périphériques qui sont compatibles avec Skype Entreprise. Reportez-vous aux webcams répertoriées dans https://docs.microsoft.com/en-us/SkypeForBusiness/certification/devices-usb-devices.
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://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/network-requirements.
Clients Compatible Peer Skype Entreprise (non-VDI)	■ Client Skype Entreprise 2016 avec les dernières mises à jour ■ Client Skype Entreprise 2015 avec les dernières mises à jour ■ Client Lync 2013 avec les dernières mises à jour ■ Client Lync 2010 (appels audio uniquement)
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.

Installation du pack de virtualisation VMware pour Skype Entreprise

Pour utiliser Skype Entreprise, vous devez installer le pack de virtualisation VMware pour Skype Entreprise sur la machine cliente. Le logiciel Pack de virtualisation VMware pour Skype Entreprise est installé par défaut dans le cadre des programmes d'installation d'Horizon Client pour Windows, d'Horizon Client pour Linux et d'Horizon Client pour Mac. Pour plus d'informations sur l'installation d'Horizon Client, consultez le guide d'installation et de configuration de la version d'Horizon Client.

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

Le pack de virtualisation VMware pour Skype Entreprise contient les modules logiciels suivants :

- Horizon Media Proxy installé dans le poste de travail virtuel
- Horizon Media Provider installé sur le point de terminaison client

Pour vérifier si le pack de virtualisation VMware pour Skype Entreprise est installé sur la machine virtuelle, vérifiez ces clés de registre :

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Lync\VdiMediaProvider - GUID(REG_SZ)`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\Lync\VdiMediaProvider - GUID(REG_SZ)`

Modes de couplage d'une session

Lync.exe charge le plug-in Pack de virtualisation VMware pour Skype Entreprise lors du démarrage. Le plug-in recherche une session valide et écrit l'état du mode de couplage dans le registre. Pour interroger les modes de couplage, vérifiez que Lync.exe est en cours d'exécution dans la liste de processus, puis vérifiez `HKEY_CURRENT_USER\Software\VMware, Inc.\VMWMMAPlugin - PairingMode(REG_SZ)`.

Voici les modes de couplage valides :

- Optimisé : une session valide
- Recours : aucune session valide
- Optimisé (incompatibilité de version)
- Recours (incompatibilité de version)
- Connexion
- Déconnecté
- Non défini

Lorsque Lync.exe se ferme, le plug-in supprime la valeur du mode de couplage du registre.

Les utilisateurs n'ont pas besoin de privilèges d'administrateur pour vérifier le mode de couplage. Plusieurs utilisateurs connectés sur des postes de travail distants peuvent trouver le mode de couplage de chaque utilisateur dans la ruche HKCU.

Configuration des paramètres de stratégie de groupe du pack de virtualisation VMware pour Skype Entreprise

Vous pouvez configurer des paramètres de stratégie de groupe pour modifier la configuration par défaut. Reportez-vous à la section Paramètres de la stratégie Pack de virtualisation VMware pour Skype Entreprise.

Limites du pack de virtualisation VMware pour Skype Entreprise

Le pack de virtualisation VMware pour Skype Entreprise présente les limites suivantes :

- Les serveurs proxy Socks et http ne sont pas pris en charge.
- Le pack de virtualisation VMware pour Skype Entreprise ne prend pas en charge l'interopérabilité avec les unités de conférence à plusieurs participants tierces, telles que Pexip.
- La vue Galerie n'est pas prise en charge pour le moment.
- Vous ne pouvez pas enregistrer les appels.
- Le contournement de média n'est pas pris en charge. Pour plus d'informations, reportez-vous à https://kb.vmware.com/s/article/56977.

- Le scénario à deux tronçons, comme Horizon Agent imbriqué avec Horizon Client, n'est pas pris en charge.
- La solution optimisée VDI Skype Entreprise n'est pas compatible pour l'interopératibilité avec les clients Lync 2010.
- 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'utilisation de Microsoft Teams 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
- 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 voulez que la caméra se mette à jour de façon dynamique, utilisez le programme d'installation Skype Entreprise 2016 Démarrer en un clic version 16.0.11001.20097 ou ultérieure.
- 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.

Collecter des journaux pour dépanner Skype Entreprise

Pour dépanner Skype Entreprise, collectez des journaux à partir d'Horizon Agent et d'Horizon Client pour Windows.

Procédure

1. Pour collecter des journaux Horizon, notamment les journaux de Media Proxy, à partir d'Horizon Agent, connectez-vous à une machine virtuelle sur laquelle Horizon Agent est installé.
2. Ouvrez une fenêtre d'invite de commande, puis exécutez `C:\Program Files\VMware\VMware View\Agent\DCT\support.bat`.
3. Pour collecter des journaux Horizon, notamment les journaux de Media Provider, à partir d'Horizon Client, connectez-vous à une machine physique ou virtuelle sur laquelle Horizon Client est installé.
4. Ouvrez une fenêtre d'invite de commande, puis exécutez `support.bat`.
5. Entrez `C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT\support.bat`

Résultats

Un dossier nommé `vdm-sdct` contenant des fichiers journaux compressés s'affiche sur le poste de travail et inclut des répertoires contenant des journaux pour le pack de virtualisation VMware pour Skype Entreprise :

- Périphérique client : `%TEMP%\vmware-<nom_utilisateur>\VMWMediaProvider`
- Poste de travail virtuel :
  - `%TEMP%\vmware-<nom_utilisateur>\VMWMediaProviderProxy`
  - `%TEMP%\vmware-<nom_utilisateur>\VMWMediaProviderProxyLocal`
  - `%TEMP%\vmware-<nom_utilisateur>\MMAPlugin`

Le niveau de journalisation par défaut est de 7. Sa taille et ses vidages sur incident sont faibles. Vous pouvez augmenter le niveau de journalisation jusqu'à 8 pour maximiser la journalisation et bénéficier de vidages sur incident complets. Tous les paramètres sont de type DWORD :

- Client : HKEY_CURRENT_USER/SOFTWARE/VMware, Inc./VMWMediaProvider/DebugLogging/LoggingPriority = 8
- Agent : HKEY_CURRENT_USER/SOFTWARE/VMware, Inc./VMWMediaProviderProxy/DebugLogging/LoggingPriority = 8
- Agen : HKEY_CURRENT_USER/SOFTWARE/VMware, Inc./VMWMediaProviderProxyLocal/DebugLogging/LoggingPriority = 8

Configurer VMware Integrated Printing

VMware Integrated Printing permet aux utilisateurs d'imprimer depuis un poste de travail distant vers n'importe quelle imprimante locale ou en réseau disponible sur leur ordinateur client. VMware Integrated Printing fonctionne avec les périphériques clients Windows, Mac, Linux et mobiles. Il fonctionne également avec les clients basés sur un navigateur.

VMware Integrated Printing prend en charge la redirection d'imprimante cliente, l'impression basée sur l'emplacement et les paramètres d'impression persistants.

Redirection d'imprimante cliente

La redirection d'imprimante cliente permet aux utilisateurs d'imprimer depuis un poste de travail distant vers n'importe quelle imprimante locale ou en réseau disponible sur leur ordinateur client. Pour les imprimantes redirigées depuis un client Windows vers un poste de travail distant, VMware Integrated Printing prend en charge les types de pilotes d'imprimante suivants sur le poste de travail distant :

- Pilote d'imprimante natif (NPD). Sur le poste de travail distant, vous devez installer le même pilote d'imprimante que le pilote de l'imprimante cliente. NPD prend uniquement en charge les imprimantes v3.

- Pilote d'imprimante universel (UPD). Il n'est pas nécessaire d'installer de pilote sur le poste de travail distant.

Par défaut, si vous installez le pilote natif sur l'ordinateur Horizon Agent, NPD est utilisé. Dans le cas contraire, UPD est utilisé. Vous pouvez sélectionner le type de pilote d'imprimante à utiliser sur un poste de travail distant en configurant un paramètre de stratégie de groupe.

Pour déterminer le type de pilote d'imprimante utilisé dans un poste de travail distant, accédez à **Panneau de configuration > Matériel et audio > Périphériques et imprimantes**, cliquez avec le bouton droit sur l'imprimante virtuelle et sélectionnez **Propriétés de l'imprimante** dans le menu contextuel. Dans l'onglet **Général**, si le **Modèle** est le pilote VMware Universal EMF, UPD est utilisé. Dans le cas contraire, NPD est utilisé.

Impression basée sur l'emplacement

La fonctionnalité d'impression basée sur l'emplacement mappe les imprimantes physiquement proches des systèmes clients vers des postes de travail distants. Pour plus d'informations, reportez-vous à la section Configuration de l'impression basée sur l'emplacement.

Redirection en mode imbriqué

Dans une installation en mode imbriqué, vous pouvez rediriger les imprimantes locales installées sur les première et deuxième couches vers le poste de travail distant ou l'application publiée sur la troisième couche. En fonction du paramètre de stratégie de groupe et selon que les pilotes d'impression natifs sont installés ou non, les imprimantes redirigées sur la troisième couche peuvent utiliser UPD ou NPD.

Noms d'imprimantes statiques

Les imprimantes redirigées conservent leur nom entre les sessions avec le suffixe `vdi`, afin que les utilisateurs n'aient pas besoin de remapper l'imprimante manuellement lorsqu'ils se connectent à une autre session. Le nom de l'imprimante statique est uniquement pris en charge sur les machines mono-utilisateur et n'est pas pris en charge sous Windows Server avec le mode VDI.

Paramètres d'impression persistants

Les paramètres d'imprimante des imprimantes clientes redirigées, notamment le NPD et le UPD, ou des imprimantes basées sur l'emplacement sont conservés lorsqu'un utilisateur ferme une session ou se déconnecte du poste de travail distant. Par exemple, un utilisateur peut choisir d'utiliser une imprimante cliente redirigée ou une imprimante basée sur l'emplacement en mode noir et blanc. Lorsque l'utilisateur se déconnecte et se reconnecte au poste de travail distant, le paramètre d'impression précédent est persistant.

Le paramètre d'impression persistant peut être désactivé en configurant un paramètre de stratégie de groupe.

Paramètres d'impression du pilote d'imprimante universel

Vmware Integrated Printing fournit les paramètres d'impression suivants pour les imprimantes UPD redirigées à partir de clients Windows.

- **Orientation** : sélectionnez l'orientation portrait ou paysage du papier. Les options de finition par agrafage et poinçonnage dépendent de l'orientation du papier.
- **Imprimer des deux côtés** : sélectionnez l'impression recto verso pour les imprimantes compatibles.
- **Plusieurs pages par feuille** : pour imprimer plusieurs pages de document sur une page physique, sélectionnez le nombre de pages à imprimer sur une page physique, puis sélectionnez la disposition des pages.
- **Alimentation papier** : sélectionnez le nom du bac à papier d'entrée.
- **Format du papier** : sélectionnez le format du papier :
  - Formats de papier standard : formats de papier généralement pris en charge par la plupart des imprimantes, telles que A4, lettre et légal.
  - Formats de papier définis par le fournisseur (également appelés formats de papier non standard) : formats de papier définis par un fournisseur d'imprimantes.
  - Formats de papier définis par l'utilisateur (également appelés formats de papier personnalisés) : formats de papier définis par les administrateurs système.
- **DPI** : spécifiez la résolution de l'imprimante.
- **Couleur** : indiquez si une imprimante couleur doit imprimer en couleur ou en monochrome.
- **Impression et aperçu** : sélectionnez **Imprimer directement** ou **Aperçu avant impression** :
  - Avec **Imprimer directement**, vous pouvez sélectionner **Avec la boîte de dialogue des préférences d'ouverture** qui ouvre les préférences de l'imprimante cliente avant l'impression, pour que vous puissiez changer les paramètres d'impression.
  - Avec **Aperçu avant impression**, l'option **Avec la boîte de dialogue des préférences d'ouverture** n'est pas disponible.
- **Nombre de copies** : spécifiez le nombre de copies.
- **Imprimer en tant qu'image** : imprimer chaque page en tant qu'image.
- **Compression** : spécifiez comment les images dans le document imprimé doivent être compressées.
- **Finition** : spécifiez les options d'agrafage et de poinçonnage pour les imprimantes spécifiées.

Par défaut, vous ne pouvez pas définir le type de support sur une imprimante UPD. Pour modifier le type de support sur une imprimante UPD, activez le paramètre de stratégie de groupe **Désactiver la persistance de propriété de l'imprimante** et remplacez le paramètre de type de support de l'imprimante cliente par le paramètre souhaité. Pour plus d'informations sur le paramètre de stratégie de groupe **Désactiver la persistance de propriété de l'imprimante**, reportez-vous à Paramètres de stratégie de VMware Integrated Printing.

Options de finition de pilote d'imprimante natif

Ces imprimantes natives redirigées prennent en charge une option de finition lorsque le matériel spécifique est connecté aux imprimantes.

Imprimante	Option de finition	Conditions requises sur l'imprimante locale côté client
FX ApeosPort-IV C5575 PCL 6	agrafage, livret	Vérifiez que le périphérique matériel de finition est connecté à l'imprimante. Mettez à jour les informations de l'imprimante avec la communication bidirectionnelle dans les propriétés de l'imprimante. Activez les options de finition dans les préférences de l'imprimante.
Ricoh MP C5003	agrafage, poinçonnage	Ajoutez manuellement le finisseur en fonction de son paramètre de périphérique pour activer l'option de finition, qui est ainsi disponible dans les préférences de l'imprimante.

Installation de la redirection de VMware Integrated Printing

VMware Integrated Printing est une option d'installation personnalisée du programme d'installation d'Horizon Agent. Cette option n'est pas sélectionnée par défaut. Vous devez sélectionner VMware Integrated Printing pour l'installer.

Pour installer cette fonctionnalité sur une machine virtuelle, reportez-vous au document *Configuration des postes de travail virtuels dans Horizon*. Pour installer cette fonctionnalité sur un hôte RDS, reportez-vous au document *Configuration d'applications et de postes de travail publiés dans Horizon*.

VMware Integrated Printing utilise le port TCP 9427.

Configuration des paramètres de stratégie de groupe de VMware Integrated Printing

Pour personnaliser VMware Integrated Printing, y compris la désactivation de l'impression basée sur l'emplacement, la désactivation de la persistance du paramètre d'impression, la sélection du pilote d'imprimante pour une imprimante cliente redirigée et la désactivation de l'impression sur des clients autres que des postes de travail, utilisez les paramètres de stratégie de groupe dans le fichier de modèle ADMX VMware Integrated Printing (`printerRedirection.admx`). Reportez-vous à la section Paramètres de stratégie de VMware Integrated Printing.

Configuration de l'impression basée sur l'emplacement

La fonctionnalité d'impression basée sur l'emplacement mappe les imprimantes physiquement proches des systèmes clients vers des postes de travail distants. L'impression basée sur l'emplacement permet aux services informatiques de mapper des postes de travail distants à 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.

L'impression basée sur l'emplacement fonctionne avec les périphériques clients Windows, Mac, Linux et mobiles. Il fonctionne également avec les clients basés sur un navigateur. L'impression basée sur l'emplacement est prise en charge sur les applications et postes de travail distants suivants.

- Les postes de travail distants qui sont déployés sur des machines mono-utilisateur, notamment les machines de poste de travail Windows et Windows Server.
- Les postes de travail publiés et applications publiées qui sont déployés sur des hôtes RDS, où les hôtes RDS sont des machines virtuelles ou des machines physiques.

Pour utiliser l'impression basée sur l'emplacement, vous devez installer l'option de configuration VMware Integrated Printing dans Horizon Agent, installer les pilotes d'imprimante corrects sur le poste de travail distant et définir des règles de traduction pour chaque imprimante basée sur l'emplacement. Les règles de traduction déterminent si l'imprimante est mappée au poste de travail distant pour un système client particulier. Lorsqu'un utilisateur se connecte à un poste de travail distant, VMware Horizon compare le système client avec les règles de traduction. Si le système client satisfait toutes les règles de traduction, VMware Horizon mappe l'imprimante au poste de travail distant au cours de la session de l'utilisateur.

Vous pouvez désactiver l'impression basée sur l'emplacement en activant le paramètre de stratégie de groupe **Désactiver l'impression basée sur l'emplacement**. Pour plus d'informations, reportez-vous à la section Paramètres de stratégie de VMware Integrated Printing.

Installer l'interface utilisateur de l'impression basée sur l'emplacement

Avant de pouvoir configurer l'impression basée sur l'emplacement, vous devez installer l'interface utilisateur de cette dernière. L'interface utilisateur d'impression basée sur l'emplacement est distribuée en tant que bibliothèque de liens dynamiques (DLL) nommée `vmware-print-lbpsettingui.dll`. Vous pouvez installer le fichier DLL en tant que composant logiciel enfichable MMC en exécutant `InstallUtil.exe`.

Conditions préalables

Parfois, le système d'exploitation traite le fichier `vmware-print-lbpsettingui.dll` comme un fichier binaire non sécurisé et bloque le chargement de la DLL. Pour débloquer le fichier, cliquez avec le bouton droit sur le nom de fichier, sélectionnez **Propriétés**, cliquez sur l'onglet **Général**, puis cliquez sur **Débloquer** dans la section Sécurité.

Procédure

1 Téléchargez le fichier ZIP GPO Bundle de VMware Horizon sur le site de téléchargement VMware sur https://my.vmware.com/web/vmware/downloads sur votre serveur Active Directory.

   Sous Poste de travail et informatique pour l'utilisateur, sélectionnez le téléchargement de VMware Horizon, qui inclut GPO Bundle. Le fichier est nommé `VMware-Horizon-Extras-Bundle-YYMM-x.x.x-yyyyyyyy.zip`, où *YYMM* est la version marketing, *x.x.x* et la version interne et *yyyyyyyy* est le numéro de build.

2 Extrayez le fichier `vmware-print-lbpsettingui.dll` du fichier ZIP.

3 Ouvrez une invite de commande avec des privilèges d'administrateur.

   Par exemple, cliquez sur **Démarrer**, entrez **command**, cliquez avec le bouton droit **Invite de commande** et sélectionnez **Exécutez en tant qu'administrateur**.

4 À l'invite de commande, exécutez `InstallUtil.exe` pour installer le fichier `vmware-print-lbpsettingui.dll`.

   Par exemple :

   ```
   installutil.exe C:\vmware-print-lbpsettingui.dll
   ```

   `InstallUtil.exe` se trouve généralement dans le répertoire `Microsoft.NET`, par exemple, `C:\Windows\Microsoft.NET\Framework64\v4.0.30319`.

5 Pour vérifier que l'interface utilisateur de l'impression basée sur l'emplacement est installée, ouvrez l'Éditeur de gestion de stratégie de groupe et accédez à **Configuration ordinateur > Paramètres du logiciel**.

   Le paramètre de stratégie de groupe **Interface utilisateur du paramètre LBP** s'affiche sous **Paramètres du logiciel** dans le volet de navigation de gauche.

Étape suivante

Configurez le paramètre de stratégie de groupe **Interface utilisateur du paramètre LBP**. Reportez-vous à la section Configurer l'impression basée sur l'emplacement.

Configurer l'impression basée sur l'emplacement

Pour configurer l'impression basée sur l'emplacement, vous devez configurer le paramètre de stratégie de groupe de l'**Interface utilisateur de configuration de LBP**. Le paramètre de stratégie de groupe est un tableau de traduction de noms qui mappe des imprimantes à des postes de travail distants. 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 distant pour un système client particulier.

Lorsqu'un utilisateur se connecte à un poste de travail distant, VMware Horizon 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, VMware Horizon mappe l'imprimante au poste de travail distant 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. Un groupe comporte plusieurs utilisateurs, et un utilisateur peut appartenir à plusieurs groupes. Selon le type de groupe, vous pouvez imbriquer des groupes et accorder l'accès aux ressources.

Vous pouvez spécifier une règle de traduction, ou une combinaison de plusieurs règles de traduction, pour une imprimante spécifique.

Si vous avez défini des règles de traduction dans une version précédente de VMware Horizon et que ces règles se trouvent dans un fichier XML, vous pouvez importer le fichier XML dans le paramètre de stratégie de groupe de **l'interface utilisateur de configuration de LBP**.

Les informations utilisées pour mapper l'imprimante au poste de travail distant sont stockées dans l'entrée de registre `LBPSettingData` sur le poste de travail distant sous `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\VMware, Inc.\VMware VDM\PrintRedir`.

Conditions préalables

- 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.
- Installez le fichier `vmware-print-lbpsettingui.dll` sur votre serveur Active Directory. Reportez-vous à la section Installer l'interface utilisateur de l'impression basée sur l'emplacement.
- Familiarisez-vous avec la syntaxe du tableau de traduction des noms. Reportez-vous à la section Syntaxe du tableau de traduction de l'impression basée sur l'emplacement.
- 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 distants. Reportez-vous à Créer des GPO pour les stratégies de groupe Horizon pour obtenir un exemple de création de GPO pour des stratégies de groupe Horizon.
- Comme les travaux d'impression sont envoyés directement du poste de travail distant vers l'imprimante, vérifiez que les pilotes d'imprimante requis sont installés sur vos postes de travail distants.

Procédure

1 Sur votre serveur Active Directory, ouvrez l'éditeur de gestion de stratégie de groupe.

2 Développez l'option **Configuration de l'ordinateur** , ouvrez le dossier **Paramètres du logiciel**, puis sélectionnez **Interface utilisateur de configuration de LBP**.

   Les stratégies spécifiques à l'ordinateur s'appliquent à tous les postes de travail distants, quelle que soit la personne qui se connecte au poste de travail distant.

3 Dans le volet Stratégie, double-cliquez sur **Configurer la connexion automatique**.

4 Sélectionnez **Activé** pour activer le paramètre de stratégie de groupe.

   Note Si vous cliquez sur **Désactivé**, cela supprime toutes les entrées du tableau. Par précaution, enregistrez votre configuration pour pouvoir l'importer ultérieurement.

5 Ajoutez les imprimantes que vous souhaitez mapper à des postes de travail distants et définissez leurs règles de traduction associées.

   Si vous disposez d'une configuration existante dans un fichier XML, vous pouvez cliquer sur le bouton **Importer la configuration à partir d'un fichier de données existant** pour importer le fichier XML.

6 Cliquez sur **OK** pour enregistrer les modifications.

Syntaxe du tableau de traduction de l'impression basée sur l'emplacement

L'interface utilisateur de configuration de LBP est un tableau de traduction de noms qui identifie des imprimantes et définit des règles de traduction associées. L'impression basée sur l'emplacement mappe les imprimantes locales aux postes de travail distants.

Tableau 2-5. Colonnes et valeurs contenues dans le tableau de traduction

Colonne	Description
`Default`	Indique si l'imprimante est l'imprimante par défaut. Par défaut, cette valeur n'est pas sélectionnée.
`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 (valeur par défaut) pour inclure toutes les adresses IP. **Important** Dans un environnement en mode mixte IPv6, ajoutez deux plages d'adresses IP pour une imprimante (une plage pour les adresses IPv4 et une autre pour les adresses IPv6) afin de vous assurer que cette dernière s'affiche dans les sessions distantes, quel que soit le protocole utilisé par Horizon Client pour se connecter.
`Client Name`	Règle de traduction spécifiant un nom d'ordinateur. La longueur maximale est de 1 024 caractères. 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* Exemples pour un utilisateur : **`\\mydomain\Mary`** et **`Mary`** Exemple pour un groupe : **`\\localdomain\Sales`** Un utilisateur peut appartenir à de nombreux groupes et ceux-ci comportent plusieurs utilisateurs. L'impression basée sur l'emplacement prend en charge les types de groupes que Microsoft prend en charge dans le domaine. 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.

Tableau 2-5. Colonnes et valeurs contenues dans le tableau de traduction (suite)

Colonne	Description
`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.
`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 distant vers l'imprimante, le pilote d'imprimante doit être installé sur le poste de travail distant.
`IP Port`	Pour les imprimantes en réseau, adresses IP de l'imprimante avec le préfixe **`IP_`**. 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, pour IPv4 : **`IP_10.114.24.1:9104`** Par exemple, pour IPv6 : **`IP_1:1:1:1::1:PORT_9100`**

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.

Note Les stratégies d'impression basée sur l'emplacement qui utilisent l'adresse MAC ou le nom de client ne sont pas prises en charge si vous utilisez HTML Access pour vous connecter à des postes de travail distants.

Le tableau suivant montre un exemple de deux lignes de table de traduction.

Tableau 2-6. 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	Port IP	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.

Configuration des paramètres de Registre Windows pour la gestion des événements du curseur

Pour optimiser la gestion des événements du curseur, configurez les paramètres de Registre Windows situés dans `\\HKLM\SOFTWARE\VMware Inc.\VMware Blast\Config` sur le système agent.

Ces paramètres de Registre Windows sur la machine agent permettent de configurer la fusion des événements de déplacement de la souris autorisés et l'utilisation du canal à faible latence.

Paramètre	Type	Description
MouseMoveEventsCoalescingEnabled	REG_SZ	Détermine si la fusion des événements de déplacement de la souris est activée ou non. Les valeurs sont 1 ou 0. La valeur par défaut est 1 (true).
ReflectCursorPositionEnabled	REG_SZ	Détermine si le canal à faible latence est utilisé pour les mises à jour du curseur. Les valeurs sont 1 ou 0. La valeur par défaut est 1 (true).

Vous pouvez également configurer la gestion des événements du curseur sur la machine cliente. Pour activer la fonctionnalité, les paramètres sur le client et l'agent doivent correspondre. Pour plus d'informations sur les paramètres côté client, reportez-vous aux sections *Guide d'installation et de configuration de VMware Horizon Client pour Windows*, *Guide d'installation et de configuration de VMware Horizon Client pour Mac* et *Guide d'installation et de configuration de VMware Horizon Client pour Linux*.

Vous pouvez également configurer un paramètre de stratégie de groupe pour la déformation du curseur. Reportez-vous à la section Paramètres de stratégie VMware Blast.

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 un poste de travail distant ou une application publiée. Vous pouvez rediriger des URL que les utilisateurs tapent dans la barre d'adresses du navigateur ou dans une application.

Ce chapitre contient les rubriques suivantes :

Comprendre la redirection de contenu URL

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

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

Vous pouvez configurer la fonctionnalité de redirection de contenu URL pour des raisons de sécurité. Par exemple, si un utilisateur final clique sur un lien dans son navigateur client qui pointe vers une URL en dehors du réseau de votre entreprise, ce lien peut être ouvert de façon plus sécurisée dans une application publiée. Avec la redirection client vers agent, vous pouvez désigner une application publiée spécifique pour ouvrir le lien à partir du client.

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.

Pour obtenir la liste des navigateurs qui prennent en charge la redirection agent vers client, consultez la section « Navigateurs Web pour les agents Windows » sous Configuration système requise pour la redirection de contenu URL.

Redirection client vers agent

Avec la redirection client vers agent, Horizon Client ouvre un poste de travail distant ou une application publiée 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 publiée, le lien est ouvert par l'application publiée spécifiée. L'utilisateur final doit être autorisé à accéder au pool de postes de travail ou d'applications.

Pour obtenir la liste des navigateurs qui prennent en charge la redirection client vers agent, consultez les sections des clients spécifiques à la plate-forme sous Configuration système requise pour la redirection de contenu URL.

Vous pouvez rediriger certaines URL depuis un poste de travail distant ou une application publiée vers un client et rediriger d'autres URL depuis un client vers un poste de travail distant ou une application publiée. Vous pouvez rediriger n'importe quel nombre de protocoles, notamment HTTP, HTTPS, mailto et callto. Le protocole callto n'est pas pris en charge pour la redirection avec le navigateur Chrome. Vous pouvez également spécifier les applications prises en charge pour le protocole dans l'URL.

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*.

Configuration système 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.

Navigateurs Web pour les agents Windows

Les navigateurs suivants sont pris en charge sur les agents Windows.

- Internet Explorer 11
- Chrome 60.0.3112.101 et versions ultérieures (build officiel), 64 bits ou 32 bits
- Microsoft Edge (Chromium) 80.0.361.48 et versions ultérieures (build officiel), 64 bits ou 32 bits

Navigateurs Web pour les clients Windows

Les navigateurs suivants sont pris en charge sur les clients Windows.

- Internet Explorer 11
- Chrome 60.0.3112.101 et versions ultérieures (build officiel), 64 bits ou 32 bits
- Microsoft Edge (Chromium) 80.0.361.48 et versions ultérieures (build officiel), 64 bits ou 32 bits

Navigateurs Web pour les clients Mac

Les navigateurs suivants sont pris en charge sur les clients Mac.

- Chrome 60.0.3112.101 et versions ultérieures (build officiel), 64 bits ou 32 bits
- Microsoft Edge (Chromium) 87.0.664.60 et versions ultérieures (build officielle)

Navigateurs Web pour les clients Linux

Les navigateurs suivants sont pris en charge sur les clients Linux.

- Firefox 70.0 et versions ultérieures
- Chrome 87.0.4280.88 et versions ultérieures (build officielle), 64 bits

Extensions de navigateur Web

Vous devez installer l'extension de redirection de contenu URL VMware Horizon pour utiliser la plupart des navigateurs pris en charge avec la redirection de contenu URL. Vous n'avez pas besoin d'installer une extension pour Internet Explorer. Pour obtenir des

instructions d'installation, consultez le document Installation d'extensions de navigateur pour la redirection de contenu URL.

Note Vous devez installer les extensions du navigateur avant d'activer la redirection de contenu URL dans Horizon Agent ou Horizon Client. Si vous ne le faites pas, le fichier JSON ne se charge pas et la redirection de contenu URL ne fonctionne pas.

Si vous modifiez une règle de redirection de contenu URL, l'extension peut se souvenir du cache de données précédent. Vous devez actualiser l'extension, soit en redémarrant le navigateur, soit en fermant et en rouvrant l'extension, afin que la nouvelle règle puisse être effective immédiatement.

Clients Windows

Installer Horizon Client pour Windows.

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. Reportez-vous à la section Installation d'Horizon Client pour Windows avec la fonctionnalité de redirection de contenu URL activée. 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

Installez Horizon Client pour Mac. Horizon Client pour Mac ajoute la prise en charge de la redirection client vers agent par défaut. Aucune autre étape d'installation n'est requise.

clients Linux

Installer Horizon Client pour Linux. Horizon Client pour Linux ajoute la prise en charge de la redirection client vers agent par défaut. Aucune autre étape d'installation n'est requise.

Postes de travail virtuels et hôtes RDS

Pour utiliser la redirection agent vers client, installez Horizon Agent avec la fonctionnalité de redirection de contenu URL activée. Reportez-vous à la section Installation de Horizon Agent avec la fonctionnalité de redirection de contenu URL activée.

Protocoles d'affichage

- VMware Blast
- PCoIP

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, effectuez les tâches de configuration suivantes dans l'ordre indiqué.

1 Installez les extensions des navigateurs que vous prévoyez d'utiliser sur la machine agent Windows.

Navigateur	Instructions
Chrome	Installer et activer l'extension Aide à la redirection de contenu URL pour Chrome sous Windows
Microsoft Edge (Chromium)	Installer l'extension Aide à la redirection de contenu URL pour Microsoft Edge (Chromium) sous Windows

Note Pour Internet Explorer, le plug-in de filtrage d'URL de VMware Horizon View est installé par défaut avec Horizon Agent. Reportez-vous à la section Installation d'Horizon Agent avec la fonctionnalité de redirection de contenu URL activée.

2 Activez la fonctionnalité de redirection de contenu URL dans Horizon Agent. Reportez-vous à la section Installation de Horizon Agent avec la fonctionnalité de redirection de contenu URL activée.

3 Appliquez les paramètres de stratégie de groupe de redirection de contenu URL à vos postes de travail distants et vos applications publiées. Reportez-vous à la section Ajouter le modèle d'administration ADMX de redirection de contenu URL à un GPO.

4 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.

Installation de Horizon Agent avec la fonctionnalité de redirection de contenu URL activée

Pour utiliser la redirection de contenu URL depuis un poste de travail distant ou une application publiée vers un client (redirection agent vers client), 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-Horizon-Agent-x86-YYMM-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`. Si vous utilisez la fonctionnalité de redirection de contenu URL avec Internet Explorer, vérifiez également que le module complémentaire Internet Explorer Plug-in de filtrage URL VMware Horizon View est activé.

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.admx`, contient des paramètres vous permettant de contrôler si un lien URL est ouvert sur le client (redirection agent vers client) ou dans un poste de travail distant ou une application publiée (redirection client vers agent).

Pour appliquer les paramètres de stratégie de groupe de redirection de contenu URL à vos postes de travail distants et vos applications publiées, 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 un poste de travail distant ou une application publiée, 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.

Conditions préalables

- Vérifiez que la fonctionnalité de redirection de contenu URL est incluse lorsque vous installez Horizon Agent. Reportez-vous à la section Installation de Horizon Agent avec la fonctionnalité de redirection de contenu URL activée.
- 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 VMware Horizon 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, qui inclut GPO Bundle.

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

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

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

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

   Par exemple, pour l'anglais, copiez le fichier `urlRedirection.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**.

Étape suivante

Configurez les paramètres de stratégie de groupe. Reportez-vous à la section Paramètres de stratégie de groupe de redirection de contenu URL.

Paramètres de stratégie de groupe de redirection de contenu URL

Le fichier de modèle de redirection de contenu URL (`urlRedirection.admx`) 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 contient des stratégies Configuration ordinateur et Configuration utilisateur. 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	Ordinateur	Utilisateur	Propriétés
`IE Policy: Automatically enable URL Redirection plugin`	X		Détermine si les plug-ins Internet Explorer qui viennent d'être installés sont automatiquement activés. Ce paramètre n'est pas configuré par défaut.
`IE Policy: Prevent users from changing URL Redirection plugin loading behavior`	X		Détermine si les utilisateurs peuvent désactiver la fonctionnalité de redirection de contenu URL. Ce paramètre n'est pas configuré par défaut.
`Url Redirection Enabled`	X		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.

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

Paramètre	Ordinateur	Utilisateur	Propriétés
`Url Redirection IP Rules Enabled`	X		Lorsque ce paramètre est activé, vous pouvez entrer une adresse IP ou une plage d'adresses IP spécifique dans **Règles de client** ou **Règles d'agent**. Pour plus d'informations, reportez-vous à la section Filtrage d'adresse IP et de plage d'adresses IP. Ce paramètre est désactivé par défaut. **Note** Cette fonctionnalité n'est prise en charge qu'avec Internet Explorer et IPv4.
`Url Redirection Protocol '...'`	X		Utilisez ce paramètre pour n'importe quel protocole autre que HTTP et HTTPS, tel qu'email ou callto. Les options sont les mêmes que pour `Url Redirection Protocol 'http'` et `Url Redirection Protocol 'https'`. 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. Ce paramètre n'est pas configuré par défaut.
`Url Redirection whitelist configuration`	X		Spécifie les applications prises en charge par la fonctionnalité de redirection de contenu URL sous Windows pour le protocole dans l'URL. Les applications suivantes sont prises en charge par défaut : ■ Internet Explorer (`iexplore. exe`) ■ Chrome (`chrome.exe`) ■ Firefox (`firefox.exe`) ■ Microsoft Outlook (`outlook.exe`) ■ Skype for Business (`lync.exe`) ■ Skype (`skype.exe`) ■ Windows Media Player (`vmplayer.exe`) Vous pouvez modifier la liste des applications prises en charge sous Windows en configurant ce paramètre de stratégie de groupe. Par exemple, si vous entrez les fichiers exécutables suivants dans la zone de texte **Liste blanche**, la redirection de contenu URL prend en charge uniquement Chrome, Microsoft Outlook et Skype : ■ `chrome.exe` ■ `outlook.exe` ■ `skype.exe` Ce paramètre n'est pas configuré par défaut.

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

Paramètre	Ordinateur	Utilisateur	Propriétés
`Url Redirection Protocol 'http'`	X		Pour toutes les URL qui utilisent le protocole HTTP, spécifie les URL qui doivent être redirigées. Ce paramètre dispose des options suivantes : ■ **Nom d'hôte de broker** : adresse IP ou nom complet de l'hôte du Serveur de connexion à utiliser lors de la redirection d'URL vers une application ou un poste de travail distant. ■ **Élément distant** : nom d'affichage du pool d'applications ou de postes de travail distants qui peut traiter les URL spécifiées dans **Règles d'agent**. ■ **Règles de client** : URL devant être redirigées vers le client. Par exemple, si vous définissez **Règles de client** sur **`.*mycompany.com`**, toutes les URL contenant la chaîne `mycompany.com` sont redirigées vers le client basé sur Windows et sont ouvertes dans le navigateur par défaut sur le client. **Note** La plage d'URL redirigées peut varier en fonction de la syntaxe de règle que vous utilisez. ■ Syntaxe de la règle **`.*mycompany.com`** prend en charge la redirection de toutes les URL qui contiennent la chaîne `mycompany.com`, y compris `http://mycompany.com`. ■ Syntaxe de la règle **`.*.mycompany.com`** prend en charge la redirection de toutes les URL qui contiennent la chaîne `.mycompany.com`. Il ne prend pas en charge la redirection de l'URL racine. Par exemple, `http://mycompany.com` n'est pas redirigé. ■ **Règles d'agent** : URL devant être redirigées vers l'application ou le poste de travail distant spécifié dans **Élément distant**. Par exemple, si vous définissez **Règles d'agent** sur **`.*mycompany.com`**, toutes les URL qui contiennent la chaîne `mycompany.com` sont redirigées vers l'application ou le poste de travail distant. **Note** La plage d'URL redirigées peut varier en fonction de la syntaxe de règle que vous utilisez. ■ Syntaxe de la règle **`.*mycompany.com`** prend en charge la redirection de toutes les URL qui contiennent la chaîne `mycompany.com`, y compris `http://mycompany.com`. ■ Syntaxe de la règle **`.*.mycompany.com`** prend en charge la redirection de toutes les URL qui contiennent la chaîne `.mycompany.com`. Il ne prend pas en charge la redirection de l'URL racine. Par exemple, `http://mycompany.com` n'est pas redirigé.

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

Paramètre	Ordinateur	Utilisateur	Propriétés
			Vous pouvez entrer des expressions régulières dans **Règles de client** et **Règles d'agent**. Si le paramètre `Url Redirection IP Rules Enabled` est activé, vous pouvez également entrer une adresse IP ou une plage d'adresses IP spécifique. Pour obtenir des informations sur la syntaxe complète, consultez Syntaxe pour les règles de redirection de contenu URL. Lorsque vous créez des règles d'agent, vous devez également utiliser l'option **Nom d'hôte de broker** pour spécifier l'adresse IP ou le nom de domaine complet de l'hôte du Serveur de connexion et l'option **Élément distant** pour spécifier le nom d'affichage du pool de postes de travail ou d'applications. 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 fonctionne 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 est activé par défaut.
`Url Redirection Protocol 'https'`	X		Pour toutes les URL qui utilisent le protocole HTTPS, spécifie les URL qui doivent être redirigées. Les options sont les mêmes que pour `Url Redirection Protocol 'http'`. Ce paramètre n'est pas configuré par défaut.
`Install the Chrome extension that is required in the URL content redirection feature.`		X	Si ce paramètre est activé, l'extension Chrome requise par la fonctionnalité de redirection de contenu URL est installée automatiquement en mode silencieux. Cette installation inclut également l'octroi des autorisations nécessaires. L'inversion de cette installation requiert des privilèges d'administration. Si ce paramètre est désactivé ou n'est pas configuré, l'extension Chrome requise par la fonctionnalité de redirection de contenu URL n'est pas installée, et la redirection de contenu URL ne fonctionne pas dans le navigateur Chrome, même si la redirection est définie, sauf si l'extension est installée à partir du Chrome Web Store manuellement. 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.

La méthode préférée pour configurer la redirection client vers agent consiste à utiliser l'utilitaire de ligne de commande `vdmutil` plutôt que des paramètres de stratégie de groupe.

Syntaxe pour les règles de redirection de contenu URL

Lorsque vous utilisez des paramètres de stratégie de groupe de Redirection de contenu URL, vous devez spécifier les URL qui s'ouvrent sur le client (option **Règles de client**) ou dans un poste de travail distant ou une application publiée (option **Règles d'agent**).

URL

Vous pouvez entrer des URL dans **Règles de client** et **Règles d'agent**. Vous pouvez utiliser des caractères génériques (`*`) pour spécifier un modèle d'URL qui correspond à plusieurs URL. Vous devez ajouter un caractère d'échappement (`\`) avant un point pour spécifier un point dans une entrée de règle. Par exemple, si vous spécifiez `".*\.net"`, `xxxx.net` est redirigé, mais `http://intranet` ne l'est pas.

Le tableau suivant présente des exemples d'entrées de règle qui incluent des URL.

Entrée de règle	Description
`.*`	Spécifie que toutes les URL sont redirigées. Si vous utilisez ce paramètre pour des règles d'agent (option **Règles d'agent**), toutes les URL sont ouvertes dans l'application publiée ou le poste de travail distant spécifié. Si vous utilisez ce paramètre pour des règles de client (option **Règles de client**), toutes les URL sont redirigées vers le client.
`.*\.acme\.com;.*\.example\.com`	Spécifie que toutes les URL qui contiennent le texte `.acme.com` ou `.example.com` sont redirigées. Utilisez des points-virgules pour séparer plusieurs entrées. Les espaces ne sont pas autorisés entre les entrées.
`.*\.acme\.com/software`	Spécifie que toutes les URL qui contiennent le texte `.acme.com` et le sous-répertoire `/software` sont redirigées. Par exemple, `http://www.acme.com/software` est redirigé. `http://www.acme.com/software/consumer` est également redirigé.
[espace ou laissez vide]	Spécifie qu'aucune URL n'est redirigée. Par exemple, laisser l'option **Règles de client** vide spécifie qu'aucune URL n'est redirigée vers le client.

Expressions régulières

Vous pouvez entrer des expressions régulières dans **Règles de client** et **Règles d'agent**. Pour obtenir des informations sur la syntaxe, consultez Règles d'expression régulière prises en charge par la redirection de contenu URL.

Filtrage d'adresse IP et de plage d'adresses IP

Si vous activez le paramètre de stratégie de groupe Règles IP de redirection URL activées, vous pouvez entrer une adresse IP ou une plage d'adresses IP spécifique dans **Règles de client** et **Règles d'agent**.

Par exemple, si vous activez Règles IP de redirection URL activées et que vous entrez `".*\.mycompany\.com;22.22.22.22;10.10.1.2-10.10.12.20"`, les URL et adresses IP suivantes sont redirigées.

- Toutes les URL qui incluent .mycompany.com

- L'adresse IP 22.22.22.22
- Toutes les adresses IP qui se situent dans la plage 10.10.1.2 à 10.10.12.20
- Toutes les URL qui sont résolues dans l'adresse IP 22.22.22.22
- Toutes les URL qui sont résolues dans la plage d'adresses IP 10.10.1.2 à 10.10.12.20

Si vous entrez à la fois une URL et une adresse IP ou une plage d'adresses IP, la règle d'URL a la priorité la plus élevée. Si l'URL fait l'objet d'une correspondance, la redirection se produit directement à l'aide de l'URL. Si l'URL ne fait pas l'objet d'une correspondance, Horizon exécute une requête DNS, puis effectue le filtrage de l'adresse IP ou de la plage d'adresses IP.

Cette fonctionnalité est prise en charge uniquement avec Internet Explorer/Microsoft Edge (Chromium-IE-Mode) et IPv4. Elle est désactivée par défaut.

Règles d'expression régulière prises en charge par la redirection de contenu URL

Vous pouvez entrer une expression régulière dans **Règles de client** et **Règles d'agent**. Une expression régulière est un objet qui décrit un modèle de caractères. Les expressions régulières exécutent des fonctions de recherche et de remplacement et de correspondance au modèle sur du texte.

La redirection de contenu URL prend en charge les règles d'expression régulière suivantes.

Règle	Détail
Accolades	[ ], [^], ( ), (?:), (?=)
\+métacaractère ou métacaractère	'\w', '\W', '\d', '\D', '\b', '.'
Quantificateurs	+, *, ?, {x}, {x,y}, {x,}
Alternative	|

Pour obtenir des informations détaillées sur les expressions régulières, consultez la rubrique à l'adresse https://en.wikipedia.org/wiki/Regular_expression.

Le tableau suivant contient des exemples de règles d'expression régulière prises en charge par la redirection de contenu URL.

Entrée de règle	Exemples d'URL et d'adresses IP correspondantes
.*\.net	www.hello.net, www.inter.net, train.word.net, test.train.net et train.chromeie.net.com.cn.
.*\.sth\.ctirial	example.sth.ctirial, www.google.sth.ctirial et www.google.com/test.sth.ctirial/editpage.action.
.*administra	www.administra.com, www.askadministra-tor.net et google.akmkda.eae/administra.cn.
.*a{4}custom\.com	world.banada.cn/aaaacustom.com, www.aaaacustom.com et exple.aaaacustom.com.net/nodepad.action.

Entrée de règle	Exemples d'URL et d'adresses IP correspondantes
.*a{2,3}custom\.com	world.banada.aacustom.com, www.aaacustom.com et exple.aacustom.com.net/nodepad.action.
.*train[abc]\.net	hello.traina.net, hello.trainb.net, example.trainc.net.com et www.testtraina.net.com/edit.
.*train[^abc]\.net	hello.traind.net, hello.traine.net, example.train2.net.com et www.testtrain3.net.com/edit.
.*a+c*tra\.net	www.actra.net.com. aactra.net.cn, atra.net.www.train et aaccctra.netword.
.*example(test)?\.cn	www.example.cn, www.exampletest.cn, example.cn/editpage et exampletest.cn/editpage.
sac(?=sprt)	helloworld.sacsprt.net, examplesacsprt.com/text et www.sacsprtexam.com.
sac(?!sprt)	helloworld.sacspra.net, examplesacbprt.com/text et www.sacexam.com.
10\.1\.1\.1[0-5]	10.1.1.10 à 10.1.1.15.
10\.1\.(1|2)\.1[0-5]	10.1.1.10 à 10.1.1.15 et 10.1.2.10 à 10.1.2.15.
10\.[2-4]\.19\.12	10.2.19.12, 10.3.19.12 et 10.4.19.12.
10\.[^2-4]\.19\.12	10.6.19.12, 10.1.19.12,10.5.19.12 et 10.7.19.12.
a(\w)cd(\d)345a\.com	www.abccd2345a.com.net et train.adc2cd1345a.com/edit.action.
abc(\W)cd(\D)345a\.com	google.abc+cda345a.com et test.train.net/abc&cda345a.com.
((25[0-5]|2[0-4][0-9]|[01]?[0-9]?[0-9])\.){3} (25[0-5]|2[0-4][0-9]|[01]?[0-9]?[0-9])	Toutes les adresses IPv4.
.*example(test)? \.cn;10\.1\.1\.1[0-5];a(\w)cd(\d)345a\.com	www.example.cn, example.cn/editpage,10.1.1.10 to 10.1.1.15, www.abccd2345a.com.net et train.adc2cd1345a.com/edit.action.

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 regardent des vidéos sur un poste de travail distant ou une application publiée, par exemple, vous pouvez rediriger ces URL vers la machine cliente afin qu'aucune charge supplémentaire ne soit placée sur le centre de données. Pour les employés qui travaillent à l'extérieur du réseau d'entreprise, vous voulez peut-être que toutes les URL qui pointent vers des emplacements en dehors du réseau d'entreprise s'ouvrent sur la machine cliente de l'employé pour des raisons de sécurité.

Par exemple, vous pouvez configurer des règles afin que toutes les URL qui ne pointent pas vers le réseau d'entreprise soient redirigées afin de s'ouvrir sur la machine cliente. Dans cet exemple, vous pouvez utiliser les paramètres suivants, qui incluent des expressions régulières :

- Pour **Règles d'agent** : `.*.mycompany.com`

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

- Pour **Règles de client** : `.*`

  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 publiée ou un poste de travail distant, les règles de 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 s'ouvre localement. Dans cet exemple, l'URL s'ouvre sur la machine agent.
4. S'il n'existe aucun conflit, l'URL est redirigée vers le client.

   Dans cet 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`** s'ouvrent 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 s'ouvre 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 s'ouvre sur le client.

Configuration de la redirection client vers agent

Avec la redirection client vers agent, Horizon Client ouvre un poste de travail distant ou une application publiée 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 publiée est ouverte, elle traite l'URL.

Pour utiliser la redirection client vers agent, effectuez les tâches de configuration suivantes dans l'ordre indiqué.

1. Installez les extensions de navigateur pour les clients et les navigateurs que vous prévoyez d'utiliser avec la fonctionnalité de redirection de contenu URL.

Client	Navigateur	Instructions
Linux	Firefox	Installer et activer l'extension de redirection d'URL VMware Horizon pour Firefox sous Linux
Linux	Chrome	Installer et activer l'aide à la redirection de contenu URL VMware Horizon pour Chrome sous Linux
Windows	Chrome	Installer et activer l'extension Aide à la redirection de contenu URL pour Chrome sous Windows

Client	Navigateur	Instructions
Windows	Microsoft Edge (Chromium)	Installer l'extension Aide à la redirection de contenu URL pour Microsoft Edge (Chromium) sous Windows
Mac	Chrome	Activer l'Aide à la redirection de contenu URL pour Chrome sur un Mac
Mac	Microsoft Edge (Chromium)	Installer et activer l'extension Aide à la redirection de contenu URL pour Microsoft Edge (Chromium) sur un Mac

Note Pour Internet Explorer, le plug-in de filtrage d'URL de VMware Horizon View est installé par défaut avec Horizon Client. Reportez-vous à la section Installation d'Horizon Client pour Windows avec la fonctionnalité de redirection de contenu URL activée.

2 Installez la fonctionnalité de redirection de contenu URL sur la machine cliente.

   a Pour les clients Windows, installez Horizon Client pour Windows avec la fonctionnalité de redirection de contenu URL activée. Reportez-vous à la section Installation d'Horizon Client pour Windows avec la fonctionnalité de redirection de contenu URL activée.

   b Pour les clients Mac et Linux, installez Horizon Client. La fonctionnalité de redirection de contenu URL est activée par défaut lorsque vous installez Horizon Client pour Mac et Horizon Client pour Linux. Aucune étape supplémentaire n'est requise pour activer la fonctionnalité de redirection de contenu URL sur ces clients.

3 Utilisez l'utilitaire de ligne de commande `vdmutil` sur une instance du Serveur de connexion 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 ou Créer un paramètre global de redirection de contenu URL.

4 Utilisez l'utilitaire de ligne de commande `vdmutil` sur une instance du Serveur de connexion pour attribuer le paramètre de redirection de contenu URL à des utilisateurs ou à des groupes Active Directory. Reportez-vous à la section Attribuer un paramètre de redirection de contenu URL à un utilisateur ou un groupe.

5 Vérifiez le paramètre de redirection de contenu URL. Reportez-vous à la section Tester un paramètre de redirection de contenu URL.

Important 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 sur l'utilisation des paramètres de stratégie de groupe, reportez-vous à la section Utilisation de paramètres de stratégie de groupe pour configurer la redirection client vers agent. Pour les clients Mac et Linux, vous devez utiliser `vdmutil` pour configurer la redirection client vers agent. Comme macOS et Linux ne prennent pas en charge les GPO, vous ne pouvez pas utiliser les paramètres de stratégie de groupe pour définir la configuration client vers agent si vous disposez de clients Mac.

Utilisation de l'utilitaire de ligne de commande vdmutil sur une instance du Serveur de connexion

Vous pouvez utiliser l'interface de ligne de commande `vdmutil` sur une instance du Serveur de connexion pour créer, attribuer et gérer les paramètres de redirection de contenu URL pour la redirection client vers agent.

Note Vous devez utiliser la commande `vdmutil` pour configurer la redirection client vers agent pour les clients Mac. Comme les GPO ne sont pas pris en charge par macOS, vous ne pouvez pas les utiliser pour définir la configuration client vers agent si vous disposez de clients Mac.

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 Console pour attribuer le rôle Administrateurs à un utilisateur. Pour plus d'informations, reportez-vous au document *Administration d'Horizon*.

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`**.

Syntaxe pour l'option --agentURLPattern

Lorsque vous utilisez la commande `vdmutil` sur une instance du Serveur de connexion pour créer un paramètre de redirection de contenu URL, entrez une chaîne entre guillemets qui spécifie l'URL (ou les URL) qui doit être ouverte sur le poste de travail distant ou l'application publiée dans l'option `--agentURLPattern`.

La chaîne entre guillemets contient une expression régulière et doit inclure le préfixe du protocole. Vous pouvez utiliser des caractères génériques pour spécifier un modèle d'URL qui correspond à plusieurs URL.

Le tableau suivant décrit des exemples de modèles d'URL.

Modèle d'URL de l'agent	Description
".*"	Toutes les URL clientes sont redirigées vers le poste de travail distant ou l'application publiée.
"http://google.*"	Toutes les URL clientes qui contiennent le texte **google** sont redirigées vers le poste de travail distant ou l'application publiée.
"http://acme.com/software"	Toutes les URL clientes qui contiennent le texte **acme.com** et le sous-répertoire **/software** sont redirigées vers le poste de travail distant ou l'application publiée. Par exemple, `http://www.acme.com/software` est redirigé. `http://www.acme.com/software/consumer` est également redirigé.

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 un poste de travail distant ou une application publiée. Un paramètre local de redirection de contenu URL n'est visible que dans l'espace local.

Vous pouvez configurer un nombre quelconque de protocoles, notamment HTTP, HTTPS, mailto et callto. Le protocole callto n'est pas pris en charge pour la redirection avec le navigateur Chrome.

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 fonctionne 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.

VMware recommande de ne pas créer plus d'un paramètre pour la redirection de contenu URL.

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.

Conditions préalables

- 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 sur une instance du Serveur de connexion.
- Familiarisez-vous avec la syntaxe des URL dans les paramètres de redirection de contenu URL. Reportez-vous à la section Syntaxe pour l'option --agentURLPattern.

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 url-filtering --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 doit être **`url-filtering`**.
--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 `Win10`. Pour les pools de postes de travail RDS, utilisez l'option `--entitledApplication`.
--agentURLPattern	Chaîne entre guillemets qui spécifie l'URL devant être ouverte sur le poste de travail distant ou l'application publiée.

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 url-filtering --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
```

Étape suivante

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.

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 un poste de travail distant ou une application publiée 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 un nombre quelconque de protocoles, notamment HTTP, HTTPS, mailto et callto. Le protocole callto n'est pas pris en charge pour la redirection avec le navigateur Chrome.

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 fonctionne 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*.

VMware recommande de ne pas créer plus d'un paramètre pour la redirection de contenu URL.

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

Conditions préalables

- 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 sur une instance du Serveur de connexion.
- Familiarisez-vous avec la syntaxe des URL dans les paramètres de redirection de contenu URL. Reportez-vous à la section Syntaxe pour l'option --agentURLPattern.

Procédure

1. Ouvrez une session sur 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 url-filtering --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 doit être **`url-filtering`**.
--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.

Option	Description
--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 le poste de travail distant ou l'application publiée.

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 url-filtering --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 local de redirection de contenu URL appelé `url-filtering` qui redirige toutes les URL de client contenant le texte `http://google.*` vers le droit d'application global appelé `GAE1`.

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

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

```
vdmutil --updateURLSetting --urlSettingName url-filtering --urlRedirectionScope GLOBAL
--urlScheme https --entitledApplication GAE1 --agentURLPattern "https://google.*" -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 droit d'application global appelé `GA2`.

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

Étape suivante

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.

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 à un groupe Active Directory.

Conditions préalables

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 sur une instance du Serveur de connexion.

Procédure

- Pour attribuer un paramètre de redirection de contenu URL à un utilisateur, sur l'instance du Serveur de connexion, 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. Il doit s'agir du paramètre **`url-filtering`**.
--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. Il doit s'agir du paramètre **`url-filtering`**.
--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
```

Étape suivante

Vérifiez vos paramètres de redirection de contenu URL. Reportez-vous à la section Tester un paramètre de redirection de contenu URL.

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

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

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-YYMM-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

Pour vérifier que la fonctionnalité de redirection de contenu URL est activée, 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`. Si vous utilisez la fonctionnalité de redirection de contenu URL avec Internet Explorer, vérifiez également que le module complémentaire Internet Explorer Plug-in de filtrage URL VMware Horizon View est installé.

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.

Conditions préalables

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 sur une instance du Serveur de connexion.

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 un client Windows, procédez comme suit.

a 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.

b Ouvrez l'éditeur du registre (`regedit`) et vérifiez les clés de registre au 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.

4 Sur un client Mac, procédez comme suit.

a Ouvrez Horizon Client et connectez-vous à l'instance du Serveur de connexion.

b Dans une application tierce, telle que Notes, cliquez sur les URL qui correspondent aux modèles d'URL configurés dans le paramètre et vérifiez que les URL sont redirigées comme prévu.

c Vérifiez que le fichier JSON est créé.

Note Le fichier JSON est créé lorsque l'extension Aide à la redirection de contenu URL VMware est installée.

Navigateur	Chemin d'accès
Chrome	`~/Library/Application Support/Google/Chrome/Default/Extensions/lfidjngibpklhhijphdmbmedchiiolgk/version/data.json`
Edge	`~/Library/Application Support/Microsoft Edge/Default/Extensions/lfidjngibpklhhijphdmbmedchiiolgk/version/data.json`

5 Sur un client Linux, procédez comme suit.

a Ouvrez Horizon Client et connectez-vous à l'instance du Serveur de connexion.

b Vérifiez que le fichier JSON est créé pour l'application tierce et le navigateur.

Note Le fichier JSON est créé lorsque l'extension Aide à la redirection de contenu URL VMware est installée.

Composant	Chemin d'accès
Application tierce	`~/.vmware/broker-url-config.json`
Chrome	`~/.config/google-chrome/Default/Extensions/lfidjngibpklhhijphdmbmedchiiolgk/version/data.json`
Firefox	`~/.mozilla/managed-storage/url_redirection@vmware.com.json`

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 sur une instance du Serveur de connexion.

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 pour la redirection de contenu URL (`urlRedirection.admx`) contient des paramètres de stratégie de groupe que vous pouvez utiliser pour créer des règles qui redirigent des URL du client vers un poste de travail distant ou une application publiée (redirection client vers agent).

Important La méthode préférée pour configurer la redirection client vers agent consiste à utiliser l'interface de ligne de commande `vdmutil`. Comme les stratégies de groupe ne sont pas prises en charge par macOS, vous ne pouvez pas les utiliser pour définir la configuration client vers agent si vous disposez de clients Mac.

Pour créer une règle pour la redirection client vers agent, vous utilisez l'option **Élément distant** pour spécifier le nom complet d'un pool d'applications ou de postes de travail et l'option **Règles d'agent** pour spécifier les URL qui doivent être redirigées vers l'application publiée ou le poste de travail distant. Vous devez également utiliser l'option **Nom d'hôte de broker** pour spécifier l'adresse IP ou le nom de domaine complet de l'hôte du Serveur de connexion à utiliser lors de la redirection des URL vers une application publiée 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 publiée ou un poste de travail distant. Dans ce cas, vous pouvez définir l'option **Règles d'agent** sur `.*.mycompany.com`.

Pour obtenir des instructions d'installation de fichier de modèle d'administration de Redirection de contenu URL, des descriptions des paramètres de stratégie de groupe et la syntaxe de l'option **Règles d'agent**, reportez-vous à la section Configuration de la redirection agent vers client.

Installation d'extensions de navigateur pour la redirection de contenu URL

Vous devez installer l'extension de redirection de contenu URL VMware Horizon pour utiliser la plupart des navigateurs pris en charge avec la redirection de contenu URL. Vous n'avez pas besoin d'installer une extension pour Internet Explorer. Vous devez installer les extensions du navigateur avant d'activer la redirection de contenu URL dans Horizon Agent ou Horizon Client.

Installer et activer l'extension Aide à la redirection de contenu URL pour Chrome sous Windows

Pour utiliser le navigateur Chrome avec la fonctionnalité de redirection de contenu URL sur un client Windows ou une machine agent Windows, vous devez installer et activer l'extension Aide à la redirection de contenu URL VMware Horizon pour Chrome.

Vous pouvez installer et activer l'extension Aide à la redirection de contenu URL VMware Horizon en activant un paramètre de stratégie de groupe Redirection de contenu URL.

Cette procédure décrit comment appliquer le paramètre de stratégie de groupe Redirection de contenu URL à des GPO sur votre serveur Active Directory. Pour les machines clientes Windows, le GPO doit être lié à l'UO qui contient vos ordinateurs clients Windows. Pour les applications et les postes de travail distants, le GPO doit être lié à l'UO qui contient vos postes de travail virtuels et vos hôtes RDS.

Si vous n'utilisez pas de stratégie de groupe pour installer et activer l'extension Aide à la redirection de contenu URL VMware Horizon, vous devez installer manuellement l'extension à partir du Chrome Web Store.

Conditions préalables

- Installez le navigateur Chrome. Pour connaître les versions prises en charge, reportez-vous à la section Configuration système requise pour la redirection de contenu URL.
- 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.

- Ajoutez le fichier de modèle d'administration ADMX de redirection de contenu URL à votre serveur Active Directory. Reportez-vous à la section Ajouter le modèle d'administration ADMX de redirection de contenu URL à un GPO.

Procédure

1 Pour appliquer le paramètre de stratégie de groupe de redirection de contenu URL à des GPO sur votre serveur Active Directory, procédez comme suit.

   a Sur votre serveur Active Directory, ouvrez l'Éditeur de gestion de stratégie de groupe et accédez au dossier **Configuration utilisateur > Stratégies > Modèles d'administration > Redirection URL de VMware Horizon**.

   b Ouvrez le paramètre **Installez l'extension Chrome qui est requise dans la fonctionnalité de redirection de contenu URL**, sélectionnez **Activé** et cliquez sur **OK**.

   c Démarrez Chrome sur la machine Windows.

   L'extension Aide à la redirection de contenu URL VMware Horizon est installée en mode silencieux.

   d Pour vérifier que l'extension Chrome est installée, tapez **`chrome://extensions`** dans le navigateur Chrome.

   Aide à la redirection de contenu URL VMware Horizon s'affiche dans la liste Extensions et la case **Activé** est cochée.

2 Pour installer l'extension manuellement à partir de Chrome Web Store, procédez comme suit.

   a Dans le navigateur Chrome, accédez à Chrome Web Store.

   b Recherchez **Aide à la redirection de contenu URL VMware Horizon**.

   c Sélectionnez **Aide à la redirection de contenu URL VMware Horizon**, puis cliquez sur **Ajouter à Chrome**.

Résultats

La première fois qu'une URL est redirigée depuis le navigateur Chrome sur le client, l'utilisateur est invité à ouvrir l'URL dans Horizon Client. L'utilisateur doit cliquer sur **Ouvrir l'URL : protocole VMware Horizon Client**, sinon la redirection URL ne se produit pas. Si l'utilisateur coche la case **Mémoriser mon choix pour l'URL : liens de protocole VMware Horizon Client** (recommandé), cette invite ne s'affiche plus.

Installer l'extension Aide à la redirection de contenu URL pour Microsoft Edge (Chromium) sous Windows

Pour utiliser le navigateur Microsoft Edge (Chromium) avec la fonctionnalité de redirection de contenu URL sur un client Windows ou une machine agent Windows, vous devez installer l'extension Aide à la redirection de contenu URL VMware Horizon dans le navigateur Microsoft Edge (Chromium).

Vous pouvez installer l'extension Aide à la redirection de contenu URL VMware Horizon dans Chrome Web Store.

Conditions préalables

Installez le navigateur Microsoft Edge (Chromium) sur la machine cliente Windows. Pour obtenir les versions prises en charge, reportez-vous à la section Configuration système requise pour la redirection de contenu URL.

Procédure

1. Dans le navigateur Microsoft Edge (Chromium), entrez https://chrome.google.com/webstore/detail/vmware-horizon-url-conten/lfidjngibpklhhijphdmbmedchiiolgk.
2. Cliquez sur le bouton **Ajouter des extensions d'autres magasins** en haut de la fenêtre de navigateur et cliquez sur **Autoriser**.
3. Cliquez sur **Ajouter à Chrome**.
4. Lorsque vous êtes invité à ajouter l'extension à Microsoft Edge (Chromium), cliquez sur **Ajouter une extension**.
5. Pour vérifier que l'extension est installée, cliquez sur l'icône **Paramètres, etc. (...)** dans le coin supérieur droit de la fenêtre de navigateur et sélectionnez **Extensions**.

   Aide à la redirection de contenu URL VMware Horizon s'affiche dans la liste des extensions installées.

Résultats

La première fois qu'une URL est redirigée depuis le navigateur Microsoft Edge (Chromium) sur le client, l'utilisateur est invité à ouvrir l'URL dans Horizon Client. L'utilisateur doit cliquer sur **Ouvrir l'URL : protocole VMware Horizon Client**, sinon la redirection URL ne se produit pas.

Activer l'Aide à la redirection de contenu URL pour Chrome sur un Mac

Pour utiliser le navigateur Chrome avec la fonctionnalité de redirection de contenu URL sur un client Mac, vous devez activer l'extension Aide à la redirection de contenu URL VMware Horizon pour Chrome.

Conditions préalables

Installez le navigateur Chrome sur le client Mac. Pour connaître les versions prises en charge, reportez-vous à la section Configuration système requise pour la redirection de contenu URL.

Procédure

1. Dans le navigateur Chrome, accédez à Chrome Web Store.
2. Recherchez **Aide à la redirection de contenu URL VMware Horizon.**

3 Sélectionnez **Aide à la redirection de contenu URL VMware Horizon**, puis cliquez sur **Ajouter à Chrome**.

4 Pour vérifier que l'extension Chrome est installée, tapez **`chrome://extensions`** dans le navigateur Chrome.

   Aide à la redirection de contenu URL VMware Horizon s'affiche dans la liste Extensions et la case **Activé** est cochée.

Résultats

La première fois qu'une URL est redirigée depuis le navigateur Chrome sur le client Mac, l'utilisateur est invité à ouvrir l'URL dans Horizon Client. L'utilisateur doit cliquer sur **Ouvrir VMware Horizon Client**, sinon la redirection URL ne se produit pas. Si l'utilisateur coche la case **Mémoriser mon choix pour les liens de VMware Horizon Client** (recommandé), cette invite ne s'affiche pas à nouveau.

Installer et activer l'extension Aide à la redirection de contenu URL pour Microsoft Edge (Chromium) sur un Mac

Pour utiliser le navigateur Microsoft Edge (Chromium) avec la fonctionnalité de redirection de contenu URL sur un client Mac, vous devez installer l'extension Aide à la redirection de contenu URL VMware Horizon dans le navigateur Edge (Chromium).

Vous pouvez installer l'extension Aide à la redirection de contenu URL VMware Horizon dans Chrome Web Store.

Conditions préalables

Installez le navigateur Microsoft Edge (Chromium) sur le client Mac. Pour obtenir les versions prises en charge, reportez-vous à la section Configuration système requise pour la redirection de contenu URL.

Procédure

1 Dans le navigateur Microsoft Edge (Chromium), entrez https://chrome.google.com/webstore/detail/vmware-horizon-url-conten/lfidjngibpklhhijphdmbmedchiiolgk.

2 Cliquez sur le bouton **Ajouter des extensions d'autres magasins** en haut de la fenêtre de navigateur et cliquez sur **Autoriser**.

3 Cliquez sur **Ajouter à Chrome**.

4 Lorsque vous êtes invité à ajouter l'extension à Microsoft Edge (Chromium), cliquez sur **Ajouter une extension**.

5 Pour vérifier que l'extension est installée, cliquez sur l'icône **Paramètres, etc. (...)** dans le coin supérieur droit de la fenêtre de navigateur et sélectionnez **Extensions**.

   Aide à la redirection de contenu URL VMware Horizon s'affiche dans la liste des extensions installées.

Résultats

Lorsque vous démarrez Horizon Client et que vous vous connectez à une instance du Serveur de connexion sur laquelle les paramètres de redirection de contenu URL ont été configurés, Horizon Client télécharge les configurations de redirection de contenu URL nécessaires sur le client Mac. Redémarrez le navigateur Microsoft Edge (Chromium) sur le client Mac.

Installer et activer l'extension de redirection d'URL VMware Horizon pour Firefox sous Linux

Pour utiliser le navigateur Firefox pour la redirection de contenu URL client vers agent à partir d'un client Linux, vous devez installer et activer l'extension de redirection d'URL VMware Horizon pour Firefox.

Vous pouvez utiliser le gestionnaire de modules complémentaires de Firefox pour rechercher le programme d'installation de l'extension de redirection de l'URL VMware Horizon.

Conditions préalables

- Installez le navigateur Firefox sur le système client Linux. Pour connaître les versions de navigateur prises en charge, reportez-vous à la section Configuration système requise pour la redirection de contenu URL.
- Installez Horizon Client pour Linux sur le système client Linux. Pour obtenir des instructions, reportez-vous au document *Guide d'installation et de configuration de VMware Horizon Client pour Linux*.
- Configurez les paramètres de redirection de contenu URL sur l'instance du Serveur de connexion. Reportez-vous à la section Configuration de la redirection client vers agent.

Procédure

1. Démarrez Firefox sur le système Linux.

   Le lancement du navigateur crée un dossier de profil sur le système client, qui est requis pour prendre en charge la fonctionnalité de redirection de contenu URL.
2. Dans le menu Firefox, sélectionnez **Modules complémentaires**.
3. Dans la page **Gestionnaire de modules complémentaires**, tapez **`vmware`** dans la zone de texte de recherche pour localiser l'extension de redirection de l'URL VMware Horizon.
4. Sélectionnez l'extension de redirection de l'URL VMware Horizon, puis suivez les invites pour ajouter cette extension à Firefox.
5. Pour vérifier que l'extension Firefox est installée, revenez à la page **Gestionnaire de modules complémentaires**, puis cliquez sur **Extensions**. Vérifiez que l'extension s'affiche dans la liste **Activées**.

6 Démarrez Horizon Client sur le système Linux et connectez-vous à une instance du Serveur de connexion sur laquelle des paramètres de redirection de contenu URL ont été configurés.

   Horizon Client télécharge les configurations de redirection de contenu URL nécessaires sur le système Linux.

7 Redémarrez Firefox.

Étape suivante

La première fois qu'une URL est redirigée depuis le navigateur Firefox sur le client Linux, l'utilisateur est invité à ouvrir l'URL dans Horizon Client. L'utilisateur doit spécifier Horizon Client comme application pour ouvrir l'URL et cliquer sur **Ouvrir le lien**, sinon la redirection d'URL ne se produit pas. Si l'utilisateur sélectionne l'option pour mémoriser ce choix et toujours autoriser l'ouverture des liens avec Horizon Client (recommandé), cette invite ne s'affiche pas à nouveau.

Installer et activer l'aide à la redirection de contenu URL VMware Horizon pour Chrome sous Linux

Pour utiliser le navigateur Chrome pour la redirection de contenu URL client vers agent à partir d'un client Linux, vous devez installer et activer l'extension Aide à la redirection de contenu URL VMware Horizon pour Chrome.

Vous pouvez utiliser la page des extensions Chrome pour rechercher le programme d'installation de l'aide à la redirection de contenu URL VMware Horizon.

Conditions préalables

- Installez le navigateur Chrome sur le système client Linux. Pour connaître les versions de navigateur prises en charge, reportez-vous à la section Configuration système requise pour la redirection de contenu URL.
- Installez Horizon Client pour Linux sur le système client Linux. Pour obtenir des instructions, reportez-vous au document *Guide d'installation et de configuration de VMware Horizon Client pour Linux*.
- Configurez les paramètres de redirection de contenu URL sur l'instance du Serveur de connexion. Reportez-vous à la section Configuration de la redirection client vers agent.

Procédure

1 Démarrez le navigateur Chrome sur le système Linux et accédez à la page des extensions.

2 Sur celle-ci, recherchez l'aide à la redirection de contenu URL VMware Horizon.

3 Sélectionnez l'aide à la redirection de contenu URL VMware Horizon, puis suivez les invites pour ajouter cette extension à Chrome.

4 Pour confirmer l'installation et l'activation de l'extension, revenez à la page des extensions. Vérifiez que l'aide à la redirection de contenu URL VMware Horizon s'affiche sur la page et que son option d'activation est définie sur la position Activé.

5 Démarrez Horizon Client sur le système Linux et connectez-vous à une instance du Serveur de connexion sur laquelle des paramètres de redirection de contenu URL ont été configurés.

   Horizon Client télécharge les configurations de redirection de contenu URL nécessaires sur le système Linux.

6 Redémarrez Chrome.

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.
- Si vous n'installez pas les extensions du navigateur pour la redirection de contenu URL avant d'activer la fonctionnalité de redirection de contenu URL dans Horizon Agent ou Horizon Client, le fichier JSON ne se charge pas et la fonctionnalité de redirection de contenu URL ne fonctionne pas.
- Les profils itinérants ne sont pas pris en charge avec la fonctionnalité de redirection de contenu URL dans l'agent Windows ou le client Windows.
- Pour prendre en charge les navigateurs Chrome et Microsoft Edge (Chromium) publiés dans un hôte RDS, l'extension du navigateur de redirection de contenu URL doit utiliser un processus d'aide lancé par l'Explorateur Windows (`explorer.exe`). Si le processus d'aide

n'est pas démarré, la redirection de contenu URL ne fonctionne pas dans Chrome et Microsoft Edge (Chromium). La redirection de contenu URL est prise en charge si l'application publiée est le navigateur Internet Explorer ou une application sans navigateur, telle que WordPad ou Word.

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.

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 virtuel. Cette fonctionnalité est appelée redirection USB. Un poste de travail virtuel peut recevoir jusqu'à 255 périphériques USB.

Vous pouvez également rediriger certains périphériques USB connectés localement pour les utiliser dans des applications et des postes de travail publiés. Pour plus d'informations sur les types spécifiques de périphériques pris en charge, reportez-vous à la section Limitations concernant les types de périphérique USB.

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 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 les types de périphériques USB auxquels 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 fonctionnalité de redirection USB n'est disponible que sur certains types de clients. Pour savoir si cette fonctionnalité est prise en charge sur un client particulier, consultez la matrice de prise en charge des fonctionnalités incluse dans le document d'installation et de configuration d'Horizon Client pour ce client.

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 VMware Horizon sécurisé.

Ce chapitre contient les rubriques suivantes :

Limitations concernant les types de périphérique USB

Bien que VMware Horizon n'empêche pas de manière explicite les périphériques de fonctionner avec la fonctionnalité de redirection USB, 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.

Limites des périphériques USB 3.0

Vous pouvez connecter des périphériques USB 3.0 à des ports USB 3.0 sur la machine cliente. Les périphériques USB 3.0 sont uniquement pris en charge avec un flux unique. Comme la prise en charge multi-flux n'est pas mise en œuvre, les performances du périphérique 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 distante en raison de la latence réseau.

Redirection USB avec des postes de travail virtuels

Les types de périphériques USB 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 même, les lecteurs de CD/DVD USB et les scanners USB ne fonctionnent pas correctement sur un réseau latent tel qu'un réseau WAN.
- La redirection de scanners USB dépend de l'état du réseau, et les numérisations peuvent être anormalement longues.

Redirection USB avec des applications et des postes de travail publiés

Vous pouvez rediriger des clés et des disques durs USB localement connectés pour une utilisation dans des applications et des postes de travail publiés. Les applications et les postes de travail publiés peuvent également prendre en charge des périphériques USB plus génériques, tels que les tablettes de signature TOPAZ ou Wacom, ainsi que la pédale de contrôle de dictaphone Olympus. Les autres types de périphériques USB, tels que les lecteurs de stockage de sécurité et les lecteurs CD-ROM USB, ne sont pas pris en charge dans les applications et les postes de travail publiés.

Recommandations pour la redirection USB

Vous pouvez utiliser des solutions recommandées pour la redirection USB pour certains types de périphériques USB.

Au lieu d'utiliser la redirection USB, utilisez ces fonctionnalités de redirection qui offrent de meilleures performances et une meilleure expérience utilisateur :

- Pour les scanners, utilisez la redirection de scanner. Reportez-vous à la section Configuration de la redirection de scanner.
- Pour les imprimantes, utilisez la redirection d'imprimante. Reportez-vous à la section Configurer VMware Integrated Printing .
- Pour les lecteurs de carte à puce, utilisez la redirection de carte à puce. Reportez-vous au document *Administration d'Horizon*.
- Pour les périphériques de port série, utilisez la redirection de port série. Reportez-vous à la section Configuration de la redirection de port série.
- Utilisez la redirection du lecteur client pour le partage de fichiers au lieu de la redirection USB pour les disques USB et les périphériques de stockage volumineux. Reportez-vous à la section Gestion de l'accès à la redirection de lecteur client.

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 Horizon Administrator.

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

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 d'installation et de configuration pour le type spécifique de périphérique client.

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 VMware Horizon sécurisé.

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, incluez 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 Horizon Administrator.

Dans Horizon Administrator, accédez à **Stratégies > Stratégies 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 stratégies pour contrôler la redirection USB.

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 clients Windows, vous pouvez configurer des stratégies de groupe. Pour les clients Mac, vous utilisez une commande de ligne de commande. Pour plus d'informations, consultez le document d'installation et de configuration pour le type spécifique de périphérique client.

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.

Configuration de la redirection USB pour Chrome et les clients HTML Access

Pour utiliser la fonctionnalité de redirection USB avec Horizon Client pour Chrome et les clients HTML Access, vous devez suivre des étapes supplémentaires.

1 Installez le composant Redirection USB dans Horizon Agent. Reportez-vous à la section Présentation de la configuration de la redirection USB.

2 Définissez la clé de registre `UsbVirtualChannelEnabled` sur `true` sur la machine agent. Reportez-vous à la section Activation de la fonctionnalité Kit de développement logiciel (SDK) d'amélioration USB sur session.

3 À l'aide du compte d'administrateur, installez le pilote de périphérique USB sur la machine agent.

Pour plus d'informations sur la configuration de la redirection USB pour les postes de travail à distance Linux, reportez-vous à la section « Pilote VHCI pour la redirection USB » du document *Configuration des postes de travail Linux dans Horizon*.

Pour plus d'informations sur l'utilisation de la redirection USB dans Horizon Client pour Chrome ou HTML Access, reportez-vous au guide de l'utilisateur ou au guide d'installation et de configuration du client.

Configuration de la redirection de scanner d'empreintes digitales et de microscope

Vous pouvez rediriger des périphériques biométriques, notamment des scanners d'empreintes digitales, qui sont connectés à un port USB sur un système client Windows, vers des postes de travail virtuels. Vous pouvez également rediriger des microscopes USB Dino-Lite d'un système client Windows, Mac ou Linux vers des postes de travail virtuels.

Configuration de la redirection de scanner d'empreintes digitales

Pour rediriger ces scanners d'empreintes digitales, vous devez disposer d'une bande passante réseau d'au moins 200 Mbits/s sur le poste de travail d'agent distant.

Ces scanners d'empreintes digitales sont pris en charge :

Tableau 4-1. Scanners d'empreintes digitales pris en charge

Périphérique	Système d'exploitation du client	Serveurs de système d'exploitation Windows	Protocoles
Lecteur d'empreinte digitale U.are.U 5160	Windows 10 1809 64 bits	Windows 10 1809 64 bits Windows 10 1903 64 bits	PCoIP, Blast
Lecteur d'empreinte digitale U.are.U 5300	Windows 10 1809 64 bits	Windows 10 1809 64 bits Windows 10 1903 64 bits	PCoIP, Blast

Configuration de la redirection de microscope

Pour rediriger des microscopes USB, vous devez respecter les exigences réseau suivantes :

Tableau 4-2. Configuration réseau requise pour la redirection de microscope

Configuration réseau requise	Pour le transfert de données du client vers l'agent	Pour le transfert de données de l'agent vers le client
Bande passante	Au moins 400 Mbits/s	Au moins 20 Mbits/s
Retard	Au plus 1 ms	Au plus 2 ms
Perte	Au plus 0,005 %	Au plus 0,005 %

Les systèmes clients Windows et Mac autorisent la redirection USB des microscopes pris en charge par défaut.

Les systèmes clients Linux excluent par défaut les microscopes de la redirection USB. Pour utiliser la redirection, vous devez autoriser le microscope en définissant la propriété **viewusb.IncludeVidPid**. Reportez-vous à la rubrique « Définition de propriétés de configuration USB » dans *Guide d'installation et de configuration de VMware Horizon Client pour Linux*.

Pour optimiser les performances, configurez les paramètres du microscope comme suit :

- Définissez la résolution sur **640 x 480**.
- Définissez **Encodeur vidéo** sur **MJPEG**.
- Réduisez ou désactivez le paramètre d'exposition automatique.

Les microscopes USB suivants sont pris en charge :

Tableau 4-3. Microscopes USB pris en charge

Périphérique	Système d'exploitation du client	Poste de travail de l'agent distant du système d'exploitation Windows	Protocoles
Dino-Lite Premier AM4113ZT	Windows Mac Linux (version du noyau 3.3-rc1 ou ultérieure)	Windows 10	PCoIP, Blast

Configuration de la redirection du lecteur de carte

Vous pouvez rediriger les lecteurs de carte qui sont connectés à un port USB sur un canal virtuel PCoIP sur un système client Windows vers des postes de travail virtuels.

Les lecteurs de carte suivants sont pris en charge :

Tableau 4-4. Lecteurs de carte pris en charge

Périphérique	Système d'exploitation du client	Serveurs de système d'exploitation Windows	Protocole
Sony FeliCa RC-S320	Windows 10 1809 64 bits	Windows 10 1809 64 bits Windows 10 1903 64 bits	PCoIP
Sony PaSoRi RC-S380	Windows 10 1809 64 bits	Windows 10 1809 64 bits Windows 10 1903 64 bits	PCoIP

Configurer USB sur un canal virtuel PCoIP

Pour configurer l'USB sur un canal virtuel PCoIP à l'aide du port UDP 4172, modifiez le registre dans Horizon Agent :

1. Définissez le registre HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration\UsbVirtualChannelEnabled (REG_SZ) sur true.
2. Définissez le registre HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware UsbRedirection\sideChannelType (REG_SZ) sur pcoip.

3 Redémarrez la VM Horizon Agent.

Pour vérifier si la configuration est effective :

1 Connectez le poste de travail Horizon Agent avec le protocole PCoIP.

2 Vérifiez le journal d'Horizon Client dans « C:\Users\<username>\AppData\Local\Temp\vmware-<username>\vmware-UsbRedirectionClient-xxxx.log ». Si la configuration est effective, vous pouvez trouver « RPCManager::OnChannelDataObjectStateChanged(): Requesting virtual side channel » dans ce fichier.

Trafic réseau et redirection USB

Le trafic réseau entre un système client et une application ou un poste de travail distant peut prendre différents itinéraires, 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.

La redirection USB fonctionne indépendamment du protocole d'affichage et le trafic USB utilise habituellement le port TCP 32111.

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

Si le système client se trouve à l'extérieur du réseau d'entreprise, le client peut se connecter via un dispositif Unified Access Gateway. Les dispositifs Unified Access Gateway communiquent avec des instances du routeur de connexions situées derrière le pare-feu de votre entreprise et fournissent une couche supplémentaire de sécurité en protégeant les instances du routeur de connexions d'un contact direct avec l'Internet public.

Un dispositif Unified Access Gateway (méthode recommandée) ne nécessite pas l'ouverture de ports supplémentaires sur le pare-feu pour le trafic USB.

Vous pouvez configurer la fonctionnalité Kit de développement logiciel (SDK) d'amélioration USB sur session pour éviter d'ouvrir le port TCP 32111. Reportez-vous à la section Activation de la fonctionnalité Kit de développement logiciel (SDK) d'amélioration USB sur session.

Activation de la fonctionnalité Kit de développement logiciel (SDK) d'amélioration USB sur session

Grâce à la fonctionnalité Kit de développement logiciel (SDK) d'amélioration USB sur session, vous n'avez plus besoin d'ouvrir le port TCP 32111 pour le trafic USB. Cette fonctionnalité est prise en charge pour les postes de travail virtuels et publiés sur des hôtes RDS.

Pour activer la fonctionnalité Kit de développement logiciel (SDK) d'amélioration USB sur session, ouvrez l'Éditeur du Registre Windows (`regedit.exe`) sur le poste de travail distant, accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration`, puis définissez la clé `UsbVirtualChannelEnabled` sur `true`.

Lorsque cette fonctionnalité est activée, le trafic USB peut utiliser la même connexion TCP que le protocole d'affichage, ou bien utiliser une connexion TCP dédiée. La connexion que le trafic USB utilise dépend de votre configuration.

Par exemple, avec le protocole d'affichage VMware Blast, le trafic USB peut utiliser le canal VVC (VMware Virtual Channel) ou le canal côté TCP. Avec le protocole d'affichage PCoIP, le trafic USB utilise uniquement le canal côté TCP.

Par défaut, le canal côté TCP utilise le port TCP 9427. Le canal côté VVC utilise le même port que le protocole d'affichage VMware Blast.

Les compteurs USB affichés à l'aide de Perfmon sur les agents Windows sont valides si le trafic USB est configuré pour utiliser VVC.

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.

Sur les clients Windows, les fonctionnalités de connexion automatique USB, notamment les requêtes URI, les options de ligne de commande et les paramètres de stratégie de groupe, s'appliquent aux applications publiées et aux postes de travail distants.

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, 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. Parfois, 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 une application ou 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, l'application ou le poste de travail distant reçoit une entrée tactile, mais pas une entrée de clavier.

Si vous avez défini l'application ou 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.

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. Pour obtenir des instructions, reportez-vous au document *Guide d'installation et de configuration de VMware Horizon Client pour Windows*.

Déploiement de périphériques USB dans un environnement VMware Horizon 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 VMware Horizon contre cette vulnérabilité de sécurité.

En désactivant la redirection USB, vous pouvez empêcher toute redirection de périphérique USB vers les applications et les postes de travail distants 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 applications et leurs postes de travail distants.

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 VMware Horizon. 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 Console, 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 publiés. Vous ne pouvez pas définir cette stratégie pour des pools d'applications ou de postes de travail publiés individuels.
- Dans Horizon Console, après avoir défini la stratégie au niveau du pool de postes de travail ou d'applications, vous pouvez remplacer la stratégie pour 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 4-5. 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 `Exclude All Devices` dans Horizon Agent n'est pas transmise à Horizon Client, mais Horizon Agent et Horizon Client appliquent la valeur locale `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
```

Note 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 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 autorisée interdisant la redirection de tous les périphériques, mais en 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 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 *Guide d'installation et de configuration 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 4-6. 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 stratégies 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.

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. Ces paramètres de stratégie de redirection USB s'appliquent à des applications et des postes de travail publiés, ainsi qu'à des postes de travail distants qui s'exécutent sur des machines mono-utilisateur.

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 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 4-7. 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
`Allow - Override Client Setting`	Aucun ou non défini	Fractionnement automatique activé
Non défini	Non défini	Fractionnement automatique désactivé

Note 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 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 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 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 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 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 n'inclut pas automatiquement les composants que vous n'avez pas explicitement exclus. Vous devez spécifier une stratégie de filtre telle que `Include Vid/Pid Device` pour inclure ces composants.

Tableau 4-8. Modificateurs de fractionnement pour des paramètres de règle de fractionnement de périphérique sur Horizon Agent 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 4-8. 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 4-9. Exemples d'application de modificateurs de fractionnement sur des paramètres de règle de fractionnement de périphérique 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 4-9. 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`

Tableau 4-9. Exemples d'application de modificateurs de fractionnement sur des paramètres de règle de fractionnement de périphérique (suite)

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-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 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 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 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 4-10. 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 4-11. 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 4-12. 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 `Include a device by Vendor/Product ID`

2 `Include a device by USB family`

3 `Exclude a device by Vendor/Product ID`

4 `Exclude a device by USB family`

5 `Exclude all USB devices`

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.

- 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 de périphériques USB lorsque vous créez des règles de filtrage USB pour Horizon Client ou pour Horizon Agent.

Note Certains périphériques ne lisent pas certaines familles de périphériques.

Tableau 4-13. 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 périphériques de pointage.
`hid-bootable`	Périphériques d'interface humaine disponibles au démarrage, à l'exclusion des claviers et des périphériques de pointage.
`imaging`	Périphériques graphiques tels que des scanners.

Tableau 4-13. Familles de périphériques USB (suite)

Nom de la famille de périphériques	Description
keyboard	Périphérique de type clavier.
mouse	Périphérique de pointage tel qu'une souris.
other	Famille non spécifiée.
pda	Assistants numériques personnels.
physical	Périphériques à retour de force, tels que les joysticks à retour de force.
printer	Périphériques d'impression.
security	Périphériques de sécurité, tels que des lecteurs d'empreintes digitales.
smart-card	Périphériques à carte à puce.
storage	Périphériques de stockage de masse tels que des disques à mémoire flash et des disques durs externes.
unknown	Famille inconnue.
vendor	Périphériques disposant de fonctions spécifiques au fournisseur.
video	Périphériques d'entrée vidéo.
wireless	Adaptateurs réseau sans fil.
wusb	Périphériques USB sans fil.

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 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, 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.

Tableau 4-14. 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 n'est pas définie, ce qui correspond à **`false`**.
`Exclude Automatically Connection Device Family`	Empêche le transfert automatique d'une famille de périphériques. Le format du paramètre est `{m|o}:<family-name>[;...]` Définissez le modificateur de fusion (`m`) pour fusionner le paramètre client avec le paramètre agent ou le modificateur de remplacement (`o`) pour que le paramètre agent remplace le paramètre client. Par exemple : **`o:storage;hid`**
`Exclude Automatically Connection Vid/Pid Device`	Empêche le transfert automatique d'un périphérique portant des ID de fournisseur et de produit spécifiés. Le format du paramètre est `{m|o}:<vid-<xxxx>_pid-<xxxx|*>>[;...]` Définissez le modificateur de fusion (`m`) pour fusionner le paramètre client avec le paramètre agent ou le modificateur de remplacement (`o`) pour que le paramètre agent remplace le paramètre client. Par exemple : **`m:vid-0781_pid-554c;vid-0781_pid-9999`**

Tableau 4-14. Modèle de configuration d'Horizon Agent : paramètres de fractionnement de périphérique (suite)

Paramètre	Propriétés
`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 individuels 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 individuels dans un ID. Par exemple : **`o:vid-0781_pid-554c(exintf:01;exintf:02)`** **Note** Horizon n'inclut pas automatiquement les composants que vous n'avez pas explicitement exclus. Vous devez spécifier une règle de filtre telle que `Include Vid/Pid Device` pour inclure ces composants. La valeur par défaut n'est pas définie.

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 > Configuration USB de View** 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 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.

Tableau 4-15. 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 n'est pas définie, 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 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 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 individuels 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 HID Optimization Vid/Pid Device` Propriété : `HidOptIncludeVidPid`	Inclut des périphériques portant des ID de fournisseur et de produit spécifiés pouvant être optimisés. Le format du paramètre est `vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]...` Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (**`*`**) à la place de chiffres individuels dans un ID. Par exemple : **`vid-056a_pid-0302;vid-046d_pid-c628`** 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 individuels 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 4-16. 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 n'est pas définie, ce qui correspond à **`true`**.
`Allow Audio Output Devices` Propriété : `AllowAudioOut`	Permet la transmission de périphériques de sortie audio. La valeur par défaut n'est pas définie, 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 n'est pas définie, 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 n'est pas définie, ce qui correspond à **`false`**.
`Allow Smart Cards` Propriété : `AllowSmartcard`	Permet la transmission de périphériques à carte à puce. La valeur par défaut n'est pas définie, ce qui correspond à **`false`**.
`Allow Video Devices` Propriété : `AllowVideo`	Permet la transmission de périphériques vidéo. La valeur par défaut n'est pas définie, ce qui correspond à **`true`**.

Tableau 4-16. Modèle de configuration d'Horizon Agent : paramètres interprétés par un client (suite)

Paramètre	Propriétés

`Exclude Automatically Connection Device Family`	Empêche le transfert automatique des familles de périphériques.
	Utilisez la syntaxe suivante :
	`{m|o}:family-name[;...]`
	`m` indique la fusion du paramètre client avec le paramètre agent. `o` indique le remplacement du paramètre client par le paramètre agent.
	Par exemple :
	`o:storage;hid`

`Exclude Automatically Connection Vid/Pid Device`	Empêche le transfert automatique des périphériques portant des ID de fournisseur et de produit spécifiques.
	Utilisez la syntaxe suivante :
	`{m|o}:vid-xxxx_pid-xxxx|*[;...]`
	`m` indique la fusion du paramètre client avec le paramètre agent. `o` indique le remplacement du paramètre client par le paramètre agent.
	Par exemple :
	`m:vid-0781_pid-554c;vid-0781_pid-9999`

Résolution de problèmes de redirection USB

Plusieurs problèmes peuvent se produire avec la redirection USB dans Horizon.

Problème

L'USB a ses limites. Pour plus d'informations, reportez-vous à la section Limitations concernant les types de périphérique USB. Les fonctionnalités de redirection de scanner, d'audio/vidéo en temps réel, de redirection de port série et de redirection du lecteur client permettent de contourner ces limites dans la plupart des cas d'utilisation. VMware recommande l'utilisation d'une autre technologie, lorsqu'elle est disponible, car la redirection USB pour le son, les scanners, etc., peut être peu fiable en raison de la latence du réseau.

La redirection USB dans Horizon Client ne parvient pas à rendre disponibles des périphériques locaux sur l'application ou le poste de travail distant, ou certains périphériques ne semblent pas être disponibles pour la redirection dans Horizon Client.

Cause

La redirection USB peut ne pas fonctionner correctement ou comme prévu pour les raisons suivantes :

- Vérifiez que le système d'exploitation virtuel est pris en charge. Reportez-vous à la section *Exigences et considérations pour Horizon Agent* dans le document *Mises à niveau d'Horizon*.

  Note Pour les systèmes d'exploitation de serveur déployés en tant que serveurs RDSH, il existe des limitations avec les périphériques pris en charge. Les lecteurs de stockage et un ensemble limité de types de périphériques légers sont pris en charge. Par exemple, les périphériques CD-ROM ne sont pas pris en charge.

- 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 contourner ce problème, reportez-vous à la section Configuration de paramètres de règle de fractionnement de périphérique pour des périphériques USB composites.
- Par défaut, Horizon Client pour Windows ne vous permet pas de sélectionner le clavier, la souris, la carte à puce et des périphériques de sortie audio pour la redirection. Reportez-vous à la section Configuration de paramètres de règle de filtre pour des périphériques USB.
- 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.
- 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 s'afficher dans Windows Explorer et peuvent convenir à la redirection de lecteurs client.
- Le chargement des cartes flash USB formatées avec le système de fichiers FAT32 est lent. Reportez-vous à l'article de la base de connaissances La redirection d'un lecteur Flash USB peut prendre plusieurs minutes.
- 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 Console.
- Des pilotes de redirection USB sont manquants ou désactivés sur le client.

Solution

- S'il est disponible, utilisez VMware Blast ou 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 Console, accédez à **Stratégies > Stratégies générales**, et vérifiez que l'accès USB est défini sur **Autoriser** sous Afficher les stratégies.
- 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 connaître l'emplacement de ces fichiers journaux, reportez-vous à Utilisation de fichiers journaux pour le dépannage et pour déterminer les ID de périphérique USB.
- 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 contient les rubriques suivantes :

Définition de stratégies dans Horizon Console

Vous utilisez Horizon Console pour configurer des stratégies pour les sessions clientes.

Vous pouvez définir ces stratégies 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 stratégies qui affectent toutes les sessions et utilisateurs sont appelées des stratégies 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 stratégie 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.

Note Seules les stratégies générales sont disponibles pour les pools de postes de travail et d'applications publiés. Vous ne pouvez pas définir des stratégies de niveau utilisateur ou des stratégies de niveau pool pour les pools de postes de travail et d'applications publiés.

Stratégies Horizon

Vous pouvez configurer des stratégies Horizon pour affecter toutes les sessions clientes, ou vous pouvez les appliquer pour affecter des pools de postes de travail ou des utilisateurs spécifiques.

Le tableau suivant décrit chaque paramètre de stratégie d'Horizon.

Tableau 5-1. Stratégies Horizon

Stratégie	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**.

Configurer des paramètres de règle générale

Vous pouvez configurer des règles générales pour contrôler le comportement de tous les utilisateurs de sessions client.

Conditions préalables

Familiarisez-vous avec les descriptions de règles. Reportez-vous à la section Stratégies Horizon.

Procédure

1 Dans Horizon Console, sélectionnez **Paramètres > Stratégies générales**.

2 Cliquez sur **Modifier les stratégies**.

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

Utilisation de Stratégies de carte à puce

Vous pouvez utiliser des Stratégies de carte à puce pour les paramètres d'environnement utilisateur dans une application ou un poste de travail publié, ainsi que pour les paramètres

d'environnement d'ordinateur qui s'appliquent lors du démarrage de l'ordinateur ou de la reconnexion de session.

Vous pouvez créer des stratégies pour les paramètres d'environnement utilisateur qui contrôlent une gamme de comportements. Les stratégies de carte à puce Horizon pour les paramètres d'environnement utilisateur sont appliquées lors de la connexion et peuvent être actualisées lors de la reconnexion d'une session. Pour réappliquer les stratégies de carte à puce Horizon lorsqu'un utilisateur se reconnecte à une session, vous pouvez configurer une tâche déclenchée.

Vous pouvez créer des stratégies pour les paramètres d'environnement de l'ordinateur que Dynamic Environment Manager applique lorsque les ordinateurs des utilisateurs finaux démarrent. Les stratégies de carte à puce Horizon pour les paramètres d'environnement ordinateur sont appliquées lors du démarrage de l'ordinateur et peuvent être actualisées lors de la reconnexion d'une session.

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.

Pour plus d'informations sur l'utilisation de Stratégies de carte à puce pour contrôler le comportement des fonctionnalités sur un poste de travail Linux distant, reportez-vous à la section *Configuration des postes de travail Linux dans Horizon*.

Configuration requise pour les Stratégies de carte à puce

Pour utiliser des Stratégies de carte à puce, votre environnement VMware Horizon doit répondre à certaines exigences.

- Vous devez installer Horizon Agent et VMware Dynamic Environment Manager 9.0 ou version ultérieure sur les postes de travail Windows distants que vous voulez gérer avec des Stratégies de carte à puce.
- Les utilisateurs doivent utiliser Horizon Client pour se connecter à des postes de travail distants que vous gérez avec des Stratégies de carte à puce.

Installation de Dynamic 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 Dynamic Environment Manager 9.0 ou version ultérieure sur le poste de travail distant.

Vous pouvez télécharger le programme d'installation de Dynamic Environment Manager sur la page de téléchargement de VMware. Vous devez installer VMware DEM FlexEngine sur chaque poste de travail distant que vous voulez gérer avec Dynamic Environment Manager. Vous pouvez installer le composant Console de gestion Dynamic Environment Manager sur les postes de travail que vous voulez pour gérer l'environnement Dynamic Environment Manager.

Pour un pool de postes de travail RDS, vous installez Dynamic Environment Manager sur l'hôte RDS qui fournit les sessions de poste de travail publié.

Pour voir des instructions sur la configuration système requise et sur l'installation complète de Dynamic Environment Manager, consultez le document *Installation et configuration de VMware Dynamic Environment Manager*.

Configuration d'Dynamic Environment Manager

Vous devez configurer Dynamic 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 Dynamic Environment Manager, suivez les instructions de configuration dans le *Guide d'administration de VMware Dynamic Environment Manager*. Les étapes de configuration suivantes complètent les informations dans ce document.

Pour configurer Dynamic Environment Manager, suivez les instructions de configuration dans le *Guide d'administration de VMware Dynamic Environment Manager*.

- Lors de la configuration du composant client VMware DEM FlexEngine sur des postes de travail distants, créez des scripts d'ouverture et de fermeture de session FlexEngine. Pour plusieurs sessions. comme un poste de travail RDSH et une application RDSH ou une session d'application RDSH multiple pour le même utilisateur sur le même hôte RDSH, utilisez le paramètre **`-HorizonViewMultiSession -r`** pour le script d'ouverture de session. Pour le script de fermeture de session, utilisez le paramètre **`-HorizonViewMultiSession -s`**.

  Note 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 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 Dynamic 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.

  Note 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 distantes dans Dynamic Environment Manager en créant une stratégie de carte à puce Horizon.

Vous pouvez créer des stratégies pour les paramètres d'environnement utilisateur qui contrôlent une gamme de comportements. Les stratégies de carte à puce Horizon pour les paramètres d'environnement utilisateur sont appliquées lors de la connexion et peuvent être actualisées lors de la reconnexion d'une session. Pour réappliquer les stratégies de carte à puce Horizon lorsqu'un utilisateur se reconnecte à une session, vous pouvez configurer une tâche déclenchée. Reportez-vous à la liste complète des stratégies dans la rubrique « Configurer les stratégies de carte à puce Horizon pour les paramètres d'environnement utilisateur » dans le *Guide d'administration de VMware Dynamic Environment Manager*.

Vous pouvez créer des stratégies pour les paramètres d'environnement de l'ordinateur que Dynamic Environment Manager applique lorsque les ordinateurs des utilisateurs finaux démarrent. Les stratégies de carte à puce Horizon pour les paramètres d'environnement ordinateur sont appliquées lors du démarrage de l'ordinateur et peuvent être actualisées lors de la reconnexion d'une session. Reportez-vous à la liste complète des stratégies dans la rubrique « Configurer les stratégies de carte à puce Horizon pour les paramètres d'environnement de l'ordinateur » dans le *Guide d'administration de VMware Dynamic Environment Manager*.

En général, les paramètres de stratégie de carte à puce Horizon que vous configurez pour les fonctionnalités distantes dans Dynamic 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 5-2. Profils de bande passante

Profil de bande passante	Bande passante de session max. (Kbit/s)	Bande passante de session min. (Kbit/s)	Activer le développement sans perte (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	64	Oui	100	50	60	1 600	50
Réseau LAN	900 000	64	Oui	90	50	30	1 600	50
Réseau WAN dédié	900 000	64	Non	80	40	30	500	50
Réseau WAN à large bande	5 000	64	Non	70	40	20	500	50

Tableau 5-2. Profils de bande passante (suite)

Profil de bande passante	Bande passante de session max. (Kbit/s)	Bande passante de session min. (Kbit/s)	Activer le développement sans perte (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	64	Non	70	30	15	200	25
Connexion très basse vitesse	1 000	64	Non	70	30	10	90	0

Ajout de conditions aux définitions de stratégies de carte à puce Horizon

Lorsque vous définissez une stratégie de carte à puce Horizon dans Dynamic 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. Remarque : vous pouvez également activer une stratégie sans ajouter de conditions et la stratégie reste appliquée.

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 Dynamic Environment Manager, reportez-vous à la section *Guide d'administration de VMware Dynamic 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 routeur de connexions 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.

Note 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 5-3. Propriétés prédéfinies pour la condition de propriété d'Horizon Client 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 5-3. 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 définition du réseau interne et externe en configurant l'emplacement de la passerelle pour un Serveur de connexion, reportez-vous à la section Configurer l'emplacement de la passerelle pour une instance d'Horizon Connection Server dans Horizon. Pour plus d'informations sur la configuration de l'emplacement de passerelle d'un dispositif Access Point, consultez le document *Déploiement et configuration de VMware 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 routeur de connexions et à des pools de postes de travail, reportez-vous à 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. **Note** 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 Dynamic 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.

Note 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 d'administration de VMware Dynamic Environment Manager*.

Configurer l'emplacement de la passerelle pour une instance d'Horizon Connection Server dans Horizon

Par défaut, les instances d'Horizon Connection Server définissent l'emplacement de la passerelle sur `Interne`. Vous pouvez modifier l'emplacement par défaut de la passerelle en définissant la propriété `gatewayLocation` dans le fichier `locked.properties`.

L'emplacement de la passerelle détermine la valeur de clé de registre `ViewClient_Broker_GatewayLocation` dans un poste de travail distant. Vous pouvez utiliser cette valeur avec des stratégies de carte à puce pour créer une stratégie qui ne prend effet que si un utilisateur se connecte à un poste de travail distant à l'intérieur ou à l'extérieur du réseau d'entreprise. Pour plus d'informations, reportez-vous à la section Utilisation de Stratégies de carte à puce.

Procédure

1. Créez ou modifiez le fichier `locked.properties` dans le dossier de configuration de la passerelle TLS/SSL sur Horizon Connection Server.

   Par exemple : *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

   Les propriétés dans le fichier `locked.properties` sont sensibles à la casse.

2. Ajoutez la ligne suivante au fichier `locked.properties` :

   `gatewayLocation=`*`value`*

   value peut être `Externe` ou `Interne`. `Externe` indique que la passerelle est disponible pour les utilisateurs à l'extérieur du réseau d'entreprise. `Interne` indique que la passerelle est disponible pour les utilisateurs à l'intérieur du réseau d'entreprise.

   Par exemple : `gatewayLocation=External`

3. Enregistrez le fichier `locked.properties`.

4. Redémarrez le service VMware Horizon Connection Server pour que vos modifications prennent effet.

Créer une stratégie de carte à puce Horizon dans Dynamic Environment Manager

Vous utilisez la console de gestion Dynamic Environment Manager pour créer une stratégie de carte à puce Horizon dans Dynamic 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.

Conditions préalables

- Installez et configurez Dynamic Environment Manager. Reportez-vous aux sections Installation de Dynamic Environment Manager et Configuration d'Dynamic Environment Manager.
- 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.
- 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 aux définitions de stratégies de carte à puce Horizon.

Vous pouvez créer des stratégies pour les paramètres d'environnement utilisateur qui contrôlent une gamme de comportements. Les stratégies de carte à puce Horizon pour les paramètres d'environnement utilisateur sont appliquées lors de la connexion et peuvent être actualisées lors de la reconnexion d'une session. Pour réappliquer les stratégies de carte à puce Horizon lorsqu'un utilisateur se reconnecte à une session, vous pouvez configurer une tâche déclenchée.

Vous pouvez créer des stratégies pour les paramètres d'environnement de l'ordinateur que Dynamic Environment Manager applique lorsque les ordinateurs des utilisateurs finaux démarrent. Les stratégies de carte à puce Horizon pour les paramètres d'environnement ordinateur sont appliquées lors du démarrage de l'ordinateur et peuvent être actualisées lors de la reconnexion d'une session.

Pour obtenir des informations complètes sur l'utilisation de la console de gestion Dynamic Environment Manager, consultez le document *Guide d'administration de VMware Dynamic Environment Manager*.

Procédure

1 Dans la console de gestion de Dynamic Environment Manager, sélectionnez l'environnement utilisateur pour créer une stratégie pour les paramètres d'environnement utilisateur ou l'onglet **Environnement informatique** pour créer une stratégie pour les paramètres d'environnement de l'ordinateur.

   Les définitions de stratégie de carte à puce Horizon existantes, le cas échéant, apparaissent dans le volet Stratégies de carte à puce Horizon.

2 Sélectionnez **Stratégies de carte à puce Horizon** et cliquez sur **Créer** pour créer une nouvelle stratégie de carte à puce.

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.

Résultats

Dynamic 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.

Dynamic 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 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 au niveau d'un domaine pour contrôler diverses zones de l'environnement Horizon. 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 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, 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.

Note Le traitement en boucle est seulement une des approches existantes pour gérer les GPO dans Horizon. Vous devrez peut-être implémenter une approche différente.

Utilisation des fichiers de modèle d'administration de stratégie de groupe Horizon

Horizon 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 Horizon sont disponibles dans `VMware-Horizon-Extras-Bundle-YYMM-x.x.x-yyyyyyyy.zip`, où *YYMM* est la version marketing, *x.x.x* est la version interne et *yyyyyyyy* est le numéro de build. Vous pouvez télécharger le fichier sur le site de téléchargements de VMware à l'adresse https://my.vmware.com/web/vmware/downloads. Sous Informatique de bureau et d'utilisateur final, sélectionnez le téléchargement de VMware Horizon, qui comprend le bundle GPO contenant le fichier ZIP.

Les modèles de fichier ADMX d'Horizon 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

Les fichiers de modèle ADMX Horizon fournissent des paramètres de stratégie de groupe qui permettent de contrôler et d'optimiser les composants Horizon.

Les fichiers ADMX sont disponibles dans `VMware-Horizon-Extras-Bundle-YYMM-x.x.x-yyyyyyyy.zip`, que vous pouvez télécharger sur le site de téléchargements de VMware à l'adresse. Accédez à https://my.vmware.com/web/vmware/downloads. Recherchez Informatique de bureau et d'utilisateur final et, dans cette catégorie, sélectionnez Télécharger le produit sous VMware Horizon. Sélectionnez ensuite la version d'Horizon appropriée et cliquez sur **Accéder aux téléchargements**. D'ici, vous trouverez Horizon GPO Bundle qui inclut le fichier VMware-Horizon-Extras-Bundle-YYMM-x.x.x-yyyyyyyy.zip.

Tableau 5-4. Fichiers de modèle ADMX Horizon

Nom du modèle	Fichier de modèle	Description
VMware Blast	`vdm_blast.admx`	Contient des paramètres de stratégie relatifs au protocole d'affichage VMware Blast. Reportez-vous à la section Paramètres de stratégie VMware Blast.
Configuration de VMware View Agent	`vdm_agent.admx`	Contient des paramètres de stratégie liés aux composants d'authentification et d'environnement d'Horizon Agent.
Redirection du Presse-papiers	`vdm_agent_clipboard.admx`	Contient des paramètres de stratégie liés à la redirection du Presse-papiers.
Glisser-déposer	`vdm_agent_dnd.admx`	Contient des paramètres de stratégie liés à la redirection du glisser-déposer.
Configuration de VMware 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. Reportez-vous au document *Guide d'installation et de configuration de VMware Horizon Client pour Windows*.

Tableau 5-4. Fichiers de modèle ADMX Horizon (suite)

Nom du modèle	Fichier de modèle	Description
Redirection URL de VMware Horizon	`urlRedirection.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 aux documents Chapitre 3 Configuration de la redirection de contenu URL et *Guide d'installation et de configuration de VMware Horizon Client pour Windows*.
Configuration de VMware View Server	`vdm_server.admx`	Contient des paramètres de stratégie liés au Serveur de connexion. Reportez-vous au document *Administration d'Horizon*.
Configuration commune de VMware View	`vdm_common.admx`	Contient des paramètres de stratégie communs à tous les composants Horizon. Reportez-vous au document *Administration d'Horizon*.
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. Reportez-vous au document *Guide d'installation et de configuration de VMware Horizon Client pour Windows*.
VMware Integrated Printing	`printerRedirection.admx`	Contient des paramètres de stratégie liés à la fonctionnalité VMware Integrated Printing.
Afficher la configuration RTAV	`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 .
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.

Tableau 5-4. Fichiers de modèle ADMX Horizon (suite)

Nom du modèle	Fichier de modèle	Description
COM 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.
Redirection d'imprimante de VMware Horizon	`vdm_agent_printing.admx`	Contient des paramètres de stratégie liés au filtrage des imprimantes redirigées.
View Agent Direct-Connection	`view_agent_direct_connection.admx`	Contient des paramètres de stratégie liés au plug-in View Agent Direct-Connection. Consultez le document *Administration du plug-in View Agent Direct-Connection*.
VMware Horizon Performance Tracker	`vdm_agent_perfTracker.admx`	Contient des paramètres de stratégie liés à la fonctionnalité VMware Horizon Performance Tracker.
Redirection du lecteur de VMware Horizon Client	`vdm_agent_cdr.admx`	Contient des paramètres de stratégie liés à la fonctionnalité de redirection du lecteur client. Reportez-vous à la section Utiliser une stratégie de groupe pour configurer le comportement de la lettre de lecteur.

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 à des objets de stratégie de groupe (GPO) dans Active Directory.

Conditions préalables

- 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 de machine virtuelle et sur 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 postes de travail de machine virtuelle ou 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.
- Vérifiez que la fonctionnalité Gestion de stratégie de groupe est disponible sur votre serveur Active Directory.

Procédure

1 Téléchargez le fichier VMware Horizon 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, qui inclut GPO Bundle.

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

2 Décompressez le fichier `VMware-Horizon-Extras-Bundle-`*`YYMM-x.x.x-yyyyyyyy`*`.zip` et copiez les fichiers ADMX sur votre serveur Active Directory.

a Copiez les fichiers `.admx`, ainsi que le dossier `en-US` dans le dossier `%systemroot%\PolicyDefinitions` sur votre serveur Active Directory.

b Copiez les fichiers de ressources de la langue (`.adml`) dans le sous-dossier correspondant dans `%systemroot%\PolicyDefinitions\` sur votre serveur Active Directory.

3 Sur le serveur 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.

Étape suivante

Configurez les paramètres de stratégie de groupe.

Paramètres du modèle d'administration ADMX pour la configuration de VMware View Agent

Le fichier de modèle d'administration ADMX pour la configuration de VMware View 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 `VMware-Horizon-Extras-Bundle-`*`YYMM-x.x.x-yyyyyyyy`*`.zip`, que vous pouvez télécharger sur le site de téléchargements de VMware à l'adresse. Accédez à https://my.vmware.com/web/vmware/downloads. Recherchez Informatique de bureau et d'utilisateur final et, dans cette catégorie, sélectionnez Télécharger le produit sous VMware Horizon. Sélectionnez ensuite la version d'Horizon appropriée et cliquez sur **Accéder aux téléchargements**. D'ici, vous trouverez Horizon GPO Bundle qui inclut le fichier VMware-Horizon-Extras-Bundle-YYMM-x.x.x-yyyyyyyy.zip.

Les tableaux suivants décrivent les paramètres de stratégie dans le fichier de modèle d'administration ADMX pour la configuration de VMware View Agent. 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.

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

Configuration de l'agent

Les paramètres de configuration d'agent se trouvent dans le dossier **Configuration de VMware View Agent > Configuration d'agent** dans l'Éditeur de gestion de stratégie de groupe.

Tableau 5-5. Paramètres de stratégie de configuration d'agent

Filtrer Microsoft Chart and Smart Art 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 distant, vous pouvez utiliser RDP pour vous connecter à la machine virtuelle. La connexion RDP met fin à la session de poste de travail distant 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 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 est activé par défaut.

Tableau 5-5. Paramètres de stratégie de configuration d'agent (suite)

Filtrer Microsoft Chart and Smart Art Paramètre	Ordinateur	Utilisateur	Propriétés
`Audio option for single session Windows 10 physical Remote Desktop machine`	X		Spécifie le périphérique audio à utiliser sur une machine physique Horizon Windows 10 hébergeant la session de poste de travail distant. Lorsque cette option est activée, sélectionnez l'une des options suivantes : ■ Utiliser le périphérique audio attaché au point de terminaison Horizon Client. Il s'agit du paramètre par défaut. ■ Utiliser le périphérique audio attaché à un point de terminaison de poste de travail distant physique Windows 10 pour Horizon. Ce paramètre n'est pas configuré 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. Pour plus d'informations, reportez-vous à la section Exécution de commandes sur des postes de travail Horizon.
`CommandsToRunOnDisconnect`	X		Spécifie la liste des commandes ou des scripts de commande à exécuter lorsqu'une session est déconnectée. Pour plus d'informations, reportez-vous à la section Exécution de commandes sur des postes de travail Horizon.
`CommandsToRunOnReconnect`	X		Spécifie une liste de commandes ou de scripts de commande à exécuter lorsqu'une session est reconnectée après une déconnexion. Pour plus d'informations, reportez-vous à la section Exécution de commandes sur des postes de travail Horizon.
`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.
`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.

Tableau 5-5. Paramètres de stratégie de configuration d'agent (suite)

Filtrer Microsoft Chart and Smart Art Paramètre	Ordinateur	Utilisateur	Propriétés
`Disable Time Zone Synchronization`	X	X	Détermine si le fuseau horaire du poste de travail distant 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 est désactivé par défaut.
`Disconnect Session Time Limit (VDI)`	X		Spécifie la durée après laquelle une session de poste de travail déconnectée se ferme automatiquement. ■ **Jamais** : les sessions déconnectées sur cette machine ne se ferment jamais. ■ **Immédiatement** : les sessions déconnectées se ferment immédiatement. Vous pouvez également configurer la limite de temps dans le paramètre de pool de postes de travail **Fermeture de session automatique après la déconnexion** dans Horizon Console. Si vous configurez ce paramètre aux deux emplacements, le paramètre de stratégie de groupe est prioritaire. Par exemple, la sélection de l'option **Jamais** permet de ne jamais fermer une session déconnectée sur cette machine, quel que soit le paramètre dans Horizon Console.
`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. Pour obtenir la liste des systèmes d'exploitation invités pris en charge, reportez-vous à la section « Utilisation de la synchronisation DPI » du document *Guide d'installation et de configuration de VMware Horizon Client pour Windows*. Ce paramètre est activé par défaut.

Tableau 5-5. Paramètres de stratégie de configuration d'agent (suite)

Filtrer Microsoft Chart and Smart Art Paramètre	Ordinateur	Utilisateur	Propriétés
DPI Synchronization Per Monitor	X	X	Ajuste le paramètre DPI dans plusieurs moniteurs au cours d'une session distante. Lorsque ce paramètre est activé, le paramètre DPI sur tous les moniteurs change pour correspondre au paramètre DPI par moniteur client lors d'une session distante. Si le paramètre DPI est personnalisé, le paramètre DPI personnalisé est mis en correspondance. L'option **Autoriser la mise à l'échelle de l'affichage** est grisée dans Horizon Client. Lorsque ce paramètre est désactivé, les utilisateurs doivent se déconnecter et se reconnecter au poste de travail distant pour que les modifications du paramètre DPI prennent effet sur tous les moniteurs. Pour obtenir la liste des systèmes d'exploitation invités pris en charge, reportez-vous à la section « Utilisation de la synchronisation DPI » du document *Guide d'installation et de configuration de VMware Horizon Client pour Windows*. Ce paramètre est activé par défaut.
Enable Battery State Redirection	X		Détermine si la redirection de l'état de la batterie est activée. Cette fonctionnalité est prise en charge avec les systèmes clients Windows et Linux. Lorsque ce paramètre est activé, les informations sur la batterie du système client Windows ou Linux sont redirigées vers un poste de travail distant Windows. L'icône de la batterie dans la barre d'état système sur le poste de travail distant indique le pourcentage de charge de la batterie. Si la charge de la batterie est inférieure ou égale à 10 %, un message indique que la batterie est faible. Ce paramètre est activé par défaut.
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 décodées directement sur le client sur lequel elles sont lues. Vous pouvez désactiver MMR si le client ne dispose pas de ressources suffisantes pour gérer le décodage multimédia local. Ce paramètre est activé par défaut.

Tableau 5-5. Paramètres de stratégie de configuration d'agent (suite)

Filtrer Microsoft Chart and Smart Art Paramètre	Ordinateur	Utilisateur	Propriétés
Enable Unauthenticated Access	X		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 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 un utilisateur fait glisser WMP vers 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 est activé par défaut.
Idle Time Until Disconnect (VDI)	X		Spécifie la durée après laquelle une session de poste de travail distant se déconnecte en raison de l'inactivité de l'utilisateur. Si elles sont désactivées, non configurées ou activées avec le paramètre **Jamais**, les sessions de poste de travail distant ne se déconnectent jamais. Si le pool de postes de travail ou la machine sont configurés pour se déconnecter automatiquement après une déconnexion, ce paramètre est honoré.
Prewarm Session Time Limit	X		Spécifie la durée après laquelle une session de préchauffage se ferme automatiquement. Ce paramètre n'est pas configuré par défaut.
ShowDiskActivityIcon	X		Ce paramètre n'est pas pris en charge dans cette version.

Tableau 5-5. Paramètres de stratégie de configuration d'agent (suite)

Filtrer Microsoft Chart and Smart Art Paramètre	Ordinateur	Utilisateur	Propriétés
`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 est activé par défaut.
`Toggle Display Settings Control`	X		Détermine si l'onglet **Paramètres** du panneau de configuration **Affichage** est désactivé lorsqu'une session client utilise le protocole d'affichage PCoIP. Ce paramètre est activé par défaut.

Note Le paramètre `Connect using DNS Name` a été supprimé dans Horizon 6 version 6.1. Vous pouvez définir l'attribut LDAP d'Horizon 8, **pae-PreferDNS**, pour demander au Serveur de connexion 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 l'Horizon Connection Server renvoie des informations d'adresse » dans le document *Installation d'Horizon*.

Sécurité de l'agent

Le paramètre de sécurité d'agent se trouve dans le dossier **Configuration de VMware View Agent > Sécurité d'agent** dans l'Éditeur de gestion de stratégie de groupe.

Tableau 5-6. Paramètre de stratégie de sécurité d'agent

Paramètre	Ordinateur	Utilisateur	Propriétés
`Accept SSL encrypted framework channel`		X	Active le canal d'infrastructure chiffré TLS. Vous pouvez spécifier l'une des options suivantes : ■ **Désactiver** : désactivez TLS. ■ **Activer** : activez TLS. Autorisez les clients hérités à se connecter sans TLS. ■ **Appliquer** : activez TLS. Refusez les connexions des clients hérités. Ce paramètre est activé par défaut.

Redirection du Presse-papiers

Les paramètres de stratégie pour la redirection du Presse-papiers se trouvent dans le fichier de modèle ADMX `vdm_agent_clipboard.admx`. Les paramètres de redirection du Presse-papiers se trouvent dans le dossier **Configuration de VMware View Agent > Redirection du Presse-papiers** dans l'Éditeur de gestion de stratégie de groupe.

Tableau 5-7. Paramètres de stratégie de redirection du Presse-papiers

Paramètre	Ordinateur	Utilisateur	Description
`Clipboard memory size on server`	X	X	Spécifie la valeur de taille de mémoire du Presse-papiers du serveur en octets ou en kilo-octets, selon la sélection. Si elle n'est pas configurée, la taille de la mémoire est en kilo-octets. Le client a aussi une valeur pour la taille de mémoire du Presse-papiers, qui est toujours en kilo-octets. 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. 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. **Note** La taille maximale de la mémoire du Presse-papiers pour les opérations de copier-coller est de 65 535 Ko. Comme cette limite inclut les métadonnées et les données de formatage, la taille réelle des données doit être légèrement inférieure à 65 535 Ko. Pour transférer des quantités de données plus importantes, utilisez la fonctionnalité de redirection du lecteur client.
`Configure clipboard audit`	X	X	Spécifie si la fonctionnalité d'audit du Presse-papiers est activée sur la machine agent. Lorsque ce paramètre est activé, les options sont les suivantes : ■ **Désactivé dans les deux sens**. Les informations sur les données de Presse-papiers ne sont pas enregistrées. ■ **Activé uniquement du client vers le serveur**. Les informations sur les données de Presse-papiers qui sont copiées de la machine cliente vers la machine agent sont enregistrées dans un journal des événements sur la machine agent. ■ **Activé dans les deux sens**. Les informations sur les données de Presse-papiers qui sont copiées de la machine cliente vers la machine agent et de la machine agent vers la machine cliente sont enregistrées dans un journal des événements sur la machine agent. ■ **Activé uniquement du serveur vers le client**. Les informations sur les données de Presse-papiers qui sont copiées de la machine agent vers la machine cliente sont enregistrées dans un journal des événements sur la machine agent. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, la valeur par défaut est **Désactivé dans les deux sens**.

Tableau 5-7. Paramètres de stratégie de redirection du Presse-papiers (suite)

Paramètre	Ordinateur	Utilisateur	Description
			Vous pouvez utiliser l'Observateur d'événements Windows sur la machine agent pour afficher le journal des événements. Le nom de journal est VMware Horizon RX Audit. Pour afficher le journal des événements dans un emplacement centralisé, vous pouvez configurer VMware Log Insight ou le Collecteur d'événements de Windows. **Note** Seul le client Windows prend en charge l'audit de Presse-papiers entre la machine agent et la machine cliente.
`Configure clipboard redirection`	X	X	Détermine le sens dans lequel la redirection du Presse-papiers est autorisée. Vous pouvez sélectionner l'une des valeurs suivantes : ■ **Activé uniquement du client vers l'agent** ■ **Désactivé dans les deux sens** ■ **Activé dans les deux sens** ■ **Activé uniquement de l'agent vers le 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 ne s'applique qu'à Horizon Agent. Lorsque ce paramètre est désactivé ou non configuré, la valeur par défaut est **Activé uniquement de client vers agent**.

Tableau 5-7. Paramètres de stratégie de redirection du Presse-papiers (suite)

Paramètre	Ordinateur	Utilisateur	Description
`Configure clipboard redirection formats`	X	X	Détermine si un filtre est activé ou désactivé sur la machine agent pour chaque format de données. ■ **Filtrer les fichiers et les dossiers des données de Presse-papiers entrantes** : spécifie si les fichiers ou les dossiers sélectionnés peuvent être copiés dans le Presse-Papiers de la machine cliente vers la machine agent. Si ce paramètre est activé, la copie des fichiers et des dossiers depuis la machine cliente est bloquée. S'il est désactivé, la copie et le collage des fichiers et des dossiers depuis la machine cliente sont autorisés. ■ **Filtrer les fichiers et les dossiers des données de Presse-papiers sortantes** : spécifie si les fichiers ou les dossiers sélectionnés peuvent être copiés dans le Presse-Papiers de la machine agent vers la machine cliente. Si ce paramètre est activé, la copie des fichiers et des dossiers depuis la machine agent est bloquée. S'il est désactivé, la copie et le collage des fichiers et des dossiers depuis la machine agent sont autorisés. ■ **Filtrer le texte des données de Presse-papiers entrantes** : spécifie si les données textuelles sont filtrées dans les données de Presse-papiers provenant de la machine cliente vers la machine agent. Lorsque ce paramètre est activé, les données sont filtrées. Lorsque ce paramètre est désactivé, les données sont autorisées. ■ **Filtrer le texte des données de Presse-papiers sortantes** : spécifie si les données textuelles sont filtrées dans les données de Presse-papiers envoyées de la machine agent vers la machine cliente. Lorsque ce paramètre est activé, les données sont filtrées. Lorsque ce paramètre est désactivé, les données sont autorisées. ■ **Filtrer les données au format RTF des données de Presse-papiers entrantes** : spécifie si les données RTF sont filtrées dans les données de Presse-papiers provenant de la machine cliente vers la machine agent. Lorsque ce paramètre est activé, les données sont filtrées. Lorsque ce paramètre est désactivé, les données sont autorisées. ■ **Filtrer les données au format RTF des données de Presse-papiers sortantes** : spécifie si les données RTF sont filtrées dans les données de Presse-papiers envoyées de la machine agent vers la machine cliente. Lorsque ce paramètre est activé, les données sont filtrées. Lorsque ce paramètre est désactivé, les données sont autorisées.

Tableau 5-7. Paramètres de stratégie de redirection du Presse-papiers (suite)

Paramètre	Ordinateur	Utilisateur	Description
			■ **Filtrer les images des données de Presse-papiers entrantes** : spécifie si les données d'images sont filtrées dans les données de Presse-papiers provenant de la machine cliente vers la machine agent. Lorsque ce paramètre est activé, les données sont filtrées. Lorsque ce paramètre est désactivé, les données sont autorisées. ■ **Filtrer les images des données de Presse-papiers sortantes** : spécifie si les données d'images sont filtrées dans les données de Presse-papiers envoyées de la machine agent vers la machine cliente. Lorsque ce paramètre est activé, les données sont filtrées. Lorsque ce paramètre est désactivé, les données sont autorisées. ■ **Filtrer les données texte Microsoft Office des données de Presse-papiers entrantes** : spécifie si les données au format de texte Microsoft Office (format BIFF12) sont filtrées dans les données de Presse-papiers provenant de la machine cliente vers la machine agent. Lorsque ce paramètre est activé, les données sont filtrées. Lorsque ce paramètre est désactivé, les données sont autorisées. ■ **Filtrer les données de texte Microsoft Office des données de Presse-papiers sortantes** : spécifie si les données au format de texte Microsoft Office (format BIFF12) sont filtrées dans les données de Presse-papiers envoyées de la machine agent vers la machine cliente. Lorsque ce paramètre est activé, les données sont filtrées. Lorsque ce paramètre est désactivé, les données sont autorisées. ■ **Filtrer les données Microsoft Chart and Smart Art des données de Presse-papiers entrantes** : 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 la machine cliente vers la machine agent. Lorsque ce paramètre est activé, les données sont filtrées. Lorsque ce paramètre est désactivé, les données sont autorisées. ■ **Filtrer les données Microsoft Chart and Smart Art des données de Presse-papiers sortantes** : 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 la machine agent vers la machine cliente. Lorsque ce paramètre est activé, les données sont filtrées. Lorsque ce paramètre est désactivé, les données sont autorisées.

Tableau 5-7. Paramètres de stratégie de redirection du Presse-papiers (suite)

Paramètre	Ordinateur	Utilisateur	Description
			■ **Filtrer les données Microsoft Text Effects des données de Presse-papiers entrantes** : spécifie si les données d'effets de texte Microsoft Office (format HTML) sont filtrées dans les données de Presse-papiers provenant de la machine cliente vers la machine agent. Lorsque ce paramètre est activé, les données sont filtrées. Lorsque ce paramètre est désactivé, les données sont autorisées. ■ **Filtrer les données Microsoft Text Effects des données de Presse-papiers sortantes** : spécifie si les données d'effets de texte Microsoft Office (format HTML) sont filtrées dans les données de Presse-papiers envoyées de la machine agent vers la machine cliente. Lorsque ce paramètre est activé, les données sont filtrées. Lorsque ce paramètre est désactivé, les données sont autorisées. Lorsque le paramètre n'est pas configuré ou qu'il est désactivé, les filtres de redirection du Presse-papiers sont désactivés pour tous les formats. Ce paramètre n'est pas configuré par défaut.

Tableau 5-7. Paramètres de stratégie de redirection du Presse-papiers (suite)

Paramètre	Ordinateur	Utilisateur	Description
`Configure file transfer`	X		Configure le fonctionnement de la fonctionnalité de transfert de fichiers entre le poste de travail distant et HTML Access. Les valeurs valides sont les suivantes. Ce paramètre ne s'applique qu'aux postes de travail distants. ■ **Chargement et téléchargement désactivés** ■ **Chargement et téléchargement activés** ■ **Chargement de fichiers uniquement activé.** Les utilisateurs peuvent charger des fichiers depuis le système client vers le poste de travail distant. ■ **Téléchargement de fichiers uniquement activé.** Les utilisateurs peuvent télécharger des fichiers depuis le poste de travail distant vers le système client uniquement. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, la valeur par défaut est **Chargement de fichiers uniquement activé**.
`Whether block clipboard redirection to client side when client doesn't support audit`	X	X	Spécifie s'il faut bloquer la redirection du Presse-papiers vers les clients qui ne prennent pas en charge la fonctionnalité d'audit du Presse-papiers. Lorsque ce paramètre est activé, vous devez sélectionner une des valeurs suivantes. ■ **Bloquer** : bloque la redirection du Presse-papiers agent vers client si la fonctionnalité d'audit du Presse-papiers est prise en charge sur la machine agent, mais pas sur la machine cliente. ■ **Relais** : autorise la redirection du Presse-papiers agent vers client si la fonctionnalité d'audit du Presse-papiers est prise en charge sur la machine agent, mais pas sur la machine cliente. Si ce paramètre est désactivé ou n'est pas configuré, la valeur par défaut est **Bloquer**. Vous devez activer le paramètre de stratégie de groupe `Configure clipboard audit` pour que ce paramètre prenne effet.

Collaboration

Les paramètres de collaboration se trouvent dans le dossier **Configuration de VMware View Agent > Collaboration** dans l'Éditeur de gestion de stratégie de groupe.

Tableau 5-8. Paramètres de stratégie de collaboration

Paramètre	Description
`Allow control passing to collaborators`	Lorsque ce paramètre est activé, les utilisateurs peuvent transmettre le contrôle d'entrée à d'autres collaborateurs lors de la collaboration. Lorsqu'il est désactivé, le bouton bascule ne s'affiche pas dans la fenêtre de collaboration. Ce paramètre est activé par défaut.
`Allow inviting collaborators by e-mail`	Lorsque ce paramètre est activé, vous pouvez envoyer des invitations de collaboration en utilisant une application de messagerie installée. Lorsqu'il est désactivé, vous ne pouvez pas utiliser un e-mail pour inviter des collaborateurs, même si une application de messagerie est installée. Ce paramètre est activé par défaut.
`Allow inviting collaborators by IM`	Lorsque ce paramètre est activé, vous pouvez envoyer des invitations de collaboration en utilisant une application de messagerie instantanée installée. Lorsqu'il est désactivé, vous ne pouvez pas utiliser une messagerie instantanée pour inviter des collaborateurs, même si une application de messagerie instantanée est installée. Ce paramètre est activé par défaut.
`Include Outlook-formatted URL in clipboard text`	Lorsque ce paramètre est activé, une URL d'invitation au format Microsoft Outlook est incluse dans le texte d'invitation du Presse-papiers. Activez ce paramètre si vous vous attendez à ce que les utilisateurs finaux collent le texte d'invitation du Presse-papiers dans un message électronique. Ce paramètre est désactivé par défaut.
`Separator used for multiple e-mail addresses in mailto: links`	Configure le séparateur utilisé pour plusieurs adresses électroniques dans les liens mailto: afin de permettre une meilleure compatibilité avec différents clients de messagerie. Lorsque ce paramètre n'est pas configuré, la valeur par défaut est un point-virgule sans espace pour séparer les adresses électroniques. Si votre client de messagerie par défaut n'autorise pas le point-virgule comme séparateur, essayez d'autres combinaisons, par exemple une virgule et un espace ou un point-virgule et un espace.
`Server URLs to include in invitation message`	Définit les URL de serveurs à inclure dans les invitations de collaboration. Si ce paramètre n'est pas configuré, une URL par défaut est utilisée. Toutefois, elle peut être incorrecte dans tous les déploiements, sauf les plus simples.
`Turn off collaboration`	Lorsque ce paramètre est activé, la fonctionnalité de collaboration de session est désactivée. Lorsque ce paramètre est désactivé ou non configuré, vous pouvez contrôler la fonctionnalité au niveau de la batterie de serveurs ou du pool de postes de travail. Ce paramètre prend effet après le redémarrage des machines Horizon Agent.
`Maximum number of invited collaborators`	Spécifie le nombre maximal de collaborateurs que vous pouvez inviter à rejoindre une session. La valeur par défaut maximale est de 5. La limite est de 20.

Glisser-déposer

Les paramètres de stratégie pour le glisser-déposer se trouvent dans le fichier de modèle ADMX `vdm_agent_dnd.admx`. Les paramètres du glisser-déposer se trouvent dans le dossier **Configuration de VMware View Agent > Glisser-déposer** dans l'Éditeur de gestion de stratégie de groupe.

Tableau 5-9. Paramètres de stratégie du glisser-déposer

Paramètre	Description
`Configure drag and drop direction`	Spécifie le sens dans lequel le glisser-déposer est autorisé. Lorsqu'il est activé, les options sont les suivantes : ■ **Désactivé dans les deux sens** ■ **Activé uniquement du client vers l'agent**. Permet le glisser-déposer uniquement du système client vers l'agent. ■ **Activé uniquement de l'agent vers le client**. Permet le glisser-déposer uniquement de l'agent vers le système client. ■ **Activé dans les deux sens** Lorsque ce paramètre est désactivé ou non configuré, la valeur par défaut est **Activé uniquement de client vers agent**. Ce paramètre ne s'applique qu'à l'agent.
`Configure drag and drop formats`	Détermine le sens du glisser-déposer (**Désactivé dans les deux sens**, **Activé uniquement de l'agent vers le client**, **Activé uniquement du client vers l'agent** ou **Activé dans les deux sens**) qui est autorisé pour chaque format de données. Lorsque ce paramètre est activé, les options sont les suivantes : ■ **Option pour le format de fichier** : ■ **Option pour le format de texte** : ■ **Option pour le format RTF** : ■ **Option pour le format d'image** : ■ **Option pour le format HTML** : ■ **Option pour le format de contenu de fichier** : Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, la valeur par défaut pour tous les formats est **Activé dans les deux sens**. Ce paramètre ne s'applique qu'à l'agent.
`Configure drag and drop size threshold`	Détermine la limite de taille pour le glissement des types de données communs autres que des fichiers et des dossiers. Lorsque ce paramètre est activé, sélectionnez l'unité de la taille des données glissées dans le menu déroulant **Choisir l'unité de la taille du glisser-déposer**. Vous pouvez sélectionner **Octets**, **Kilo-octets** ou **Mégaoctets**. Sélectionnez ou entrez la taille des données glissées dans la zone de texte **Seuil de taille du glisser-déposer**. La plage de données effective de chaque unité est la suivante : ■ **Octets** : entre 1 et 1 023 ■ **Kilo-octets** : entre 1 et 1 023 ■ **Mégaoctets** : entre 1 et 16 (la taille de données maximale du glisser-déposer est de 16 mégaoctets) Si ce paramètre est désactivé ou n'est pas configuré, un seuil par défaut de 1 mégaoctet est défini. Ce paramètre ne s'applique qu'à l'agent.

Performance Tracker

Les paramètres de stratégie pour Performance Tracker se trouvent dans le fichier de modèle ADMX `vdm_agent_perfTracker.admx`. Les paramètres de Performance Tracker se trouvent dans le dossier **Configuration de VMware View Agent > Performance Tracker** dans l'Éditeur de gestion de stratégie de groupe.

Tableau 5-10. Paramètres de stratégie de Performance Tracker

Paramètre	Description
Activer le démarrage automatique d'Horizon Performance Tracker dans une connexion de poste de travail distant	Lorsqu'il est activé, Horizon Performance Tracker démarre automatiquement lorsqu'un utilisateur ouvre une session sur un poste de travail distant. Pour effacer ce paramètre de GPO de préférence, sélectionnez **Désactiver**.
Activer le démarrage automatique d'Horizon Performance Tracker dans une connexion d'application distante	Lorsqu'il est activé, Horizon Performance Tracker démarre automatiquement lorsqu'un utilisateur ouvre une session sur une application distante. Pour effacer ce paramètre de GPO de préférence, sélectionnez **Désactiver**.
Paramètre basique de Performance Tracker	Lorsqu'il est activé, vous pouvez définir la fréquence en secondes à laquelle Horizon Performance Tracker collecte des données.

Redirection de scanner

Les paramètres de stratégie pour la redirection de scanner se trouvent dans le fichier de modèle ADMX `vdm_agent_scanner.admx`. Les paramètres de redirection de scanner se trouvent dans le dossier **Configuration de VMware View Agent > Redirection de scanner** dans l'Éditeur de gestion de stratégie de groupe.

Tableau 5-11. Paramètres de stratégie de groupe de redirection de scanner

Paramètre	Ordinateur	Utilisateur	Description
`BandwidthLimit`		X	Spécifie la bande passante maximale autorisée, en kilo-octets par seconde, pour le transfert des données analysées vers une session utilisateur. Si vous spécifiez 0 ou si vous ne spécifiez aucune valeur, la bande passante est illimitée.
`Compression`		X	Spécifie le taux de compression d'image à utiliser pendant le transfert d'images vers un poste de travail distant ou une application publiée. Vous pouvez sélectionner l'un des modes de compression suivants : ■ **Désactiver** : la compression d'images 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. Vous sélectionnez le niveau de qualité d'image dans le menu déroulant **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. 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.
`Default Color Mode`			Lorsque ce paramètre est activé, vous pouvez configurer le mode de couleur par défaut : noir et blanc, nuances de gris ou couleur. Ce paramètre est pris en charge sous Windows XP Professionnel ou Windows Server 2003 ou version ultérieure.
`Default Duplex`			Lorsque ce paramètre est activé, vous pouvez configurer le mode de numérisation par défaut : recto ou recto verso. En mode recto verso, l'application d'analyse doit prendre en charge la numérisation recto verso et demander deux pages depuis le scanner. Ce paramètre est pris en charge sous Windows XP Professionnel ou Windows Server 2003 ou version ultérieure.

Tableau 5-11. Paramètres de stratégie de groupe de redirection de scanner (suite)

Paramètre	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 pouvez sélectionner l'une des 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.
`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.
`Force the TWAIN Scanning Properties dialog`		X	Lorsque ce paramètre est activé, la boîte de dialogue Propriétés d'analyse TWAIN s'affiche toujours, même lorsqu'une application d'analyse n'affiche pas la boîte de dialogue d'analyse.

Tableau 5-11. Paramètres de stratégie de groupe de redirection de scanner (suite)

Paramètre	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.

Tableau 5-11. Paramètres de stratégie de groupe de redirection de scanner (suite)

Paramètre	Ordinateur	Utilisateur	Description
`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.
`TWAIN Scanner Properties dialog location`		X	Indique l'emplacement d'affichage de la boîte de dialogue Propriétés d'analyse TWAIN. Vous pouvez sélectionner l'une des options suivantes : ■ **Agent** : la boîte de dialogue Propriétés du scanner VMware s'affiche du côté agent. ■ **Client** : la boîte de dialogue TWAIN du scanner du fournisseur natif s'affiche du côté client. (Cette option n'est pas prise en charge pour le client Linux.)

COM série

Les paramètres de stratégie pour COM série se trouvent dans le fichier de modèle ADMX `vdm_agent_serialport.admx`. Les paramètres COM série se trouvent dans le dossier **Configuration de VMware View Agent > COM série** dans l'Éditeur de gestion de stratégie de groupe.

Tableau 5-12. Paramètres de stratégie de COM série

Paramètre	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 **Numéro du port source** spécifie le numéro du port COM physique connecté au système client.
			■ Le paramètre **Numéro du port virtuel de destination** spécifie le numéro du port COM virtuel redirigé sur le poste de travail distant.
			■ Le paramètre **Se connecter automatiquement** 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 avant l'envoi des données (en millisecondes)** 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 ont besoin de ce retard pour conserver les données transmises. 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 **Désactiver les erreurs dans le masque d'attente** désactive la valeur d'erreur dans le masque de port COM. Ce paramètre de dépannage est requis pour certaines applications. Pour plus d'informations, reportez-vous à la documentation Microsoft pour la fonction `WaitCommEvent` sur 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.
			■ Le paramètre **Permanent** conserve l'état du port COM redirigé dans la session distante, même si le client se déconnecte.

Tableau 5-12. Paramètres de stratégie de COM série (suite)

Paramètre	Ordinateur	Utilisateur	Description
			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 définir le port pour qu'il soit redirigé automatiquement lorsqu'ils se connectent au poste de travail distant, et ils ne peuvent pas ignorer le signal DSR. Ces propriétés sont contrôlées par le paramètre de stratégie de groupe. **Note** 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. 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.
`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.

Tableau 5-12. Paramètres de stratégie de COM série (suite)

Paramètre	Ordinateur	Utilisateur	Description
`COM Port Isolation Mode`	X		Spécifie le mode d'isolation des ports COM. Lorsque vous activez ce paramètre, vous pouvez sélectionner l'un des modes d'isolation suivants : ■ **Isolation complète** : les ports série virtuels sont visibles et accessibles uniquement dans les sessions utilisateur. Les noms de ports COM peuvent être identiques dans des sessions utilisateur différentes. Les services système, tels que `spoolsrv.exe`, ne peuvent pas accéder aux ports série isolés dans ce mode. ■ **Isolation désactivée** : les ports série virtuels sont visibles globalement. N'importe quel port est accessible à partir de n'importe quelle session. Les ports ne pouvant pas porter le même nom dans différentes sessions utilisateur, les noms de ports doivent être uniques pour chaque utilisateur. Les services système, tels que `spoolsrv.exe`, peuvent accéder à n'importe quel port série. Si ce paramètre n'est pas configuré, la redirection du port série fonctionne en mode **Isolation complète**.
`Connect all ports automatically`	X		Lorsque vous activez ce paramètre, tous les ports COM sont connectés automatiquement, même si aucun paramètre de stratégie de groupe individuel n'est activé. Si des paramètres de stratégie de groupe individuel sont configurés pour des ports spécifiques, les paramètres de stratégie de groupe individuel sont utilisés. Si ce paramètre est désactivé ou s'il n'est pas configuré, la fonctionnalité de connexion automatique est déterminée par les paramètres de stratégie de groupe de port individuel ou par des paramètres de programme locaux. Ce paramètre n'est pas configuré par défaut.
`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.

Tableau 5-12. Paramètres de stratégie de COM série (suite)

Paramètre	Ordinateur	Utilisateur	Description
`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.
`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.

Paramètres de redirection de carte à puce

Les paramètres de redirection de carte à puce se trouvent dans le dossier **Configuration de VMware View Agent > Redirection de carte à puce > Accès au lecteur local** dans l'Éditeur de gestion de stratégie de groupe.

Tableau 5-13. Paramètres de stratégie de redirection de carte à puce

Paramètre	Ordinateur	Utilisateur	Propriétés
`Allow applications access to Local Smart Card readers`	X		Lorsque ce paramètre est activé, les applications peuvent accéder à tous les lecteurs de carte à puce locaux même si la fonctionnalité de redirection de carte à puce est installée. Lorsque ce paramètre est activé, le poste de travail est surveillé pour détecter la présence d'un lecteur local. Lorsqu'un lecteur local est détecté, la redirection de carte à puce désactive l'autorisation d'accès aux lecteurs locaux. La redirection reste désactivée jusqu'à ce qu'un utilisateur se connecte de nouveau à la session. Lorsque l'accès local est activé, les applications ne peuvent plus accéder aux lecteurs distants présents sur le client. Ce paramètre ne s'applique pas à RDP ou aux hôtes RDS lorsque le rôle Services Bureau à distance est activé. Ce paramètre est désactivé par défaut.
`Local Reader Name`	X		Spécifie le nom d'un lecteur local à surveiller pour activer l'accès local. Par défaut, la carte doit être insérée dans le lecteur pour activer l'accès local. Vous pouvez désactiver cette exigence en utilisant le paramètre `Require an inserted Smart Card`. Ce paramètre est activé par défaut.
`Require an inserted Smart Card`	X		Si ce paramètre est activé, l'accès au lecteur local n'est activé que si une carte est insérée dans le lecteur local. Si ce paramètre est désactivé, l'accès local est activé tant qu'un lecteur local est détecté. Ce paramètre est activé par défaut.

Paramètres de configuration de l'authentification unique réelle

Les paramètres de configuration de l'authentification unique réelle se trouvent dans le dossier **Configuration de VMware View Agent > Configuration de l'authentification unique réelle** dans l'éditeur de gestion de stratégie de groupe. Reportez-vous au document *Administration d'Horizon*.

Paramètres d'Unity Touch et des applications hébergées

Les paramètres d'Unity Touch et des applications hébergées se trouvent dans le dossier **Configuration de VMware View Agent > Unity Touch et applications hébergées** dans l'Éditeur de gestion de stratégie de groupe.

Tableau 5-14. Paramètres de stratégie d'Unity Touch et des applications hébergées

Paramètre	Ordinateur	Utilisateur	Propriétés
`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 est désactivé par défaut.
`Enable UWP support on RDSH platforms`	X		Lorsque ce paramètre est activé, les applications de la plate-forme Windows (UWP) peuvent s'exécuter sur des hôtes WVD (Virtual Desktop) Windows 10 sur Horizon Cloud Service sur Azure. Lorsqu'il est désactivé, l'état de l'application indique non disponible dans Horizon Agent et l'utilisateur ne peut pas accéder à l'application. Redémarrez la VM agent pour que ce paramètre prenne effet. 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 publiées dans Horizon Client et permet aux utilisateurs d'appareils mobiles d'accéder aux applications dans la barre latérale Unity Touch. 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 publiées. Ce paramètre est activé par défaut.
`Enable user profile customization for Hosted Apps`	X	X	Spécifie s'il faut personnaliser le profil d'utilisateur lorsque des applications publiées 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 est désactivé par défaut.
`Only launch new instances of Hosted Apps if arguments are different`	X		Cette stratégie contrôle le comportement lorsqu'une application publiée est démarrée, mais qu'une instance existante de l'application est déjà en cours d'exécution dans une session de protocole déconnectée. Lorsque ce paramètre est désactivé, l'instance existante de l'application s'active. Lorsqu'il est activé, l'instance existante interne de l'application ne s'active que si les paramètres de ligne de commande correspondent. Ce paramètre est désactivé par défaut.

Tableau 5-14. Paramètres de stratégie d'Unity Touch et des applications hébergées (suite)

Paramètre	Ordinateur	Utilisateur	Propriétés
`Limit usage of Windows hooks`	X		Désactive la plupart des hooks lorsque des applications publiées 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 est désactivé par défaut, ce qui signifie que tous les hooks préférés sont utilisés.
`Unity Filter rule list`	X		Spécifie des règles de filtre pour des fenêtres Unity lorsque des applications publiées sont utilisées. Horizon Agent utilise ces règles pour prendre en charge les applications personnalisées. Pour plus d'informations sur la création de règles de filtrage, reportez-vous à la section Gestion des fenêtres Unity spéciales. Ce paramètre n'est pas configuré par défaut.

Configuration de View Agent Direct-Connection

Les paramètres de stratégie pour la configuration de View Agent Direct-Connection se trouvent dans le fichier de modèle ADMX `vdm_agent_direct_connection.admx`. Les paramètres de configuration de View Agent Direct-Connection se trouvent dans le dossier **Configuration de VMware View Agent > Configuration de View Agent Direct-Connection** dans l'éditeur de gestion de stratégie de groupe. Consultez le document *Administration du plug-in View Agent Direct-Connection*.

Configuration de l'Audio/Vidéo en temps réel

Les paramètres de stratégie pour la configuration de l'Audio/Vidéo en temps réel se trouvent dans le fichier de modèle ADMX `vdm_agent_rtav.admx`. Les paramètres de configuration RTAV se trouvent dans le dossier **Configuration de VMware View Agent > Afficher la configuration RTAV** dans l'Éditeur de gestion de stratégie de groupe. Reportez-vous à la section Paramètres de stratégie de groupe de l'Audio/Vidéo en temps réel .

Configuration USB

Les paramètres de configuration USB se trouvent dans le dossier **Configuration de VMware View Agent > Configuration USB de View** dans l'Éditeur de gestion de stratégie de groupe. Reportez-vous à la section Utilisation de stratégies pour contrôler la redirection USB.

Configuration de VMware AppTap

Le paramètre de configuration de VMware AppTap se trouve dans le dossier **Configuration de VMware View Agent > Configuration de VMware AppTap** dans l'Éditeur de gestion de stratégie de groupe.

Tableau 5-15. Paramètre de configuration de VMware AppTap

Paramètre	Ordinateur	Utilisateur	Propriétés
`Processes to ignore when detecting empty application sessions`	X		Spécifie la liste des processus à ignorer lors de la détection des sessions d'application vides. Vous pouvez spécifier un nom de fichier de processus ou un chemin d'accès complet. Les valeurs ne sont pas sensibles à la casse. N'utilisez pas de variables d'environnement dans les chemins d'accès. Les chemins d'accès réseau UNC sont autorisés, par exemple : `\\vmware\temp\app.exe`. Ce paramètre n'est pas configuré par défaut.

Redirection du lecteur client

Les paramètres de stratégie pour la redirection du lecteur client se trouvent dans le fichier de modèle ADMX `vdm_agent_cdr.admx`. Les paramètres de redirection du lecteur client se trouvent dans le dossier **Configuration de VMware View Agent > Redirection du lecteur de VMware Horizon Client** dans l'Éditeur de gestion de stratégie de groupe. Reportez-vous à la section Paramètres de stratégie de redirection du lecteur client.

Fonctionnalités HTML5 de VMware

Les fonctionnalités HTML5 de VMware comportent les paramètres Redirection de navigateur, Redirection de géolocalisation, Redirection multimédia HTML5 et Redirection de WebRTC. Les paramètres de stratégie pour ces fonctionnalités se trouvent dans le dossier **Configuration de VMware View Agent > Fonctionnalités HTML5 de VMware** dans l'Éditeur de gestion de stratégie de groupe. Reportez-vous à la section Paramètres de stratégie de fonctionnalité HTML5 de VMware.

VMware Integrated Printing

Les paramètres de stratégie pour VMware Integrated Printing se trouvent dans le fichier de modèle ADMX `printerRedirection.admx`. Les paramètres de VMware Integrated Printing se trouvent dans le dossier **Configuration de VMware View Agent > VMware Integrated Printing** dans l'Éditeur de gestion de stratégie de groupe. Reportez-vous à la section Paramètres de stratégie de VMware Integrated Printing.

Pack de virtualisation VMware pour Skype Entreprise

Les paramètres de Pack de virtualisation VMware pour Skype Entreprise se trouvent dans le dossier **Configuration de VMware View Agent > Pack de virtualisation VMware pour Skype Entreprise** dans l'Éditeur de gestion de stratégie de groupe. Reportez-vous à la section Paramètres de la stratégie Pack de virtualisation VMware pour Skype Entreprise.

Configuration de filigrane

Les paramètres de configuration du filigrane se trouvent dans le dossier **Configuration utilisateur** situé dans le dossier **Configuration utilisateur > Stratégies > Modèles d'administration > Configuration de VMware View Agent > Filigrane** dans l'Éditeur de gestion de stratégie de groupe.

Tableau 5-16. Paramètre de configuration de filigrane

Paramètre	Ordinateur	Utilisateur	Propriétés

`Watermark Configuration`		X	Ce paramètre permet de configurer un filigrane afin qu'il s'affiche sur votre poste de travail virtuel. Entrez les informations que vous souhaitez afficher en filigrane dans la section **Texte**. Les options sont les suivantes :
			`%ViewClient_IP_Address%`
			`%ViewClient_Broker_UserName%`
			`%ViewClient_Broker_DomainName%`
			`%COMPUTERNAME%`
			`%USERDOMAIN%`
			`%USERNAME%`
			`%ViewClient_ConnectTime%`
			La limite de caractères est de 256 caractères et de 1 024 caractères après l'extension.
			Disposition de l'image : la disposition du filigrane à l'écran, qui est divisée en neuf carrés :
			■ Vignette : le filigrane est placé dans les 9 carrés. Cette disposition est toujours utilisée pour les sessions d'application.
			■ Multiple : le filigrane est placé dans les carrés au centre et aux quatre coins. Si la taille du filigrane dépasse la taille de la case, elle est mise à l'échelle pour conserver les proportions.
			■ Centre : le filigrane est placé dans le carré central.
			Rotation du texte : angle spécifique du texte du filigrane.
			Opacité : niveau de transparence du texte. La plage est comprise entre 0 et 255. La valeur par défaut est 255.
			Marge : espace autour du filigrane pour la disposition de vignette. Si le filigrane est mis à l'échelle, la marge l'est également.
			Ce paramètre n'est pas configuré par défaut.

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.

Note Les informations sur le système client sont transmises au poste de travail de second saut lors de la connexion de protocole initiale. 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 la section Exécution de commandes sur des postes de travail Horizon.

Tableau 5-17. Informations sur le système client 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 5-17. 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
`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

Tableau 5-17. 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_Machine_Domain`	Domaine du système client.	Oui	VDI (machine mono-utilisateur) RDS	Windows
`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 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.
`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
`ViewClient_Broker_DNS_Name`	Nom DNS de l'instance du Serveur de connexion.		VDI (machine mono-utilisateur) RDS	La valeur est envoyée directement depuis le Serveur de connexion, elle n'est pas recueillie par Horizon Client.
`ViewClient_Broker_URL`	URL de l'instance du Serveur de connexion.		VDI (machine mono-utilisateur) RDS	La valeur est envoyée directement depuis le Serveur de connexion, elle n'est pas recueillie par Horizon Client.

Tableau 5-17. 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_Tunneled`	État de la connexion du tunnel du Serveur de connexion qui peut être `true` (activé) ou `false` (désactivé).		VDI (machine mono-utilisateur) RDS	La valeur est envoyée directement depuis le Serveur de connexion, elle n'est pas recueillie par Horizon Client.
`ViewClient_Broker_Tunnel_URL`	URL de la connexion du tunnel du Serveur de connexion, si elle est activée.		VDI (machine mono-utilisateur) RDS	La valeur est envoyée directement depuis le Serveur de connexion, elle n'est pas recueillie par Horizon Client.
`ViewClient_Broker_Remote_IP_Address`	Adresse IP du système client qui est vue par l'instance du Serveur de connexion.		VDI (machine mono-utilisateur) RDS	La valeur est envoyée directement depuis le Serveur de connexion, elle n'est pas recueillie par Horizon Client.
`ViewClient_Broker_Request_Path`	Toutes les adresses IP, à partir de l'adresse IP publique du système client qui est visible par l'instance du Serveur de connexion.		VDI (machine mono-utilisateur) RDS	La valeur est envoyée directement depuis le Serveur de connexion, 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

Tableau 5-17. 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_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
`ViewClient_Broker_DomainName`	Nom de domaine utilisé pour s'authentifier auprès du Serveur de connexion.		VDI (machine mono-utilisateur) RDS	La valeur est envoyée directement depuis le Serveur de connexion, elle n'est pas recueillie par Horizon Client.
`ViewClient_Broker_UserName`	Nom d'utilisateur utilisé pour s'authentifier auprès du Serveur de connexion.		VDI (machine mono-utilisateur) RDS	La valeur est envoyée directement depuis le Serveur de connexion, 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
`ViewClient_Displays.Number`	Spécifie le nombre de moniteurs utilisés actuellement par le client.		VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac, Android, iOS
`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
`ViewClient_Keyboard.Type`	Spécifie le type de clavier utilisé actuellement par le client. Par exemple : japonais, coréen.		VDI (machine mono-utilisateur) RDS	Windows

Tableau 5-17. 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_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 depuis le Serveur de connexion, 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
ViewClient_Language	Spécifie la langue du système d'exploitation.		VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac, Android, iOS
ViewClient_Launch_Matched_Tags	Spécifie une ou plusieurs balises.		VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac, Android, iOS
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
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

Note Les définitions de `ViewClient_LoggedOn_Username` et de `ViewClient_LoggedOn_Domainname` dans Tableau 5-17. Informations sur le système client s'appliquent à Horizon Client pour Windows.

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 de redirection du lecteur client

Le fichier de modèle d'administration ADMX de redirection du lecteur de VMware Horizon Client (`vdm_agent_cdr.admx`) contient des paramètres de stratégie liés à la fonctionnalité de redirection du lecteur client.

Les paramètres de redirection du lecteur client se trouvent dans le dossier **Configuration de VMware View Agent > Redirection du lecteur de VMware Horizon Client** dans l'Éditeur de gestion de stratégie de groupe.

Tableau 5-18. Paramètres de redirection du lecteur client

Paramètre	Ordinateur	Utilisateur	Propriétés
`Configure drive letter mapping mode`	X		Spécifie le mode de mappage des lettres de lecteur. Lorsque ce paramètre est activé, vous pouvez sélectionner une des valeurs suivantes : ■ **Mappage un à un**, qui mappe la lettre de lecteur sur la machine cliente à la même lettre de lecteur sur la machine agent. Par exemple, le lecteur X sur la machine cliente est mappé au lecteur X sur la machine agent. ■ **Mappage défini**, qui mappe des lettres de lecteur sur la machine cliente à certaines lettres de lecteur sur la machine agent en fonction d'un tableau de mappage défini dans le paramètre de stratégie de groupe **Définir la table de mappage de lettre de lecteur**. En cas de conflit de lettre de lecteur, par exemple, si une lettre de lecteur à mapper est déjà utilisée sur la machine de l'agent, la première lettre de lecteur disponible de Z à A est utilisée. Si aucune lettre de lecteur n'est disponible, aucune lettre de lecteur n'est attribuée. Ce paramètre est valide uniquement lorsque le paramètre de stratégie de groupe **Afficher le périphérique redirigé avec la lettre de lecteur** n'est pas désactivé.
`Define drive letter mapping table`	X		Lorsque ce paramètre est activé, vous pouvez cliquer sur **Afficher** et définir une table de mappage des lettres de lecteur. Dans la colonne **Nom de la valeur**, entrez la lettre du lecteur sur la machine cliente. Dans la colonne **Valeur** correspondante, entrez la lettre de lecteur à utiliser sur la machine agent. Ce paramètre est valide uniquement lorsque vous sélectionnez **Mappage défini** dans le paramètre de stratégie de groupe **Configurer le mode de mappage de lettre de lecteur**.
`Display redirected device with drive letter`	X		Détermine s'il convient d'afficher une lettre de lecteur pour les lecteurs qui sont redirigés à l'aide de la fonctionnalité de redirection du lecteur client. Ce paramètre est activé par défaut.
`Timeout for drive letter initialization`	X		Spécifie le délai d'attente, en millisecondes, pour que l'Explorateur Windows initialise et affiche une lettre de lecteur pour les lecteurs qui sont redirigés à l'aide de la fonctionnalité de redirection du lecteur client. Si ce paramètre est désactivé ou n'est pas configuré, la valeur par défaut est de 5 000 millisecondes.

Paramètres de stratégie pour filtrer des périphériques clients

Les paramètres de filtrage des périphériques pour la redirection du lecteur client se trouvent dans le dossier **Configuration de VMware View Agent > Redirection du lecteur de VMware Horizon Client > Filtrage des périphériques** dans l'Éditeur de gestion de stratégie de groupe.

La fonctionnalité de filtrage des périphériques fonctionne uniquement dans Horizon Client pour Windows, Mac et Linux. Lorsque ces stratégies de filtrage de périphérique sont définies, la redirection du lecteur client est désactivée pour les autres clients, y compris Horizon Client pour Android et iOS.

Tableau 5-19. Paramètres de filtrage des périphériques

Paramètre	Ordinateur	Utilisateur	Propriétés
`Exclude Vid/Pid Device`	X		Exclut les périphériques qui ont un ID de fournisseur et un ID de produit spécifiés de la redirection avec la fonctionnalité de redirection du lecteur client. Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (*) à la place de chiffres individuels dans un ID. Utilisez un point-virgule pour séparer plusieurs périphériques. Par exemple : `vid-0781_pid-554c;vid-0781_pid-****` La valeur par défaut n'est pas définie (aucun périphérique n'est exclu). Ce paramètre est prioritaire sur le paramètre **Inclure un périphérique Vid/Pid**. **Note** Pour désactiver la redirection du lecteur client pour tous les périphériques, vous pouvez spécifier `vid-****_pid-****`.
`Include Vid/Pid Device`	X		Spécifie les périphériques avec un ID de fournisseur et un ID de produit spécifiés pouvant être redirigés avec la fonctionnalité de redirection du lecteur client. Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (*) à la place de chiffres individuels dans un ID. Utilisez un point-virgule pour séparer plusieurs périphériques. Par exemple : `vid-054C_pid-0099;vid-8888_pid-****` La valeur par défaut n'est pas définie (tous les périphériques sont inclus).

Paramètres de stratégie de fonctionnalité HTML5 de VMware

Le fichier de modèle ADMX pour la configuration de VMware View Agent (`vdm_agent.admx`) contient des paramètres de stratégie liés aux fonctionnalités HTML5.

Paramètres généraux de la fonctionnalité VMware HTML5

Les paramètres généraux de la fonctionnalité VMware HTML5 se trouvent dans l'Éditeur de gestion de stratégie de groupe, dans le dossier **Configuration ordinateur > Modèles d'administration > Configuration de VMware View Agent > Fonctionnalités HTML5 VMware**.

Tableau 5-20. Paramètres généraux de la fonctionnalité VMware HTML5

Paramètre	Description
`Enable VMware HTML5 Features`	Active les fonctionnalités VMware HTML5. Vous devez activer ce paramètre pour utiliser la fonctionnalité de redirection multimédia HTML5 de VMware, de redirection de géolocalisation ou de redirection de navigateur. Ce paramètre prend effet lors de la prochaine connexion.
`Disable Automatically Detect Intranet`	Lorsque la stratégie est activée, les paramètres d'intranet « Inclure tous les sites locaux (intranet) non mentionnés dans d'autres zones » et « Inclure tous les sites qui n'utilisent pas de serveur proxy » sont désactivés lors de la prochaine connexion. Lorsque cette stratégie est désactivée, aucune modification n'est apportée à la zone Intranet local d'Internet Explorer. **Important** Vous devez activer ce paramètre si vous activez le navigateur Edge pour la fonctionnalité de redirection multimédia HTML5 ou activez la fonctionnalité de redirection de géolocalisation.

Paramètres de la fonctionnalité de redirection multimédia HTML5 VMware

Les paramètres de la fonctionnalité de redirection multimédia HTML5 de VMware figurent dans l'Éditeur de gestion de stratégie de groupe, dans le dossier **Configuration ordinateur > Modèles d'administration > Configuration de VMware View Agent > Fonctionnalités HTML5 de VMware > Redirection de multimédia HTML5 de VMware**.

Tableau 5-21. Paramètres de stratégie de redirection multimédia HTML5 de VMware

Paramètre	Description
`Enable VMware HTML5 Multimedia Redirection`	Permet d'activer la fonctionnalité de redirection multimédia HTML5 de VMware. Ce paramètre prend effet lors de la prochaine connexion.
`Enable URL list for VMware HTML5 Multimedia Redirection`	Permet de spécifier les sites Web qui utilisent la fonctionnalité de redirection multimédia HTML5. Entrez la liste d'URL des sites Web qui peuvent rediriger du contenu multimédia HTML5 dans la colonne Nom de valeur. Incluez le préfixe `http://` ou `https://` dans les URL. Vous pouvez utiliser des modèles de correspondance dans les URL. Par exemple, pour rediriger toutes les vidéos sur YouTube, entrez `https://www.youtube.com/*`. Pour rediriger toutes les vidéos sur Vimeo, entrez `https://www.vimeo.com/*`. Laissez vide la colonne Valeur.

Tableau 5-21. Paramètres de stratégie de redirection multimédia HTML5 de VMware (suite)

Paramètre	Description
`Enable Chrome Browser for VMware HTML5 Multimedia Redirection`	Cette stratégie n'est utilisée que lorsque la fonctionnalité de redirection multimédia HTML5 de VMware est activée. Si cette stratégie n'est pas configurée, la valeur par défaut est identique à la valeur du paramètre Activer la redirection multimédia HTML5 de VMware.
`Enable Edge Browser for VMware HTML5 Multimedia Redirection`	Cette stratégie n'est utilisée que lorsque la fonctionnalité de redirection multimédia HTML5 de VMware est activée. Si cette stratégie n'est pas configurée, la valeur par défaut est identique à la valeur du paramètre Activer la redirection multimédia HTML5 de VMware.

Paramètres de la fonctionnalité de redirection de géolocalisation VMware

Les paramètres de la fonctionnalité de redirection de géolocalisation VMware figurent dans l'Éditeur de gestion de stratégie de groupe, dans le dossier **Configuration ordinateur > Modèles d'administration > Configuration de VMware View Agent > Fonctionnalités HTML5 de VMware > Redirection de géolocalisation VMware**.

Tableau 5-22. Paramètres de redirection de géolocalisation VMware

Paramètre	Description
`Enable VMware Geolocation Redirection`	Active la fonctionnalité Redirection de géolocalisation. Ce paramètre prend effet lors de la prochaine connexion.
`Enable URL list for VMware Geolocation Redirection`	Spécifie quels sites Web utilisent la fonctionnalité de redirection de géolocalisation. Entrez la liste d'URL des sites Web qui peuvent rediriger les informations de géolocalisation dans la colonne Nom de valeur. Incluez le préfixe `http://` ou `https://` dans les URL. Vous pouvez utiliser des modèles de correspondance dans les URL. Par exemple, pour spécifier toutes les vidéos YouTube, entrez `https://www.youtube.com/*`. Pour spécifier toutes les vidéos Vimeo, entrez `https://www.vimeo.com/*`. Laissez vide la colonne Valeur.
`Set the minimum distance for which to report location updates`	Spécifie la distance minimale, en mètres, entre une mise à jour d'emplacement dans le client et la dernière mise à jour signalée à l'agent, dont le nouvel emplacement doit être signalé à l'agent. Par défaut, la distance minimale utilisée est de 75 mètres.

Paramètres de la fonctionnalité Redirection de VMware Browser

Les paramètres de la fonctionnalité Redirection de VMware Browser figurent dans l'Éditeur de gestion de stratégie de groupe, dans le dossier **Configuration ordinateur > Modèles d'administration > Configuration de VMware View Agent > Fonctionnalités HTML5 de VMware > Redirection de VMware Browser**.

Tableau 5-23. Paramètres de Redirection de VMware Browser

Paramètre	Description
`Enable VMware Browser Redirection`	Permet la fonctionnalité de redirection de navigateur.
`Enable URL list for VMware Browser Redirection`	Spécifie toutes les URL de la fonctionnalité de redirection de navigateur. Les utilisateurs peuvent accéder à ces URL en les entrant dans la barre d'adresse Chrome ou dans la barre d'adresse personnalisée. Ils peuvent également consulter ces URL en y accédant à partir d'une autre URL de la liste ou à partir de toute page rendue du côté agent. Entrez les URL dans la colonne Nom de la valeur. Incluez le préfixe `http://` ou `https://` dans les URL. Vous pouvez utiliser des modèles de correspondance dans les URL. Les modèles de correspondance doivent suivre https://developer.chrome.com/extensions/match_patterns. Par exemple, pour spécifier l'intégralité du contenu YouTube, entrez `https://www.youtube.com/*`. Laissez vide la colonne Valeur.
`Enable Navigation URL list for VMware Browser Redirection`	Spécifie les URL auxquelles un utilisateur est autorisé à accéder à partir d'une URL spécifiée dans la liste verte **Activer la liste d'URL pour la redirection de VMware Browser**, soit en entrant l'URL directement dans la barre d'adresse personnalisée, soit en accédant à l'URL à partir d'une URL dans la liste verte. Les utilisateurs ne peuvent pas accéder directement à ces URL en les tapant dans la barre d'adresse Chrome ou en y accédant à partir d'une page rendue du côté agent. Entrez la liste des URL dans la colonne Nom de la valeur. Incluez le préfixe `http://` ou `https://` dans les URL. Vous pouvez utiliser des modèles de correspondance dans les URL. Les modèles de correspondance doivent suivre https://developer.chrome.com/extensions/match_patterns. Par exemple, pour spécifier l'intégralité du contenu YouTube, entrez `https://www.youtube.com/*`. Laissez vide la colonne Valeur.

Tableau 5-23. Paramètres de Redirection de VMware Browser (suite)

Paramètre	Description
`Enable automatic fallback after a whitelist violation`	Lorsque ce paramètre est activé, si un utilisateur accède à une URL qui n'est pas spécifiée dans l'une des listes vertes de redirection de navigateur, en l'entrant dans la barre d'adresse personnalisée ou en y accédant à partir d'une URL dans une liste verte, la redirection s'arrête pour cet onglet et l'URL est extraite et affichée plutôt sur l'agent. **Note** Si un utilisateur tente d'accéder à une URL qui n'est pas spécifiée dans le paramètre **Activer la liste d'URL pour la redirection de VMware Browser**, l'onglet revient toujours à l'extraction et au rendu de l'URL sur l'agent, que ce paramètre soit ou non activé.
`Show a page with error information before automatic fallback`	Lorsque ce paramètre est activé et qu'une violation de la liste verte se produit, une page s'affiche et indique un compte à rebours de cinq secondes. Lorsque la période de cinq secondes s'est écoulée, l'onglet revient à l'extraction et au rendu de l'URL qui a provoqué la violation sur l'agent. Si ce paramètre est désactivé, la page d'avertissement de cinq secondes ne s'affiche pas. Ce paramètre ne prend effet que si le paramètre **Activer le secours automatique après une violation de la liste blanche** est également activé.

Paramètres des fonctionnalités de redirection de VMware WebRTC

Les paramètres généraux de la fonctionnalité HTML5 de VMware figurent dans l'éditeur de gestion des règles de groupe, dans le dossier **Configuration ordinateur > Modèles d'administration > Configuration de VMware View Agent > Fonctionnalités HTML5 de VMware > Fonctionnalités de redirection de VMware WebRTC**.

Tableau 5-24. Paramètres des fonctionnalités de redirection de VMware WebRTC

Paramètre	Description
`Enable software acoustic echo cancellation for Media Optimization for Microsoft Teams`	Cette stratégie active ou désactive l'annulation de l'écho acoustique dans le logiciel, indépendamment de la disponibilité d'annulation de l'écho acoustique dans le matériel. Si la stratégie n'est pas configurée, l'annulation de l'écho acoustique est activée dans le logiciel dès lors qu'elle n'est pas disponible dans le matériel.
`Enable sharing the client desktop screen while remoting the Microsoft Teams application in application sharing mode`	Si vous activez cette stratégie, lorsque vous utilisez la fonctionnalité de partage d'écran dans Microsoft Teams sur un poste de travail distant, la fonctionnalité de partage d'écran partagera l'écran du poste de travail client au lieu de l'écran du poste de travail distant. Désactivez la stratégie pour désactiver la fonctionnalité de partage d'écran en mode de partage d'applications. Si la stratégie n'est pas configurée, le partage d'écran partagera l'écran du poste de travail client par défaut.
`Enable Media Optimization for Microsoft Teams`	Activez cette stratégie pour appliquer l'optimisation du milieu pour Microsoft Teams. Si la stratégie n'est pas configurée, elle est désactivée.

Paramètres de la stratégie Pack de virtualisation VMware pour Skype Entreprise

Le fichier de modèle d'administration ADMX pour la configuration de VMware View Agent (`vdm_agent.admx`) contient des paramètres de stratégie liés au pack de virtualisation VMware pour Skype Entreprise.

Ces paramètres se trouvent dans l'Éditeur de gestion de stratégie de groupe dans le dossier **Configuration ordinateur > Modèles d'administration > Configuration de VMware View Agent > Pack de virtualisation VMware pour Skype Entreprise**.

Tableau 5-25. Paramètres de la stratégie Pack de virtualisation pour Skype Entreprise

Paramètre	Description
`Disable extended filter for acoustic echo cancellation in VMware Virtualization Pack for Skype for Business`	Activé par défaut, le filtre étendu pour l'annulation de l'écho acoustique fournit une meilleure annulation de l'écho et du retour et est particulièrement efficace dans les scénarios où le microphone et le haut-parleur du système Horizon Client sont proches l'un de l'autre. Activez cette stratégie si vous ne souhaitez pas que le Pack de virtualisation VMware pour Skype Entreprise utilise ce filtre.
`EnableDetectProxySettings`	Activez cette stratégie pour réduire les retards lorsque le système Horizon Client doit utiliser un serveur proxy. Lorsqu'il est activé, le Pack de virtualisation pour Skype Entreprise vérifie les paramètres de proxy sur le système Horizon Client et utilise ces paramètres pour le trafic des supports. Si les paramètres de proxy sont absents du système Horizon Client, le Pack de virtualisation pour Skype Entreprise utilise une connexion directe.

Tableau 5-25. Paramètres de la stratégie Pack de virtualisation pour Skype Entreprise (suite)

Paramètre	Description
`Force Skype for Business in non-optimized mode`	Vous pouvez forcer Skype Entreprise à s'exécuter en mode non optimisé pour les connexions d'Horizon Client en détectant automatiquement les connexions externes qui sont déterminées lorsque Horizon Client se connecte à une passerelle externe. Dans ce scénario, la variable d'environnement ViewClient_Broker_GatewayType est présente et ViewClient_Broker_GatewayLocation est définie sur Externe. Si vous cochez la case permettant de détecter automatiquement les connexions externes, le Pack de virtualisation pour Skype Entreprise revient au mode de secours si la connexion est déterminée comme étant externe. Vous pouvez également forcer Skype Entreprise à s'exécuter en mode non optimisé pour les connexions d'Horizon Client en définissant le nom de la variable d'environnement qui est présente lors de la connexion à la machine sur laquelle Horizon Agent est installé. Si le nom de la variable est défini, le pack de virtualisation pour Skype Entreprise repasse en mode de secours. Par exemple, si la variable d'environnement ViewClient_F5_APM est définie sur la machine agent de poste de travail distant lorsque la machine Horizon Client se connecte depuis l'extérieur du réseau à l'aide de l'équilibrage de charge F5 et que vous voulez forcer le mode non optimisé, définissez cette valeur sur ViewClient_F5_APM. Cette stratégie n'est pas configurée par défaut.
`Show Icon`	Affiche l'icône du pack de virtualisation VMware pour Skype Entreprise. Cette stratégie est activée par défaut. L'icône ne s'affiche pas si la stratégie Afficher l'icône est désactivée pour le pack de virtualisation pour Skype Entreprise. Lorsqu'il est désactivé, vous ne pouvez pas afficher les statistiques d'appel ou les messages.
`Show Messages`	Affiche les messages du pack de virtualisation VMware pour Skype Entreprise. Cette stratégie est activée par défaut. Les messages ne s'affichent pas si les stratégies Afficher l'icône et Afficher les messages sont désactivées pour le pack de virtualisation VMware pour Skype Entreprise.
`Suppress minor version mismatch warning`	La zone de notification affiche un avertissement si le Pack de virtualisation pour Skype Entreprise n'a pas la même version mineure de l'API sur le système Horizon Client et sur le poste de travail Horizon. Lorsque cette stratégie est activée, l'avertissement est supprimé. Notez que s'il existe une discordance de version mineure de l'API, les appels Skype Entreprise sont optimisés, mais le Pack de virtualisation ne dispose pas nécessairement des dernières fonctionnalités.

Paramètres de stratégie de VMware Integrated Printing

Le fichier de modèle ADMX de VMware Integrated Printing (`printerRedirection.admx`) contient des paramètres de stratégie relatifs à la fonctionnalité VMware Integrated Printing.

Ces paramètres se trouvent dans l'Éditeur de gestion de stratégie de groupe dans le dossier **Configuration ordinateur > Modèles d'administration > VMware Integrated Printing** et également dans le dossier **Configuration utilisateur > Stratégies > Modèles d'administration > Configuration de VMware View Agent > VMware Integrated Printing**. Si le paramètre Configuration utilisateur est activé, il remplace le paramètre Configuration ordinateur équivalent. Si le paramètre Configuration utilisateur n'est pas activé, le paramètre Configuration ordinateur est utilisé.

Tableau 5-26. Paramètres de stratégie de VMware Integrated Printing

Paramètre	Description
`Disable LBP`	Spécifie si l'impression basée sur l'emplacement est activée. Lorsque ce paramètre est activé, l'impression basée sur l'emplacement est désactivée. Si ce paramètre est désactivé ou s'il n'est pas configuré, l'impression basée sur l'emplacement est activée.
`Disable Printer Property Persistence`	Détermine si les propriétés de l'imprimante sont persistantes. Lorsque ce paramètre est activé, les propriétés de l'imprimante ne sont pas persistantes entre l'imprimante cliente locale et l'imprimante redirigée. Si ce paramètre est désactivé ou s'il n'est pas configuré, les propriétés de l'imprimante sont persistantes entre l'imprimante locale du client et l'imprimante redirigée. Ce paramètre n'est pas configuré par défaut.
`Disable printer redirection for non-desktop client`	Détermine si la fonctionnalité VMware Integrated Printing est prise en charge par les points de terminaison du client externe au poste de travail. Lorsque ce paramètre est activé, la fonctionnalité VMware Integrated Printing n'est pas prise en charge par les points de terminaison du client externe au poste de travail. Si ce paramètre n'est pas configuré ou s'il est désactivé, la fonctionnalité VMware Integrated Printing est prise en charge par les points de terminaison du client externe au poste de travail. Ce paramètre n'est pas configuré par défaut.
`Do not change default printer`	Détermine si VMware Integrated Printing modifie l'imprimante par défaut dans les sessions distantes. Par défaut, si une imprimante basée sur l'emplacement est configurée comme imprimante par défaut, elle est définie comme telle dans les sessions distantes. Si aucune imprimante basée sur l'emplacement n'est configurée comme imprimante par défaut, l'imprimante cliente par défaut est définie comme imprimante par défaut dans les sessions distantes et remplace toute imprimante sélectionnée dans l'image de la VM. Vous pouvez utiliser ce paramètre pour modifier ce comportement. Si vous activez ce paramètre, VMware Integrated Printing ne modifie pas l'imprimante par défaut dans les sessions distantes. Si vous désactivez ou ne configurez pas ce paramètre, VMware Integrated Printing modifie l'imprimante par défaut dans les sessions distantes. Il s'agit du comportement par défaut. Ce paramètre n'est pas configuré par défaut.

Tableau 5-26. Paramètres de stratégie de VMware Integrated Printing (suite)

Paramètre	Description
`Do not redirect client printer(s)`	Détermine si les imprimantes clientes sont redirigées. Lorsque ce paramètre est activé, aucune imprimante cliente n'est redirigée. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, toutes les imprimantes clientes sont redirigées. Ce paramètre n'est pas configuré par défaut. Les modifications apportées à ce paramètre ne prennent pas effet tant que l'utilisateur ne s'est pas déconnecté, puis reconnecté au poste de travail distant.
`Limit Tx Rate (KBps)`	Limite le taux de transmission en kilo-octets par seconde (Kbit/s) de toutes les tâches d'impression. Le débit de transmission minimal autorisé est de 200 Kbits/s. Le débit de transmission maximal autorisé est de 4 000 Kbits/s. Lorsque ce paramètre n'est pas configuré, désactivé ou réglé sur un débit de transmission supérieur au maximum (4 000 Kbits/s), le débit de transmission n'est pas limité. Ce paramètre n'est pas configuré par défaut.
`Print Preview Setting`	Configure le comportement de l'aperçu avant impression. L'option **Désactiver les choix d'impression** détermine si la cible d'impression est activée. Lorsque ce paramètre est sélectionné, les utilisateurs ne peuvent pas sélectionner la cible d'impression. Si ce paramètre n'est pas sélectionné ou s'il n'est pas configuré, les utilisateurs peuvent sélectionner la cible d'impression, qui peut être affichée dans un aperçu avant impression ou imprimée directement. Il n'est pas configuré par défaut. L'option **Choix par défaut de la cible d'impression** spécifie la cible d'impression par défaut. Vous pouvez sélectionner l'une des options suivantes : ■ **Imprimer directement** : l'option d'impression par défaut dans l'interface utilisateur d'impression est d'imprimer directement. ■ **Aperçu avant impression** : l'option d'impression par défaut dans l'interface utilisateur d'impression est l'aperçu avant impression.
`Printer Driver Selection`	Spécifie le pilote d'imprimante à utiliser pour les imprimantes clientes redirigées. Lorsque ce paramètre est activé, les options sont les suivantes : ■ **Toujours utiliser NPD** utilise le pilote d'imprimante natif pour l'imprimante redirigée. ■ **Toujours utiliser UPD** utilise le pilote d'imprimante universel pour l'imprimante redirigée. ■ **Utiliser d'abord NPD, puis UPD** utilise d'abord le pilote d'imprimante natif et, si l'imprimante native n'existe pas, utilise le pilote d'imprimante universel. ■ **Utiliser d'abord UPD, puis NPD** utilise d'abord le pilote d'imprimante natif et, si le pilote d'imprimante universel n'existe pas, utilise le pilote d'imprimante natif. Si ce paramètre est désactivé ou s'il n'est pas configuré, la valeur par défaut est **Utiliser d'abord NPD, puis UPD**.

Tableau 5-26. Paramètres de stratégie de VMware Integrated Printing (suite)

Paramètre	Description
`Printer Name Schema`	Détermine la convention de dénomination des imprimantes lorsque vous utilisez VMware Integrated Printing. Lorsque ce paramètre est activé, vous pouvez modifier le schéma de nom d'imprimante utilisé pour les postes de travail virtuels, les postes de travail publiés et les applications publiées. Le schéma de nom d'imprimante doit être au format « `%P (*)` », où `*` représente la partie configurable du nom de l'imprimante. Vous pouvez spécifier les variables suivantes : ■ `%S` : ID de session ■ `%C` : nom de la machine cliente Si ce paramètre est activé, mais que le schéma de nom d'imprimante est vide ou non valide, le schéma de nom d'imprimante par défaut est utilisé. Lorsque ce paramètre n'est pas configuré ou qu'il est désactivé, les postes de travail virtuels utilisent le schéma de nom d'imprimante « `%P (vdi)` ». Les postes de travail publiés et les applications publiées utilisent le schéma de nom d'imprimante « `%P (v%S)` ». Ce paramètre n'est pas configuré par défaut.

`Specify a filter in redirecting client printers`	Spécifie une règle qui filtre les imprimantes clientes à partir de la redirection d'imprimante. Lorsque ce paramètre est activé, vous pouvez entrer une règle de filtrage dans la zone de texte **Filtre d'imprimante**. La règle de filtrage est une expression régulière qui spécifie les imprimantes qui ne sont pas redirigées (une liste de refus). Les imprimantes qui ne correspondent pas aux imprimantes inscrites dans cette règle de filtrage sont redirigées.
	Les attributs, les opérateurs et les caractères génériques suivants sont pris en charge dans la règle de filtrage :
	■ Attributs : NomPilote, NomFournisseur et NomImprimante
	■ Opérateurs : AND, OR et NOT
	■ Caractères génériques : * et ?
	Voici des exemples de règles de filtrage.
	`(DriverName="DrName1" OR VendorName="VeName1") AND NOT PrinterName="PrNa.?e"`
	`PrinterName=".*HP.*" OR PrinterName=".*EPSON.*" AND DriverName="PDF"`
	`PrinterName!=".*PDFCreator.*"`
	Note La règle de filtrage n'est pas sensible à la casse. Pour utiliser une correspondance exacte, utilisez une expression régulière, telle que « `^HP$` » plutôt que « `HP` ».
	Par défaut, la règle de filtrage est vide, ce qui signifie que toutes les imprimantes clientes sont redirigées.

Paramètres de stratégie PCoIP

Le fichier de modèle d'administration ADMX PCoIP (`pcoip.admx`) contient des paramètres de stratégie liés au protocole d'affichage PCoIP. 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 `VMware-Horizon-Extras-Bundle-YYMM-x.x.x-yyyyyyyy.zip`, que vous pouvez télécharger sur le site de téléchargements de VMware à l'adresse. Accédez à https://my.vmware.com/web/vmware/downloads. Recherchez Informatique de bureau et d'utilisateur final et, dans cette catégorie, sélectionnez Télécharger le produit sous VMware Horizon. Sélectionnez ensuite la version d'Horizon appropriée et cliquez sur **Accéder aux téléchargements**. D'ici, vous trouverez Horizon GPO Bundle qui inclut le fichier VMware-Horizon-Extras-Bundle-YYMM-x.x.x-yyyyyyyy.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 5-27. 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.

Tableau 5-27. Paramètres de stratégie généraux PCoIP (suite)

Paramètre	Description
`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 5-27. 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.

Tableau 5-27. Paramètres de stratégie généraux PCoIP (suite)

Paramètre	Description
`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.
`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 5-27. 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.

Tableau 5-27. Paramètres de stratégie généraux PCoIP (suite)

Paramètre	Description
	Par défaut, tous les périphériques sont autorisés et aucun n'est interdit.
`Configure PCoIP virtual channels`	Spécifie les canaux virtuels qui peuvent et ne peuvent pas fonctionner sur des sessions 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. Par défaut, tous les canaux virtuels sont activés.

Tableau 5-27. Paramètres de stratégie généraux PCoIP (suite)

Paramètre	Description
`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 5-27. 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 de ports TCP détermine le nombre de ports supplémentaires à essayer si le port de base n'est pas disponible. La plage de ports 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 de ports. 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 de poste de travail distant 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.

Tableau 5-27. Paramètres de stratégie généraux PCoIP (suite)

Paramètre	Description
`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 de ports 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 de ports. 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 de poste de travail distant 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 5-27. 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 ou qu'il n'est pas configuré, la synchronisation est autorisée. Lorsque ce paramètre est désactivé, la synchronisation n'est pas autorisée. Ce paramètre s'applique à Horizon Agent uniquement.

Tableau 5-27. 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.
`Configure SSL cipher list`	Configure une liste de chiffrements SSL pour limiter l'utilisation des suites de chiffrement avant l'établissement d'une connexion SSL chiffrée. La liste se compose d'une ou de plusieurs chaînes de la suite de chiffrement séparées par deux points. Toutes les chaînes de suite de chiffrement sont insensibles à la casse. La valeur par défaut est ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:@STRENGTH. Si ce paramètre est configuré, la case **Appliquer des chiffrements AES-256 ou plus forts pour la négociation de connexion SSL** dans le paramètre **Configurer des connexions SSL pour satisfaire les outils de sécurité** est ignorée. Ce paramètre doit être appliqué sur le serveur PCoIP et sur le client PCoIP.

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 5-28. 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.

Tableau 5-28. Variables de bande passante de la session PCoIP d'Horizon (suite)

Paramètre	Description
	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.
`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 5-28. 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.

Tableau 5-28. Variables de bande passante de la session PCoIP d'Horizon (suite)

Paramètre	Description
	Pour plus d'informations sur la fonction de développement sans perte PCoIP, reportez-vous à la section Fonction de développement sans perte PCoIP.

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 5-29. 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.

Paramètres de stratégie VMware Blast

Le fichier de modèle ADMX de VMware Blast (`vdm_blast.admx`) contient des paramètres de stratégie pour le protocole d'affichage VMware Blast. Après l'application de la stratégie, le système stocke les paramètres dans la clé de Registre `HKLM\Software\Policies\VMware, Inc.\VMware Blast\Config`.

Ces paramètres s'appliquent à HTML Access et à toutes les plates-formes Horizon Client.

Tableau 5-30. Paramètres de stratégie VMware Blast

Paramètre	Description
`Audio playback`	Spécifie si la lecture audio est activée pour les postes de travail distants. Ce paramètre permet d'activer la lecture audio.
`Blast Codec Quality`	Les valeurs minimales et maximales du paramètre de quantification (QP) contrôlent la qualité d'image de l'affichage distant lors de l'utilisation de la compression de codecs Blast. La plage de valeurs de QP [1-8] est grossièrement mappée à la valeur de qualité JPEG dans la plage [20-88]. Cette quantification s'applique à des régions non textuelles et n'a aucune incidence sur la compression de texte. Le paramètre QP maximal est mappé à la configuration de qualité JPEG faible et la valeur zéro pour le paramètre QP maximal entraîne le remplacement de la configuration par la configuration de qualité JPEG faible. Le paramètre QP minimal est mappé à la configuration de qualité JPEG élevée et la valeur zéro pour le paramètre QP minimal entraîne le remplacement de la configuration par la configuration de qualité JPEG élevée.

Tableau 5-30. Paramètres de stratégie VMware Blast (suite)

Paramètre	Description
`Blast Encoders Global Quality`	Ce paramètre contrôle le niveau de qualité de l'image d'affichage distant sur tous les codeurs Blast. ■ Le niveau sélectionné est mappé sur tous les codecs, ce qui met à jour la valeur QP maximale pour H.264, la valeur QP maximale pour le code Blast et la qualité JPEG faible dans le codeur adaptatif en fonction de la valeur sélectionnée. ■ Le niveau de qualité global de l'encodeur prend des valeurs comprises entre 1 et 5. Une valeur inférieure reflète une qualité inférieure, tandis qu'une valeur supérieure reflète une qualité supérieure. Plus le niveau de qualité est élevé, plus la bande passante utilisée est importante et plus la latence est potentiellement grande lorsque les régions de l'écran changent souvent, par exemple lors du défilement de l'écran. La valeur par défaut est de 1 (équilibré). Le mappage de qualité peut être remplacé par les valeurs QP des codeurs correspondants.
`Blast Optimizer`	Configuration unique permettant aux utilisateurs Blast de choisir entre les valeurs par défaut qui améliorent l'expérience utilisateur ou l'efficacité des ressources. ■ Valeur de 5 (par défaut) : utilise les paramètres par défaut de Blast. ■ Valeur supérieure à 5 : améliore l'expérience utilisateur en augmentant les valeurs par défaut de Blast pour encoderGlobalQualityLevel, la pente de la bande passante et la valeur maxFPS du codeur. ■ Valeur inférieure à 5 : améliore l'efficacité des ressources en diminuant les valeurs par défaut de Blast pour encoderGlobalQualityLevel, la pente de la bande passante et la valeur maxFPS du codeur.
`Cookie Cleanup Interval`	Détermine la fréquence, en millisecondes, à laquelle le système supprime les cookies associés aux sessions inactives. La valeur par défaut est de 100 ms.
`Cursor warping`	Lorsque ce paramètre est activé, la fonctionnalité de distorsion du curseur est activée. Lorsque cette option est activée et que la souris est en mode absolu, l'agent distant détecte les mouvements de curseur soudains et les répercute sur le client en déplaçant le curseur local. Si ce paramètre n'est pas activé, le client ignore les mouvements brusques du curseur dans l'agent distant. Ce paramètre est désactivé par défaut.

Tableau 5-30. Paramètres de stratégie VMware Blast (suite)

Paramètre	Description
DSCP Marking	Lorsqu'il est activé ou qu'il n'est pas configuré, ce paramètre permet d'établir des valeurs DSCP (Differentiated Services Code Point) dans le trafic réseau Blast sortant, tel que spécifié par les divers paramètres spécifiques de chaque tronçon de réseau. Lorsqu'elles sont désactivées, les valeurs DSCP ne sont pas établies dans le trafic réseau Blast. Lorsque cette option est activée, vous pouvez définir une valeur numérique comprise entre 0 et 63 pour les connexions réseau suivantes : ■ DSCP from Agent, TCP/IPv4 ■ DSCP from Agent, TCP/IPv6 ■ DSCP from Agent, UDP/IPv4 ■ DSCP from Agent, UDP/IPv6 ■ DSCP from BSG to Client, TCP/IPv4 ■ DSCP from BSG to Client, TCP/IPv6 ■ DSCP from BSG to Client, UDP/IPv4 ■ DSCP from BSG to Client, UDP/IPv6 ■ DSCP from BSG to Agent, TCP/IPv4 ■ DSCP from BSG to Agent, TCP/IPv6 ■ DSCP from BSG to Agent, UDP/IPv4 ■ DSCP from BSG to Agent, UDP/IPv6 ■ DSCP from Client, TCP/IPv4 ■ DSCP from Client, TCP/IPv6 ■ DSCP from Client, UDP/IPv4 ■ DSCP from Client, UDP/IPv6
Encoder Image Cache Size (KB)	Taille maximale du cache d'images du codeur. ■ La taille finale du cache est la plus petite de la valeur définie ici et la configuration associée du client. ■ La taille finale du cache ne peut pas dépasser la moitié de la mémoire RAM disponible sur Horizon Agent.
H264	Spécifie si vous voulez utiliser le codage H.264 ou JPEG/PNG. L'option par défaut est d'utiliser le codage H.264.
H264 High Color Accuracy	La précision de la couleur augmente avec le codage H.264 en utilisant l'espace de couleur YUV 4:4:4 plutôt que 4:2:0. Cela peut entraîner une dégradation des performances à des résolutions très élevées ou avec plusieurs moniteurs.
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 avec 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 QP (Quantization Parameter) à plus ou moins 5 de la plage de valeurs disponible. Comme ces paramètres déterminent la quantité de données ignorées, une valeur inférieure entraîne une qualité d'image supérieure.

Tableau 5-30. Paramètres de stratégie VMware Blast (suite)

Paramètre	Description
HEVC High Color Accuracy	Activez ce paramètre pour demander une meilleure précision de couleur en utilisant l'espace de couleur YUV 4:4:4 au lieu de 4:2:0 avec le codage HEVC. Le client requiert la prise en charge du matériel HEVC 4:4:4 pour que cette stratégie soit appliquée. Ce paramètre est activé par défaut.
HEVC	Activez ou ne configurez pas ce paramètre afin d'autoriser le codage HEVC pour accéder à distance au poste de travail. Désactivez ce paramètre pour utiliser H.264 ou JPEG/PNG pour le codage.
HTTP Service	Spécifie le port utilisé pour la communication sécurisée (HTTPS) entre le 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.
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 : ■ **Faible qualité JPEG** (plage de valeurs disponible : 10 à 100, valeur par défaut : 25) ■ **Moyenne qualité JPEG** (plage de valeurs disponible : 10 à 100, valeur par défaut : 35) ■ **Haute qualité JPEG** (plage de valeurs disponible : 10 à 100, valeur par défaut : 90)
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 se produit. Ce paramètre s'applique uniquement à Horizon Agent.
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.
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.
Max Session Bandwidth kbit/s Megapixel Slope	Spécifie la pente de bande passante maximale, en kilobits par seconde (Kbits/s), 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.
Min Session Bandwidth	Spécifie la bande passante minimale, en kilobits par seconde (Kbits/s), réservée pour une session VMware Blast. La valeur par défaut est de 256 Kbits/s.
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.

Tableau 5-30. Paramètres de stratégie VMware Blast (suite)

Paramètre	Description
`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.
`UDP Protocol`	Spécifie si vous voulez utiliser le protocole UDP ou TCP. Le protocole UDP est utilisé par défaut. Le paramètre est appliqué lorsqu'un utilisateur effectue une connexion-déconnexion de session sur 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.

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 Frame Rate`
- `Image Quality`

Les paramètres **Bande passante max. de session** et **Bande passante min. de session** s'appliquent lorsqu'un utilisateur se connecte à une session sur la machine Horizon Agent sur laquelle le paramètre existe. Toute modification apportée à ces paramètres peut ne pas s'appliquer entièrement sur une session déjà connectée. Bien que les nouveaux paramètres puissent s'appliquer pour limiter l'utilisation de la bande passante du codeur dans la session actuelle, ils ne le sont pas sur les canaux virtuels, tels que le transfert de fichiers, tant que la session ne se reconnecte pas.

Pour toutes les autres stratégies VMware Blast, les règles de mise à jour de stratégies de groupe Microsoft s'appliquent. Les objets de stratégie 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.

Note 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.

Gestion des fenêtres Unity spéciales

Vous pouvez utiliser le paramètre de stratégie de groupe d'agent **Liste des règles de filtre Unity** pour filtrer des fenêtres Unity ou pour mapper des fenêtres Unity à un type spécifique, lors de l'utilisation d'applications publiées. Cette fonctionnalité est utile si vous avez un problème d'affichage de fenêtre, comme une fenêtre avec un fond d'écran noir ou une fenêtre déroulante qui n'est pas correctement dimensionnée.

Le paramètre de stratégie de groupe **Liste des règles de filtre Unity** est fourni dans le fichier de modèle ADMX pour la configuration de VMware View Agent (`vdm_agent.admx`), qui est inclus dans le fichier `VMware-Horizon-Extras-Bundle-YYMM-x.x.x-yyyyyyyy.zip`. Pour obtenir des instructions d'installation, consultez le document Ajouter les fichiers de modèle d'administration ADMX à Active Directory.

Lorsque vous activez le paramètre de stratégie de groupe **Liste des règles de filtre Unity**, cliquez sur **Afficher** et saisissez une règle de filtrage dans la zone de texte **Valeur**. Une règle de filtrage se compose de caractéristiques et d'actions. Si vous spécifiez l'action `map`, vous devez également inclure un type. Le tableau suivant répertorie les caractéristiques, les actions et les types que vous pouvez utiliser dans les règles de filtrage.

Tableau 5-31. Caractéristiques, actions et types des règles de filtre Unity

Caractéristiques	Actions	Types
classname, company, product, major, minor, build, revision	block, map	normal, panel, dialog, tooltip, splash, toolbar, dock, desktop, widget, combobox, startscreen, sidepanel, taskbar, metrofullscreen, metrodocked

Le nom de classe Windows est généralement la caractéristique préférée, par exemple, `classname=CustomClassName`. Les caractéristiques `company`, `product`, `major`, `minor`, `build` et `revision` sont fournies au cas où vous devez limiter des règles à un produit spécifique. Vous trouvez les valeurs de ces caractéristiques dans la fenêtre **Propriétés** d'un fichier exécutable. Les valeurs de ces caractéristiques doivent respecter la casse exacte et inclure les mêmes caractères spéciaux. Si vous fournissez plusieurs caractéristiques, toutes les valeurs doivent correspondre pour que la règle s'applique à la fenêtre.

Pour spécifier une action, tapez `action=value`, par exemple, `action=block`. L'action `block` indique à Horizon Agent de ne pas afficher la fenêtre sur le client. Utilisez l'action `block` lorsqu'une fenêtre est trop grande ou interfère avec un comportement normal de fenêtre sur le client.

L'action `map`, par exemple, `action=map`, indique à Horizon Agent de traiter la fenêtre comme un certain type codé en dur. Pour spécifier le type, vous devez inclure `type=value` dans la règle, par exemple, `type=normal`. Comme il est difficile de déterminer si une fenêtre est mappée à un type incorrect, le mappage d'une fenêtre à un type est nécessaire uniquement si le support VMware vous invite à le faire.

Exemples de règles de filtrage

La règle de filtrage suivante bloque toutes les fenêtres avec le nom de classe MyClassName.

```
classname=MyClassName;action=block
```

La règle de filtrage suivante bloque toutes les fenêtres du produit nommé MyProduct.

```
product=MyProduct;action=block
```

La règle de filtrage suivante mappe une classe personnalisée au type combobox.

```
classname=MyClassName;action=map;type=combobox
```

Note Le paramètre de stratégie de groupe **Liste des règles de filtre Unity** a une priorité inférieure aux règles de filtrage qui sont spécifiées dans un fichier dans le répertoire `%ProgramData%\VMware\RdeServer\Unity Filters` sur l'hôte RDS.

Exemple de stratégie de groupe Active Directory

L'une des méthodes d'implémentation des stratégies de groupe Active Directory dans Horizon consiste à créer une unité d'organisation (UO) pour les machines qui fournissent des sessions Bureau à distance, puis 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.

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.

Note Chaque environnement Horizon 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

Pour appliquer des stratégies de groupe aux machines qui fournissent des sessions Bureau à distance sans affecter d'autres ordinateurs Windows du même domaine Active Directory, vous devez créer une UO propre à vos machines Horizon. Vous pouvez créer une UO pour l'ensemble de votre déploiement Horizon ou des UO distinctes pour des machines de poste de travail virtuel 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 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. Ajoutez des machines Horizon 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 dans le volet de droite et sélectionnez **Déplacer**.

   c. Sélectionnez l'UO et cliquez sur **OK**.

      La machine Horizon s'affiche dans le volet de droite lorsque vous sélectionnez l'UO.

Étape suivante

Créez des GPO pour les stratégies de groupe Horizon.

Créer des GPO pour les stratégies de groupe Horizon

Créez des GPO contenant des stratégies de groupe pour des composants Horizon et l'impression basée sur l'emplacement et liez-les à l'unité d'organisation de vos machines Horizon.

Conditions préalables

- Créez une unité d'organisation pour vos machines Horizon.

- Vérifiez que vous pouvez vous connecter en tant qu'utilisateur de domaine Administrateur sur la machine qui héberge votre serveur Active Directory.
- Vérifiez que la console MMC (Microsoft Management Console) et le composant logiciel enfichable Gestion des stratégies de groupe sont disponibles sur votre serveur Active Directory.

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 l'unité d'organisation qui contient vos machines Horizon et sélectionnez **Créer un objet GPO dans ce domaine, et le lier 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) Appliquez le GPO à des machines Horizon spécifiques de l'UO.
   a. Sélectionnez le GPO dans le volet de gauche.
   b. Sélectionnez **Filtrage de sécurité > Ajouter**.
   c. Entrez les noms d'ordinateur des machines Horizon et cliquez sur **OK**.

      Les machines Horizon s'affichent dans le volet Filtrage de sécurité. Les paramètres du GPO ne s'appliquent qu'à ces machines.

Étape suivante

Ajoutez les modèles d'administration ADMX Horizon au GPO.

Ajouter un fichier de modèle d'administration ADMX Horizon à un GPO

Pour appliquer des paramètres de stratégie de groupe de composant Horizon à vos postes de travail et applications, ajoutez leurs fichiers de modèle d'administration ADMX à des GPO.

Conditions préalables

- Créez des GPO pour les paramètres de stratégie de groupe du composant Horizon et liez-les à l'UO qui contient vos machines Horizon.
- Vérifiez que vous pouvez vous connecter en tant qu'utilisateur de domaine Administrateur sur la machine qui héberge votre serveur Active Directory.
- Vérifiez que la console MMC (Microsoft Management Console) et le composant logiciel enfichable Gestion des stratégies de groupe sont disponibles sur votre serveur Active Directory.

Procédure

1. Téléchargez le fichier VMware Horizon 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, qui inclut GPO Bundle.

   Le fichier est nommé `VMware-Horizon-Extras-Bundle-`*`YYMM`*`-`*`x.x.x`*`-`*`yyyyyyyy`*`.zip`, où *YYMM* est la version marketing, *x.x.x* est la version interne et *yyyyyyyy* est le numéro de build. Tous les fichiers ADMX qui fournissent des paramètres de stratégie de groupe pour VMware Horizon sont disponibles dans ce fichier.
2. Décompressez le fichier `VMware-Horizon-Extras-Bundle-`*`YYMM`*`-`*`x.x.x`*`-`*`yyyyyyyy`*`.zip` et copiez les fichiers ADMX sur votre serveur Active Directory.
   a. Copiez les fichiers `.admx`, ainsi que le dossier `en-US` dans le dossier `%systemroot%\PolicyDefinitions` sur votre serveur Active Directory.
   b. Copiez les fichiers de ressources de la langue (`.adml`) dans le sous-dossier correspondant dans `%systemroot%\PolicyDefinitions\` sur votre serveur Active Directory.
3. Sur le serveur 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.

Étape suivante

Configurez les paramètres de stratégie de groupe et activez le traitement en boucle pour vos machines Horizon.

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.

Conditions préalables

- Créez des GPO pour les paramètres de stratégie de groupe du composant Horizon et liez-les à l'UO qui contient vos machines Horizon.
- Vérifiez que vous pouvez vous connecter en tant qu'utilisateur de domaine Administrateur sur la machine qui héberge votre serveur Active Directory.
- Vérifiez que la console MMC (Microsoft Management Console) et le composant logiciel enfichable Gestion des stratégies de groupe sont disponibles sur votre serveur Active Directory.

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 ordinateur > Stratégies > Modèles administratifs : définitions de stratégies > Système > Stratégie de groupe**.

4 Dans le volet de droite, double-cliquez sur **Mode de traitement par boucle de rappel de la stratégie de groupe utilisateur**.

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.
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.

Définition de stratégies de poste de travail avec des scripts de démarrage de session

6

Les scripts de démarrage de session vous permettent de configurer des paramètres de poste de travail Horizon spécifiques avant le démarrage d'une session de poste de travail en fonction des informations provenant d'Horizon Client et du Horizon Connection Server.

Par exemple, au lieu de configurer plusieurs pools de postes de travail avec des stratégies différentes, vous pouvez utiliser un script de démarrage de session pour configurer des stratégies de poste de travail en fonction de l'emplacement du périphérique client et de l'utilisateur. Un script de démarrage de session peut activer des lecteurs mappés, la redirection de Presse-papiers et d'autres fonctionnalités de poste de travail pour un utilisateur dont l'adresse IP est située dans le domaine interne de votre organisation, tout en désactivant ces fonctionnalités pour un utilisateur dont l'adresse IP est située dans un domaine externe.

Ce chapitre contient les rubriques suivantes :

Obtention de données d'entrée pour un script de démarrage de session

Les scripts de démarrage de session ne peuvent pas s'exécuter de manière interactive. Un script de démarrage de session s'exécute dans un environnement créé par Horizon et doit obtenir ses données d'entrée à partir de cet environnement.

Les scripts de démarrage de session collectent les données d'entrée à partir des variables d'environnement sur l'ordinateur client. Les variables d'environnement de démarrage de session ont le préfixe `VDM_StartSession_`. Par exemple, la variable d'environnement de démarrage de session qui contient l'adresse IP du système client est `VDM_StartSession_IP_Address`. Vous devez vous assurer qu'un script de démarrage de session valide l'existence des variables d'environnement qu'il utilise.

Pour obtenir la liste des variables semblables aux variables d'environnement de démarrage de session, reportez-vous à la section Envoi d'informations sur le système client à des postes de travail distants.

Meilleures pratiques pour l'utilisation de scripts de démarrage de session

Suivez ces meilleures pratiques lors de l'utilisation de scripts de démarrage de session.

Conditions d'utilisation des scripts de démarrage de session

Utilisez des scripts de démarrage de session seulement lorsque vous avez besoin de configurer des stratégies de poste de travail avant le démarrage d'une session.

Nous vous recommandons d'utiliser les paramètres de stratégie de groupe Horizon Agent`CommandsToRunOnConnect` et `CommandsToRunOnReconnect` pour exécuter des scripts de commande après une connexion/reconnexion de session de poste de travail. L'exécution de scripts au sein d'une session de poste de travail, au lieu de l'utilisation de scripts de démarrage de session, répond à la plupart des cas d'utilisation.

Pour plus d'informations, reportez-vous à la section Exécution de commandes sur des postes de travail Horizon.

Gérer les délais d'expiration de démarrage de session

Assurez-vous que vos scripts de démarrage de session s'exécutent rapidement.

Si vous définissez la valeur de `WaitScriptsOnStartSession` dans le Registre Windows, l'exécution de votre script de démarrage de session doit se terminer avant qu'Horizon Agent puisse répondre au message StartSession envoyé par le Horizon Connection Server. Un script dont l'exécution prend un certain temps est susceptible de provoquer l'expiration de la demande StartSession.

Si un délai d'expiration se produit et que le pool utilise des attributions flottantes, le Serveur de connexion tente de connecter l'utilisateur à une autre machine virtuelle. En cas d'expiration du délai et si aucune machine virtuelle n'est disponible, le Serveur de connexion rejette la demande de connexion.

Nous vous recommandons de définir un délai d'expiration fixe pour l'opération de l'hôte de script afin qu'une erreur spécifique puisse être renvoyée en cas d'exécution trop longue d'un script.

Rendre les scripts de démarrage de session accessibles

Le chemin d'accès dans lequel vous configurez vos scripts de démarrage de session doit être accessible uniquement au compte SYSTÈME et aux administrateurs locaux. Définissez la liste de contrôle d'accès de la clé de base pour que seuls ces comptes puissent y accéder.

Nous vous recommandons de placer les scripts de démarrage de session dans le répertoire *View_Agent_install_path*\scripts, par exemple :

```
%ProgramFiles%\VMware\VMware View\Agent\scripts\sample.vbs
```

Par défaut, ce répertoire est accessible uniquement aux comptes SYSTÈME et Administrateur.

Préparation d'un poste de travail Horizon pour utiliser un script de démarrage de session

Pour préparer un poste de travail Horizon afin d'utiliser un script de démarrage de session, vous devez activer le service Hôte de script VMware Horizon View et ajouter des entrées dans le registre Windows.

Vous devez configurer tous les postes de travail Horizon qui ont besoin d'exécuter des scripts de démarrage de session. Horizon ne fournit pas de mécanisme pour propager les modifications du registre, les modifications de configuration du service Hôte de script VMware Horizon View et les scripts de démarrage de session sur plusieurs machines virtuelles de poste de travail Horizon.

Activer le service de l'hôte de script VMware Horizon View

Vous devez activer le service de l'hôte de script VMware Horizon View sur chaque machine virtuelle de poste de travail Horizon sur laquelle Horizon doit exécuter un script de démarrage de session. Le service de l'hôte de script VMware Horizon View est désactivé par défaut.

Lorsque vous configurez le service de l'hôte de script VMware Horizon View, vous pouvez éventuellement spécifier le compte d'utilisateur sous lequel s'exécute le script de démarrage de session. Les scripts de démarrage de session s'exécutent dans le contexte du service de l'hôte de script VMware Horizon View. Par défaut, le service d'hôte de script VMware View est configuré pour fonctionner en tant qu'utilisateur SYSTÈME.

Important Les scripts de démarrage de session sont exécutés en dehors d'une session d'utilisateur de poste de travail et non par le compte d'utilisateur de poste de travail. Les informations sont envoyées directement à partir de l'ordinateur client au sein d'un script exécuté en tant qu'utilisateur SYSTÈME.

Procédure

1. Connectez-vous à la machine virtuelle de poste de travail Horizon.
2. À l'invite de commande, tapez `services.msc` pour démarrer l'outil Services Windows.
3. Dans le volet de détails, cliquez avec le bouton droit sur l'entrée du service de l'hôte de script VMware Horizon View, puis sélectionnez **Propriétés**.
4. Sous l'onglet **Général**, sélectionnez **Automatique** dans le menu déroulant **Type de démarrage**.

5 (Facultatif) Si vous ne voulez pas que le compte Système local exécute le script de démarrage de session, sélectionnez l'onglet **Ouvrir une session**, puis **Ce compte**, et tapez le nom d'utilisateur et le mot de passe du compte pour exécuter le script de démarrage de session.

6 Cliquez sur **OK** et quittez l'outil Services Windows.

Ajouter des entrées de Registre Windows pour un script de démarrage de session

Vous devez ajouter les entrées de Registre Windows sur chaque machine virtuelle de poste de travail Horizon sur laquelle vous voulez qu'Horizon exécute un script de démarrage de session.

Conditions préalables

- Vérifiez que le chemin d'accès dans lequel vous avez configuré vos scripts de démarrage de session n'est accessible qu'au compte SYSTÈME et aux administrateurs locaux. Pour plus d'informations, reportez-vous à la section Meilleures pratiques pour l'utilisation de scripts de démarrage de session.
- Assurez-vous que vos scripts de démarrage de session s'exécutent rapidement. Si vous définissez la valeur de `WaitScriptsOnStartSession` dans le Registre Windows, l'exécution de votre script de démarrage de session doit se terminer avant qu'Horizon Agent puisse répondre au message StartSession envoyé par le Horizon Connection Server. Pour plus d'informations, reportez-vous à la section Meilleures pratiques pour l'utilisation de scripts de démarrage de session.

Procédure

1 Connectez-vous à la machine virtuelle de poste de travail Horizon.

2 À l'invite de commande, tapez `regedit` pour démarrer l'Éditeur du Registre de Windows.

3 Dans le Registre, accédez à `HKLM\SOFTWARE\VMware, Inc.\VMware VDM\ScriptEvents`.

4 Ajoutez le chemin d'accès au script de démarrage de session au Registre.

   a Dans la zone de navigation, cliquez avec le bouton droit sur `ScriptEvents`, sélectionnez **Nouveau > Clé**, puis créez une clé nommée `StartSession`.

   b Dans la zone de navigation, cliquez avec le bouton droit sur `StartSession`, sélectionnez **Nouveau > Valeur de chaîne**, puis créez une valeur de chaîne qui identifie le script de démarrage de session à exécuter, par exemple, `SampleScript`.

   Pour exécuter plusieurs scripts de démarrage de session, créez une entrée de valeur de chaîne pour chaque script sous la clé `StartSession`. Vous ne pouvez pas spécifier l'ordre dans lequel ces scripts s'exécutent. Si les scripts doivent s'exécuter dans un ordre particulier, appelez-les à partir d'un script de contrôle unique.

c Dans la zone de rubrique, cliquez avec le bouton droit sur l'entrée de la nouvelle valeur de chaîne, puis sélectionnez **Modifier**.

d Dans le champ **Données de valeur**, tapez la ligne de commande qui appelle le script de démarrage de session, puis cliquez sur **OK**.

Tapez le chemin complet du script de démarrage de session et de tous les fichiers dont il a besoin.

5 Ajoutez et activez une valeur de démarrage de session dans le Registre.

a Accédez à `HKLM\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration`.

b (Facultatif) Si la clé `Configuration` n'existe pas, cliquez avec le bouton droit sur **Agent**, sélectionnez **Nouveau > Clé**, puis créez la clé.

c Dans la zone de navigation, cliquez avec le bouton droit sur `Configuration`, sélectionnez **Nouveau > Valeur DWORD (32 bits)**, puis tapez `RunScriptsOnStartSession`.

d Dans la zone de rubrique, cliquez avec le bouton droit sur l'entrée de la nouvelle valeur DWORD, puis sélectionnez **Modifier**.

e Dans la zone de texte **Données de valeur**, tapez 1 pour activer le script de démarrage de session, puis cliquez sur **OK**.

Vous pouvez taper 0 pour désactiver cette fonctionnalité. La valeur par défaut est 0.

f (Facultatif) Pour qu'Horizon Agent retarde la réponse StartSession, ajoutez une deuxième valeur DWORD à la clé `Configuration` nommée `WaitScriptsOnStartSession`.

Une valeur de donnée de 1 pour `WaitScriptsOnStartSession` force Horizon Agent à retarder l'envoi d'une réponse StartSession et provoque un échec si les scripts ne se terminent pas. Une valeur de 0 signifie qu'Horizon Agent n'attend pas que les scripts se terminent ou vérifient les codes de sortie de script avant d'envoyer la réponse StartSession. La valeur par défaut est 0.

6 Définissez une valeur de Registre pour spécifier les valeurs de délai d'expiration en secondes plutôt qu'en minutes, afin d'empêcher des scripts d'arriver à expiration.

Le fait de définir cette valeur de délai d'expiration en secondes vous permet de configurer également la valeur du délai d'expiration du service d'hôte de script VMware View en secondes. Par exemple, si vous définissez le délai d'expiration du service d'hôte de script VMware View sur 30 secondes, vous pouvez garantir qu'un script de démarrage de session est terminé ou expiré avant la fin d'un délai d'expiration du Serveur de connexion.

a Accédez à `HKLM\SOFTWARE\VMware, Inc.\VMware VDM\ScriptEvents`.

b Ajoutez une valeur DWORD nommée `TimeoutsInMinutes`.

c Définissez une valeur de donnée de 0.

7 (Facultatif) Pour permettre au service d'hôte de script VMware View de déclencher l'expiration du script de démarrage de session, définissez une valeur de délai d'expiration.

   a Accédez à `HKLM\SOFTWARE\VMware, Inc.\VMware VDM\ScriptEvents\StartSession`.

   b Dans la zone de rubrique, cliquez avec le bouton droit sur la clé `Par défaut (@)` et sélectionnez **Modifier**.

   c Dans la zone de texte **Données de valeur**, tapez la valeur de délai d'expiration de votre choix, puis cliquez sur **OK**.

   Une valeur de 0 signifie qu'aucun délai d'expiration n'est défini.

8 Quittez l'Éditeur du Registre, puis redémarrez le système.

Exemples de scripts de démarrage de session

Ces exemples de scripts de démarrage de session montrent comment écrire des variables d'environnement dans un fichier, tester la fonctionnalité de délai d'expiration et tester un code de sortie non nul.

L'exemple de script Visual Basic suivant écrit toutes les variables d'environnement fournies au script dans un fichier. Vous pouvez utiliser cet exemple de script pour afficher les données d'exemple dans votre propre environnement. Vous pouvez enregistrer ce script sous la forme `C:\sample.vbs`.

```
Option Explicit
Dim WshShell, FSO, outFile, strOutputFile, objUserEnv, strEnv

strOutputFile = "c:\setvars.txt"

Set FSO = CreateObject("Scripting.fileSystemObject")
Set outFile = FSO.CreateTextFile(strOutputFile, TRUE)
outFile.WriteLine("Script was called at (" & Now & ")")

Set WshShell = CreateObject( "WScript.Shell" )
Set objUserEnv = WshShell.Environment("PROCESS")
For Each strEnv In objUserEnv
outFile.WriteLine(strEnv)
Next

outFile.Close
```

L'exemple de script suivant teste la fonctionnalité de délai d'expiration.

```
Option Explicit
WScript.Sleep 60000
```

L'exemple de script suivant teste un code de sortie non nul.

```
Option Explicit
WScript.Quit 2
```

Examen des statistiques de session PCoIP avec WMI

7

Vous pouvez utiliser Windows Management Instrumentation (WMI) pour examiner les statistiques de performances d'une session PCoIP à l'aide de l'une des interfaces de programmation prises en charge, telles que C#, C++, PowerShell, VBScript, VB .NET et WMIC (Windows Management Instrumentation Command-Line).

Vous pouvez également utiliser l'outil Microsoft WMI Code Creator pour générer du code VBScript, C# et VB .NET capable d'accéder aux compteurs de performances PCoIP. Pour plus d'informations sur WMI, WMIC et l'outil de création de code WMI, rendez-vous sur http://technet.microsoft.com/fr-fr/library/bb742610.aspx.

Ce chapitre contient les rubriques suivantes :

Utilisation des statistiques de session PCoIP

L'espace de noms WMI des statistiques de session PCoIP est `root\CIMV2`. Les noms des statistiques sont modifiés par l'ajout du suffixe `(Serveur)` ou `(Client)`, selon que la statistique est enregistrée sur le serveur PCoIP ou le client PCoIP.

Vous pouvez utiliser le moniteur de performances Windows (PerfMon) avec les compteurs pour calculer les moyennes sur une période d'échantillonnage définie. Vous devez disposer des privilèges d'administrateur pour accéder à distance aux compteurs de performances.

Toutes les statistiques sont réinitialisées à 0 lorsqu'une session PCoIP est fermée. Si la propriété WMI `SessionDurationSeconds` est une valeur non nulle et reste constante, le serveur PCoIP a été arrêté de force ou s'est bloqué. Si la propriété `SessionDurationSeconds` passe d'une valeur non nulle à 0, la session PCoIP est fermée.

Pour éviter une erreur de division par zéro, vérifiez que le dénominateur des expressions pour le calcul du pourcentage de bande passante ou de perte de paquets ne corresponde pas à zéro.

Les statistiques USB sont enregistrées pour les clients zéro, mais pas pour les clients légers ou les clients logiciels.

Statistiques générales de session PCoIP

Le nom de classe WMI pour les statistiques générales de session PCoIP est `Win32_PerfRawData_TeradiciPerf_PCoIPSessionGeneralStatistics`.

Tableau 7-1. Statistiques générales de session

Nom de propriété WMI	Description
`BytesReceived`	Nombre total, en octets, de données PCoIP reçues depuis le démarrage de la session PCoIP.
`BytesSent`	Nombre total, en octets, de données PCoIP transmises depuis le démarrage de la session PCoIP.
`PacketsReceived`	Nombre total de paquets reçus avec succès depuis le démarrage de la session PCoIP. Les paquets n'ont pas tous la même taille.
`PacketsSent`	Nombre total de paquets transmis depuis le démarrage de la session PCoIP. Les paquets n'ont pas tous la même taille.
`RXPacketsLost`	Nombre total de paquets reçus qui ont été perdus depuis le démarrage de la session PCoIP.
`SessionDurationSeconds`	Nombre total de secondes pendant lequel la session PCoIP a été ouverte.
`TXPacketsLost`	Nombre total de paquets transmis qui ont été perdus depuis le démarrage de la session PCoIP.

Calcul de la bande passante pour les données PCoIP reçues

Pour calculer la bande passante en kilobits par seconde pour les données PCoIP reçues pendant l'intervalle de temps entre l'instant `t1` et le l'instant `t2`, utilisez la formule suivante.

```
(BytesReceived[t2]-BytesReceived[t1]) * 8 / (1024 * (t2-t1))
```

Calcul de la bande passante pour les données PCoIP transmises

Pour calculer la bande passante en kilobits par seconde pour les données PCoIP transmises pendant l'intervalle de temps entre l'instant `t1` et l'instant `t2`, utilisez la formule suivante.

```
(BytesSent[t2]-BytesSent[t1]) * 8 / (1024 * (t2-t1))
```

Calcul de la perte de paquets pour les données PCoIP reçues

Utilisez la formule suivante pour calculer le pourcentage de paquets reçus qui sont perdus.

```
100 / (1 + ((PacketsReceived[t2]-PacketsReceived[t1])/(RXPacketsLost[t2]-RXPacketsLost[t1])))
```

Calcul de la perte de paquets pour les données PCoIP transmises

Utilisez la formule suivante pour calculer le pourcentage de paquets transmis qui sont perdus.

```
100 * (TXPacketsLost[t2]-TXPacketsLost[t1]) / (PacketsSent[t2]-PacketsSent[t1])
```

Statistiques audio PCoIP

Le nom de classe WMI des statistiques audio PCoIP est `Win32_PerfRawData_TeradiciPerf_PCoIPSessionAudioStatistics`.

Note Les statistiques audio n'incluent pas les données audio contenues dans les données USB.

Tableau 7-2. Statistiques audio PCoIP

Nom de la propriété WMI	Description
`AudioBytesReceived`	Nombre total d'octets de données audio reçus depuis le démarrage de la session PCoIP.
`AudioBytesSent`	Nombre total d'octets de données audio envoyés depuis le démarrage de la session PCoIP.
`AudioRXBWkbitPersec`	Moyenne de bande passante pour les paquets audio entrants durant la période d'échantillonnage, en secondes.
`AudioTXBWkbitPersec`	Moyenne de la bande passante pour les paquets audio sortants pendant la période d'échantillonnage, en secondes.
`AudioTXBWLimitkbitPersec`	Limite de bande passante de transmission en kilobits par seconde pour les paquets audio sortants. La limite est définie par un paramètre GPO.

Calcul de la bande passante pour les données audio reçues

Utilisez la formule suivante pour calculer la bande passante en kilobits par seconde pour les données audio reçues pendant l'intervalle de temps entre l'instant `t1` et l'instant `t2`.

```
(AudioBytesReceived[t2]-AudioBytesReceived[t1]) * 8 / (1024 * (t2-t1))
```

N'utilisez pas `AudioRXBWkbitPersec` pour ce calcul.

Calcul de la bande passante pour les données audio transmises

Utilisez la formule suivante pour calculer la bande passante en kilobits par seconde pour les données audio transmises pendant l'intervalle de temps entre l'instant `t1` et l'instant `t2`.

```
(AudioBytesSent[t2]-AudioBytesSent[t1]) * 8 / (1024 * (t2-t1))
```

N'utilisez pas `AudioTXBWkbitPersec` pour ce calcul.

Statistiques de création d'images PCoIP

Le nom de classe WMI des statistiques de création d'images PCoIP est `Win32_PerfRawData_TeradiciPerf_PCoIPSessionImagingStatistics`.

Tableau 7-3. Statistiques de création d'images PCoIP

Nom de la propriété WMI	Description
`ImagingBytesReceived`	Nombre total d'octets de données de création d'images reçus depuis le démarrage de la session PCoIP.
`ImagingBytesSent`	Nombre total d'octets de données de création d'images transmis depuis le démarrage de la session PCoIP.
`ImagingDecoderCapabilitykbitPersec`	Capacité de traitement estimée du décodeur d'image en kilobits par seconde. Cette statistique est mise à jour une fois par seconde.
`ImagingEncodedFramesPersec`	Nombre de trames d'images codées sur une période d'échantillonnage d'une seconde.
`ImagingActiveMinimumQuality`	Valeur codée de qualité la plus faible sur une échelle de 0 à 100. Cette statistique est mise à jour une fois par seconde. Ce compteur ne correspond pas au paramètre de GPO pour la qualité minimale.
`ImagingRXBWkbitPersec`	Moyenne de bande passante pour les paquets d'images entrants durant la période d'échantillonnage, en secondes.
`ImagingTXBWkbitPersec`	Moyenne de bande passante pour les paquets d'images sortants durant la période d'échantillonnage, en secondes.

Calcul de la bande passante pour les données de création d'images reçues

Utilisez la formule suivante pour calculer la bande passante en kilobits par seconde pour les données de création d'images reçues pendant l'intervalle de temps entre l'instant `t1` et l'instant `t2`.

```
(ImagingBytesReceived[t2]-ImagingBytesReceived[t1]) * 8 / (1024 * (t2-t1))
```

N'utilisez pas `ImagingRXBWkbitPersec` pour ce calcul.

Calcul de la bande passante pour les données de création d'images transmises

Utilisez la formule suivante pour calculer la bande passante en kilobits par seconde pour les données de création d'images transmises pendant l'intervalle de temps entre l'instant `t1` et l'instant `t2`.

```
(ImagingBytesSent[t2]-ImagingBytesSent[t1]) * 8 / (1024 * (t2-t1))
```

N'utilisez pas `ImagingTXBWkbitPersec` pour ce calcul.

Statistiques de réseau PCoIP

Le nom de classe WMI des statistiques de réseau PCoIP est `Win32_PerfRawData_TeradiciPerf_PCoIPSessionNetworkStatistics`.

Tableau 7-4. Statistiques de réseau PCoIP

Nom de la propriété WMI	Description
`RoundTripLatencyms`	Latence de parcours circulaire, en millisecondes, entre le serveur PCoIP et le client PCoIP.
`RXBWkbitPersec`	Moyenne de bande passante globale pour les paquets PCoIP entrants durant la période d'échantillonnage, en secondes.
`RXBWPeakkbitPersec`	Bande passante maximale en kilobits par seconde pour les paquets PCoIP entrants durant une période d'échantillonnage d'une seconde.
`RXPacketLossPercent`	Pourcentage de paquets reçus perdus pendant une période d'échantillonnage.
`TXBWkbitPersec`	Moyenne de bande passante globale pour les paquets PCoIP sortants durant la période d'échantillonnage, en secondes.
`TXBWActiveLimitkbitPersec`	Estimation de bande passante réseau disponible en kilobits par seconde. Cette statistique est mise à jour une fois par seconde.
`TXBWLimitkbitPersec`	Limite de bande passante de transmission, en kilobits par seconde, pour les paquets sortants. La limite correspond au minimum des valeurs suivantes. ■ Limite de bande passante GPO pour le client PCoIP ■ Limite de bande passante GPO pour le serveur PCoIP ■ Limite de bande passante pour la connexion de réseau local ■ Limite de bande passante négociée pour le microprogramme Zero Client en fonction des limites de chiffrement
`TXPacketLossPercent`	Pourcentage de paquets transmis perdus pendant une période d'échantillonnage.

Calcul de la bande passante pour les données de réseau reçues

Utilisez la formule suivante pour calculer la bande passante en kilobits par seconde pour les données reçues pendant l'intervalle de temps entre l'instant `t1` et l'instant `t2`.

```
(BytesReceived[t2]-BytesReceived[t1]) * 8 / (1024 * (t2-t1))
```

N'utilisez pas `RXBWkbitPersec` pour ce calcul.

Calcul de la bande passante pour les données de réseau transmises

Utilisez la formule suivante pour calculer la bande passante en kilobits par seconde pour les données transmises pendant l'intervalle de temps entre l'instant `t1` et l'instant `t2`.

```
(BytesSent[t2]-BytesSent[t1]) * 8 / (1024 * (t2-t1))
```

N'utilisez pas `TXBWkbitPersec` pour ce calcul.

Calcul de la perte de paquets pour les données de réseau reçues

Utilisez la formule suivante pour calculer le pourcentage de perte de paquets pour les données reçues pendant l'intervalle de temps entre l'instant `t1` et l'instant `t2`.

```
PacketsReceived during interval = (PacketsReceived[t2]-PacketsReceived[t1])

RXPacketsLost during interval = (RXPacketsLost[t2]-RXPacketsLost[t1])

RXPacketsLost % = RXPacketsLost during interval /
(RXPacketsLost during interval + PacketsReceived during interval) * 100
```

N'utilisez pas `RXPacketLostPercent` ou `RXPacketLostPercent_Base` pour ce calcul.

Calcul de la perte de paquets pour les données de réseau transmises

Utilisez la formule suivante pour calculer le pourcentage de perte de paquets pour les données transmises pendant l'intervalle de temps entre l'instant `t1` et l'instant `t2`.

```
PacketsSent during interval = (PacketsSent[t2]-PacketsSent[t1])

TXPacketsLost during interval = (TXPacketsLost[t2]-TXPacketsLost[t1])

TXPacketsLost % = TXPacketsLost during interval /
(TXPacketsLost during interval + PacketsSent during interval) * 100
```

N'utilisez pas `TXPacketLostPercent` ou `TXPacketLostPercent_Base` pour ce calcul.

Utilisez cette formule pour empêcher le pourcentage de perte de paquets de dépasser les 100 %. Ce calcul est nécessaire, car `PacketsLost` et `PacketsSent` sont asynchrones.

Statistiques PCoIP USB

Le nom de classe WMI des statistiques PCoIP USB est `Win32_PerfRawData_TeradiciPerf_PCoIPSessionUSBStatistics`.

Tableau 7-5. Statistiques PCoIP USB

Nom de la propriété WMI	Description
`USBBytesReceived`	Nombre total, en octets, de données USB reçues depuis le démarrage de la session PCoIP.
`USBBytesSent`	Nombre total, en octets, de données USB transmises depuis le démarrage de la session PCoIP.
`USBRXBWkbitPersec`	Moyenne de bande passante pour les paquets USB entrants pendant la période d'échantillonnage, en secondes.
`USBTXBWkbitPersec`	Moyenne de bande passante pour les paquets USB sortants pendant la période d'échantillonnage, en secondes.

Calcul de la bande passante pour les données USB reçues

Utilisez la formule suivante pour calculer la bande passante en kilobits par seconde pour les données USB reçues pendant l'intervalle de temps entre l'instant `t1` et l'instant `t2`.

```
(USBBytesReceived[t2]-USBBytesReceived[t1]) * 8 / (1024 * (t2-t1))
```

N'utilisez pas `USBRXBWkbitPersec` pour ce calcul.

Calcul de la bande passante pour les données USB transmises

Utilisez la formule suivante pour calculer la bande passante en kilobits par seconde pour les données USB transmises pendant l'intervalle de temps entre l'instant `t1` et l'instant `t2`.

```
(USBBytesSent[t2]-USBBytesSent[t1]) * 8 / (1024 * (t2-t1))
```

N'utilisez pas `USBTXBWkbitPersec` pour ce calcul.

Exemples d'utilisation de cmdlets PowerShell pour examiner les statistiques PCoIP

Vous pouvez utiliser les cmdlets PowerShell pour examiner les statistiques PCoIP.

Dans l'exemple suivant, la cmdlet `Get-WmiObject` récupère les statistiques de réseau PCoIP pour le client cm-02.

```
Get-WmiObject -namespace "root\cimv2" -computername cm-02 -class
Win32_PerfRawData_TeradiciPerf_PCoIPSessionNetworkStatistics
```

Dans l'exemple suivant, la cmdlet `Get-WmiObject` récupère les statistiques de session générale PCoIP pour le poste de travail dt-03, en cas de perte de paquets transmis.

```
Get-WmiObject -namespace "root\cimv2" -computername desktop-03 -query "select * from
Win32_PerfRawData_TeradiciPerf_PCoIPSessionGeneralStatistics where TXPacketsLost > 0"
```