Utilisation de VMware Horizon Client pour Mac OS X

Septembre 2014
VMware Horizon

Ce document prend en charge la version de chacun des produits répertoriés, ainsi que toutes les versions publiées par la suite jusqu'au remplacement dudit document par une nouvelle édition. Pour rechercher des éditions plus récentes de ce document, rendez-vous sur : http://www.vmware.com/fr/support/pubs.

FR-001482-01

vmware®

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

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

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

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

docfeedback@vmware.com

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

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

Table des matières

Utilisation de VMware Horizon Client pour Mac OS X

L'utilisation de VMware Horizon Client pour Mac OS X fournit des informations sur l'installation et l'utilisation du logiciel VMware Horizon™ Client™ sur un Mac pour se connecter à une application ou à un poste de travail distant du centre de données.

Ces informations sont destinées aux administrateurs qui doivent configurer un déploiement de View comportant des périphériques clients Mac. Les informations sont rédigées pour des administrateurs système expérimentés qui connaissent parfaitement la technologie des machines virtuelles et les opérations de datacenter.

Configuration et installation 1

La configuration d'un déploiement de View pour des clients Mac implique d'utiliser certains paramètres de configuration du Serveur de connexion View, de respecter la configuration système requise pour les serveurs View Server et les clients Mac, et de télécharger Horizon Client pour Mac sur le site Web de VMware afin de l'installer.

Ce chapitre aborde les rubriques suivantes :

Configuration système requise pour les clients Mac

Vous pouvez installer Horizon Client pour Mac OS X sur tous les modèles à processeur Intel 64 bits qui utilisent le système d'exploitation Mac OS X 10.6.8 ou version ultérieure.

L'ordinateur Mac sur lequel vous installez Horizon Client, ainsi que les périphériques qu'il utilise, doivent respecter un certain nombre de configurations système.

Modèle	Mac à processeur Intel 64 bits
Mémoire	Au moins 2 Go de RAM
Systèmes d'exploitation	■ Mac OS X Snow Leopard (10.6.8) ■ Mac OS X Lion (10.7) ■ Mac OS X Mountain Lion (10.8)

	■ Mac OS X Mavericks (10.9) Vous devez installer Horizon Client sur Mac OS X Mountain Lion (10.8) ou version ultérieure pour utiliser les applications distantes. Les applications distantes ne s'affichent pas dans Horizon Client si le système client s'exécute sur une version antérieure d'OS X.
Serveur de connexion View, serveur de sécurité et View Agent	Dernière version de maintenance de View 4.6.x et versions ultérieures. Si les systèmes clients se connectent en dehors du pare-feu d'entreprise, VMware recommande d'utiliser un serveur de sécurité. Avec un serveur de sécurité, les systèmes client ne requièrent pas de connexion VPN. Les applications distantes sont disponibles uniquement sur les serveurs Horizon 6.0 avec View.
Protocole d'affichage pour View	PCoIP ou RDP
Exigences logicielles pour RDP	Les versions 2.0 à 2.1.1 de Remote Desktop Connection Client pour Mac de Microsoft. Vous pouvez télécharger ce client sur le site Web de Microsoft. **REMARQUE** Horizon Client pour Mac OS X ne fonctionne pas avec Microsoft Remote Desktop 8.0 et versions ultérieures.

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

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

Poste de travail distant View	View Agent 5.2 ou version ultérieure doit être installé sur les postes de travail. La version correspondante de Remote Experience Agent doit également être installée sur les postes de travail, le cas échéant. Par exemple, si View Agent 5.3 est installé, vous devez aussi installer Remote Experience Agent depuis View 5.3 Feature Pack 1. Consultez le document *Installation et administration de View Feature Pack* pour View. Si vous disposez de View Agent 6.0 ou version ultérieure, aucun Feature Pack n'est requis.
Ordinateur Horizon Client ou périphérique d'accès client	■ La fonction Audio-Vidéo en temps réel est prise en charge sur Mac OS X Mountain Lion (10.8) et versions ultérieures. Elle est désactivée sur tous les systèmes d'exploitation Mac OS X antérieurs. ■ Les pilotes des webcams et des périphériques audio doivent être installés, et la webcam ainsi que le périphérique audio doivent être opérationnels sur l'ordinateur client. Pour utiliser l'Audio/Vidéo en temps réel, vous n'avez pas à installer les pilotes des périphériques sur le système d'exploitation du poste de travail où View Agent est installé.
Protocole d'affichage pour View	PCoIP L'Audio/Vidéo en temps réel n'est pas pris en charge par les sessions postes de travail RDP.

Systèmes d'exploitation de poste de travail pris en charge

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

Pour obtenir la liste des systèmes d'exploitation invités, consultez la rubrique « Systèmes d'exploitation pris en charge par View Agent » dans la documentation d'installation d'View 4.6.x, 5.x ou 6.x.

Préparation du Serveur de connexion View pour Horizon Client

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

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

- Si vous utilisez un serveur de sécurité comme le recommande VMware, assurez-vous de disposer des dernières versions de maintenance du Serveur de connexion View 4.6.x et du Serveur de sécurité View 4.6.x ou versions ultérieures. Consultez le document *Installation de View*.
- Si vous prévoyez d'utiliser une connexion tunnel sécurisée pour des périphériques client et si la connexion sécurisée est configurée avec un nom d'hôte DNS pour le Serveur de connexion View ou un serveur de sécurité, vérifiez que le périphérique client peut résoudre ce nom DNS.

  Pour activer ou désactiver le tunnel sécurisé, dans View Administrator, allez à la boîte de dialogue Modifier les paramètres du Serveur de connexion View et cochez la case **Utiliser une connexion tunnel sécurisée vers le poste de travail**.
- Vérifiez qu'un pool de postes de travail ou d'applications a été créé et que le compte d'utilisateur que vous souhaitez utiliser est autorisé à accéder au pool. Pour le serveur de connexion View 5.3 et versions antérieures, consultez les rubriques sur la création de pools de postes de travail dans le document Administration de *View*. Pour le Serveur de connexion View 6.0 et versions antérieures, consultez les rubriques sur la création de pools de postes de travail et d'applications dans le document Configuration de pools de postes de travail et d'applications pour *View*.

  IMPORTANT Si les utilisateurs finaux disposent d'un écran Retina et prévoient d'utiliser le paramètre client Mode haute résolution lors de l'affichage de leur poste de travail distant en mode plein écran, vous devez allouer suffisamment de mémoire VRAM pour chaque poste de travail distant Windows 7 ou version ultérieure. La quantité de mémoire vRAM requise dépend du nombre de moniteurs configurés pour les utilisateurs finaux et de la résolution d'affichage. Pour estimer la quantité de mémoire vRAM requise, reportez-vous à la section « Taille de la RAM pour des configurations de moniteur spécifiques en cas d'utilisation de PCoIP » dans la rubrique « Estimation de la mémoire requise pour les postes de travail virtuels » du document *Planification de l'architecture de View*.
- Pour pouvoir utiliser une authentification à deux facteurs, telle que l'authentification RSA SecurID ou RADIUS, avec Horizon Client, vous devez activer cette fonctionnalité sur le Serveur de connexion View. L'authentification RADIUS est disponible avec View 5.1 et versions ultérieures et le Serveur de connexion View. Pour plus d'informations, consultez les rubriques concernant l'authentification à deux facteurs dans le document *Administration de View*.

Configurez les liens de téléchargement client affichés dans View Portal 5.2 et versions antérieures

Si vous utilisez le Serveur de connexion View 5.2 ou versions antérieures, et que vous ne disposez pas de HTML Access, par défaut, lorsque vous ouvrez un navigateur et que vous entrez l'URL d'une instance du Serveur de connexion View, la page de portail qui s'affiche contient des liens vers le site de téléchargement de VMware pour télécharger Horizon Client. Vous pouvez modifier la valeur par défaut.

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

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

IMPORTANT Si vous personnalisez les liens de la page de portail, comme décrit dans cette rubrique, et que vous installez ultérieurement HTML Access ou le Serveur de connexion View 6.0 ou version ultérieure sur le serveur, votre page de portail personnalisée est remplacée par une page de portail Web VMware Horizon, et une icône permettant l'utilisation de HTML Access est ajoutée. Pour plus d'informations sur la personnalisation de cette page, reportez-vous au document *Utilisation de HTML Access* ou *Mises à jour de View* 6.0 ou version ultérieure.

Prérequis

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

Procédure

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

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

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

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

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

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

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

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

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

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

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

   ```
   link.win=https://server-name/downloads/VMware-Horizon-Client-x86_64-y.y.y-XXXX.exe#win
   link.win.1=https://server-name/downloads/VMware-Horizon-Client-y.y.y-XXXX.exe#win
   link.linux=https://server-name/downloads/VMware-Horizon-Client-y.y.y-XXXX.i386.rpm#linux
   link.mac=https://server-name/downloads/VMware-Horizon-Client-y.y.y-XXXX.dmg#mac
   ```

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

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

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

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

   ```
   text.win=Horizon Client for Windows 32-bit client users
   text.win.1=Horizon Client for Windows 64-bit client users
   ```

7 Redémarrez le service Serveur de connexion VMware View.

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

Installer Horizon Client sur Mac OS X

Les utilisateurs finaux ouvrent Horizon Client pour se connecter à des applications et des postes de travail distants à partir d'une machine physique Mac OS X. Vous installez Horizon Client sur des systèmes clients Mac OS X à partir d'un fichier image de disque.

Prérequis

- Vérifiez que le système client utilise un système d'exploitation pris en charge. Reportez-vous à la section « Configuration système requise pour les clients Mac », page 7.
- Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur le système client.
- Si vous prévoyez d'utiliser le protocole d'affichage RDP pour vous connecter à un poste de travail distant, vérifiez que la version 2.0 ou ultérieure de Remote Desktop Connection Client pour Mac de Microsoft est installée sur le système client Mac.
- Vérifiez que vous disposez de l'URL d'accès à une page de téléchargement contenant le programme d'installation de VMware Horizon Client. Il peut s'agir de l'URL de la page de téléchargements de VMware à l'adresse http://www.vmware.com/go/viewclients ou de l'URL d'une instance du Serveur de connexion View.

Lorsque vous accédez à une URL du Serveur de connexion View, les liens de cette page de portail pointent par défaut vers la page de téléchargements de VMware. Vous pouvez configurer les liens afin qu'ils pointent vers un autre emplacement. Pour plus d'informations, reportez-vous à la section « Configurez les liens de téléchargement client affichés dans View Portal 5.2 et versions antérieures », page 10. Selon la façon dont la page est configurée, vous pouvez également voir un lien vers HTML Access. HTML Access vous permet de vous connecter à une application ou un poste de travail distant à l'aide du navigateur, sans installer de logiciel client. Comme VMware Horizon Client offre davantage de fonctionnalités et de meilleures performances que le client HTML Access, VMware recommande généralement d'installer le logiciel client.

Procédure

1 Sur votre Mac, accédez à l'URL permettant de télécharger le fichier d'installation d'Horizon Client.

Pour Horizon Client 3.0, le format du nom de fichier est `VMware-Horizon-View-Client-y.y.y-xxxxxx.dmg`. Pour Horizon Client 3.1, le format du nom de fichier est `VMware-Horizon-Client-y.y.y-xxxxxx.dmg`. *xxxxxx* est le numéro de build et *y.y.y* le numéro de version.

2 Double-cliquez sur le fichier `.dmg` pour l'ouvrir et cliquez sur **Accepter**.

Le contenu de l'image disque apparaît dans une fenêtre Finder Horizon Client.

3 Dans la fenêtre du Finder, faites glisser l'icône **VMware Horizon View Client** (Horizon Client 3.0) ou **VMware Horizon Client** (Horizon Client 3.1) vers l'icône du dossier **Applications**.

Si vous n'êtes pas connecté en tant qu'utilisateur administrateur, vous êtes invité à saisir un nom d'utilisateur et un mot de passe d'administrateur.

Suivant

Démarrez Horizon Client et vérifiez que vous pouvez vous connecter à une application ou à un poste de travail distant. Reportez-vous à la section « Se connecter à une application ou à un poste de travail distant pour la première fois », page 23.

Ajouter Horizon Client à votre Dock

Vous pouvez ajouter Horizon Client à votre Dock, comme n'importe quelle autre application.

Procédure

1 Dans le dossier **Applications**, sélectionnez **VMware Horizon View Client** (Horizon Client 3.0) ou **VMware Horizon Client** (Horizon Client 3.1).

2 Faites glisser l'icône **VMware Horizon View Client** (Horizon Client 3.0) ou **VMware Horizon Client** (Horizon Client 3.1) vers le Dock.

3 Pour configurer l'icône du Dock afin d'ouvrir Horizon Client à l'ouverture de session ou d'afficher l'icône dans l'outil de recherche, sélectionnez **Options**, puis sélectionnez la commande appropriée dans le menu contextuel.

Lorsque vous quittez Horizon Client, le raccourci de l'application reste sur le Dock.

Configuration de la vérification des certificats pour les utilisateurs finaux

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

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

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

Pour plus d'informations sur les types de vérifications effectuées, reportez-vous à la section « Modes de vérification des certificats pour Horizon Client », page 26.

Vous pouvez définir le mode de vérification afin que les utilisateurs ne puissent pas le modifier. Définissez la clé « Security Mode » (Mode de sécurité) du fichier `/Library/Preferences/com.vmware.view.plist` (Horizon Client 3.0) ou le fichier `/Library/Preferences/com.vmware.horizon.plist` (Horizon Client 3.1) sur les clients Mac sur l'une des valeurs suivantes :

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

Configurer les options SSL avancées

Vous pouvez sélectionner les protocoles de sécurité qu'Horizon Client peut utiliser. Vous pouvez également spécifier la chaîne de contrôle de chiffrement.

Les options SSL avancées que vous configurez dans Horizon Client servent à chiffrer les communications entre Horizon Client et Serveur de connexion View et View Agent. Dans Horizon Client 3.1 et version ultérieure, ces options sont également utilisées pour chiffrer le canal USB (communication entre le démon du service USB et View Agent).

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

Prérequis

Vérifiez le protocole de sécurité que le serveur View Server peut utiliser. Si vous configurez un protocole de sécurité pour Horizon Client qui n'est pas activé sur le serveur View Server auquel le client se connecte, une erreur SSL se produit et la connexion échoue. Pour obtenir des informations sur la configuration des protocoles de sécurité qui sont acceptés par les instances du Serveur de connexion View, reportez-vous au document *Sécurité de View*.

Par défaut, Horizon Client et le Serveur de connexion View prennent en charge TLS v1.0 et TLS v1.1. Vous devez uniquement modifier les protocoles de sécurité d'Horizon Client si votre administrateur View vous le demande ou si votre serveur View ne prend pas en charge les paramètres actuels.

Procédure

1 Sélectionnez **VMware Horizon View Client > Préférences** (Horizon Client 3.0) ou **VMware Horizon Client > Préférences** (Horizon Client 3.1) dans la barre de menus et cliquez sur **Avancé** dans la boîte de dialogue Préférences.

2 Pour activer ou désactiver un protocole de sécurité, cochez la case en regard du nom du protocole de sécurité.

Par défaut, TLSv 1.0 et TLSv 1.1 sont activés.

3 Pour modifier la chaîne de contrôle de chiffrement, remplacez la chaîne par défaut dans la zone de texte.

La chaîne de contrôle de chiffrement par défaut (AES:!aNULL:@STRENGTH) contient des suites de chiffrements qui utilisent le chiffrement AES 128 bits ou 256 bits, à l'exception des algorithmes DH anonymes, et les trie par niveau de sécurité.

Remarque Dans Horizon Client 3.1 et version ultérieure, le démon du service USB ajoute RC4 (:RC4-SHA : +RC4) à la fin de la chaîne de contrôle de chiffrement lorsqu'il se connecte à un poste de travail distant.

4 (Facultatif) Si vous avez besoin de rétablir les paramètres par défaut, cliquez sur **Restaurer les paramètres par défaut**.

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

Vos modifications seront appliquées lors de votre prochaine connexion au Serveur de connexion View.

Configuration des valeurs de collecte de fichiers journaux

Dans Horizon Client 3.1, Horizon Client génère dans le répertoire `~/Library/Logs/VMware Horizon Client` du client Mac. Les administrateurs peuvent configurer le nombre maximal de fichiers journaux et le nombre maximal de jours de conservation des fichiers journaux en définissant des clés dans le fichier `/Library/Preferences/com.vmware.horizon.plist` sur un client Mac.

Tableau 1-1. Clés plist pour la collecte de fichiers journaux

Clé	Description
MaxDebugLogs	Spécifie le nombre maximal de fichiers journaux. La valeur maximale est de 100.
MaxDaysToKeepLogs	Spécifie le nombre maximal de jours de conservation des fichiers journaux. Cette valeur n'a pas de limite.

Les fichiers qui ne correspondent pas à ces critères sont supprimés lorsque vous lancez Horizon Client.

Si les clés MaxDebugLogs ou MaxDaysToKeepLogs ne sont pas définies dans le fichier `com.vmware.horizon.plist`, le nombre par défaut de fichiers journaux est de 5 et les fichiers sont conservés 7 jours par défaut.

Données Horizon Client collectées par VMware

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

Remarque Cette fonctionnalité est disponible uniquement si votre déploiement View utilise le Serveur de connexion View 5.1 ou versions ultérieures.

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

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

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

Tableau 1-2. Données collectées depuis Horizon Client pour le programme d'amélioration du produit

Description	Ce champ reste-t-il anonyme ?	Exemple
Entreprise ayant produit l'application Horizon Client	Non	VMware
Nom du produit	Non	VMware Horizon Client
Version du produit client	Non	(Le format est *x.x.x-yyyyyy*, où *x.x.x* est le numéro de version du client et *yyyyyy* est le numéro de build.)
Architecture binaire du client	Non	Exemples : ■ i386 ■ x86_64 ■ arm
Nom du build du client	Non	Exemples : ■ VMware-Horizon-View-Client-Win32-Windows ■ VMware-Horizon-View-Client-Linux ■ VMware-Horizon-View-Client-iOS ■ VMware-Horizon-View-Client-Mac ■ VMware-Horizon-View-Client-Android ■ VMware-Horizon-View-Client-WinStore
Système d'exploitation hôte	Non	Exemples : ■ Windows 8.1 ■ Windows 7, 64 bits Service Pack 1 (Build 7601) ■ iPhone OS 5.1.1 (9B206) ■ Ubuntu 10.04.4 LTS ■ Mac OS X 10.8.5 (12F45)
Noyau du système d'exploitation hôte	Non	Exemples : ■ Windows 6.1.7601 SP1 ■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X ■ Darwin 11.4.2 ■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012 ■ inconnu (pour Windows Store)
Architecture du système d'exploitation hôte	Non	Exemples : ■ x86_64 ■ i386 ■ armv71 ■ ARM

Tableau 1-2. Données collectées depuis Horizon Client pour le programme d'amélioration du produit (suite)

Description	Ce champ reste-t-il anonyme ?	Exemple
Modèle du système hôte	Non	Exemples : ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision WorkStation T3400 (A04 03/21/2008)
Processeur du système hôte	Non	Exemples : ■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH ■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH ■ inconnu (pour iPad)
Nombre de cœurs dans le processeur du système hôte	Non	Par exemple : 4
Mo de mémoire sur le système hôte	Non	Exemples : ■ 4096 ■ inconnu (pour Windows Store)
Nombre de périphériques USB connectés	Non	2 (la redirection de périphériques USB est prise en charge uniquement pour les clients Linux, Windows et Mac OS X.)
Nombre maximal de connexions de périphériques USB simultanées	Non	2
ID de fournisseur de périphériques USB	Non	Exemples : ■ Kingston ■ NEC ■ Nokia ■ Wacom
ID de produit de périphérique USB	Non	Exemples : ■ DataTraveler ■ Gamepad ■ Disque de stockage ■ Souris sans fil
Famille de périphériques USB	Non	Exemples : ■ Sécurité ■ Périphérique d'interface humaine ■ Imagerie
Nombre d'utilisations du périphérique USB	Non	(Nombre de partages du périphérique)

Utilisation d'URI pour configurer Horizon Client

2

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

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

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

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

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

Ce chapitre aborde les rubriques suivantes :

Syntaxe pour la création d'URI vmware-view

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

Spécification d'URI

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

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

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

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

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

---

authority-part

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

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

`user1@`*`server-address`*

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

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

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

path-part

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

query-part

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

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

Requêtes prises en charge

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

action

Tableau 2-1. Valeurs pouvant être utilisées avec la Requête d'action

Valeur	Description
`browse`	Affiche une liste des postes de travail ou applications disponibles hébergées sur le serveur spécifié. Il ne vous est pas demandé de spécifier un poste de travail ou une application pour l'utilisation de cette action. Si vous utilisez l'action `browse` et que vous spécifiez un poste de travail ou une application, ceux-ci sont mis en surbrillance dans la liste des postes de travail ou d'applications disponibles.
`start-session`	Lance le poste de travail ou l'application spécifiée. Si aucune requête d'action n'est fournie et que le nom du poste de travail ou de l'application est fourni, `start-session` est l'action par défaut.
`reset`	Éteint puis redémarre le poste de travail spécifié. Les données non enregistrées sont perdues. La réinitialisation d'un poste de travail distant équivaut à appuyer sur le bouton Réinitialiser d'un ordinateur physique. Dans Horizon Client 3.0, si vous spécifiez une application, l'action sera ignorée.
`logoff`	Déconnecte l'utilisateur du système d'exploitation invité sur le poste de travail distant. Si vous spécifiez une application, l'action sera ignorée ou l'utilisateur final verra le message d'avertissement « Action d'URI non valide ».

connectUSBOnInsert

Connecte un périphérique USB au poste de travail virtuel au premier plan lorsque vous branchez le périphérique. Cette requête est paramétrée de façon implicite si vous spécifiez la requête `unattended`. Pour utiliser cette requête, vous devez paramétrer la requête `action` sur **`start-session`** ou ne pas utiliser de requête `action`. Les valeurs valides sont **`true`** et **`false`**. Exemple de syntaxe : **`connectUSBOnInsert=true`**.

connectUSBOnStartup

(Pour Horizon Client 1.7 et versions ultérieures) Redirige tous les périphériques USB actuellement connectés au système client vers le poste de travail. Cette requête est paramétrée de façon implicite si vous spécifiez la requête `unattended`. Pour utiliser cette requête, vous devez paramétrer la requête `action` sur **`start-session`** ou ne pas utiliser de requête `action`. Les valeurs valides sont **`true`** et **`false`**. Exemple de syntaxe : **`connectUSBOnStartup=true`**.

desktopLayout

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

Tableau 2-2. Valeurs valides pour la requête desktopLayout

Valeur	Description
`fullscreen`	Tous les moniteurs externes connectés affichent leur contenu en plein écran. Il s'agit du réglage par défaut.
`windowLarge`	Fenêtre de grande taille.

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

Valeur	Description
`windowSmall`	Fenêtre de petite taille.
*W*x*H*	Personnalisez la résolution, spécifiez la largeur et la hauteur en pixels. Exemple de syntaxe : **`desktopLayout=1280x800`**.

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

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

Exemples d'URI de vmware-view

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

Exemples de syntaxe URI

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7 `vmware-view://`

Horizon Client est lancé et l'utilisateur est dirigé vers la page pour entrer l'adresse d'une instance de Serveur de connexion View.

Exemples de code HTML

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

```
<html>
<body>

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

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

</body>
</html>
```

Gestion des connexions aux applications et postes de travail distants

3

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

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

Ce chapitre aborde les rubriques suivantes :

Se connecter à une application ou à un poste de travail distant pour la première fois

Avant de laisser vos utilisateurs finaux accéder à leurs applications et postes de travail distants, vérifiez que vous pouvez vous connecter à une application ou un poste de travail distant à partir du système client.

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

Prérequis

- Obtenez les informations d'identification dont vous avez besoin pour ouvrir une session, telles que le nom d'utilisateur et le mot de passe Active Directory, le nom d'utilisateur et le code secret RSA SecurID ou le nom d'utilisateur et le code secret pour l'authentification RADIUS.
- Obtenez le nom de domaine pour ouvrir une session.

- Effectuez les tâches administratives décrites dans « Préparation du Serveur de connexion View pour Horizon Client », page 9.
- Si vous vous trouvez à l'extérieur du réseau d'entreprise et si vous n'utilisez pas de serveur de sécurité pour accéder au poste de travail distant, vérifiez que votre périphérique client est configuré pour utiliser une connexion VPN et activez cette connexion.

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

- Vérifiez que vous disposez du nom de domaine complet (FQDN) du serveur qui fournit l'accès à l'application ou au poste de travail distant. Notez que les traits de soulignement (_) ne sont pas pris en charge dans les noms de serveur. Vous avez également besoin du numéro de port si le port n'est pas 443.
- Si vous prévoyez d'utiliser le protocole d'affichage RDP pour vous connecter à un poste de travail distant, vérifiez que le paramètre de stratégie de groupe AllowDirectRDP de View Agent est activé.
- Si votre administrateur l'a autorisé, vous pouvez configurer le mode de vérification des certificats pour le certificat SSL que le serveur View server présente. Reportez-vous à la section « Modes de vérification des certificats pour Horizon Client », page 26.
- Si les utilisateurs finaux sont autorisés à utiliser le protocole d'affichage Microsoft RDP, vérifiez que le système client dispose de la version 2.0 ou ultérieure de Remote Desktop Connection Client pour Mac de Microsoft. Vous pouvez télécharger ce client sur le site Web de Microsoft.

Procédure

1. Dans le dossier **Applications**, double cliquez sur **VMware Horizon View Client** (Horizon Client 3.0) ou **VMware Horizon Client** (Horizon Client 3.1).
2. Cliquez sur **Continuer** pour démarrer les services USB et d'impression du poste de travail distant ou sur **Annuler** pour utiliser Horizon Client sans ces services.

   Si vous cliquez sur **Continuer**, vous devez fournir des informations d'identification système. Si vous cliquez sur **Annuler**, vous pouvez activer les services USB et d'impression du poste de travail distant.

   REMARQUE L'invite pour démarrer les services USB et d'impression du poste de travail distant s'affiche la première fois que vous lancez Horizon Client. Il n'apparaît plus, que vous cliquiez sur **Annuler** ou **Continuer**.

3. Cliquez sur l'icône **Ajouter un serveur** (Horizon Client 3.0) ou **Nouveau serveur** (Horizon Client 3.1) sur l'écran d'accueil d'Horizon Client.
4. Tapez le nom de serveur et un numéro de port si nécessaire, puis cliquez sur **Continuer** (Horizon Client 3.0) ou **Connecter** (Horizon Client 3.1).

   Voici un exemple d'utilisation d'un port non défini comme port par défaut : **`view.company.com:1443`**.
5. Si un message demande les informations d'identification RSA SecurID ou les informations d'identification de l'authentification RADIUS, entrez le nom d'utilisateur et le code secret, puis cliquez sur **Connexion**.
6. Entrez vos nom d'utilisateur et mot de passe, sélectionnez un domaine et cliquez sur **Ouverture de session**.

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

7 Si l'indicateur de sécurité de poste de travail devient rouge et qu'un message d'avertissement apparaît, répondez à l'invite.

   Généralement, cet avertissement indique que le Serveur de connexion View n'a pas envoyé d'empreinte numérique de certificat au client. L'empreinte numérique est un hachage de la clé publique du certificat et elle est utilisée comme abréviation de la clé publique. Le Serveur de connexion View 4.6.1, 5.0.1 et les versions supérieures envoient des informations d'empreinte numérique, contrairement aux versions antérieures.

8 (Facultatif) Si vous êtes connecté à un poste de travail distant, sélectionnez le protocole d'affichage à utiliser.

   Le protocole d'affichage par défaut est **PCoIP**. Si vous préférez utiliser RDP Microsoft, sélectionnez le nom du poste de travail, cliquez sur Contrôle sur le clavier Apple et sélectionnez **RDP**.

9 Double-cliquez sur une application ou un poste de travail distant pour vous connecter.

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

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

- Déterminez si le Serveur de connexion View est configuré pour ne pas utiliser SSL. Horizon Client requiert des connexions SSL. Vérifiez si le paramètre général dans View Administrator de la case **Use SSL for client connections (Utiliser SSL pour les connexions client)** est désélectionné. Si c'est le cas, vous devez cocher la case pour que SSL soit utilisé ou configurer votre environnement de sorte que les clients puissent se connecter à un équilibreur de charge activé pour HTTPS ou à un autre périphérique intermédiaire configuré pour établir une connexion HTTP vers Serveur de connexion View.
- Vérifiez que le certificat de sécurité pour le Serveur de connexion View fonctionne correctement. Si ce n'est pas le cas, dans View Administrator, vous pouvez également voir que View Agent sur des postes de travail n'est pas accessible.
- Vérifiez que les balises définies sur l'instance de Serveur de connexion View autorisent les connexions depuis cet utilisateur. Consultez le document *Administration de View*.
- Vérifiez que l'utilisateur est autorisé à accéder à ce poste de travail ou à cette application. Consultez le document *Configuration de pools de postes de travail et d'applications dans View*.
- Si vous utilisez le protocole d'affichage RDP pour vous connecter à un poste de travail distant, vérifiez que l'ordinateur client autorise les connexions à des postes de travail distants.

Masquer la fenêtre VMware Horizon Client

Pour une expérience transparente d'application ou de poste de travail distant, vous pouvez masquer la fenêtre VMware Horizon Client après le lancement d'une application ou d'un poste de travail distant.

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

Procédure

- Pour masquer la fenêtre VMware Horizon Client après avoir lancé une application ou un poste de travail distant, cliquez sur le bouton **Fermer** dans le coin de la fenêtre VMware Horizon Client.

  L'icône de VMware Horizon Client s'affiche dans le Dock.

- Pour définir une préférence afin de toujours masquer la fenêtre VMware Horizon Client après le lancement d'une application ou d'un poste de travail distant, effectuez la procédure suivante avant de vous connecter à un serveur View Server.

  a Sélectionnez **VMware Horizon Client > Préférences** dans la barre de menus, puis cliquez sur **Général** dans la boîte de dialogue Préférences.

  b Sélectionnez **Masquer la fenêtre du client après le lancement d'une application ou d'un poste de travail**.

  c Fermez la boîte de dialogue Préférences.

  Vos modifications prennent effet à la fermeture de la boîte de dialogue.

- Pour afficher la fenêtre VMware Horizon Client lorsqu'elle est masquée, sélectionnez **Fenêtre > Ouvrir une fenêtre de sélection** dans la barre de menus ou cliquez avec le bouton droit sur l'icône de VMware Horizon Client dans le Dock, puis sélectionnez **Afficher toutes les fenêtres**.

Modes de vérification des certificats pour Horizon Client

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

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

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

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

Remarque Pour plus d'informations sur la distribution d'un certificat racine auto-signé et sur son installation sur des systèmes client Mac OS X, consultez le document *Advanced Server Administration* (Administration avancée de serveur) pour le serveur Mac OS X que vous utilisez, disponible sur le site Web d'Apple.

Outre la présentation d'un certificat de serveur, le Serveur de connexion View 4.6.1, 5.0.1 et les versions ultérieures envoient une empreinte numérique de certificat à Horizon Client. L'empreinte numérique est un hachage de la clé publique du certificat et elle est utilisée comme abréviation de la clé publique. Si le serveur View server n'envoie pas d'empreinte numérique, un avertissement s'affiche pour indiquer que la connexion n'est pas autorisée.

Si votre administrateur l'a autorisé, vous pouvez définir le mode de vérification des certificats. Sélectionnez **VMware Horizon View Client > Préférences** (Horizon Client 3.0) ou **VMware Horizon Client > Préférences** (Horizon Client 3.1) dans la barre de menus. Vous avez trois possibilités :

- **Ne jamais se connecter à des serveurs non autorisés**. Si l'une des vérifications de certificat échoue, le client ne peut pas se connecter au serveur. Un message d'erreur répertorie les vérifications qui ont échoué.

- **Signaler avant de se connecter à des serveurs non autorisés**. Si une vérification de certificat échoue car le serveur utilise un certificat auto-signé, vous pouvez cliquer sur **Continuer** pour ignorer l'avertissement. Pour les certificats auto-signés, le nom du certificat ne doit pas nécessairement correspondre au nom du Serveur de connexion View que vous avez entré dans Horizon Client.
- **Ne pas vérifier les certificats d'identité des serveurs**. Ce paramètre signifie que View n'effectue aucune vérification de certificat.

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

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

Recherche de postes de travail ou d'applications

Dès que vous êtes connecté à un serveur View Server, les applications et postes de travail disponibles sur ce serveur s'affichent dans la fenêtre de sélection des postes de travail et applications. Vous pouvez rechercher un poste de travail ou une application spécifique en tapant dans la fenêtre.

Lorsque vous commencez à taper, Horizon Client affiche en surbrillance la première application ou le premier poste de travail correspondant. Pour vous connecter à une application ou un poste de travail affiché en surbrillance, appuyez sur la touche Entrée. À mesure que vous tapez le nom du poste de travail, Horizon Client continue à rechercher les applications et postes de travail correspondants. Si Horizon Client trouve plusieurs applications ou postes de travail correspondants, appuyez sur la touche de tabulation pour passer au résultat suivant. Si vous arrêtez de taper pendant deux secondes avant de recommencer, Horizon Client suppose que vous démarrez une nouvelle recherche.

Sélectionner une application ou un poste de travail distant favori

Vous pouvez sélectionner des postes de travail et des applications distants comme favoris. Les favoris sont identifiés par une étoile. Cette étoile vous permet de trouver rapidement vos postes de travail et applications favoris. Vos sélections favorites sont sauvegardées, même après la fermeture de votre session sur le serveur.

Prérequis

Obtenez les informations d'identification dont vous avez besoin pour vous connecter au serveur, telles qu'un nom d'utilisateur et un mot de passe ou un jeton RSA SecurID et un code secret.

Procédure

1 Sur l'écran d'accueil Horizon Client, double-cliquez sur l'icône du serveur.

2 Si vous y êtes invité, entrez votre nom d'utilisateur et code secret RSA, votre nom d'utilisateur et mot de passe Active Directory, ou les deux.

3 Procédez comme suit pour sélectionner ou désélectionner un poste de travail ou une application comme favori.

Option	Description
Sélectionner un favori	Sélectionnez le raccourci du poste de travail ou de l'application, cliquez sur Contrôle et sélectionnez **Marquer comme favori** dans le menu contextuel. Une étoile apparaît dans le coin supérieur droit du raccourci du poste de travail ou de l'application.
Désélectionner un favori	Sélectionnez le raccourci du poste de travail ou de l'application, cliquez sur Contrôle et désélectionnez **Marquer comme favori** dans le menu contextuel. L'étoile disparaît du coin supérieur droit du raccourci du poste de travail ou de l'application.

4 (Facultatif) Pour afficher uniquement les applications et les postes de travail favoris, cliquez sur le bouton **Favoris** (icône étoile) dans le coin supérieur droit de la fenêtre de sélection des postes de travail et des applications.

Vous pouvez cliquer de nouveau sur le bouton **Favoris** pour afficher tous les postes de travail et toutes les applications disponibles.

Basculer entre des postes de travail ou des applications

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

Procédure

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

Option	Action
Choisir une autre application ou un autre poste de travail sur le même serveur	Effectuez l'une des opérations suivantes : ■ Pour maintenir le poste de travail actuel ouvert et vous connecter également à un autre poste de travail distant, sélectionnez **Fenêtre > VMware Horizon View Client** (Horizon Client 3.0) ou **Fenêtre > VMware Horizon Client** (Horizon Client 3.1) dans la barre de menus et double-cliquez sur le raccourci de l'autre poste de travail. Ce poste de travail s'ouvre dans une nouvelle fenêtre pour vous permettre d'avoir plusieurs postes de travail ouverts. Vous pouvez passer d'un poste de travail à un autre à partir du menu **Fenêtre** de la barre de menus. ■ Pour fermer le poste de travail actuel et vous connecter à un autre poste de travail, sélectionnez **Connexion > Se déconnecter** dans la barre de menus et double-cliquez sur le raccourci de l'autre poste de travail. ■ Pour ouvrir une autre application, double-cliquez sur le raccourci de l'application en question. Cette application s'ouvre dans une nouvelle fenêtre. Vous pouvez avoir plusieurs applications ouvertes simultanément et basculer de l'une à l'autre en cliquant sur la fenêtre d'une application.
Choisir une application ou un poste de travail sur un serveur différent	Si vous êtes autorisé à utiliser plusieurs postes de travail ou applications, et que souhaitez garder la fenêtre de sélection des postes de travail et applications ouverte, cliquez sur le bouton **Se déconnecter du serveur** dans la partie gauche de la barre d'outils de la fenêtre de sélection des postes de travail et applications, puis déconnectez-vous du serveur. Si vous n'êtes autorisé à utiliser qu'un poste de travail ou une application et que la fenêtre de sélection des postes de travail et applications n'est pas ouverte, vous pouvez sélectionner **Fichier > Déconnexion du serveur** dans la barre de menus, puis vous connecter à un serveur différent.

Fermer une session ou se déconnecter

Si vous vous déconnectez d'un poste de travail distant sans fermer votre session, les applications du poste de travail restent ouvertes. Vous pouvez également vous déconnecter d'un serveur tout en gardant des applications distantes en cours d'exécution.

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

Remarque La combinaison de touches Windows Ctrl+Alt+Suppr n'est pas prise en charge sur les postes de travail distants. Pour utiliser l'équivalent de la combinaison de touches Ctrl+Alt+Del, sélectionnez **Connexion > Envoyer Ctrl-Alt-Del** dans la barre de menus.

Vous pouvez également appuyer sur Fn-Control-Option-Delete sur un clavier Apple.

Procédure

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

Option	Action
Se déconnecter et quitter Horizon Client	Horizon Client 3.0 : ■ Cliquez sur le bouton **Fermer** dans l'angle de la fenêtre ou sélectionnez **Fichier > Fermer** dans la barre de menus. Horizon Client 3.1 : a Cliquez sur le bouton **Fermer** dans l'angle de la fenêtre ou sélectionnez **Fichier > Fermer** dans la barre de menus. b Sélectionnez **VMware Horizon Client > Quitter VMware Horizon Client** dans la barre de menus.
Se déconnecter et rester dans Horizon Client	Cliquez sur le bouton **Déconnecter** dans la barre d'outils ou sélectionnez **Connexion > Déconnecter** dans la barre de menus.

Remarque Votre administrateur View peut configurer votre poste de travail pour que la session soit fermée automatiquement lors de la déconnexion. Dans ce cas, toutes les applications ouvertes sur votre poste de travail sont arrêtées.

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

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

- Se déconnecter d'une application distante.

Option	Action
Se déconnecter du serveur et garder l'application en cours d'exécution	Effectuez l'une des opérations suivantes : ■ Cliquez sur le bouton **Se déconnecter du serveur** sur le côté gauche de la barre d'outils de la fenêtre de sélection des postes de travail et applications. ■ Sélectionnez **Fichier > Se déconnecter du serveur** dans la barre de menus.
Fermer l'application et se déconnecter du serveur	a Quittez l'application de la façon habituelle, par exemple en cliquant sur le bouton **Fermer** dans le coin de la fenêtre d'application. b Cliquez sur le bouton **Se déconnecter du serveur** sur le côté gauche de la barre d'outils de la fenêtre de sélection des postes de travail et applications ou sélectionnez **Fichier > Se déconnecter du serveur** dans la barre de menus.

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

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

Option	Action
Depuis l'écran d'accueil	a Double-cliquez sur le raccourci de serveur et entrez les informations d'identification. Il peut s'agir des informations d'identification RSA SecurID et des informations d'identification pour ouvrir une session sur le poste de travail. b Sélectionnez le poste de travail et choisissez **Connexion > Fermer la session** dans la barre de menus.
Depuis la fenêtre de sélection des postes de travail et applications	Sélectionnez le poste de travail et choisissez **Connexion > Fermer la session** dans la barre de menus.

Configurer le comportement de reconnexion des applications distantes

Si un utilisateur se déconnecte du serveur View sans fermer l'application distante, Horizon Client invite l'utilisateur à rouvrir l'application à sa prochaine reconnexion au serveur. Vous pouvez changer ce comportement en modifiant le paramètre Comportement de reconnexion dans Horizon Client.

Prérequis

Obtenez les informations d'identification dont vous avez besoin pour vous connecter au serveur, telles qu'un nom d'utilisateur et un mot de passe ou un nom d'utilisateur RSA SecurID et un code secret.

Procédure

1 Sur l'écran d'accueil Horizon Client, double-cliquez sur l'icône du serveur.

2 Si vous y êtes invité, entrez votre nom d'utilisateur et code secret RSA, votre nom d'utilisateur et mot de passe Active Directory, ou les deux.

3 Cliquez sur le bouton **Paramètres** (icône d'engrenage) dans l'angle supérieur droit de la fenêtre de sélection du poste de travail et de l'application.

4 Sélectionnez **Applications** dans le volet de gauche de la boîte de dialogue Paramètres.

5 Sélectionnez une option de comportement de reconnexion à l'application.

Ces options déterminent de quelle manière Horizon Client se comporte lorsqu'un utilisateur se connecte au serveur et que des applications distantes sont toujours en cours d'exécution.

Option	Description
Demander la reconnexion pour ouvrir des applications	Horizon Client affiche le message **Une ou plusieurs applications distantes sont en cours d'exécution. Voulez-vous les ouvrir maintenant ?** . Les utilisateurs peuvent répondre en cliquant sur **Se reconnecter aux applications** ou **Pas maintenant**. Les utilisateurs peuvent également cocher la case **Ne plus afficher ce message.** pour supprimer ce message à l'avenir. Ce paramètre est activé par défaut.
Se reconnecter automatiquement pour ouvrir des applications	Horizon Client rouvre immédiatement les applications en cours d'exécution.
Ne pas demander la reconnexion et ne pas se reconnecter automatiquement	Horizon Client n'invite pas les utilisateurs à rouvrir les applications en cours d'exécution, ni ne rouvre les applications en cours d'exécution. Ce paramètre a le même effet que la case à cocher **Ne plus afficher ce message.**.

6 Cliquez sur **Continuer** pour enregistrer vos modifications.

Le nouveau paramètre s'applique la prochaine fois qu'un utilisateur se connecte au serveur.

Supprimer un raccourci de serveur View Server de l'écran d'accueil

Dès que vous êtes connecté à un serveur View Server, un raccourci du serveur est enregistré sur l'écran d'accueil d'Horizon Client.

Vous pouvez supprimer un raccourci de Serveur de connexion View en sélectionnant le raccourci et en appuyant sur la touche Supprimer, ou bien en cliquant sur Contrôle ou en cliquant avec le bouton droit sur le raccourci sur l'écran d'accueil et en sélectionnant **Supprimer**.

Vous ne pouvez pas supprimer des raccourcis d'applications ou de postes de travail distants qui s'affichent une fois que vous êtes connecté à un serveur.

Réorganisation des raccourcis

Vous pouvez réorganiser les raccourcis des serveurs View Server et les raccourcis d'applications et de postes de travail distants.

Chaque fois que vous vous connectez à un serveur View Server, Horizon Client enregistre un raccourci du serveur sur l'écran d'accueil. Pour réorganiser les raccourcis des serveurs View Server, sélectionnez-en un et faites-le glisser vers un nouvel emplacement sur l'écran d'accueil.

Dès que vous êtes connecté à un serveur View Server, les applications et postes de travail disponibles sur ce serveur s'affichent dans la fenêtre de sélection des postes de travail et applications. Les raccourcis des postes de travail apparaissent en premier, suivi des raccourcis d'applications. Les raccourcis des postes de travail et d'applications s'affichent par ordre alphabétique et ne peuvent pas être réorganisés. Lorsque vous êtes dans la vue Favoris (après avoir cliqué sur le bouton **Favoris** dans le coin supérieur droit de la fenêtre de sélection des postes de travail et applications), vous pouvez réorganiser les raccourcis des postes de travail et d'applications en sélectionnant un raccourci et en le faisant glisser vers un nouvel emplacement de la fenêtre.

Restaurer un poste de travail

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

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

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

Prérequis

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

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

Procédure

1. Si l'écran d'accueil Horizon Client affiche des raccourcis vers le Serveur de connexion View, double-cliquez sur le raccourci du serveur pouvant accéder au poste de travail et entrez les informations d'authentification.
   a. Si un message demande les informations d'identification RSA SecurID ou les informations d'identification pour l'authentification RADIUS, entrez le nom d'utilisateur et le code secret et cliquez sur **Continuer**.
   b. Saisissez votre nom d'utilisateur et votre mot de passe dans la boîte de dialogue de connexion.
2. Sur l'écran d'accueil d'Horizon Client qui affiche les raccourcis des postes de travail distants, sélectionnez le poste de travail, puis choisissez **Connexion > Restaurer** dans la barre de menus.

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

Utilisation d'un poste de travail ou d'une application Microsoft Windows sur un ordinateur Mac

4

Horizon Client pour Mac OS X prend en charge plusieurs fonctionnalités.

Ce chapitre aborde les rubriques suivantes :

Matrice de prise en charge des fonctions

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

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

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

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

Fonction	Poste de travail Windows 8.x	Poste de travail Windows 7	Poste de travail Windows Vista	Poste de travail Windows XP	Poste de travail Windows Server 2008 R2
Impression virtuelle	X	X	X	X	X
Impression basée sur l'emplacement	X	X	X	X	X
Cartes à puce					
Plusieurs écrans	X	X	X	X	X

Les restrictions suivantes s'appliquent aux fonctionnalités prises en charge sur des postes de travail Windows pour Horizon Client Mac OS X.

- Les postes de travail Windows 8.x sont uniquement pris en charge si vous disposez de serveurs et de postes de travail View 5.2 ou version ultérieure.
- Les postes de travail Windows Server 2008 R2 sont pris en charge uniquement si vous possédez des serveurs et des postes de travail View 5.3 ou version ultérieure.
- Pour plus d'informations sur l'établissement d'une connexion RDP avec un poste de travail Windows 8.1, consultez l'article de la base de connaissance VMware à l'adresse http://kb.vmware.com/kb/2059786.
- La fonctionnalité Audio/Vidéo en temps réel est uniquement prise en charge si vous disposez de View 5.2 avec Feature Pack 2 ou version ultérieure. Pour voir la liste complète des exigences, reportez-vous à « Configuration système requise pour l'Audio/Vidéo en temps réel », page 8.
- L'impression virtuelle et l'impression basée sur l'emplacement sont prises en charge pour les postes de travail Windows Server 2008 R2, les postes de travail RDS (sur les hôtes RDS de machine virtuelle), et sur les applications distantes uniquement dans Horizon Client 3.1 et les serveurs Horizon 6.0.1 avec View et version ultérieure.

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

Vous ne pouvez utiliser des applications distantes que si vous êtes connecté à un Serveur de connexion View 6.0 ou version ultérieure. Pour en savoir plus sur les systèmes d'exploitation pris en charge pour l'hôte RDS (Remote Desktop Sessions) qui fournit des applications et des postes de travail distants basés sur la session, consultez le document *Planification de l'architecture View*.

Pour plus d'informations sur ces fonctionnalités et leurs limites, consultez le document *Planification de l'architecture de View*.

Internationalisation

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

Écrans et résolution d'écran

Si vous utilisez le protocole d'affichage PCoIP, vous pouvez partager un poste de travail distant sur plusieurs écrans. Si vous disposez d'un Mac avec affichage Retina, vous pouvez afficher le poste de travail distant en pleine résolution.

Utilisation de plusieurs moniteurs

Si vous utilisez le protocole d'affichage PCoIP lorsque vous accédez au poste de travail distant, vous pouvez utiliser jusqu'à deux moniteurs, avec une résolution pouvant aller jusqu'à 2 560 x 1 600 par affichage. Si vous utilisez deux moniteurs, vous pouvez les placer côte à côte ou l'un au-dessus de l'autre.

Lorsque la fonctionnalité 3D est activée, la résolution maximale est de 1 920 x 1 200. Les thèmes Windows Aero, Microsoft Office 2010 et Google Earth sont des exemples d'applications 3D.

Pour partager un poste de travail distant sur plusieurs écrans, vous pouvez utiliser l'élément de menu **Fenêtre > Plein écran** ou les flèches de développement situées dans le coin supérieur droit de la fenêtre du poste de travail.

Utilisation d'un Mac haute résolution disposant de l'affichage Retina

Si vous utilisez le protocole d'affichage PCoIP, Horizon Client prend également en charge de très hautes résolutions pour ces systèmes clients disposant de l'affichage Retina. Une fois connecté à un poste de travail distant, vous pouvez choisir l'élément de menu **Connexion > Résolution > Résolution maximale**. Cet élément de menu apparaît seulement si le système client prend en charge l'Affichage Retina.

Si vous utilisez **Résolution maximale**, les icônes affichées sur le poste de travail distant sont plus petites, mais l'affichage est plus net.

Connecter des périphériques USB

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

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

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

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

- Si vous prévoyez d'ajouter des périphériques USB qui utilisent des pilotes MTP, tels que des smartphones et des tablettes Samsung fonctionnant sous Android, vous devez configurer Horizon Client afin qu'il connecte automatiquement des périphériques USB à votre poste de travail distant. Dans le cas contraire, si vous tentez de rediriger manuellement le périphérique USB à l'aide d'un élément de menu, le périphérique ne sera pas redirigé, sauf si vous le débranchez avant de le brancher de nouveau.
- Les webcams ne sont pas prises en charge pour la redirection USB.
- 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.

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

Remarque Ne redirigez pas les connexions Ethernet USB vers le poste de travail distant. Votre poste de travail distant peut se connecter à votre réseau si votre système local est connecté. Si vous avez configuré votre poste de travail distant afin de connecter automatiquement des périphériques USB, vous pouvez ajouter une exception pour exclure votre connexion Ethernet. Reportez-vous à la section « Configurer la redirection USB sur un client Mac OS X », page 37.

Prérequis

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

  Cette tâche inclut l'installation du composant **Redirection USB** de View Agent, et peut inclure la configuration de stratégies de groupe concernant la redirection USB. Pour plus d'informations, reportez-vous au document *Administration de View* si vous utilisez un Serveur de connexion View et View Agent 5.x ou une version antérieure. Reportez-vous à *Configuration des pools de postes de travail et d'applications dans View* si vous utilisez un Serveur de connexion View et View Agent 6.0 ou version ultérieure.
- S'il s'agit de votre première tentative de connexion d'un périphérique USB, vous devez fournir le mot de passe de l'administrateur. Horizon Client vous y invitera le moment venu.

  Certains composants requis pour la redirection USB déjà installés par Horizon Client doivent être configurés et la configuration de ces composants requiert des privilèges d'administrateur.

Procédure

- Connectez manuellement le périphérique USB à un poste de travail distant.

  a S'il s'agit de votre première utilisation de la fonctionnalité USB, dans la barre de menus VMware Horizon Client, cliquez sur **Connexion > USB > Démarrer les services USB du poste de travail distant** et fournissez le mot de passe de l'administrateur lorsque vous y êtes invité.

  b Connectez le périphérique USB au système client local.

  c Dans la barre de menus VMware Horizon Client, cliquez sur **Connexion > USB**.

  d Connectez-vous à un poste de travail distant pour répertorier les périphériques USB connectés et sélectionner un périphérique USB.

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

- Configurez Horizon Client afin de connecter automatiquement des périphériques USB au poste de travail distant lorsque vous les branchez au système local.

  Si vous prévoyez de connecter des périphériques qui utilisent des pilotes MTP, tels que des smartphones et des tablettes Samsung fonctionnant avec Android, assurez-vous d'utiliser cette fonction de connexion automatique.

  a Avant de brancher le périphérique USB, démarrez Horizon Client et connectez-vous à un poste de travail distant.

  b S'il s'agit de votre première utilisation de la fonctionnalité USB, dans la barre de menus VMware Horizon Client, cliquez sur **Connexion > USB > Démarrer les services USB du poste de travail distant** et fournissez le mot de passe de l'administrateur lorsque vous y êtes invité.

  c Dans la barre de menus VMware Horizon Client, cliquez sur **Connexion > USB > Connecter automatiquement à l'insertion**.

  d Branchez le périphérique USB.

  Les périphériques USB que vous connectez à votre système local après le démarrage d'Horizon Client sont redirigés vers le poste de travail distant.

- Configurez Horizon Client afin de connecter automatiquement des périphériques USB au poste de travail distant au démarrage d'Horizon Client.

  a S'il s'agit de votre première utilisation de la fonctionnalité USB, dans la barre de menus VMware Horizon Client, cliquez sur **Connexion > USB > Démarrer les services USB du poste de travail distant** et fournissez le mot de passe de l'administrateur lorsque vous y êtes invité.

  b Dans la barre de menus VMware Horizon Client, cliquez sur **Connexion > USB > Connecter automatiquement au démarrage**.

  c Branchez le périphérique USB et redémarrez Horizon Client.

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

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

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

Suivant

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

Configurer la redirection USB sur un client Mac OS X

Les administrateurs peuvent configurer le système client afin qu'il spécifie les périphériques USB pouvant être redirigés vers un poste de travail distant.

Vous pouvez configurer des stratégies USB pour View Agent sur le poste de travail distant et pour Horizon Client sur le système local, afin d'atteindre les objectifs suivants :

- Limiter les types de périphériques USB qu'Horizon Client rend disponibles à la redirection.
- Faire en sorte que View Agent empêche certains périphériques USB d'être transférés depuis un ordinateur client.

- Spécifier si Horizon Client doit fractionner des périphériques USB composites en composants distincts pour la redirection.

  Les périphériques USB composites sont composés de deux périphériques ou plus, tels qu'un périphérique d'entrée vidéo et un périphérique de stockage.

Les paramètres de configuration sur le client peuvent être fusionnés avec, ou remplacés par, des stratégies correspondantes, paramétrées pour View Agent sur le poste de travail distant. Pour savoir comment les paramètres USB du client fonctionnent en association avec les stratégies USB de View Agent, consultez les rubriques abordant l'utilisation de stratégies pour contrôler la redirection USB dans le document *Administration de View*.

IMPORTANT La fonctionnalité de redirection USB est uniquement disponible lorsque la version de View Agent et du Serveur de connexion View est View 4.6.1 ou une version ultérieure. Les fonctionnalités de filtre USB et de fractionnement automatique décrites dans ces rubriques sont disponibles avec le Serveur de connexion View 5.1 et versions supérieures.

Syntaxe pour la configuration de la redirection USB

Vous pouvez configurer des règles de filtrage et de fractionnement pour générer ou empêcher la redirection de périphériques USB vers un poste de travail distant. Sur un client Mac OS X, il est possible de configurer la fonctionnalité USB en utilisant Terminal (`/Applications/Utilities/Terminal.app`) et en exécutant une commande en tant que root (racine).

- Pour répertorier les règles :

  ```
  # sudo defaults read <varname id="VARNAME_95A3DC2017354B8FA8955CED8F69664D">domain</varname>
  ```

  Par exemple :

  ```
  # sudo defaults read com.vmware.viewusb
  ```

- Pour supprimer une règle :

  ```
  # sudo defaults delete <varname id="VARNAME_E3808110D7D140F3ABFD8180E81A519F">domain
  property</varname>
  ```

  Par exemple :

  ```
  # sudo defaults delete com.vmware.viewusb ExcludeVidPid
  ```

- Pour définir ou remplacer une règle de filtre :

  ```
  # sudo defaults write <varname id="VARNAME_46C33BABBB1243C4AE3F4C9D16FE45C0">domain property
  value</varname>
  ```

  Par exemple :

  ```
  # sudo defaults write com.vmware.viewusb ExcludeVidPid vid-1234_pid-5678
  ```

  IMPORTANT certains paramètres de configuration nécessitent le VID (ID du fournisseur) et le PID (ID du produit) pour un périphérique USB. Pour connaître le VID et le PID, vous pouvez rechercher le nom du produit sur Internet, associé à `vid` et `pid`. Vous pouvez également consulter le fichier journal USB après avoir connecté le périphérique USB au système local lorsqu'Horizon Client est en cours d'exécution. Pour plus d'informations, reportez-vous à la section « Activer la journalisation pour la redirection USB », page 42.

- Pour mettre en place ou remplacer une règle de fractionnement pour un périphérique composite :

  ```
  # sudo defaults write <varname id="VARNAME_5201E63FDDD54D1ABEC023C9FF47AA34">domain property
  value</varname>
  ```

Par exemple :

```
# sudo defaults write com.vmware.viewusb AllowAutoDeviceSplitting true
# sudo defaults write com.vmware.viewusb SplitExcludeVidPid vid-03f0_Pid-2a12
# sudo defaults write com.vmware.viewusb SplitVidPid "'vid-0911_Pid-149a(exintf:03)'"
# sudo defaults write com.vmware.viewusb IncludeVidPid vid-0911_Pid-149a
```

Les périphériques USB composites sont composés de deux périphériques ou plus, tels qu'un périphérique d'entrée vidéo et un périphérique de stockage. La première ligne de cet exemple active le fractionnement automatique des périphériques composites. La deuxième ligne empêche le périphérique USB composite spécifié (`Vid-03f0_Pid-2a12`) de se fractionner.

La troisième ligne indique à Horizon Client qu'il faut traiter les composants d'un périphérique composite différent (`Vid-0911_Pid-149a`) en tant que périphériques distincts, mais qu'il faut exclure le composant suivant de la redirection : le composant dont le numéro d'interface est 03. Ce composant est conservé en mode local.

Du fait que ce périphérique composite inclut un composant qui est normalement exclu par défaut, tel qu'une souris ou un clavier, la quatrième ligne est nécessaire pour que les autres composants du périphérique composite `Vid-0911_Pid-149a` puissent être redirigés vers le poste de travail distant.

Les trois premières propriétés sont des propriétés de fractionnement. La dernière propriété est une propriété de filtrage. Les propriétés de filtrage s'effectuent avant les propriétés de fractionnement.

Exemple : Exclusion d'un périphérique Ethernet USB

Il est possible que vous souhaitiez exclure de la redirection un périphérique Ethernet USB. Supposez que votre Mac utilise un périphérique Ethernet USB pour connecter le réseau du système client Mac à un poste de travail distant. Si vous redirigez le périphérique Ethernet USB, votre système client local perdra sa connexion avec le réseau et le poste de travail distant.

Si vous souhaitez masquer de manière permanente ce périphérique dans le menu de connexion USB, ou si vous avez configuré votre poste de travail distant afin qu'il connecte automatiquement des périphériques USB, vous pouvez ajouter une exception pour exclure votre connexion Ethernet.

```
sudo defaults write com.vmware.viewusb ExcludeVidPid vid-<varname
id="VARNAME_59F5F46045C64F50BC2EAC24D891DD2F">xxxx</varname>_pid-<varname
id="VARNAME_5901CF9553E84DC7A32D7C86D3892352">yyyy</varname>
```

Dans cet exemple, *xxxx* est l'ID du fournisseur et *yyyy* est l'ID du produit de l'adaptateur Ethernet USB.

Propriétés de la redirection USB

Lorsque vous créez des règles de filtrage, vous pouvez utiliser les propriétés de redirection USB.

Tableau 4-2. Configuration des propriétés pour la redirection USB

Nom et propriété de la stratégie	Description
Autoriser le fractionnement automatique de périphérique Propriété : `AllowAutoDeviceSplitting`	Autorise le fractionnement automatique de périphériques USB composites. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Exclude Vid/Pid Device From Split Propriété : `SplitExcludeVidPid`	Exclut un périphérique USB composite spécifié par des ID de fournisseur et de produit du fractionnement. Le format du paramètre est `vid-`*xxx1*`_pid-`*yyy1*`[;vid-`*xxx2*`_pid-`*yyy2*`]`..... Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (*****) à la place de chiffres dans un ID. Par exemple : **`vid-0781_pid-55**`** La valeur par défaut n'est pas définie.

Tableau 4-2. Configuration des propriétés pour la redirection USB (suite)

Nom et propriété de la stratégie	Description
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 `vid-`*xxxx*`_pid-`*yyyy*`([exintf:`*zz*`[;exintf:`*ww*`]])[;...]` Vous pouvez utiliser le mot-clé `exintf` pour exclure des composants de la redirection en spécifiant leur numéro d'interface. Vous devez spécifier les numéros d'ID au format hexadécimal et les numéros d'interface au format décimal en incluant les zéros à gauche. Vous pouvez utiliser le caractère générique (*****) à la place de chiffres dans un ID. Par exemple : **`vid-0781_pid-554c(exintf:01;exintf:02)`** **Remarque** Si le périphérique composite comprend des composants qui sont automatiquement exclus, tels qu'une souris ou un clavier, View n'inclut alors pas automatiquement les composants que vous n'avez pas explicitement exclus. Vous devez spécifier une règle de filtre telle que `Include Vid/Pid Device` pour inclure ces composants. La valeur par défaut n'est pas définie.
Allow Audio Input Devices Propriété : `AllowAudioIn`	Permet la redirection de périphériques d'entrée audio. La valeur par défaut est indéfinie, ce qui correspond à **`true`**.
Allow Audio Output Devices Propriété : `AllowAudioOut`	Permet la redirection de périphériques de sortie audio. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Autoriser HID Propriété : `AllowHID`	Autoriser la redirection des périphériques d'entrée autres que les claviers et les souris. La valeur par défaut est indéfinie, ce qui correspond à **`true`**.
Allow HIDBootable Propriété : `AllowHIDBootable`	Permet la redirection de périphériques d'entrée autres que des claviers et des souris qui sont disponibles au démarrage (ou périphériques démarrables par HID). La valeur par défaut est indéfinie, ce qui correspond à **`true`**.
Autoriser la description de périphérique a sécurité intégrée Propriété : `AllowDevDescFailsafe`	Autorise la redirection des périphériques même si Horizon Client ne parvient pas à obtenir les descripteurs de configuration/périphérique. Pour autoriser un périphérique même si config/desc échoue, incluez-le dans les filtres d'inclusion tels que `IncludeVidPid` ou `IncludePath`. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Allow Keyboard and Mouse Devices Propriété : `AllowKeyboardMouse`	Permet la redirection de claviers avec périphériques de pointage intégrés (souris, Trackball ou pavé tactile). La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Allow Smart Cards Propriété : `AllowSmartcard`	Permet la redirection de périphériques à carte à puce. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Allow Video Devices Propriété : `AllowVideo`	Permet la redirection de périphériques vidéo. La valeur par défaut est indéfinie, ce qui correspond à **`true`**.
Disable Remote Configuration Download Propriété : `DisableRemoteConfig`	Désactive l'utilisation de paramètres de View Agent lors de l'exécution du filtrage de périphérique USB. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.

Tableau 4-2. Configuration des propriétés pour la redirection USB (suite)

Nom et propriété de la stratégie	Description
Exclude All Devices Propriété : `ExcludeAllDevices`	Exclut tous les périphériques USB de la redirection. Si ce paramètre est défini sur **`true`**, vous pouvez utiliser d'autres paramètres de règle pour autoriser la redirection de périphériques spécifiques ou de familles de périphériques. Si ce paramètre est défini sur **`false`**, vous pouvez utiliser d'autres paramètres de règle pour empêcher la redirection de périphériques spécifiques ou de familles de périphériques. Si vous définissez la valeur de `Exclude All Devices` sur **`true`** sur View Agent, et si ce paramètre est transmis à Horizon Client, le paramètre de View Agent remplace celui d'Horizon Client. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Exclude Device Family Propriété : `ExcludeFamily`	Exclut des familles de périphériques de la redirection. Le format du paramètre est *family_name_1*[`;`*family_name_2*]... Par exemple : **`bluetooth;smart-card`** La valeur par défaut n'est pas définie. **Remarque** Si vous avez activé le fractionnement automatique de périphérique, View examine la famille de périphériques de chaque interface d'un périphérique USB composite pour décider quelles interfaces doivent être exclues. Si vous avez désactivé le fractionnement automatique de périphérique, View examine la famille de périphérique de l'ensemble du périphérique USB composite.
Exclude Vid/Pid Device Propriété : `ExcludeVidPid`	Exclut des périphériques avec des ID de fournisseur et de produit spécifiés de la redirection. Le format du paramètre est `vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]... Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (`*`) à la place de chiffres dans un ID. Par exemple : **`vid-0781_pid-****;vid-0561_pid-554c`** La valeur par défaut n'est pas définie.
Exclude Path Propriété : `ExcludePath`	Exclut des périphériques dans des chemins de concentrateur ou de port spécifiés de la redirection. Le format du paramètre est `bus-`*x1*[`/`*y1*]...`_port-`*z1*[`;bus-`*x2*[`/`*y2*]...`_port-`*z2*]... Vous devez spécifier des numéros de bus et de port au format hexadécimal. Vous ne pouvez pas utiliser le caractère générique dans les chemins. Par exemple : **`bus-1/2/3_port-02;bus-1/1/1/4_port-ff`** La valeur par défaut n'est pas définie.
Include Device Family Propriété : `IncludeFamily`	Inclut des familles de périphériques pouvant être redirigées. Le format du paramètre est *family_name_1*[`;`*family_name_2*]... Par exemple : **`stockage`** La valeur par défaut n'est pas définie.
Include Path Propriété : `IncludePath`	Inclut des périphériques dans des chemins de concentrateur ou de port spécifiés pouvant être redirigés. Le format du paramètre est `bus-`*x1*[`/`*y1*]...`_port-`*z1*[`;bus-`*x2*[`/`*y2*]...`_port-`*z2*]... Vous devez spécifier des numéros de bus et de port au format hexadécimal. Vous ne pouvez pas utiliser le caractère générique dans les chemins. Par exemple : **`bus-1/2_port-02;bus-1/7/1/4_port-0f`** La valeur par défaut n'est pas définie.
Include Vid/Pid Device Propriété : `IncludeVidPid`	Inclut des périphériques avec des ID de fournisseur et de produit spécifiés pouvant être redirigés. Le format du paramètre est `vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]... Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (`*`) à la place de chiffres dans un ID. Par exemple : **`vid-0561_pid-554c`** La valeur par défaut n'est pas définie.

Familles de périphériques USB

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

Remarque Certains périphériques ne lisent pas certaines familles de périphériques.

Tableau 4-3. Familles de périphériques USB

Nom de la famille de périphériques	Description
`audio`	Tout périphérique d'entrée ou de sortie audio.
`audio-in`	Périphériques d'entrée audio, tels que des microphones.
`audio-out`	Périphériques de sortie audio, tels que des haut-parleurs et des écouteurs.
`bluetooth`	Périphériques connectés par Bluetooth.
`comm`	Périphériques de communication, tels que des modems et des adaptateurs réseau filaires.
`hid`	Périphériques d'interface humaine, à l'exclusion des claviers et des pointeurs.
`hid-bootable`	Périphériques d'interface humaine disponibles au démarrage, à l'exclusion des claviers et des pointeurs.
`imaging`	Périphériques graphiques tels que des scanners.
`keyboard`	Périphérique de type clavier.
`mouse`	Périphérique de pointage tel qu'une souris.
`other`	Famille non spécifiée.
`pda`	Assistants numériques personnels.
`physical`	Périphériques à retour de force, tels que les joysticks à retour de force.
`printer`	Périphériques d'impression.
`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.

Activer la journalisation pour la redirection USB

Vous pouvez utiliser des journaux USB pour le dépannage et pour déterminer l'ID de produit et l'ID de fournisseur de divers périphériques que vous branchez sur le système client.

Vous pouvez activer la journalisation du suivi uniquement pour la session actuelle ou lors de redémarrages successifs. Pour activer la journalisation pour la session actuelle, vous utilisez une commande shell. Pour activer la journalisation lors des redémarrages, ajoutez la commande shell au fichier de profil approprié.

Prérequis

Si vous prévoyez de configurer la journalisation du suivi afin qu'elle continue lors de redémarrages système successifs, vous devez disposer d'autorisations d'administrateur ou racine sur le système client. Cette condition préalable ne s'applique pas si vous prévoyez d'activer la journalisation uniquement pour la session actuelle.

Procédure

- Pour activer la journalisation uniquement pour la session actuelle, utilisez la commande `launchctl`.
  a. Quittez Horizon Client pour que le démon du service USB s'arrête.
  b. Ouvrez un interpréteur de commandes (`/Applications/Utilities/Terminal.app`) avec le même nom d'utilisateur que celui qui démarre Horizon Client.
  c. Utilisez la commande suivante :

     ```
     launchctl setenv VMWARE_VIEW_USBD_LOG_OPTIONS "-o log:trace"
     ```

  d. Redémarrez Horizon Client.
- Pour activer la journalisation lors des redémarrages, ajoutez la commande `launchctl` au shell `rc` approprié ou au fichier de profil du shell que vous avez choisi, tel que `~/.bash_profile` pour le shell Mac OS X par défaut.

  Voici un exemple de commande `launchctl` à ajouter :

  ```
  setenv VMWARE_VIEW_USBD_LOG_OPTIONS "-o log:trace"
  ```

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

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

Cette fonctionnalité est disponible quand elle est utilisée avec View 5.2 Feature Pack 2 ou version ultérieure. Pour plus d'informations sur la configuration de la fonctionnalité Audio/Vidéo en temps réel, de la résolution et de la fréquence d'images sur un poste de travail distant, reportez-vous au guide *Installation et administration de VMware Horizon View Feature Pack*. Pour plus d'informations sur la configuration des paramètres sur les systèmes clients, consultez l'article de la base de connaissances VMware *Configuration de la fréquence et de la résolution d'images pour l'Audio/Vidéo en temps réel sur les clients Horizon View*, à l'adresse http://kb.vmware.com/kb/2053644.

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

Conditions d'utilisation de votre Webcam

Vous pouvez utiliser sur votre poste de travail une webcam intégrée ou connectée à votre ordinateur local si un administrateur View a configuré la fonctionnalité Audio/vidéo en temps réel et si le protocole d'affichage PCoIP est utilisé. Vous pouvez utiliser la webcam dans les applications de conférences telles que Skype, Webex ou Google Hangouts.

Lors de l'installation d'une application telle que Skype, Webex ou Google Hangouts sur votre poste de travail distant, vous pouvez choisir VMware Virtual Microphone et VMware Virtual Webcam comme périphériques d'entrée et VMware Virtual Audio comme périphérique de sortie dans les menus de l'application. Cette fonction marche avec plusieurs applications, et la sélection d'un périphérique d'entrée ne sera pas nécessaire.

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

Remarque Si vous utilisez une webcam USB, ne la connectez pas via le menu **Connexion > USB** d' Horizon Client En effet, cette opération achemine le périphérique via la redirection USB si bien que les conversations vidéo seront inutilisables.

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

Sélectionner un microphone par défaut sur un système client Mac OS X

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

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

Cette procédure explique comment choisir un microphone par défaut dans l'interface utilisateur du système client. Les administrateurs peuvent également configurer un microphone préféré en utilisant le système de valeurs par défaut de Mac OS X. Reportez-vous à la section « Configurer une webcam ou un microphone préféré sur un système client Mac OS X », page 46.

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

Prérequis

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

Procédure

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

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

Configuration de la fonctionnalité Audio/Vidéo en temps réel sur un client Mac OS X

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

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

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

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

Tableau 4-4. Syntaxe des commandes de configuration de la fonctionnalité Audio/Vidéo en temps réel

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

Tableau 4-4. Syntaxe des commandes de configuration de la fonctionnalité Audio/Vidéo en temps réel (suite)

vdmadmin	Description
`defaults read com.vmware.rtav`	Affiche les paramètres de configuration de la fonctionnalité Audio/Vidéo en temps réel.
`defaults delete com.vmware.rtav`*setting*	Supprime un paramètre de configuration de la fonctionnalité Audio/Vidéo en temps réel. Par exemple : `defaults delete com.vmware.rtav srcWCamFrameWidth`

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

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

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

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

Dans la plupart des environnements, il n'est pas nécessaire de configurer une webcam ou un microphone préféré. Si vous ne définissez pas de microphone préféré, les postes de travail distants utilisent le périphérique audio par défaut défini dans les Préférences systèmes du système client. Reportez-vous à la section « Sélectionner un microphone par défaut sur un système client Mac OS X », page 44. Si vous ne configurez pas de webcam préférée, les postes de travail distants sélectionnent la webcam par énumération.

Prérequis

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

Procédure

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

   a Connectez la webcam ou le périphérique audio.

   b Dans le dossier **Applications**, double-cliquez sur **VMware Horizon View Client** (Horizon Client 3.0) ou **VMware Horizon Client** (Horizon Client 3.1) pour démarrer Horizon Client.

   c Démarrez un appel, puis arrêtez-le.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Copier-coller du texte et des images

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

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

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

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

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

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

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

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

Utilisation des applications distantes

Vous pouvez utiliser de nombreuses fonctions Mac avec des applications distantes.

- Lorsque vous exécutez une application distante, son icône s'affiche dans le Dock. Vous pouvez agrandir une application distante réduite en cliquant sur son icône dans le Dock.

- Vous pouvez conserver, ouvrir et quitter une application distante dans son menu contextuel dans le Dock. Si vous sélectionnez **Conserver dans le Dock**, l'application distante reste dans le Dock, même après avoir fermé toutes les fenêtres de l'application. Dans Horizon Client 3.1 et version ultérieure, vous pouvez lancer une application distante en cliquant sur son icône dans le Dock.
- Vous pouvez démarrer la dictée vocale, réduire et zoomer sur une application distante à partir de la barre de menus.
- Vous pouvez utiliser la fonction Exposé pour afficher les applications distantes ouvertes et appuyer sur Commande-Tab pour basculer d'une application distante ouverte à une autre.
- Vous pouvez utiliser les raccourcis standard du clavier OS X pour interagir avec les applications distantes. Par exemple, vous pouvez appuyer sur Commande-W pour fermer une fenêtre d'application individuelle et Commande-S pour enregistrer le fichier en cours d'utilisation. Vous pouvez également utiliser les raccourcis standard du clavier OS X pour copier, couper et coller du texte d'une application OS X à une application distante.
- Dans Horizon Client 3.1, si une application distante crée un élément de barre d'état système Windows, cet élément s'affiche dans la zone de notification de la barre de menus sur votre système client Mac. Vous pouvez interagir avec cet élément dans la zone de notification de votre Mac de la même manière que vous le feriez dans la barre d'état système sur un système Windows.

  Remarque Lorsque vous cliquez à nouveau sur un élément redirigé Barre d'état système dans la zone de notification de votre Mac, le menu contextuel reste affiché.

Enregistrement de documents dans une application distante

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

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

Impression à partir d'un poste de travail distant

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

Activation de l'impression virtuelle sur Mac OS X Client

Lorsque vous utilisez le protocole d'affichage PCoIP, vous pouvez utiliser les imprimantes configurées pour votre ordinateur local à partir d'une application ou d'un poste de travail distant.

La fonction d'impression virtuelle ne nécessite l'installation d'aucun pilote.

Lorsque l'impression virtuelle est activée, le menu **Connexion** affiche **Impression activée**.

Vous pouvez activer l'impression virtuelle lors de la première exécution d'Horizon Client. Cliquez sur **Continuer** lorsqu'Horizon Client vous invite à démarrer les services USB et d'impression du poste de travail distant et tapez vos informations d'identification système.

Remarque Si vous installez Horizon Client pour Mac OS X sur un Mac sur lequel VMware Fusion a été précédemment lancé, les services d'impression seront déjà activés lorsque vous lancez Horizon Client. Ce comportement se produit, car VMware Fusion et Horizon Client utilisent une partie des fichiers servant à mettre en œuvre l'impression virtuelle.

Si vous n'activez pas l'impression virtuelle lors de la première exécution d'Horizon Client, vous pouvez utiliser le menu **Connexion** pour le faire.

- Pour activer l'impression virtuelle avant de vous connecter à une application ou à un poste de travail distant, sélectionnez **Connexion > Démarrer les services d'impression** dans le menu **VMware Horizon View Client** (Horizon Client 3.0) ou **VMware Horizon Client** (Horizon Client 3.1). Cliquez sur **Continuer** dans la boîte de dialogue et tapez les informations d'identification de votre système.
- Pour activer l'impression virtuelle après que vous avez connecté un poste de travail, sélectionnez **Connexion > Démarrer les services d'impression** dans le menu **VMware Horizon View Client** (Horizon Client 3.0) ou **VMware Horizon Client** (Horizon Client 3.1). Cliquez sur **Continuer**, tapez les informations d'identification de votre système, puis reconnectez-vous à l'application ou au poste de travail. Si vous annulez la reconnexion, vous pouvez cliquer sur **Connexion > Activer l'impression** ; Horizon Client vous invite alors à vous reconnecter.

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

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

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

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

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

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

- La fonction Windows pour imprimer vers un fichier.

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

Cette procédure concerne un poste de travail distant disposant d'un système d'exploitation Windows 7 ou Windows 8.x (de bureau). La procédure est similaire mais pas exactement la même pour Windows XP et Windows Vista.

Prérequis

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

L'installation de View Agent est l'une des tâches requises pour préparer une machine virtuelle à utiliser en tant que poste de travail distant. Pour plus d'informations, reportez-vous au document *Administration de View* si vous utilisez le Serveur de connexion View et View Agent 5.x ou une version antérieure. Reportez-vous à *Configuration des pools de postes de travail et d'applications dans View* si vous utilisez un Serveur de connexion View et View Agent 6.0 ou version ultérieure.

Procédure

1 Dans le poste de travail distant Windows 7 ou Windows 8.x, cliquez sur **Démarrer > Périphériques et imprimantes**.

2 Dans la fenêtre Périphériques et imprimantes, cliquez avec le bouton droit sur l'imprimante par défaut, sélectionnez **Propriétés de l'imprimante** dans le menu contextuel et choisissez l'imprimante.

Dans le poste de travail distant, les imprimantes virtuelles apparaissent sous la forme *<printer_name>#:<number>*.

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

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

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

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

6 Cliquez sur **OK**.

Utilisation d'imprimantes USB

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

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

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

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

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

  Pour plus d'informations sur la connexion d'imprimante USB, reportez-vous à « Connecter des périphériques USB », page 35.

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

Cache d'images client PCoIP

Le cache d'images client PCoIP stocke le contenu des images sur le client pour éviter la retransmission. Cette fonction réduit la bande passante.

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

Le cache d'images PCoIP capture la redondance spatiale et temporelle. Par exemple, lorsque vous faites défiler un document PDF, le nouveau contenu apparaît depuis le bas de la fenêtre et le contenu le plus ancien disparaît du haut de la fenêtre. L'autre contenu reste constant et remonte. Le cache d'images PCoIP peut détecter cette redondance spatiale et temporelle.

Comme pendant le défilement, les informations d'écran envoyées au périphérique client sont constituées principalement d'une séquence d'index de cache, l'utilisation du cache d'images permet d'économiser un quantité significative de bande passante. Ce défilement efficace offre des avantages dans un réseau LAN et dans un réseau WAN.

- Dans un réseau LAN, où la bande passante est relativement illimitée, le cache d'image client permet d'économiser une quantité significative de bande passante.
- Dans un réseau WAN, pour rester dans les limites de bande passante disponible, le défilement est dégradé si la mise en cache client n'est pas utilisée. Dans un réseau WAN, la mise en cache client peut économiser la bande passante et permettre de faire défiler les données d'une manière fluide et avec grande réactivité.

Avec la mise en cache client, le client stocke des portions de l'affichage ayant déjà été transmises. La taille du cache est de 250 Mo.

Avec View 5.2, si vous utilisez des serveurs et des postes de travail, un cache côté client de 90 Mo offre les mêmes performances que si vous utilisiez un cache de 250 Mo avec des versions antérieures.

Résolution des problèmes d' Horizon Client 5

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

Ce chapitre aborde les rubriques suivantes :

Réinitialiser une application ou un poste de travail distant

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

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

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

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

Procédure

- Utilisez la commande **Réinitialiser**.

Option	Action
Réinitialiser un poste de travail distant à partir du poste de travail	Sélectionnez **Connexion > Réinitialiser** dans la barre de menus.
Réinitialiser un poste de travail distant depuis la fenêtre de sélection des postes de travail et applications	Sélectionnez le poste de travail distant et sélectionnez **Connexion > Réinitialiser** dans la barre de menus.
Réinitialiser des applications distantes depuis la fenêtre de sélection des postes de travail et applications	Cliquez sur le bouton **Paramètres** (icône engrenage) dans le coin supérieur droit de la fenêtre, sélectionnez **Applications** dans le volet de gauche, cliquez sur **Réinitialiser**, puis sur **Continuer**.

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

Suivant

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

Désinstallation d' Horizon Client

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

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

Faites glisser l'application **VMware Horizon View Client** (Horizon Client 3.0) ou **VMware Horizon Client** (Horizon Client 3.1) du dossier **Applications** vers la **Corbeille**, puis videz celle-ci.

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

Reportez-vous à la section « Installer Horizon Client sur Mac OS X », page 11.

Index

R

S

T

U

V

W