Utilisation de VMware View Client pour Mac OS X

Décembre 2012

View Client

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

FR-000668-05

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 View Client pour Mac

1

Ce guide, *Utilisation de VMware View Client pour Mac*, explique comment installer et utiliser le logiciel VMware View™ sur un périphérique Mac pour se connecter à un poste de travail View dans le centre de données.

Les informations de ce document indiquent la configuration système requise et fournissent les instructions d'installation et d'utilisation de View Client pour Mac.

Ces informations sont conçues pour les administrateurs qui doivent configurer un déploiement VMware View comportant des périphériques client 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

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

Configuration système requise pour les clients Mac

Vous pouvez installer View Client pour Mac sur tous les modèles basés sur Intel qui utilisent le système d'exploitation Mac OS X 10.6.8 ou une version supérieure.

L'ordinateur Mac sur lequel vous installez View Client, et les périphériques qu'il utilise, doit se conformer à une certaine configuration système.

Modèle	Mac avec Intel
Mémoire	Au moins 2 Go de RAM
Systèmes d'exploitation	■ View Client 1.6 : Mac OS X Snow Leopard (10.6.8), Mac OS X Lion (10.7), et Mac OS X Mountain Lion (10.8)

	■ View Client 1.4 et 1.5 : Mac OS X Snow Leopard (10.6.8) et Mac OS X Lion (10.7)
Serveur de connexion View, serveur de sécurité et View Agent	4.6.1 ou version supérieure 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.
Protocole d'affichage pour VMware View	PCoIP ou RDP
Exigences logicielles pour RDP	Microsoft Remote Desktop Connection Client pour Mac, version 2.0 ou ultérieure. Vous pouvez télécharger ce client sur le site Web de Microsoft.

Systèmes d'exploitation de poste de travail View 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 voir une liste des systèmes d'exploitation client pris en charge, reportez-vous à la rubrique « Systèmes d'exploitation pris en charge pour View Agent » dans la documentation d'installation de VMware View 4.6.x ou 5.x.

Préparation du Serveur de connexion View pour View Client

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

Pour que les utilisateurs finaux puissent se connecter à Serveur de connexion View ou à un serveur de sécurité et accéder à un poste de travail View, vous devez configurer certains paramètres de pool et des paramètres de sécurité :

- Si vous utilisez un serveur de sécurité, comme le recommande VMware, vérifiez que vous utilisez le Serveur de connexion View 4.6.1 et le Serveur de sécurité View 4.6.1 ou une version supérieure. Consultez la documentation *Installation de VMware View* pour View 4.6 ou ultérieur.
- 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 Administrateur View, 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 virtuels a été créé et que le compte d'utilisateur que vous prévoyez d'utiliser est autorisé à accéder à ce poste de travail View. Consultez les rubriques sur la création de pools de postes de travail dans la documentation *Administration de VMware View*.
- Pour pouvoir utiliser l'authentification à 2 facteurs, telle que l'authentification RSA SecurID ou RADIUS, avec View Client, vous devez activer cette fonction sur le Serveur de connexion View. L'authentification RADIUS est disponible avec View 5.1 et les versions supérieures et le Serveur de connexion View. Pour plus d'informations, consultez les rubriques relatives à l'authentification à 2 facteurs dans la documentation *Administration de VMware View*.

Installer View Client sur Mac OS X

Les utilisateurs finaux ouvrent View Client pour se connecter à des postes de travail virtuels depuis une machine physique Mac OS X. Vous installez View Client sur des systèmes client Mac OS X depuis un fichier d'image 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 6.
- 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 View, vérifiez que Microsoft Remote Desktop Connection Client pour Mac, version 2.0 ou ultérieure, est installé sur le système client Mac.
- Vérifiez que vous disposez de l'URL de la page de téléchargement qui contient le fichier d'image disque de View Client pour Mac.

Procédure

1 Sur votre Mac, recherchez la page Web qui contient le fichier d'image disque de View Client.

  Le format de nom du fichier d'image disque est `VMware-View-Client-`*`y.y.y-xxxxxx`*`.dmg`, où *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 VMware View Client Finder.

3 Dans la fenêtre Finder, faites glisser l'icône **[View Client]** vers l'icône de 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 View Client et vérifiez que vous pouvez ouvrir une session sur le bon poste de travail virtuel. Reportez-vous à la section « Première connexion à un poste de travail View », page 16.

Installer View Client à l'aide de View Portal

Pour installer correctement l'application View Client, vous pouvez ouvrir un navigateur et rechercher la page Web de View Portal.

Prérequis

- Vérifiez que vous possédez l'URL pour l'instance de serveur de connexion View.
- Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur le système client.
- 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 6.
- Si vous prévoyez d'utiliser le protocole d'affichage RDP pour vous connecter à un poste de travail View, vérifiez que Microsoft Remote Desktop Connection Client pour Mac, version 2.0 ou ultérieure, est installé sur le système client Mac.

Procédure

1 Ouvrez une session sur le système client en tant qu'utilisateur avec des privilèges d'administrateur.

2 Ouvrez un navigateur et saisissez l'URL de l'instance de serveur de connexion View qui fournit l'accès vers le poste de travail virtuel.

3 Suivez les invites sur la page Web.

Suivant

Connectez-vous au poste de travail View. Reportez-vous à la section « Première connexion à un poste de travail View », page 16.

Ajouter VMware View Client au Dock

Vous pouvez ajouter View Client à votre Dock comme pour n'importe quelle autre application.

Procédure

1 Dans le dossier **[Applications]** , double-cliquez sur **[VMware View Client]** .

2 Cliquez et maintenez enfoncée l'icône **[VMware View Client]** dans le Dock jusqu'à ce que le menu contextuel apparaisse.

3 Sélectionnez **[Options]** > **[Garder dans le Dock]** .

Lorsque vous quittez VMware View Client, le raccourci de l'application reste dans 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 View 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 View Client », page 17.

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

- **1** implémente `Ne jamais se connecter à des serveurs non approuvés.`
- **2** implémente `Signaler avant de se connecter à des serveurs non approuvés.`
- **3** implémente `Ne pas vérifier les certificats d'identité des serveurs.`

Données View Client collectées par VMware

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

Remarque Cette fonctionnalité est disponible uniquement si votre déploiement View utilise Serveur de connexion View 5.1 ou versions supérieures. Les informations client sont envoyées pour les clients View Client 1.7 et versions supérieures.

VMware collecte des données sur les clients afin de hiérarchiser la compatibilité matérielle et logicielle. Si un administrateur View 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 de View Client sont d'abord envoyées au Serveur de connexion View puis à VMware, avec des données des serveurs View, des pools de postes de travail et des postes de travail 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 spécifique à l'utilisateur. Les journaux ne contiennent aucune information d'identification personnelle.

Pour participer au programme d'amélioration du produit de VMware, l'administrateur qui installe le Serveur de connexion View peut s'inscrire tout en exécutant l'Assistant d'installation du Serveur de connexion View, ou il peut définir une option dans View Administrator après l'installation.

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

Description	Ce champ reste-t-il anonyme ?	Exemple
Entreprise qui a produit l'application View Client	Non	VMware
Nom du produit	Non	VMware View 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* le numéro de build.
Architecture binaire du client	Non	Exemples : ■ x86_64 ■ arm ■ i386
Nom du build du client	Non	Exemples : ■ VMware-view-client-Linux ■ VMware-view-client-iOS ■ VMware-view-client-Mac ■ VMware-view-client-Android
Système d'exploitation hôte	Non	Exemples : ■ iPhone OS 5.1.1 (9B206) ■ Ubuntu 10.04.4 LTS ■ Mac OS X 10.7.5 (11G63)
Noyau du système d'exploitation hôte	Non	Exemples : ■ 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

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

Description	Ce champ reste-t-il anonyme ?	Exemple
Architecture du système d'exploitation hôte	Non	Exemples : ■ i386 ■ x86_64 ■ armv71 ■ ARM
Modèle du système hôte	Non	Exemples : ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision WorkStation T3400 (A04 03/21/2008)
Processeur du système hôte	Non	Exemples : ■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH ■ unknown (pour iPad)
Nombre de cœurs dans le processeur du système hôte	Non	Par exemple : `4`
Mo de mémoire sur le système hôte	Non	Par exemple : `4096`

Utiliser des URI pour configurer View Client

A l'aide des Identifiants uniformes de ressource (URI), vous pouvez créer une page Web ou un e-mail contenant des liens sur lesquels les utilisateurs finaux peuvent cliquer pour lancer View Client, se connecter au Serveur de connexion View et lancer un poste de travail spécifique avec des options de configuration spécifiques.

Avec View Client 1.6 et versions supérieures, vous pouvez simplifier le processus d'ouverture de session sur un poste de travail View 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
- Taille de fenêtre
- Actions du poste de travail dont la réinitialisation, la déconnexion et la restauration
- Protocole d'affichage
- Options pour la redirection des périphériques USB

Pour construire une URI, vous pouvez utiliser le schéma URI `vmware-view` avec des éléments de chemin et de requête spécifiques à View Client.

Remarque Vous pouvez utiliser les URI pour lancer View Client uniquement si celui-ci est déjà installé sur les ordinateurs clients des utilisateurs finaux.

Syntaxe pour la création d'URI vmware-view

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

Spécification d'URI pour VMware

Suivez la syntaxe suivante pour créer des URI pour le lancement de View 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.w3schools.com/tags/ref_urlencode.asp.

---

authority-part

Spécifie l'adresse du serveur et, éventuellement, un nom d'utilisateur, un numéro de port non défini par défaut, ou bien les deux. Les 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. Utilisez le nom affiché du poste de travail. 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 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 de View Client. Si vous créez des URI pour différents types de clients, tels que des clients de postes de travail et des clients mobiles, consultez le guide *Utilisation de VMware View Client* pour chaque type de système client.

action

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

Valeur	Description
`browse`	Affiche une liste des postes de travail disponibles hébergés sur le serveur spécifié. Il ne vous est pas demandé de spécifier un poste de travail pour l'utilisation de cette action. Si vous utilisez l'action `browse` et que vous spécifiez un poste de travail, le poste de travail est mis en surbrillance dans la liste des postes de travail disponibles.
`start-session`	Lance le poste de travail spécifié. Si aucune requête d'action n'est fournie et que le nom du poste de travail est fourni, `start-session` est l'action par défaut.
`réinitialiser`	Éteint puis redémarre le poste de travail spécifié. Les données non enregistrées sont perdues. Réinitialiser un poste de travail View est équivalent à l'utilisation du bouton de réinitialisation d'un PC physique.
`logoff`	Déconnecte l'utilisateur du système d'exploitation client sur le poste de travail View.
`rollback`	Ignore les modifications du poste de travail spécifié apportées lors de son emprunt pour une utilisation en mode local, sur un PC Windows ou sur un ordinateur portable.

connectUSBOnInsert

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

desktopLayout

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

Tableau 1-3. Valeurs valides pour la requête desktopLayout

Valeur	Description
`fullscreen`	Un moniteur affiche son contenu en plein écran. Il s'agit du réglage par défaut.
`windowLarge`	Fenêtre de grande taille.

Tableau 1-3. 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 Les valeurs valides sont **`RDP`** et **`PCoIP`**. Par exemple, pour spécifier le protocole PCoIP, utilisez la syntaxe **`desktopProtocol=PCoIP`**.

domainName Le domaine associé à l'utilisateur qui se connecte au poste de travail View.

Exemple d'URI de vmware-view

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

Exemples de syntaxe d'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`

View Client démarre et se connecte au serveur `view.mycompany.com`. Le formulaire d'identification demande à l'utilisateur d'entrer un nom d'utilisateur, un nom de domaine et un mot de passe. Une fois la session ouverte, le client se connecte au poste de travail dont le nom affiché est **[Poste de travail principal]** et l'utilisateur est connecté au 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. L'affichage en plein écran correspond à la taille de la fenêtre par défaut.

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

Cette URI a le même effet que dans l'exemple précédent, à ceci près qu'elle utilise le port non défini 7555 pour le Serveur de connexion View. (Le port par défaut est 443.) Comme un identifiant de poste de travail est fourni, le poste de travail démarre même si l'action `start-session` n'est pas inclue dans l'URI.

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

View Client démarre et se connecte au serveur `view.mycompany.com`. Dans le formulaire d'identification, le champ **[Nom d'utilisateur]** est rempli par le nom **[fred]** . L'utilisateur doit entrer le nom de domaine et le mot de passe. Une fois la session ouverte, le client se connecte au poste de travail dont le nom affiché est **[Poste de travail finance]** et l'utilisateur est connecté au système d'exploitation client. La connexion utilise le protocole d'affichage PCoIP.

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

View Client démarre et se connecte au serveur `view.mycompany.com`. Dans le formulaire d'identification, le champ **[Nom d'utilisateur]** est rempli par le nom **[fred]** et le champ **[Domaine]** est rempli par **[mycompany]** . L'utilisateur ne doit entrer qu'un mot de passe. Une fois la session ouverte, le client se connecte au poste de travail dont le nom affiché est **[Poste de travail finance]** et l'utilisateur est connecté au système d'exploitation client.

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

View Client démarre et il est demandé à l'utilisateur de se connecter au serveur `view.mycompany.com`.

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

View Client démarre et se connecte au serveur `view.mycompany.com`. Le formulaire d'identification demande à l'utilisateur d'entrer un nom d'utilisateur, un nom de domaine et un mot de passe. Une fois la session ouverte, View Client affiche une boîte de dialogue qui invite l'utilisateur à confirmer l'opération de réinitialisation pour le Poste de travail principal. Après la réinitialisation, selon le type de View Client, l'utilisateur peut voir un message indiquant si la réinitialisation a réussi ou non.

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

7 `vmware-view://`

View Client démarre et il est demandé à l'utilisateur d'entrer l'adresse d'une instance d'un Serveur de connexion View.

Exemples de code HTML

Vous pouvez utiliser les URI pour créer des liens hypertexte et des boutons à inclure dans des e-mails ou des pages Web. Les exemples suivants indiquent comment utiliser les URI à partir du premier exemple d'URI pour coder un lien hypertexte **[Lien de test]** et un bouton **[Bouton de test]** .

```
<html>
<body>

<a href="vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session">Text
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 de serveur et des postes de travail

Utilisez View Client pour vous connecter à serveur de connexion View ou à un serveur de sécurité et pour ouvrir ou fermer une session sur un poste de travail View. À des fins de dépannage, vous pouvez également réinitialiser un poste de travail View qui vous est affecté et restaurer un poste de travail que vous avez emprunté.

En fonction de la façon dont l'administrateur configure des règles pour les postes de travail View, les utilisateurs finaux peuvent être capables d'exécuter plusieurs opérations sur leurs postes de travail.

- Première connexion à un poste de travail View page 16

  Avant de laisser vos utilisateurs finaux accéder à leurs postes de travail virtuels, vérifiez que vous pouvez ouvrir une session sur un poste de travail virtuel depuis le système client.

- Modes de vérification des certificats pour View Client page 17

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

- Basculer entre postes de travail page 18

  Si vous êtes connecté à un poste de travail, vous pouvez basculer vers un autre poste de travail.

- Fermer une session ou se déconnecter d'un poste de travail page 19

  Si vous vous déconnectez d'un poste de travail View sans fermer votre session, des applications restent ouvertes.

- Supprimer un raccourci de View Server de l'écran d'accueil page 20

  Une fois que vous êtes connecté à un View Server, un raccourci de serveur est enregistré sur l'écran d'accueil de View Client.

- Restaurer un poste de travail page 20

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

Première connexion à un poste de travail View

Avant de laisser vos utilisateurs finaux accéder à leurs postes de travail virtuels, vérifiez que vous pouvez ouvrir une session sur un poste de travail virtuel depuis le système client.

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 la section « Préparation du Serveur de connexion View pour View Client », page 7.
- 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 virtuel, 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 possédez le nom de domaine complet (FQDN) du serveur qui fournit l'accès au poste de travail virtuel. 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 View, 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 View Client », page 17.
- Si les utilisateurs finaux sont autorisés à utiliser le protocole d'affichage Microsoft RDP, vérifiez que le système client dispose de Microsoft Remote Desktop Connection Client pour Mac, de version 2.0 ou supérieure. Vous pouvez télécharger ce client sur le site Web de Microsoft.

Procédure

1. Dans le dossier **[Applications]** , double-cliquez sur **[VMware View Client]** .
2. Cliquez sur l'icône **[Ajouter un serveur]** sur l'écran d'accueil de View Client.
3. Entrez le nom de serveur et un numéro de port si nécessaire, puis cliquez sur **[Continuer]** .

   Voici un exemple d'utilisation d'un port non défini comme port par défaut : **`view.company.com:1443`**.
4. 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]** .
5. Entrez vos nom d'utilisateur et mot de passe, sélectionnez un domaine et cliquez sur **[Continuer]** .

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

6 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.

7 (Facultatif) Sélectionnez le protocole.

L'option par défaut est **[PCoIP]** . Pour utiliser plutôt Microsoft RDP, cliquez sur **[PCoIP]** sous le nom de poste de travail à définir et sélectionnez **[RDP]** .

Remarque Pour utiliser le **[RDP]** , le système client doit disposer de Microsoft Remote Desktop Connection Client pour Mac, de version 2.0 ou ultérieure.

8 Double-cliquez sur un raccourci de poste de travail View pour vous connecter.

Une fois la connexion établie, la fenêtre client s'affiche. Si View Client ne peut pas se connecter au poste de travail, effectuez les tâches suivantes :

- Déterminez si le Serveur de connexion View est configuré pour ne pas utiliser SSL. View 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. Dans ce cas, vous devez cocher la case pour utiliser SSL ou configurer l'environnement pour que les clients puissent se connecter à un équilibreur de charge dont la fonction HTTPS est activée ou un autre périphérique intermédiaire configuré pour établir une connexion HTTP au Serveur de connexion View.
- Vérifiez que le certificat de sécurité du 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 du Serveur de connexion View autorisent les connexions depuis cet utilisateur. Consultez le document *Administration de VMware View*.
- Vérifiez que l'utilisateur est autorisé à accéder à ce poste de travail. Consultez le document *Administration de VMware View*.
- Si vous utilisez le protocole d'affichage RDP pour vous connecter à un poste de travail View, vérifiez que l'ordinateur client autorise les connexions vers des postes de travail distants.

Modes de vérification des certificats pour View 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 View 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 un équilibreur de charge redirige View Client vers un serveur avec un certificat qui ne correspond pas au nom d'hôte entré dans View 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 du périphérique.

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 supérieures envoient une empreinte numérique de certificat à View 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 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 View Client] > [Préférences]** dans la barre de menus Finder. 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 de certificat ne doit pas être concordant au nom du serveur de connexion que vous avez saisi dans View 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.

Basculer entre postes de travail

Si vous êtes connecté à un poste de travail, vous pouvez basculer vers un autre poste de travail.

Procédure

- Sélectionnez un poste de travail View à partir du même serveur ou d'un serveur différent.

Option	Action
Choisir un poste de travail View différent sur le même serveur	Cliquez sur le bouton **[Déconnecter]** dans la barre d'outils ou sélectionnez **[Poste de travail] > [Déconnecter]** dans la barre de menus Finder.
Choisir un poste de travail View sur un serveur différent	Cliquez sur le bouton **[Déconnexion du serveur]** sur le côté droit de la barre d'outils.

Fermer une session ou se déconnecter d'un poste de travail

Si vous vous déconnectez d'un poste de travail View sans fermer votre session, des applications restent ouvertes.

Si vous n'êtes pas connecté à un poste de travail View, vous pouvez fermer votre session sans vous connecter avant. Utiliser cette fonction a le même résultat que d'envoyer Ctrl+Alt+Suppr 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 View. Pour utiliser une action équivalente à la combinaison Ctrl+Alt+Suppr, sélectionnez **[Poste de travail] > [Envoyer Ctrl+Alt+Suppr]** dans la barre de menus.

Vous pouvez également appuyer sur Fn+Contrôle+Option+Supprimer sur un clavier Apple.

Procédure

- Déconnectez-vous sans fermer de session.

Option	Action
Quitter aussi View Client	Cliquez sur le bouton **[Fermer]** dans le coin de la fenêtre ou sélectionnez **[Fichier] > [Fermer]** dans la barre de menus Finder.
Choisir un poste de travail View différent sur le même serveur	Cliquez sur le bouton **[Déconnecter]** dans la barre d'outils ou sélectionnez **[Poste de travail] > [Déconnecter]** dans la barre de menus Finder.
Choisir un poste de travail View sur un serveur différent	Cliquez sur le bouton **[Déconnexion du serveur]** sur le côté droit de la barre d'outils.

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

- Fermez une session et déconnectez-vous.

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 **[Poste de travail] > [Fermer la session]** dans la barre de menus Finder. Si vous utilisez cette procédure, les fichiers ouverts sur le poste de travail View seront fermés sans être enregistrés.

- Fermez une session lorsque vous n'êtes pas connecté à un poste de travail View.

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

Option	Action
À partir de l'écran d'accueil avec des raccourcis de serveur	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 **[Poste de travail] > [Fermer la session]** dans la barre de menus Finder.
À partir de l'écran d'accueil avec des raccourcis de poste de travail	Sélectionnez le poste de travail et choisissez **[Poste de travail] > [Fermer la session]** dans la barre de menus Finder.

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

Une fois que vous êtes connecté à un View Server, un raccourci de serveur est enregistré sur l'écran d'accueil de View Client.

Vous pouvez supprimer un raccourci de View Connection Server 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 de poste de travail View qui apparaissent une fois que vous êtes connecté à un serveur.

Restaurer un poste de travail

La restauration ignore les modifications réalisées sur un poste de travail virtuel 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 View uniquement si votre administrateur View a activé cette fonction 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 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 de View Client affiche des raccourcis de Serveur de connexion View, double-cliquez sur le raccourci du serveur qui accède au poste de travail et entrez les informations d'identification.
   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 de View Client qui affiche des raccourcis de poste de travail View, sélectionnez le poste de travail et choisissez **[Poste de travail > Restaurer]** dans la barre de menus Finder.

Une fois le poste de travail View restauré, vous pouvez ouvrir une session dessus depuis le client Mac.

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

View Client pour Mac prend en charge les fonctions suivantes.

Matrice de prise en charge des fonctions

View Client pour Mac prend en charge un sous-ensemble de fonctionnalités disponibles sur d'autres clients, tels que les postes de travail et les ordinateurs portables View Client pour Windows.

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

Fonction	Poste de travail View Windows 7	Poste de travail View Windows Vista	Poste de travail View Windows XP
RSA SecurID ou RADIUS	X	X	X
Authentification unique	X	X	X
Protocole d'affichage RDP	X	X	X
Protocole d'affichage PCoIP	X	X	X
Accès USB	X	X	X
Wyse MMR			
Impression virtuelle			
Impression basée sur l'emplacement	X	X	X
Cartes à puce			
Plusieurs écrans			
Mode local			

Pour des descriptions de ces fonctions et leurs limites, consultez le document *Planification de l'architecture de View*.

Internationalisation

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

Copier et coller du texte et des images

Si votre administrateur active la fonction, vous pouvez copier et coller du texte mis en forme et des images entre un poste de travail View distant et votre système client ou entre deux postes de travail View. Certaines restrictions s'appliquent.

Si vous utilisez le protocole d'affichage PCoIP et un poste de travail View avec View 5.x ou ultérieur, votre administrateur View peut définir cette fonction pour que les opérations de copier-coller soient autorisées uniquement depuis votre système client sur un poste de travail View, ou uniquement depuis un poste de travail View vers votre système client, ou les deux, ou aucun.

Les administrateurs configurent le copier-coller à l'aide d'objets de stratégie de groupe (GPO) qui se rapportent à View Agent dans des postes de travail View. Pour plus d'informations, consultez la rubrique sur les variables de la session générale PCoIP de View dans le document *Administration de VMware View*, dans le chapitre sur la configuration des stratégies.

Les formats de fichier pris en charge incluent le texte, les images et RTF (Rich Text Format). Le Presse-papiers peut contenir 1 Mo de données pour les opérations copier et coller. Si vous copiez du texte mis en forme, certaines données sont du texte et d'autres sont des informations sur la mise en forme. Par exemple, un document de 800 Ko peut utiliser plus de 1 Mo de données lorsqu'il est copié car plus de 200 Ko de données RTF peuvent être placés dans le Presse-papiers.

Si vous copiez une grande quantité de texte mis en forme ou du texte et une image, lorsque vous essayez de coller le texte et l'image, vous pouvez voir tout ou partie du texte brut mais aucune mise en forme ni image. Cela est dû au fait que les trois types de données sont parfois stockés séparément. Par exemple, en fonction du type de document depuis lequel vous effectuez la copie, des images peuvent être enregistrées en tant qu'images ou en tant que données RTF.

Si le texte et les données RTF utilisent moins de 1 Mo, le texte mis en forme est collé. Souvent, les données RTF ne peuvent pas être tronquées, ainsi, si le texte et la mise en forme utilisent plus de 1 Mo, les données RTF sont ignorées et le texte brut est collé.

Si vous ne parvenez pas à coller tout le texte mis en forme et les images que vous avez sélectionnés en une seule opération, vous pouvez avoir à copier et coller de petites quantités à chaque opération.

Vous ne pouvez pas copier et coller de fichiers entre un poste de travail View et le système de fichiers sur votre ordinateur client.

Connecter des périphériques USB

Vous pouvez utiliser des périphériques USB connectés localement, tels que des lecteurs USB, des appareils photos et des imprimantes, depuis un poste de travail View. 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 dans View Client. Vous utilisez le menu pour connecter et déconnecter les périphériques.

L'utilisation de périphériques USB avec des postes de travail View a les limites suivantes :

- Lorsque vous accédez à un périphérique USB depuis un menu dans View Client et que vous utilisez le périphérique dans un poste de travail View, vous ne pouvez pas accéder au périphérique sur l'ordinateur local.
- Les périphériques USB qui n'apparaissent pas dans le menu, mais qui sont disponibles dans un poste de travail View, incluent des périphériques d'interface humaine, tels que des claviers et des pointeurs. Le poste de travail View 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 View, vous pouvez être invité à l'installer lorsque vous connectez le périphérique USB au poste de travail View.
- Si vous prévoyez d'ajouter des périphériques USB qui utilisent des pilotes MTP, tels que des smartphones et des tablettes Samsung fonctionnant avec Android, vous devez paramétrer View Client pour qu'il connecte automatiquement des périphériques USB à votre poste de travail View. 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 rebrancher 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 View manuellement ou automatiquement.

Remarque Ne redirigez pas les connexions Ethernet USB vers le poste de travail virtuel. Votre poste de travail virtuel peut se connecter à votre réseau si votre système local est connecté. Si vous avez réglé votre poste de travail virtuel pour connecter automatiquement des périphériques USB, vous pouvez ajouter une exception afin d'exclure votre connexion Ethernet. Reportez-vous à la section « Configuration de la redirection USB sur le client », page 24 .

Prérequis

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

  Cette tâche inclut l'installation du composant **[USB Redirection]** de View Agent. Pour plus d'informations, consultez le chapitre sur la création et la préparation de machines virtuelles dans le document *Administration de VMware View*.

  Cette tâche peut également inclure le réglage de stratégies de groupe pour autoriser la redirection USB. Pour plus d'informations, consultez la section « Réglages USB pour View Agent » dans le document *Administration de VMware View*.

- S'il s'agit de votre première tentative de connexion d'un périphérique USB, vous devez fournir le mot de passe de l'administrateur. View Client vous y invite le moment venu.

  Certains composants requis pour la redirection USB qui sont déjà installés par View 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 View.

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

  Vous pouvez également cliquer sur l'icône du périphérique USB dans le coin supérieur gauche de la fenêtre de View Client.

  b Connectez le périphérique USB au système client local.

  c Sur la barre de menu View Client, cliquez sur **[Poste de travail] > [USB]** .

  d Sélectionnez un périphérique USB.

  Le périphérique est redirigé manuellement depuis le système local vers le poste de travail View.

- Configurez View Client pour connecter automatiquement des périphériques USB au poste de travail View lorsque vous les branchez sur le 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 View Client et connectez-vous à un poste de travail View.

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

  Vous pouvez également cliquer sur l'icône du périphérique USB dans le coin supérieur gauche de la fenêtre de View Client.

c Sur la barre de menu View Client, cliquez sur **[Poste de travail] > [USB] > [Connexion automatique de périphériques USB au démarrage]** ou **[Connexion automatique de périphériques USB à l'insertion]** .

Si vous choisissez de connecter des périphériques au démarrage, tous les périphériques USB qui sont connectés à votre Mac lorsque vous démarrez View Client sont redirigés vers le poste de travail View.

Si vous choisissez de connecter automatiquement des périphériques USB à l'insertion, tous les périphériques USB que vous connectez à votre Mac après avoir démarré View Client sont redirigés vers le poste de travail View.

d Branchez le périphérique USB.

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 *Administration de VMware View*.

Configuration de la redirection USB sur le client

Avec View Client 1.7, vous pouvez configurer le système client pour spécifier quels périphériques USB peuvent être redirigés vers un poste de travail View.

Il est possible de configurer des stratégies USB à la fois pour View Agent sur le poste de travail distant, et pour View Client sur le système local, afin d'atteindre les objectifs suivants :

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

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 VMware View*.

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

Syntaxe pour la configuration de filtres USB

Vous pouvez définir des règles de filtrage pour empêcher la redirection de certains types de périphériques USB vers un poste de travail View.

Certaines valeurs 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 un fichier après avoir branché le périphérique USB dans le système local lorsque View Client est en cours d'exécution. Pour plus d'informations, reportez-vous à la section « Activer la journalisation pour la redirection USB », page 28.

Vous pouvez configurer des filtres USB en ouvrant un shell (`/Applications/Utilities/Terminal.app`) et en exécutant une commande comme racine à l'aide de la syntaxe suivante :

- Pour définir ou remplacer une règle de filtre :

  ```
  # defaults write domain property value
  ```

  Par exemple :

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

- Pour répertorier les règles :

  ```
  # defaults read domain
  ```

  Par exemple :

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

- Pour supprimer une règle :

  ```
  # defaults delete domain property
  ```

  Par exemple :

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

Exemple : Exclusion d'un périphérique Ethernet USB

Il est possible que vous souhaitiez exclure de la redirection un périphérique Ethernet USB. Votre poste de travail virtuel peut se connecter à votre réseau si votre système local est connecté. Si vous redirigez un périphérique Ethernet USB, votre système client local perdra sa connexion avec le réseau. Si vous avez défini votre poste de travail virtuel afin de connecter automatiquement des périphériques USB, vous pouvez ajouter une exception pour exclure votre connexion Ethernet.

```
sudo defaults write com.vmware.viewusb ExcludeVidPid vid-xxxx_pid-yyy
```

Dans cet exemple, *xxxx* est l'ID du fournisseur et *yyy* 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 1-5. Configuration des propriétés pour la redirection USB

Nom et propriété de la stratégie	Description
Autoriser les périphériques d'entrée audio Propriété : `AllowAudioIn`	Autorise la redirection des périphériques d'entrée audio. La valeur par défaut est indéfinie, ce qui correspond à **`true`**.
Autoriser les périphériques de sortie audio Propriété : `AllowAudioOut`	Autorise la redirection des 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`**.
Autoriser HIDBootable Propriété : `AllowHIDBootable`	Autorise la redirection des périphériques d'entrée autres que les claviers et les souris disponibles au moment du démarrage (également appelés périphériques hid-bootable). La valeur par défaut est indéfinie, ce qui correspond à **`true`**.

Tableau 1-5. Configuration des propriétés pour la redirection USB (suite)

Nom et propriété de la stratégie	Description
Autoriser la description de périphérique a sécurité intégrée Propriété : `AllowDevDescFailsafe`	Autorise la redirection des périphériques, même si View Client ne parvient pas à obtenir les descripteurs config/device. Pour autoriser un périphérique même si config/desc échoue, incluez-le dans les filtres d'inclusion tels que `IncludeVidPid` ou `IncludePath`. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Autoriser les claviers et les souris Propriété : `AllowKeyboardMouse`	Autoriser la redirection des claviers disposant de pointeurs intégrés (tels qu'une souris, une boule de commande ou un pavé tactile). La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Autoriser les cartes à puce Propriété : `AllowSmartcard`	Autorise la redirection des périphériques à carte à puce. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Autoriser les périphériques vidéos Propriété : `AllowVideo`	Autorise la redirection des périphériques vidéos. La valeur par défaut est indéfinie, ce qui correspond à **`true`**.
Désactiver le téléchargement de configuration distante Propriété : `DisableRemoteConfig`	Désactive l'utilisation des paramètres View Agent lors de l'exécution du filtrage du périphérique USB. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Exclure tous les périphériques Propriété : `ExcludeAllDevices`	Exclut tous les périphériques USB de la redirection. Si ce paramètre est réglé sur **`true`**, vous pouvez utiliser d'autres paramètres de stratégie pour autoriser la redirection de périphériques ou de familles de périphériques spécifiques. Si ce paramètre est réglé sur **`false`**, vous pouvez utiliser d'autres paramètres de stratégie pour empêcher la redirection de périphériques ou de familles de périphériques spécifiques. Si vous paramétrez la valeur de `Exclude All Devices` sur **`true`** dans View Agent et que ce paramètre passe à View Client, le paramètre View Agent est prioritaire sur le paramètre View Client. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
Exclure une famille de périphériques 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 est indéfinie.
Exclure le périphérique Vid/Pid. Propriété : `ExcludeVidPid`	Permet d'exclure de la redirection les périphériques associés à des ID de fournisseur et de produit donnés. Le format du paramètre est `vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]... Vous devez spécifier les numéros d'ID sous forme hexadécimale. Vous pouvez utiliser le caractère générique (**`*`**) à la place du chiffre d'un ID. Par exemple : **`vid-0781_pid-****;vid-0561_pid-554c`** La valeur par défaut est indéfinie.
Exclure un chemin Propriété : `ExcludePath`	Permet d'exclure de la redirection des périphériques correspondant à des chemins de concentrateurs ou de ports spécifiques. Le format du paramètre est `bus-`*x1*[`/`*y1*]...`_port-`*z1*[`;bus-`*x2*[`/`*y2*]...`_port-`*z2*]... Vous devez spécifier les numéros de bus et de port sous forme hexadécimale. Il n'est pas possible d'utiliser le caractère générique pour les chemins d'accès. Par exemple : **`bus-1/2/3_port-02;bus-1/1/1/4_port-ff`** La valeur par défaut est indéfinie.
Inclure des familles de périphériques Propriété : `IncludeFamily`	Permet d'inclure des familles de périphériques pouvant être redirigées. Le format du paramètre est *family_name_1*[`;`*family_name_2*]... Par exemple : **`storage`** La valeur par défaut est indéfinie.

Tableau 1-5. Configuration des propriétés pour la redirection USB (suite)

Nom et propriété de la stratégie	Description
Inclure un chemin Propriété : `IncludePath`	Permet d'inclure des périphériques correspondant à des chemins de concentrateurs ou de ports spécifiques pouvant être redirigés. Le format du paramètre est `bus-`*x1*`[/`*y1*`]...-port-`*z1*`[;bus-`*x2*`[/`*y2*`]...-port-`*z2*`]...` Vous devez spécifier les numéros de bus et de port sous forme hexadécimale. Il n'est pas possible d'utiliser le caractère générique pour les chemins d'accès. Par exemple : **`bus-1/2_port-02;bus-1/7/1/4_port-0f`** La valeur par défaut est indéfinie.
Inclure le périphérique Vid/Pid. Propriété : `IncludeVidPid`	Permet d'inclure des périphériques associés à des ID de fournisseur et de produit pouvant être redirigés. Le format du paramètre est `vid-`*xxx1*`_pid-`*yyy2*`[;vid-`*xxx2*`_pid-`*yyy2*`]...` Vous devez spécifier les numéros d'ID sous forme hexadécimale. Vous pouvez utiliser le caractère générique (**`*`**) à la place du chiffre d'un ID. Par exemple : **`vid-0561_pid-554c`** La valeur par défaut est indéfinie.

Familles de périphériques USB

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

Tableau 1-6. 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.

Tableau 1-6. Familles de périphériques USB (suite)

Nom de la famille de périphériques	Description
`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 VMware Client pour que le démon de service USB soit arrêté.
  b. Ouvrez un shell (`/Applications/Utilities/Terminal.app`) avec le même utilisateur qui démarre View Client.
  c. Utilisez la commande suivante :

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

  d. Redémarrez View 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"
  ```

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 fonction 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 supérieure.

Le cache d'images PCoIP capture la redondance spatiale et temporaire. 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 temporaire.

Comme pendant le défilement, les informations d'écran envoyées au périphérique client sont constituées principalement d'une séquence d'index de cache, 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.

Dépannage de View Client

Vous pouvez résoudre la plupart des problèmes de View Client en réinitialisant le poste de travail ou en réinstallant VMware View Client.

Réinitialiser un poste de travail

La réinitialisation arrête et redémarre le poste de travail. Les données non enregistrées sont perdues.

Vous devrez peut-être réinitialiser un poste de travail si le système d'exploitation du poste de travail cesse de répondre.

La réinitialisation d'un poste de travail View a la même finalité que d'appuyer sur le bouton Réinitialiser d'un ordinateur physique pour le forcer à redémarrer. Les fichiers ouverts sur le poste de travail View seront fermés sans être enregistrés.

Vous pouvez réinitialiser le poste de travail uniquement si votre administrateur View a activé cette fonction.

Procédure

- Utilisez la commande **[Réinitialiser]** .

Option	Action
À partir de l'OS du poste de travail	Sélectionnez **[Poste de travail]** > **[Réinitialiser]** dans la barre de menus Finder.
À partir de l'écran d'accueil avec des raccourcis de serveur	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 **[Poste de travail]** > **[Réinitialiser]** dans la barre de menus Finder.
À partir de l'écran d'accueil avec des raccourcis de poste de travail	Sélectionnez le poste de travail et choisissez **[Poste de travail]** > **[Réinitialiser]** dans la barre de menus Finder.

Le système d'exploitation dans le poste de travail View est redémarré. View Client se déconnecte du poste de travail.

Suivant

Attendez que le système démarre avant d'essayer de vous connecter au poste de travail View.

Désinstallation de View Client

Vous pouvez parfois résoudre des problèmes avec View Client en désinstallant et en réinstallant l'application VMware View Client.

Vous désinstallez View Client avec la méthode que vous utilisez habituellement pour désinstaller d'autres applications.

Faites glisser l'application **[VMware View Client]** du dossier **[Applications]** vers la **[Corbeille]** et videz la corbeille.

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

Reportez-vous à la section « Installer View Client sur Mac OS X », page 8.

Index

V