

Utilisation de HTML Access

Septembre 2015
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-001802-01

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

Copyright © 2013–2015 VMware, Inc. Tous droits réservés. [Copyright et informations sur les marques.](#)

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 HTML Access	5
1 Configuration et installation	7
Configuration système requise pour HTML Access	7
Préparer le Serveur de connexion View et les serveurs de sécurité pour HTML Access	10
Règles de pare-feu pour HTML Access	11
Préparer des postes de travail, des pools et des batteries de serveurs pour HTML Access	12
Configurer les agents HTML Access pour utiliser les nouveaux certificats SSL	14
Ajouter le composant logiciel enfichable Certificat à MMC sur un poste de travail Horizon View	15
Importer un certificat pour l'agent HTML Access dans un magasin de certificats Windows	15
Importer des certificats racine et intermédiaires pour l'agent HTML Access	16
Définir l'empreinte numérique de certificat dans le registre Windows	17
Configurer les agents HTML Access pour utiliser des suites de chiffrement spécifiques	18
Mise à niveau du logiciel HTML Access	18
Désinstaller HTML Access de Serveur de connexion View	20
Données collectées par VMware	20
2 Configuration de HTML Access pour les utilisateurs finaux	23
Configurer la page du portail Web de VMware Horizon pour les utilisateurs finaux	23
Utiliser des URI pour configurer des clients Web HTML Access	26
Syntaxe pour la création d'URI pour HTML Access	26
Exemples d'URI	28
Configurer les paramètres de stratégie de groupe de HTML Access	29
Paramètres de stratégie de groupe de HTML Access	30
3 Utilisation d'une application ou d'un poste de travail distant	33
Matrice de prise en charge des fonctions	33
Internationalisation	35
Connexion à une application ou un poste de travail distant	35
Faire confiance à un certificat racine auto-signé	36
Combinaisons de touches de raccourci	37
Claviers internationaux	40
Résolution de l'écran	41
Utilisation de la barre latérale	42
Audio	44
Copier et coller du texte	44
Utiliser la fonctionnalité de copier/coller	45
Fermer une session ou se déconnecter	46
Réinitialiser une application ou un poste de travail distant	47
Index	49

Utilisation de HTML Access

Ce guide, *Utilisation de HTML Access*, fournit des informations sur l'installation et l'utilisation de la fonctionnalité HTML Access de VMware Horizon™ 6 pour se connecter à des postes de travail virtuels sans avoir à installer de logiciel sur un système client.

Ce document contient des informations incluant la configuration système et des instructions sur l'installation du logiciel HTML Access sur un serveur View et dans une machine virtuelle de poste de travail distant afin que les utilisateurs finaux puissent utiliser un navigateur Web pour accéder à des postes de travail distants.

IMPORTANT Ces informations sont destinées aux administrateurs ayant déjà une certaine expérience de l'utilisation d'View et de VMware vSphere. Si vous découvrez View, nous vous recommandons à l'occasion de suivre les instructions pas à pas pour réaliser les procédures de base dans la documentation intitulée *Installation de View* et *Administration de View*.

Configuration et installation

La configuration d'un déploiement d'View pour HTML Access comprend l'installation d'HTML Access sur le Serveur de connexion View, l'ouverture des ports requis et l'installation du composant HTML Access sur la machine virtuelle du poste de travail distant.

Les utilisateurs finaux peuvent accéder à leurs postes de travail distants en ouvrant un navigateur pris en charge et en entrant l'URL du Serveur de connexion View.

Ce chapitre aborde les rubriques suivantes :

- [« Configuration système requise pour HTML Access », page 7](#)
- [« Préparer le Serveur de connexion View et les serveurs de sécurité pour HTML Access », page 10](#)
- [« Préparer des postes de travail, des pools et des batteries de serveurs pour HTML Access », page 12](#)
- [« Configurer les agents HTML Access pour utiliser les nouveaux certificats SSL », page 14](#)
- [« Configurer les agents HTML Access pour utiliser des suites de chiffrement spécifiques », page 18](#)
- [« Mise à niveau du logiciel HTML Access », page 18](#)
- [« Désinstaller HTML Access de Serveur de connexion View », page 20](#)
- [« Données collectées par VMware », page 20](#)

Configuration système requise pour HTML Access

Avec HTML Access, le système client ne requiert aucun autre logiciel à part un navigateur pris en charge. Le déploiement d'View doit respecter certaines exigences logicielles.

Navigateurs sur des systèmes clients

- HTML Access 3.5 prend en charge les navigateurs suivants.

Navigateur	Version
Chrome	43, 44
Internet Explorer	10, 11
Safari	7, 8 (Mobile Safari n'est pas pris en charge.)
Firefox	38, 39
Microsoft Edge	20

- HTML Access 3.4 prend en charge les navigateurs suivants.

Navigateur	Version
Chrome	41, 42, 43
Internet Explorer	10, 11
Safari	7, 8 (Mobile Safari n'est pas pris en charge.)
Firefox	36, 37, 38

Système d'exploitation client

- HTML Access 3.5 prend en charge les systèmes d'exploitation suivants.

Système d'exploitation	Version
Windows	7 SP1 (32 et 64 bits)
Windows	8.x (32 et 64 bits)
Windows	10 (32 et 64 bits)
Mac OS X	10.9.x (Mavericks)
Mac OS X	10.10.x (Yosemite)
Chrome OS	28.x et versions ultérieures

- HTML Access 3.4 prend en charge les systèmes d'exploitation suivants.

Système d'exploitation	Version
Windows	7 SP1 (32 et 64 bits)
Windows	8 (32 et 64 bits)
Mac OS X	10.9.x (Mavericks)
Mac OS X	10.10.x (Yosemite)
Chrome OS	28.x et versions ultérieures

REMARQUE Les périphériques iOS, tels que les téléphones et les tablettes, ne sont pas pris en charge. VMware vous recommande d'utiliser plutôt Horizon Client pour iOS. Si vous devez prendre en charge HTML Access sur ces périphériques, n'installez pas HTML Access 3.x. Utilisez plutôt HTML Access 2.6, qui est la version par défaut installée avec le Serveur de connexion View 6.1.1.

Postes de travail distants

- HTML Access 3.5 requiert View Agent 6.1 ou version ultérieure, et prend en charge tous les systèmes d'exploitation de poste de travail pris en charge par View 6.2. Pour plus d'informations, consultez la rubrique « Systèmes d'exploitation pris en charge pour View Agent » dans la version 6.2 de *Installation de View*.
- HTML Access 3.4 requiert View Agent 6.1.1 et prend en charge tous les systèmes d'exploitation pris en charge par View 6.1. Pour plus d'informations, consultez la rubrique « Systèmes d'exploitation pris en charge pour View Agent » dans la version 6.1 de *Installation de View*.

IMPORTANT Le poste de travail distant doit être une machine virtuelle. Bien que vous puissiez installer View Agent sur une machine physique, le protocole Blast utilisé avec HTML Access ne peut pas accéder à une machine physique. View Agent doit être installé sur une machine virtuelle.

Paramètres de pool

HTML Access nécessite les paramètres de pool suivants dans View Administrator :

- Le paramètre **Résolution max. d'un écran** doit avoir une valeur supérieure ou égale à **1 920 x 1 200** afin que le poste de travail distant dispose d'au moins 17,63 Mo de RAM vidéo.

Si vous prévoyez d'utiliser des applications 3D ou si des utilisateurs finaux utiliseront un Macbook avec écran Retina ou un Google Chromebook Pixel, reportez-vous à « [Résolution de l'écran](#) », page 41.

- Le paramètre **HTML Access** doit être activé.

Des instructions de configuration sont fournies dans « [Préparer des postes de travail, des pools et des batteries de serveurs pour HTML Access](#) », page 12.

Serveur de connexion View

Serveur de connexion View avec l'option HTML Access doit être installé sur le serveur.

HTML Access 3.5 requiert le Serveur de connexion View 6.2. Lorsque vous installez le Serveur de connexion View 6.2, vous devez sélectionner l'option **Installer HTML Access**.

HTML Access 3.4 requiert le Serveur de connexion View 6.1.1. Après avoir installé ou effectué une mise à niveau vers le Serveur de connexion View 6.1.1 et vérifié que vos postes de travail distants et vos hôtes RDS exécutent View Agent 6.1.1, vous devez exécuter un programme d'installation HTML Access distinct sur les instances du Serveur de connexion View.

Par défaut, lorsque vous installez le composant HTML Access, la règle du **Serveur de connexion VMware Horizon View (Blast-In)** est activée sur le pare-feu Windows, afin que celui-ci soit automatiquement configuré pour autoriser le trafic entrant sur le port TCP 8443.

Serveur de sécurité

Serveur de sécurité View : la version correspondante à celle du Serveur de connexion View doit être installée sur le serveur.

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.

REMARQUE Un serveur de sécurité unique peut prendre en charge jusqu'à 800 connexions simultanées à des clients Web.

Pare-feu tiers

Ajoutez des règles pour permettre le trafic suivant :

- Serveurs (y compris les serveurs de sécurité, les instances de Serveur de connexion View et les serveurs de réplica) : trafic entrant sur le port TCP 8443.
- Machines virtuelles de postes de travail à distance : trafic entrant (des serveurs) sur le port TCP 22443.

Protocole d'affichage pour View

Blast

Lorsque vous utilisez un navigateur Web pour accéder à un poste de travail distant, le protocole Blast est utilisé plutôt que PCoIP ou Microsoft RDP. Blast utilise HTTPS (HTTP sur SSL/TLS).

Préparer le Serveur de connexion View et les serveurs de sécurité pour HTML Access

Les administrateurs doivent effectuer des tâches spécifiques afin que les utilisateurs finaux puissent se connecter à des postes de travail distants en utilisant un navigateur Web.

Avant que les utilisateurs finaux puissent se connecter au Serveur de connexion View ou à un serveur de sécurité et accéder à un poste de travail distant, vous devez installer le Serveur de connexion View avec le composant HTML Access et installer les serveurs de sécurité.

IMPORTANT Pour certaines versions de HTML Access, si vous installez par erreur le Serveur de connexion View sans l'option HTML Access, puis souhaitez ultérieurement disposer du composant HTML Access, vous devez désinstaller le Serveur de connexion View et réexécuter le programme d'installation en sélectionnant l'option HTML Access. Lorsque vous désinstallez le Serveur de connexion View, ne désinstallez pas la configuration de View LDAP, nommée instance d'AD LDS Instance de VMwareVDMDS.

Pour les autres versions d'HTML Access, utilisez un programme d'installation distinct pour HTML Access afin d'éviter de réinstaller le Serveur de connexion View.

Tableau 1-1. Exigences concernant le programme d'installation pour les versions HTML Access

Version d'HTML Access	Version du Serveur de connexion View	Exigences d'installation
3.5	6.2	Pas de programme d'installation HTML Access distinct
3.4	6.1.1	Programme d'installation distinct
2.6	6.1, 6.1.1	Pas de programme d'installation HTML Access distinct

Voici la liste de contrôle des tâches à effectuer pour utiliser HTML Access :

- 1 Installez le Serveur de connexion View avec l'option HTML Access sur le ou les serveurs qui composeront un groupe répliqué de Serveur de connexion View.

Par défaut, le composant HTML Access est déjà sélectionné dans le programme d'installation. Pour obtenir des instructions d'installation, consultez la documentation *Installation de View*.

REMARQUE Pour vérifier si le composant HTML Access est installé, vous pouvez ouvrir l'applet Désinstaller un programme dans le système d'exploitation Windows et rechercher HTML Access View dans la liste.

- 2 Pour HTML Access 3.4 et pour les nouvelles installations, téléchargez le programme d'installation du portail Web HTML Access sur vos instances du Serveur de connexion View, puis exécutez-le. Pour HTML Access 3.5, cette étape n'est pas nécessaire, car HTML Access est automatiquement installé à l'étape 1.

Le programme d'installation de HTML Access 3.4 est disponible sur la page de téléchargement d'Horizon 6 version 6.1.1 (<http://www.vmware.com/go/downloadview>). Le programme d'installation se nomme VMware-Horizon-View-HTML-Access_X64-3.4.0-xxxxxx.exe, où xxxxxx est le numéro de build.

REMARQUE Si vous exécutez une mise à niveau plutôt qu'une nouvelle installation, vous devez mettre View Agent à niveau avant d'effectuer cette étape. Suivez les étapes dans « [Mise à niveau du logiciel HTML Access](#) », page 18.

- 3 Si vous utilisez des serveurs de sécurité, installez Serveur de sécurité View.

Pour obtenir des instructions d'installation, consultez la documentation *Installation de View*.

IMPORTANT La version de Serveur de sécurité View doit correspondre à celle de Serveur de connexion View.

- 4 Vérifiez que chaque instance du Serveur de connexion View ou du serveur de sécurité possède un certificat de sécurité qui peut être vérifié en utilisant le nom d'hôte que vous entrez dans le navigateur.
Pour plus d'informations, reportez-vous à la documentation *Installation de View*.
- 5 Pour pouvoir utiliser l'authentification à 2 facteurs, telle que l'authentification RSA SecurID ou RADIUS, assurez-vous que cette fonctionnalité est activée sur le Serveur de connexion View.
Pour plus d'informations, consultez les rubriques concernant l'authentification à deux facteurs dans la documentation *Administration de View*.
- 6 Si vous utilisez des pare-feu tiers, ajoutez des règles pour autoriser le trafic entrant sur le port TCP 8443 pour tous les hôtes des serveurs de sécurité et de Serveur de connexion View dans un groupe répliqué, et ajoutez une règle pour autoriser le trafic entrant (à partir des serveurs View) sur le port TCP 22443 des postes de travail distants du centre de données. Pour plus d'informations, reportez-vous à la section « Règles de pare-feu pour HTML Access », page 11.

Une fois les serveurs installés, si vous consultez View Administrator, vous constaterez que le paramètre **Blast Secure Gateway** est activé sur les instances du Serveur de connexion View et les serveurs de sécurité utilisés. De même, le paramètre **URL externe Blast** est configuré automatiquement pour utiliser pour le Blast Secure Gateway dans les instances du Serveur de connexion View et des serveurs de sécurité utilisés. Par défaut, l'URL contient le nom de domaine complet du tunnel URL externe sécurisé et le numéro de port par défaut, 8443. L'URL doit contenir le nom de domaine complet et le numéro de port qu'un système client peut utiliser pour atteindre ce Serveur de connexion View ou serveur de sécurité hôte. Pour en savoir plus, consultez « Définir les URL externes d'une instance du Serveur de connexion View » dans la documentation *Installation de View*.

REMARQUE Vous pouvez utiliser HTML Access avec VMware Workspace Portal pour permettre aux utilisateurs de se connecter à leur poste de travail à partir d'un navigateur HTML5. Pour plus d'informations sur l'installation d'Workspace Portal et sa configuration pour l'utiliser avec Serveur de connexion View, consultez la documentation Workspace Portal. Pour plus d'informations sur le couplage du Serveur de connexion View avec un serveur d'authentification SAML, reportez-vous à la documentation *Administration de View*.

Règles de pare-feu pour HTML Access

Pour autoriser les navigateurs Web clients à utiliser HTML Access pour effectuer des connexions à des serveurs de sécurité, à des instances du Serveur de connexion View et à des postes de travail distants, vos pare-feu doivent autoriser le trafic entrant sur certains ports TCP.

Les connexions HTML Access doivent utiliser HTTPS. Les connexions HTTP ne sont pas autorisées.

Par défaut, lorsque vous installez une instance du Serveur de connexion View ou un serveur de sécurité, la règle **Serveur de connexion VMware Horizon View (Blast-In)** est activée sur le pare-feu Windows, afin que celui-ci soit automatiquement configuré pour autoriser le trafic entrant sur le port TCP 8443.

Tableau 1-2. Règles de pare-feu pour HTML Access

Source	Port source par défaut	Protocole	Cible	Port cible par défaut	Remarques
Navigateur Web client	Tout port TCP	HTTPS	Serveur de sécurité ou instance de Serveur de connexion View	TCP 443	Pour établir une connexion initiale à View, le navigateur Web d'un périphérique client se connecte à un serveur de sécurité ou à une instance du Serveur de connexion View sur le port TCP 443.
Navigateur Web client	Tout port TCP	HTTPS	Blast Secure Gateway	TCP 8443	Une fois la connexion initiale à View établie, le navigateur Web d'un périphérique client se connecte à Blast Secure Gateway sur le port TCP 8443. Blast Secure Gateway doit être activé sur un serveur de sécurité ou sur une instance du Serveur de connexion View pour autoriser l'établissement de cette deuxième connexion.
Blast Secure Gateway	Tout port TCP	HTTPS	Agent HTML Access	TCP 22443	Si Blast Secure Gateway est activé, lorsqu'un utilisateur sélectionne un poste de travail distant, Blast Secure Gateway se connecte à l'agent HTML Access sur le port TCP 22443 sur le poste de travail. Ce composant d'agent est inclus lorsque vous installez View Agent.
Navigateur Web client	Tout port TCP	HTTPS	Agent HTML Access	TCP 22443	Si Blast Secure Gateway n'est pas activé, lorsqu'un utilisateur sélectionne un poste de travail View, le navigateur Web du périphérique client se connecte directement à l'agent HTML Access sur le port TCP 22443 sur le poste de travail. Ce composant d'agent est inclus lorsque vous installez View Agent.

Préparer des postes de travail, des pools et des batteries de serveurs pour HTML Access

Avant que les utilisateurs finaux puissent accéder à une application ou un poste de travail distant, les administrateurs doivent configurer certains paramètres de pool et de batterie de serveurs et installer View Agent sur les machines virtuelles de poste de travail distant et les hôtes RDS dans le centre de données.

Le client HTML Access représente une bonne alternative lorsque le logiciel Horizon Client n'est pas installé sur le système client.

REMARQUE Le logiciel Horizon Client offre plus de fonctionnalités et de meilleures performances que le client HTML Access. Par exemple, avec le client HTML Access, certaines combinaisons de touches ne fonctionnent pas sur le poste de travail distant, mais celles-ci fonctionnent avec Horizon Client.

Prérequis

- Assurez-vous que votre infrastructure vSphere et les composants View respectent la configuration système requise par HTML Access.

Reportez-vous à la section [« Configuration système requise pour HTML Access »](#), page 7.

- Assurez-vous que le composant HTML Access est installé sur l'hôte ou les hôtes du Serveur de connexion View, et que les pare-feu Windows sur les instances du Serveur de connexion View et les serveurs de sécurité autorisent le trafic entrant sur le port TCP 8443.

Reportez-vous à la section [« Préparer le Serveur de connexion View et les serveurs de sécurité pour HTML Access »](#), page 10.

- Si vous utilisez des pare-feu tiers, ajoutez une règle pour autoriser le trafic entrant à partir de serveurs View sur le port TCP 22443 des postes de travail View dans le centre de données.

- Vérifiez que la machine virtuelle que vous prévoyez d'utiliser en tant que source de poste de travail ou hôte RDS dispose des logiciels suivants : un système d'exploitation pris en charge et VMware Tools.

Pour une liste des systèmes d'exploitation pris en charge, reportez-vous à « [Configuration système requise pour HTML Access](#) », page 7.

- Familiarisez-vous avec les procédures de création de pools et de batteries de serveurs et d'octroi de droits aux utilisateurs. Consultez les rubriques sur la création de pools et de batteries de serveurs dans *Configuration de postes de travail et d'applications dans View*.
- Pour vérifier que l'application ou le poste de travail distant est accessible aux utilisateurs finaux, vérifiez que le logiciel Horizon Client est installé sur un système client. Vous devez essayer la connexion en utilisant le logiciel Horizon Client avant d'essayer de vous connecter à partir d'un navigateur.

Pour obtenir des instructions sur l'installation d'Horizon Client, reportez-vous au site de documentation d'Horizon Client à l'adresse https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

- Assurez-vous que vous disposez de l'un des navigateurs pris en charge pour accéder à un poste de travail distant. Reportez-vous à la section « [Configuration système requise pour HTML Access](#) », page 7.

Procédure

- 1 Installez View Agent avec l'option **HTML Access** sur toutes les machines virtuelles parentes pour les pools de clone lié, les modèles de machine virtuelle pour les pools de clone complet, les machines virtuelles pour les pools manuels et les hôtes RDS pour les pools de postes de travail et d'applications hébergées.
- 2 Pour les postes de travail et les applications RDS, utilisez View Administrator pour créer ou modifier la batterie de serveurs et activez l'option **Autoriser l'installation de HTML Access sur les postes de travail et les applications de cette batterie de serveurs** dans les paramètres de la batterie de serveurs.
- 3 Pour les pools de postes de travail à session unique, utilisez View Administrator pour créer ou modifier le pool de postes de travail afin que le pool puisse être utilisé avec HTML Access.
 - a Activez **HTML Access** dans les paramètres du pool de postes de travail.

Le paramètre **HTML Access** n'apparaît pas dans l'assistant Ajouter un pool de postes de travail lorsque vous créez des pools de postes de travail RDS. Au lieu de cela, vous activez l'option **Autoriser l'installation de HTML Access sur les postes de travail et les applications de cette batterie de serveurs** lors de la création ou la modification de la batterie de serveurs d'hôtes RDS.
 - b Dans les paramètres du pool, vérifiez que la **Résolution maximale de chaque moniteur** est supérieure ou égale à **1 920x1 200**.
- 4 Une fois les pools créés, recomposés ou mis à niveau pour utiliser View Agent avec l'option **HTML Access**, utilisez Horizon Client pour ouvrir une session sur un poste de travail ou une application.

Avant d'utiliser HTML Access, suivez les étapes ci-dessous pour vérifier que le pool fonctionne correctement.
- 5 Ouvrez un navigateur compatible et entrez une URL qui pointe vers votre instance de serveur de connexion View.

Par exemple :

`https://horizon.mycompany.com`

Veillez à utiliser **https** dans l'URL.
- 6 Sur la page Web qui s'affiche, cliquez sur **VMware Horizon View HTML Access** et connectez-vous comme vous le feriez avec le logiciel Horizon Client.

- 7 Sur la page de sélection des postes de travail et applications qui s'affiche, cliquez sur une icône pour vous connecter.

Vous pouvez à présent accéder à une application ou un poste de travail distant à partir d'un navigateur Web lorsque vous utilisez un périphérique client dont le système d'exploitation n'a pas ou ne peut pas prendre en charge le logiciel Horizon Client.

Suivant

Pour plus de sécurité, si vos stratégies de sécurité nécessitent que l'agent Blast du poste de travail utilise un certificat SSL d'une autorité de certification, consultez « [Configurer les agents HTML Access pour utiliser les nouveaux certificats SSL](#) », page 14.

Configurer les agents HTML Access pour utiliser les nouveaux certificats SSL

Pour respecter les réglementations de sécurité ou du secteur, vous pouvez remplacer les certificats SSL par défaut générés par l'agent HTML Access par des certificats signés par une autorité de certification.

Lors de l'installation de l'agent HTML Access sur des postes de travail View, le service de l'agent HTML Access crée des certificats auto-signés par défaut. Le service présente les certificats par défaut aux navigateurs qui utilisent HTML Access pour se connecter à View.

REMARQUE Dans le système d'exploitation client sur la machine virtuelle de poste de travail, ce service s'appelle VMware Blast.

Pour remplacer les certificats par défaut par des certificats signés obtenus auprès d'une autorité de certification, vous devez importer un certificat dans le magasin de certificats de l'ordinateur local Windows sur chaque poste de travail View. Vous devez également définir une valeur de registre sur chaque poste de travail qui autorise l'agent HTML Access à utiliser le nouveau certificat.

Si vous remplacez les certificats par défaut de l'agent HTML Access par des certificats signés par une autorité de certification, VMware vous recommande de configurer un certificat unique sur chaque poste de travail. Ne configurez pas de certificat signé par une autorité de certification sur une machine virtuelle parente ou sur un modèle utilisé pour créer un pool de postes de travail. Cela aurait pour incidence de voir des centaines ou des milliers de postes de travail avec des certificats identiques.

Procédure

- 1 [Ajouter le composant logiciel enfichable Certificat à MMC sur un poste de travail Horizon View](#) page 15
Avant de pouvoir ajouter des certificats au magasin de certificats de l'ordinateur local Windows, vous devez ajouter le composant logiciel enfichable Certificat à MMC (Microsoft Management Console) sur les postes de travail View sur lesquels l'agent HTML Access est installé.
- 2 [Importer un certificat pour l'agent HTML Access dans un magasin de certificats Windows](#) page 15
Pour remplacer un certificat par défaut de l'agent HTML Access par un certificat signé par une autorité de certification, vous devez importer ce dernier dans le magasin de certificats de l'ordinateur local Windows. Effectuez cette procédure sur chaque poste de travail où l'agent HTML Access est installé.
- 3 [Importer des certificats racine et intermédiaires pour l'agent HTML Access](#) page 16
Si le certificat racine et les certificats intermédiaires dans la chaîne de certificats ne sont pas importés avec le certificat SSL importé pour l'agent HTML Access, vous devez importer ces certificats dans le magasin de certificats de l'ordinateur local Windows.

4 [Définir l'empreinte numérique de certificat dans le registre Windows](#) page 17

Pour permettre à l'agent HTML Access d'utiliser un certificat signé par une autorité de certification importé dans le magasin de certificats Windows, vous devez configurer l'empreinte numérique de certificat dans une clé de registre Windows. Vous devez suivre cette étape sur chaque poste de travail sur lequel vous remplacez le certificat par défaut par un certificat signé par une autorité de certification.

Ajouter le composant logiciel enfichable Certificat à MMC sur un poste de travail Horizon View

Avant de pouvoir ajouter des certificats au magasin de certificats de l'ordinateur local Windows, vous devez ajouter le composant logiciel enfichable Certificat à MMC (Microsoft Management Console) sur les postes de travail View sur lesquels l'agent HTML Access est installé.

Prérequis

Vérifiez que MMC et le composant logiciel enfichable Certificat sont disponibles sur le système d'exploitation client Windows sur lequel l'agent HTML Access est installé.

Procédure

- 1 Sur le poste de travail View, cliquez sur **Démarrer** et entrez **mmc.exe**.
- 2 Dans la fenêtre MMC, sélectionnez **Fichier > Ajouter/Supprimer un composant logiciel enfichable**.
- 3 Dans la fenêtre Ajouter ou supprimer des composants logiciels enfichables, sélectionnez **Certificats** et cliquez sur **Ajouter**.
- 4 Dans la fenêtre Composant logiciel enfichable Certificats, sélectionnez **Compte d'ordinateur**, cliquez sur **Suivant**, sélectionnez **Ordinateur local** et cliquez sur **Terminer**.
- 5 Dans la fenêtre Ajouter ou supprimer des composants logiciels enfichables, cliquez sur **OK**.

Suivant

Importez le certificat SSL dans le magasin de certificats de l'ordinateur local Windows. Reportez-vous à la section « [Importer un certificat pour l'agent HTML Access dans un magasin de certificats Windows](#) », page 15.

Importer un certificat pour l'agent HTML Access dans un magasin de certificats Windows

Pour remplacer un certificat par défaut de l'agent HTML Access par un certificat signé par une autorité de certification, vous devez importer ce dernier dans le magasin de certificats de l'ordinateur local Windows. Effectuez cette procédure sur chaque poste de travail où l'agent HTML Access est installé.

Prérequis

- Vérifiez que l'agent HTML Access est installé sur le poste de travail View.
- Vérifiez que le certificat signé par une autorité de certification a été copié sur le poste de travail.
- Vérifiez que le composant logiciel Certificat a été ajouté à MMC. Reportez-vous à la section « [Ajouter le composant logiciel enfichable Certificat à MMC sur un poste de travail Horizon View](#) », page 15.

Procédure

- 1 Dans la fenêtre MMC sur le poste de travail View, développez le nœud **Certificats (Ordinateur local)** et sélectionnez le dossier **Personnel**.
- 2 Dans le volet Actions, allez dans **Autres actions > Toutes les tâches > Importer**.

- 3 Dans l'assistant Importation de certificat, cliquez sur **Suivant** et accédez à l'emplacement de stockage du certificat.
- 4 Sélectionnez le fichier du certificat et cliquez sur **Ouvrir**.
Pour afficher votre type de fichier de certificat, vous pouvez sélectionner son format de fichier dans le menu déroulant **Nom de fichier**.
- 5 Tapez le mot de passe de la clé privée incluse dans le fichier de certificat.
- 6 Sélectionnez **Marquer cette clé comme exportable**.
- 7 Sélectionnez **Inclure toutes les propriétés extensibles**.
- 8 Cliquez sur **Suivant** et sur **Terminer**.
Le nouveau certificat apparaît dans le dossier **Certificats (Ordinateur local) > Personnel > Certificats**.
- 9 Vérifiez que le nouveau certificat contient une clé privée.
 - a Dans le dossier **Certificats (Ordinateur local) > Personnel > Certificats**, double-cliquez sur le nouveau certificat.
 - b Sous l'onglet Général de la boîte de dialogue Informations sur le certificat, vérifiez que la déclaration suivante apparaît : *Vous avez une clé privée qui correspond à ce certificat*.

Suivant

Si nécessaire, importez le certificat racine et les certificats intermédiaires dans le magasin de certificats Windows. Reportez-vous à la section « [Importer des certificats racine et intermédiaires pour l'agent HTML Access](#) », page 16.

Configurez la clé de registre appropriée avec l'empreinte numérique de certificat. Reportez-vous à la section « [Définir l'empreinte numérique de certificat dans le registre Windows](#) », page 17.

Importer des certificats racine et intermédiaires pour l'agent HTML Access

Si le certificat racine et les certificats intermédiaires dans la chaîne de certificats ne sont pas importés avec le certificat SSL importé pour l'agent HTML Access, vous devez importer ces certificats dans le magasin de certificats de l'ordinateur local Windows.

Procédure

- 1 Dans la console MMC sur le poste de travail View, développez le nœud **Certificats (Ordinateur local)** et allez dans le dossier **Autorités de certification racine de confiance > Certificats**.
 - Si votre certificat racine se trouve dans ce dossier, et qu'il n'y a pas de certificat intermédiaire dans votre chaîne de certificats, ignorez cette procédure.
 - Si votre certificat racine ne se trouve pas dans ce dossier, passez à l'étape 2.
- 2 Cliquez avec le bouton droit sur le dossier **Autorités de certification racine de confiance > Certificats** et cliquez sur **Toutes les tâches > Importer**.
- 3 Dans l'assistant Importation de certificat, cliquez sur **Suivant** et allez à l'emplacement de stockage du certificat de l'autorité de certification racine.
- 4 Sélectionnez le fichier du certificat de l'autorité de certification racine et cliquez sur **Ouvrir**.
- 5 Cliquez sur **Suivant**, **Suivant** et **Terminer**.

- 6 Si votre certificat de serveur a été signé par une autorité de certification intermédiaire, importez tous les certificats intermédiaires se trouvant dans la chaîne de certificats dans le magasin de certificats de l'ordinateur local Windows.
 - a Allez dans le dossier **Certificats (Ordinateur local) > Autorités de certification intermédiaires > Certificats**.
 - b Répétez les étapes 3 à 6 pour chaque certificat intermédiaire devant être importé.

Suivant

Configurez la clé de registre appropriée avec l'empreinte numérique de certificat. Reportez-vous à la section « [Définir l'empreinte numérique de certificat dans le registre Windows](#) », page 17.

Définir l'empreinte numérique de certificat dans le registre Windows

Pour permettre à l'agent HTML Access d'utiliser un certificat signé par une autorité de certification importé dans le magasin de certificats Windows, vous devez configurer l'empreinte numérique de certificat dans une clé de registre Windows. Vous devez suivre cette étape sur chaque poste de travail sur lequel vous remplacez le certificat par défaut par un certificat signé par une autorité de certification.

Prérequis

Vérifiez que le certificat signé par une autorité de certification est importé dans le magasin de certificats Windows. Reportez-vous à la section « [Importer un certificat pour l'agent HTML Access dans un magasin de certificats Windows](#) », page 15.

Procédure

- 1 Dans la fenêtre MMC sur le poste de travail View où l'agent HTML Access est installé, accédez au dossier **Certificats (Ordinateur local) > Personnel > Certificats**.
- 2 Double-cliquez sur le certificat signé par une autorité de certification que vous avez importé dans le magasin de certificats Windows.
- 3 Dans la boîte de dialogue Certificats, cliquez sur l'onglet Détails, faites défiler la liste et sélectionnez l'icône **Empreinte numérique**.
- 4 Copiez l'empreinte numérique sélectionnée dans un fichier texte.

Par exemple : 31 2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e

REMARQUE Lorsque vous copiez l'empreinte numérique, n'incluez pas l'espace de début. Si vous le copiez par inadvertance avec l'empreinte numérique dans la clé de registre (à l'étape 7), le certificat peut ne pas être configuré correctement. Ce problème peut survenir même lorsque l'espace de début ne s'affiche pas dans la zone de texte de la valeur du registre.

- 5 Démarrez l'éditeur de Registre Windows sur le poste de travail sur lequel l'agent HTML Access est installé.
- 6 Accédez à la clé de registre HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config.
- 7 Modifiez la valeur SslHash et collez l'empreinte numérique de certificat dans la zone de texte.
- 8 Redémarrez le service VMware Blast pour que vos modifications prennent effet.

Dans le système d'exploitation client Windows, le service de l'agent HTML Access s'appelle VMware Blast.

Lorsqu'un utilisateur se connecte à un poste de travail via HTML Access, l'agent HTML Access présente le certificat signé par une autorité de certification au navigateur de l'utilisateur.

Configurer les agents HTML Access pour utiliser des suites de chiffrement spécifiques

Vous pouvez configurer l'agent HTML Access pour qu'il utilise des suites de chiffrement spécifiques au lieu du jeu de chiffrements par défaut.

Par défaut, l'agent HTML Access requiert des connexions SSL entrantes pour utiliser le cryptage basé sur certains chiffrements qui offrent une protection renforcée contre les écoutes illicites et les contrefaçons. Vous pouvez configurer une autre liste de chiffrements que peut utiliser l'agent HTML Access. Le jeu de chiffrements acceptables suit le format OpenSSL, qui est décrit à l'adresse <https://www.openssl.org/docs/apps/ciphers.html>.

Procédure

- 1 Démarrez l'éditeur de Registre Windows sur le poste de travail sur lequel l'agent HTML Access est installé.
- 2 Accédez à la clé de registre HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config.
- 3 Ajoutez une nouvelle valeur de chaîne (REG_SZ), SslCiphers, et collez la liste de chiffrements au format OpenSSL dans la zone de texte.
- 4 Redémarrez le service VMware Blast pour que vos modifications prennent effet.

Dans le système d'exploitation client Windows, le service de l'agent HTML Access s'appelle VMware Blast.

Pour reprendre l'utilisation de la liste de chiffrements par défaut, supprimez la valeur SslCiphers et redémarrez le service VMware Blast. Ne supprimez pas simplement la partie données de la valeur, car l'agent HTML Access traitera alors tous les chiffrements comme étant inacceptables, conformément à la définition de format de la liste de chiffrements OpenSSL.

Lorsque l'agent HTML Access démarre, il écrit la définition de chiffrement dans le fichier journal du service VMware Blast. Vous pouvez trouver la liste de chiffrements actuels par défaut en examinant les journaux lorsque le service VMware Blast démarre sans valeur SslCiphers configurée dans le registre Windows.

La définition de chiffrement par défaut de l'agent HTML Access peut changer d'une version à l'autre pour améliorer la sécurité.

Mise à niveau du logiciel HTML Access

Installez la dernière version de HTML Access pour obtenir les mises à jour et améliorations les plus récentes.

Pour effectuer une mise à niveau vers la dernière version de HTML Access, vous devez vérifier que la dernière version du Serveur de connexion View est installée sur toutes les instances d'un groupe répliqué.

Pour certaines versions de HTML Access, un programme d'installation HTML Access distinct est requis. Le tableau suivant répertorie les versions de HTML Access qui requièrent un programme d'installation distinct.

Tableau 1-3. Exigences concernant le programme d'installation pour les versions HTML Access

Version d'HTML Access	Version du Serveur de connexion View	Exigences d'installation
3.5	6.2	Pas de programme d'installation HTML Access distinct
3.4	6.1.1	Programme d'installation distinct
2.6	6.1, 6.1.1	Pas de programme d'installation HTML Access distinct

IMPORTANT Concernant les programmes d'installation distincts de HTML Access, lorsque vous mettez à niveau le Serveur de connexion View, vous devez également exécuter le programme d'installation de HTML Access après la mise à niveau du Serveur de connexion View. Par exemple, après la mise à niveau du Serveur de connexion View vers un nouveau correctif ou une nouvelle version de maintenance, la page du portail Web de HTML Access peut ne pas afficher l'icône de HTML Access. Si aucune nouvelle version de HTML Access n'est disponible, utilisez la fonction Désinstaller un programme de Windows pour désinstaller HTML Access, puis réinstaller la même version.

Pour HTML Access 3.5, lorsque vous faites une mise à niveau vers le Serveur de connexion 6.2, HTML Access sera automatiquement installé ou mis à niveau vers 3.5. Aucun programme d'installation distinct n'est requis.

Voici la liste de contrôle des tâches à effectuer pour exécuter une mise à niveau vers HTML Access 3.4 :

- 1 Effectuez une mise à niveau vers le Serveur de connexion View 6.1.1 avec l'option HTML Access sur le ou les serveurs qui composent un groupe répliqué de Serveur de connexion View.

Par défaut, le composant HTML Access est déjà sélectionné dans le programme d'installation.

Lorsque vous installez le Serveur de connexion View 6.1.1 de façon interactive, la version de HTML Access installée est HTML Access 2.6. À ce stade, vous ne pouvez pas utiliser d'applications distantes (hébergées) avec HTML Access. Les utilisateurs peuvent continuer à utiliser HTML Access 2.6 pour se connecter à des postes de travail exécutant View Agent 6.1.

- 2 Si vous utilisez des serveurs de sécurité, effectuez une mise à niveau vers le Serveur de sécurité View 6.1.1.

La version de Serveur de sécurité View doit correspondre à celle de Serveur de connexion View.

- 3 Effectuez la mise à niveau vers View Agent 6.1.1 sur tous les hôtes RDS et machines VDI, y compris les machines virtuelles parentes et modèles et les machines virtuelles dans vos pools de postes de travail.

Avec cette étape, vous mettez à niveau View Agent avant de mettre à niveau HTML Access sur vos instances du Serveur de connexion View. Si vous avez d'abord mis à niveau HTML Access sur vos serveurs, vos utilisateurs finaux ne pouvaient pas se connecter à des postes de travail View Agent antérieurs (version 6.1 ou antérieure) depuis leurs clients Web.

REMARQUE Le programme d'installation de View Agent inclut désormais le composant de l'agent HTML Access qui était inclus dans Remote Experience Agent pour les versions antérieures à Horizon 6.0 (avec View). Remote Experience Agent faisait partie d'Horizon View Feature Pack. Pour mettre à niveau les fonctionnalités qui étaient installées avec Remote Experience Agent, il vous suffit d'exécuter le programme d'installation de View Agent. Ce programme d'installation supprime Remote Experience Agent avant d'effectuer la mise à niveau. Si, pour certaines raisons, vous décidez de supprimer manuellement Remote Experience Agent, assurez-vous de le faire avant d'exécuter le programme d'installation de la nouvelle version de View Agent.

- Sur la page de téléchargement d'Horizon 6 version 6.1.1 (<http://www.vmware.com/go/downloadview>), téléchargez le programme d'installation du portail Web HTML Access sur vos instances du Serveur de connexion View et exécutez le programme d'installation.

Le programme d'installation se nomme VMware-Horizon-View-HTML-Access_X64-3.4.0-xxxxxx.exe, où xxxxxx est le numéro de build.

REMARQUE Pour vérifier si le composant HTML Access est installé, vous pouvez ouvrir l'applet Désinstaller un programme dans le système d'exploitation Windows et rechercher HTML Access View dans la liste.

Désinstaller HTML Access de Serveur de connexion View

Vous pouvez désinstaller HTML Access en utilisant la même méthode que pour désinstaller d'autres logiciels Windows.

Procédure

- Sur les hôtes de Serveur de connexion View sur lesquels HTML Access est installé, ouvrez l'applet Désinstaller un programme du Panneau de configuration Windows.
- Sélectionnez le programme HTML Access et cliquez sur **Désinstaller**.

Version d'HTML Access	Nom du programme HTML Access
3.5	VMware Horizon 6 HTML Access
3.4	VMware Horizon View HTML Access

- (Facultatif) Pour le pare-feu Windows de cet hôte, vérifiez que le port TCP 8443 n'autorise plus le trafic entrant.

Suivant

Interdisez le trafic entrant vers le port TCP 8443 sur le pare-feu Windows des serveurs de sécurité couplés. Le cas échéant, sur les pare-feu tiers, modifiez les règles pour interdire le trafic entrant vers le port TCP 8443 pour tous les serveurs de sécurité couplés et cet hôte de Serveur de connexion View.

Données collectées par VMware

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

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 sur le client sont d'abord envoyées au Serveur de connexion View puis à VMware, avec des données des serveurs, des pools de postes de travail et des postes de travail distants.

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 1-4. Données clientes collectées pour le programme d'amélioration du produit

Description	Nom de champ	Ce champ reste-t-il anonyme ?	Exemple
Entreprise qui a produit l'application	<client-vendor>	Non	VMware
Nom du produit	<client-product>	Non	VMware Horizon HTML Access

Tableau 1-4. Données clientes collectées pour le programme d'amélioration du produit (suite)

Description	Nom de champ	Ce champ reste-t-il anonyme ?	Exemple
Version du produit client	<client-version>	Non	3.5.0-build_number
Architecture binaire du client	<client-arch>	Non	Exemples comprenant les valeurs suivantes : <ul style="list-style-type: none"> ■ navigateur ■ arm
Architecture native du navigateur	<browser-arch>	Non	Exemples comprenant les valeurs suivantes : <ul style="list-style-type: none"> ■ Win32 ■ Win64 ■ MacIntel ■ iPad
Chaîne de l'agent utilisateur du navigateur	<browser-user-agent>	Non	Exemples comprenant les valeurs suivantes : <ul style="list-style-type: none"> ■ Mozilla/5.0 (Windows NT 6.1; WOW64) ■ AppleWebKit/703.00 (KHTML, like Gecko) ■ Chrome/3.0.1750 ■ Safari/703.00 ■ Edge/12.10240
Chaîne de version interne de navigateur	<browser-version>	Non	Exemples comprenant les valeurs suivantes : <ul style="list-style-type: none"> ■ 7.0.3 (pour Safari), ■ 29.0 (pour Firefox). ■ 12.10240 (pour Edge)
Implémentation de base du navigateur	<browser-core>	Non	Exemples comprenant les valeurs suivantes : <ul style="list-style-type: none"> ■ Chrome ■ Safari ■ Firefox ■ MSIE (pour Internet Explorer) ■ Edge
Si le navigateur tourne sur un ordinateur de poche	<browser-is-handheld>	Non	true

Configuration de HTML Access pour les utilisateurs finaux

2

Vous pouvez modifier l'apparence de la page Web que les utilisateurs finaux voient quand ils accèdent à l'URL de HTML Access. Vous pouvez également définir des stratégies de groupe qui contrôlent la qualité d'image, les ports utilisés et d'autres paramètres.

Ce chapitre aborde les rubriques suivantes :

- [« Configurer la page du portail Web de VMware Horizon pour les utilisateurs finaux », page 23](#)
- [« Utiliser des URI pour configurer des clients Web HTML Access », page 26](#)
- [« Configurer les paramètres de stratégie de groupe de HTML Access », page 29](#)
- [« Paramètres de stratégie de groupe de HTML Access », page 30](#)

Configurer la page du portail Web de VMware Horizon pour les utilisateurs finaux

Vous pouvez configurer cette page Web pour afficher ou masquer l'icône de téléchargement d'Horizon Client ou l'icône de connexion à un poste de travail distant via HTML Access. Vous pouvez également configurer d'autres liens sur cette page.

Par défaut, la page de portail affiche à la fois une icône pour télécharger et installer le client Horizon Client natif et une icône pour se connecter via HTML Access. Toutefois, dans certains cas, vous voudrez peut-être que les liens pointent vers un serveur Web interne ou que des versions de client spécifiques puissent être disponibles sur votre propre serveur. Vous pouvez reconfigurer la page pour pointer vers une URL différente.

Vous pouvez créer des liens de programme d'installation pour les systèmes d'exploitation client spécifiques. Par exemple, si vous accédez à la page de portail depuis un système Mac OS X, le lien du programme d'installation Mac OS X natif s'affiche. Pour les clients Windows, vous pouvez créer des liens distincts pour les programmes d'installation 32 bits et 64 bits.

IMPORTANT Si vous avez mis à niveau Serveur de connexion View 5.x ou une version antérieure et que le composant HTML Access n'est pas installé, et si vous aviez précédemment modifié la page du portail pour qu'elle pointe vers votre propre serveur pour télécharger Horizon Client, ces personnalisations peuvent être masquées après l'installation de Serveur de connexion View 6.0 ou version ultérieure. Avec Horizon 6 ou version ultérieure, le composant HTML Access est installé automatiquement pendant une mise à niveau de Serveur de connexion View.

Si vous avez déjà installé le composant HTML Access séparément de View 5.x, toutes les personnalisations que vous avez apportées à la page Web sont conservées. Si le composant HTML Access n'était pas installé, toutes les personnalisations que vous avez apportées sont masquées. Les personnalisations des versions antérieures se situent dans le fichier `portal-links.properties` qui n'est plus utilisé.

Procédure

- 1 Sur l'hôte serveur de connexion View, ouvrez le fichier `portal-links-html-access.properties` avec un éditeur de texte.

Ce fichier se trouve dans `CommonAppDataFolder\VMware\VDM\portal\portal-links-html-access.properties`. Pour les systèmes d'exploitation Windows Server 2008, le dossier `CommonAppDataFolder` est `C:\ProgramData`. Pour afficher le dossier `C:\ProgramData` dans l'Explorateur Windows, vous devez utiliser la boîte de dialogue Options des dossiers pour afficher les dossiers cachés.

REMARQUE Pour View 5.x et versions antérieures, les personnalisations se situaient dans le fichier `portal-links.properties` qui se trouve dans le même répertoire `CommonAppDataFolder\VMware\VDM\portal\` que le fichier `portal-links-html-access.properties`.

- 2 Modifiez les propriétés de la configuration pour les définir convenablement.

Par défaut, les icônes du programme d'installation et de HTML Access sont toutes deux activées et un lien pointe vers la page de téléchargement du client sur le site Web de VMware. Pour désactiver une icône, ce qui la supprime de la page Web, définissez la propriété sur `false`.

Option	Paramètre propriété
Désactiver HTML Access	<p><code>enable.webclient=false</code></p> <p>Si cette option est définie sur <code>false</code> alors que l'option <code>enable.download</code> est définie sur <code>true</code>, l'utilisateur est dirigé vers une page Web pour télécharger le programme d'installation natif d'Horizon Client. Si ces deux options sont définies sur <code>false</code>, l'utilisateur obtient le message suivant : « Contactez votre administrateur local pour obtenir des instructions sur l'accès à ce serveur de connexion. »</p>
Désactiver le téléchargement d'Horizon Client	<p><code>enable.download=false</code></p> <p>Si cette option est définie sur <code>false</code> alors que l'option <code>enable.webclient</code> est définie sur <code>true</code>, l'utilisateur est dirigé vers la page Web de connexion à HTML Access. Si ces deux options sont définies sur <code>false</code>, l'utilisateur obtient le message suivant : « Contactez votre administrateur local pour obtenir des instructions sur l'accès à ce serveur de connexion. »</p>
Changer l'URL de la page Web pour le téléchargement d'Horizon Client	<p><code>link.download=https://url-of-web-server</code></p> <p>Utilisez cette propriété si vous prévoyez de créer votre propre page Web</p>

Option	Paramètre propriété
Créer des liens pour des programmes d'installation spécifiques	<p>Les exemples suivants montrent des URL complètes, mais vous pouvez utiliser des URL relatives si vous placez les fichiers du programme d'installation dans le répertoire <code>downloads</code>, situé sous le répertoire <code>C:\Program Files\VMware\VMware View\Server\broker\webapps\</code> sur le Serveur de connexion View, comme décrit à l'étape suivante.</p> <ul style="list-style-type: none"> ■ Programme d'installation de Windows 32 bits : <p style="margin-left: 20px;"><code>link.win32=https://server/downloads/VMware-Horizon-Client.exe</code></p> ■ Programme d'installation de Windows 64 bits : <p style="margin-left: 20px;"><code>link.win64=https://server/downloads/VMware-Horizon-Client.exe</code></p> ■ Programme d'installation de Linux : <p style="margin-left: 20px;"><code>link.linux=https://server/downloads/VMware-Horizon-Client.tar.gz</code></p> ■ Programme d'installation de Mac OS X : <p style="margin-left: 20px;"><code>link.mac=https://server/downloads/VMware-Horizon-Client.dmg</code></p> ■ Programme d'installation d'iOS : <p style="margin-left: 20px;"><code>link.ios=https://server/downloads/VMware-Horizon-Client-iPhoneOS.zip</code></p> ■ Programme d'installation d'Android : <p style="margin-left: 20px;"><code>link.android=https://server/downloads/VMware-Horizon-Client-AndroidOS.apk</code></p> ■ Programme d'installation d'un système d'exploitation inconnu (par exemple, vous pouvez utiliser cette propriété pour le programme d'installation client Chrome) : <p style="margin-left: 20px;"><code>link.unknown=https://server/downloads/VMware-Horizon-Client-AndroidOS-arm-ARC.apk</code></p>
Changer l'URL du lien de l'aide sur la page de connexion	<p><code>link.help</code></p> <p>Par défaut, ce lien pointe vers un système d'aide hébergé sur le site Web de VMware. Le lien de l'aide apparaît en bas de la page de connexion.</p>

- 3 Pour permettre aux utilisateurs de télécharger les programmes d'installation depuis un emplacement différent du site Web VMware, placez les fichiers des programmes d'installation sur le serveur HTTP où ils résideront.

Cet emplacement doit correspondre aux URL que vous avez spécifiées dans le fichier `portal-links-html-access.properties` à l'étape précédente. Par exemple, pour placer les fichiers dans un répertoire `downloads` sur l'hôte du Serveur de connexion View, utilisez le chemin suivant :

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

Les liens vers les fichiers du programme d'installation pourront alors utiliser des URL relatives au format `/downloads/client-installer-file-name`.

- 4 Redémarrez le service du composant Web View.

Utiliser des URI pour configurer des clients Web HTML Access

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 le HTML Access Web client, se connecter au Serveur de connexion View et démarrer un poste de travail spécifique avec des options de configuration particulières.

Vous pouvez simplifier le processus de connexion 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
- Le nom d'utilisateur RADIUS ou RSA SecurID, s'il est différent du nom d'utilisateur Active Directory.
- Nom de domaine
- Nom affiché du poste de travail
- Actions incluant la navigation, la réinitialisation, la fermeture d'une session et le démarrage d'une session

Syntaxe pour la création d'URI pour HTML Access

La syntaxe inclut une partie de chemin d'accès visant à spécifier le serveur et, en option, une requête pour spécifier l'utilisateur, le poste de travail et les actions ou options de configuration du poste de travail.

Spécification d'URI

Utilisez la syntaxe suivante pour créer des URI permettant de démarrer les clients Web HTML Access :

`https://authority-part[/?query-part]`

authority-part

Spécifie l'adresse du serveur et, en option, un numéro de port non défini par défaut. Les noms de serveur doivent être conformes à la syntaxe DNS.

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

`server-address:port-number`

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 plusieurs requêtes, utilisez une esperluette (&) entre les requêtes. En cas de conflit entre des requêtes, la dernière requête de la liste est utilisée. Utilisez la syntaxe suivante :

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

Respectez les instructions suivantes lors de la création d'une partie de requête :

- Si vous n'utilisez pas au moins l'une des requêtes prises en charge, la page par défaut du portail Web de VMware Horizon s'affiche.

- Dans la partie de requête, certains caractères spéciaux ne sont pas pris en charge, et vous devez les entrer au format de codage d'URL suivant : pour le symbole dièse (#) utilisez %23, pour le signe de pourcentage (%) utilisez %25, pour l'esperluette (&) utilisez %26, pour l'arobase (@) utilisez %40 et pour la barre oblique inverse (\) utilisez %5C.

Pour en savoir plus sur le codage d'URL, consultez http://www.w3schools.com/tags/ref_urlencode.asp.

- Dans la partie de requête, 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/>.

Requêtes prises en charge

Cette rubrique répertorie les requêtes prises en charge pour le client Web HTML Access Web client. Si vous créez des URI pour plusieurs types de clients, tels que des clients de postes de travail et des clients mobiles, reportez-vous au guide *Utilisation de VMware Horizon Client* pour chaque type de système client.

domainName	Nom de domaine NETBIOS associé à l'utilisateur qui se connecte au poste de travail distant. Utilisez par exemple <code>monentreprise</code> plutôt que <code>monentreprise.com</code> .
userName	Utilisateur Active Directory qui se connecte au poste de travail distant.
tokenUserName	Nom d'utilisateur RSA ou RADIUS. N'utilisez cette requête que si le nom d'utilisateur RSA ou RADIUS est différent du nom d'utilisateur Active Directory. Si vous ne spécifiez pas cette requête et que l'authentification RSA ou RADIUS est nécessaire, le nom d'utilisateur Windows est utilisé.
desktopId	Nom affiché du poste de travail. Ce nom est celui spécifié dans View Administrator lorsque le pool de postes de travail a été créé. Si le nom affiché contient un espace, le navigateur utilisera automatique %20 pour représenter l'espace.

action

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

Valeur	Description
<code>browse</code>	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.
<code>start-session</code>	Lance le poste de travail spécifié. Si aucune requête d'action n'est fournie et que le nom du poste de travail est fourni, <code>start-session</code> est l'action par défaut.
<code>reset</code>	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.
<code>logoff</code>	Déconnecte l'utilisateur du système d'exploitation invité sur le poste de travail distant.

Exemples d'URI

Vous pouvez créer des liens hypertextes ou des boutons avec un URI 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 une application ou 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. Notez que les requêtes ne sont pas sensibles à la casse. Par exemple, vous pouvez utiliser **domainName** ou **domainname**.

1 `https://view.mycompany.com/?domainName=finance&userName=fred`

HTML Access Web 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 **finance**. L'utilisateur doit fournir uniquement un mot de passe.

2 `https://view.mycompany.com/?desktopId=Primary%20Desktop&action=start-session`

HTML Access Web 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.

3 `https://view.mycompany.com:7555/?desktopId=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.

4 `https://view.mycompany.com/?desktopId=Primary%20Desktop&action=reset`

HTML Access Web 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 affiche une boîte de dialogue qui invite l'utilisateur à confirmer l'opération de réinitialisation pour Poste de travail principal.

REMARQUE Cette action n'est disponible que si l'administrateur View a autorisé les utilisateurs finaux à réinitialiser leurs ordinateurs.

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="https://view.mycompany.com/?domainName=finance&userName=fred">Test Link</a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'https://view.mycompany.com/?domainName=finance&userName=fred'"></form> <br>

</body>
</html>
```

Configurer les paramètres de stratégie de groupe de HTML Access

Vous pouvez configurer les paramètres de stratégie de groupe qui contrôlent le comportement de HTML Access sur vos postes de travail distants. Pour appliquer ces paramètres, ajoutez le fichier de modèle ADM de configuration HTML Access aux GPO (objets de la stratégie de groupe) dans Active Directory.

Prérequis

- Vérifiez que les GPO (objets de stratégie de groupe) Active Directory sont créés pour les paramètres de stratégie de groupe de HTML Access. Les GPO (objets de stratégie de groupe) doivent être liés à l'unité d'organisation (UO) qui contient vos postes de travail distants. Pour des informations générales sur la configuration des paramètres de stratégie de groupe d'View dans Active Directory, reportez-vous à « Configuration des stratégies » dans *Configuration des postes de travail et applications dans View*.
- Vérifiez que les composants logiciels enfichables Microsoft MMC (Microsoft Management Console) et l'Éditeur d'objets de stratégie de groupe sont disponibles sur votre serveur Active Directory.
- Familiarisez-vous avec les paramètres de stratégie de groupe de HTML Access. Reportez-vous à la section « Paramètres de stratégie de groupe de HTML Access », page 30.

Procédure

- 1 Téléchargez le fichier View GPO Bundle .zip sur le site de téléchargement de VMware à l'adresse <https://my.vmware.com/web/vmware/downloads>.

Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 6, qui inclut GPO Bundle.

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

- 2 Copiez le fichier sur votre serveur Active Directory et décompressez-le.

Les GPO de HTML Access sont inclus dans le fichier de modèle ADM `vdm-blast.adm`.

- 3 Sur le serveur Active Directory, modifiez les GPO.

a Sélectionnez **Démarrer > Outils d'administration > Gestion de stratégie de groupe**.

b Développez votre domaine, cliquez avec le bouton droit sur le GPO que vous avez créé pour les paramètres de stratégie de groupe et sélectionnez **Modifier**.

La fenêtre de l'Éditeur d'objets de stratégie de groupe apparaît.

- 4 Dans l'Éditeur d'objets de stratégie de groupe, cliquez avec le bouton droit sur **Administrative Templates (Modèles administratifs)** sous **Computer Configuration (Configuration ordinateur)** et sélectionnez **Add/Remove Templates (Ajout/Suppression de modèles)**.

- 5 Cliquez sur **Ajouter**, localisez le fichier `vdm-blast.adm` et cliquez sur **Ouvrir**.

- 6 Cliquez sur **Fermer** pour appliquer les paramètres de stratégie dans le fichier de modèle d'administration au GPO.

Le dossier VMware Blast s'affiche dans le volet de gauche sous **Modèles d'administration > Modèles d'administration classiques**.

- 7 Configurez les paramètres de stratégie de groupe de HTML Access.

- 8 Assurez-vous que les paramètres de la stratégie sont appliqués aux postes de travail distants.

a Exécutez la commande `gpupdate.exe` sur les postes de travail.

b Redémarrez les postes de travail.

Paramètres de stratégie de groupe de HTML Access

Le fichier de modèle ADM de HTML Access, `vdm-blast.adm`, contient des paramètres de stratégie de groupe que vous pouvez appliquer à vos postes de travail distants. Une fois le fichier de modèle importé dans Active Directory, les paramètres de stratégie de groupe de HTML Access seront dans le dossier VMware Blast de l'éditeur de stratégie de groupe.

Tableau 2-2. Paramètres de stratégie de groupe de HTML Access

Paramètre	Description
Effacement d'écran	<p>Permet de contrôler si la machine virtuelle distante peut être vue à l'extérieur d'View pendant une session HTML Access. Par exemple, un administrateur peut utiliser vSphere Web Client pour ouvrir une console sur la machine virtuelle pendant qu'un utilisateur est connecté au poste de travail via HTML Access.</p> <p>Lorsque ce paramètre est activé ou non configuré, et lorsqu'un tente d'accéder à la machine virtuelle distante de l'extérieur d'View pendant qu'une session HTML Access est active, la machine virtuelle distante affiche un écran vide.</p> <p>Lorsque ce paramètre est désactivé, dans les conditions précédentes, la machine virtuelle distante affiche la session du poste de travail View actif au second accesseur distant.</p>
Nettoyage de la mémoire de session	<p>Permet de contrôler le nettoyage de la mémoire des sessions distantes abandonnées. Lorsque ce paramètre est activé, vous pouvez définir l'intervalle et le seuil de nettoyage de la mémoire.</p> <p>L'intervalle détermine la fréquence d'exécution du nettoyage de la mémoire. L'intervalle est défini en millisecondes.</p> <p>Le seuil détermine le temps qui doit s'écouler après qu'une session est abandonnée avant qu'elle ne devienne un candidat pour la suppression. Le seuil est défini en millisecondes.</p>
Lecture audio	<p>Permet de contrôler si la lecture audio est autorisée sur le poste de travail distant. Par défaut, ce paramètre est activé.</p>
Qualité d'image	<p>Permet de contrôler la qualité d'image de l'écran distant. Trois profils de qualité d'image sont disponibles, faible, moyenne et haute qualité. L'encodeur tente d'utiliser la meilleure qualité possible, compte tenu des contraintes de bande passante disponible, de fréquence d'images et de la zone récemment modifiée dans l'image actuelle. L'encodeur assure un suivi des zones de l'écran client dans lesquelles la qualité est faible ou moyenne et améliore progressivement ces zones pour passer en qualité élevée.</p> <p>Lorsque ce paramètre est activé, vous pouvez modifier séparément les paramètres de qualité faible, moyenne et élevée des images JPEG. Les niveaux de qualité JPEG réels utilisés pour les paramètres de qualité faible, moyenne et élevée peuvent être configurés individuellement sous forme de nombres compris entre 0 et 100.</p> <p>Le sous-échantillonnage chromatique est activé en fonction du niveau de qualité JPEG choisi. Lorsque la valeur de la qualité JPEG est supérieure ou égale à 80, le sous-échantillonnage chromatique est désactivé et le ratio est défini sur la plus haute valeur disponible, YUV-4:4:4. Lorsque la valeur de la qualité JPEG est inférieure ou égale à 79, le ratio est défini sur YUV-4:2:0.</p> <ul style="list-style-type: none"> ■ Faible qualité JPEG. Par défaut, cette valeur est 25. Vous pouvez également définir différentes valeurs pour le faible ratio de sous-échantillonnage de la couleur JPEG. Par défaut, le faible ratio est fixé à la valeur la plus faible possible, 4:1:0. ■ Qualité JPEG moyenne. Par défaut, cette valeur est 35. Vous pouvez également définir différentes valeurs pour le faible ratio de sous-échantillonnage de la couleur JPEG. Par défaut, le faible ratio est fixé à la valeur la plus faible possible, 4:2:0. ■ Haute qualité JPEG. Par défaut, cette valeur est 90. Vous pouvez également définir différentes valeurs pour le haut ratio de sous-échantillonnage de la couleur JPEG. Par défaut, le haut ratio est fixé à la valeur la plus élevée possible, 4:4:4.

Tableau 2-2. Paramètres de stratégie de groupe de HTML Access (suite)

Paramètre	Description
Configurer la redirection du presse-papiers	<p>Détermine le sens dans lequel la redirection du presse-papiers est autorisée. Il n'est possible de copier et de coller que du texte. Vous pouvez sélectionner l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> ■ Activé du client vers le serveur seulement (C'est-à-dire autoriser le copier/coller uniquement du client vers le poste de travail distant.) ■ Désactivé dans les deux sens ■ Activé dans les deux sens ■ Activé du serveur vers le client seulement (C'est-à-dire autoriser uniquement le copier/coller du poste de travail distant vers le système client.) <p>Ce paramètre s'applique uniquement à View Agent. Lorsque ce paramètre est désactivé ou n'est pas configuré, la valeur par défaut est Activé du client vers le serveur seulement.</p>
Service HTTPS	<p>Permet de changer le port TCP sécurisé (HTTPS) pour Blast Agent service. Le port par défaut est 22443.</p> <p>Activez ce paramètre pour pouvoir changer le numéro de port. Si vous modifiez ce paramètre, vous devez aussi mettre à jour les paramètres du pare-feu correspondant aux postes de travail à distance affectés (sur lesquels View Agent est installé).</p>

Utilisation d'une application ou d'un poste de travail distant

3

Le client fournit une barre latérale de navigation avec des boutons de barre d'outils. Vous pouvez donc facilement vous déconnecter d'une application ou d'un poste de travail distant ou cliquer sur le bouton pour envoyer l'équivalent de la combinaison de touches Ctrl+Alt+Suppr.

Ce chapitre aborde les rubriques suivantes :

- [« Matrice de prise en charge des fonctions »](#), page 33
- [« Internationalisation »](#), page 35
- [« Connexion à une application ou un poste de travail distant »](#), page 35
- [« Combinaisons de touches de raccourci »](#), page 37
- [« Claviers internationaux »](#), page 40
- [« Résolution de l'écran »](#), page 41
- [« Utilisation de la barre latérale »](#), page 42
- [« Audio »](#), page 44
- [« Copier et coller du texte »](#), page 44
- [« Fermer une session ou se déconnecter »](#), page 46
- [« Réinitialiser une application ou un poste de travail distant »](#), page 47

Matrice de prise en charge des fonctions

Certaines fonctions ne sont pas disponibles lorsque vous accédez à une application ou un poste de travail distant à partir d'un client HTML Access basé sur un navigateur.

Fonctions prises en charge pour les postes de travail de machine virtuelle mono-utilisateur

Tableau 3-1. Fonctionnalités prises en charge par HTML Access

Fonction	Poste de travail Windows 7	Poste de travail Windows 8.x	Poste de travail Windows 10	Poste de travail Windows Server 2008 R2	Poste de travail Windows Server 2012 R2
RSA SecurID ou RADIUS	X	X	X	X	X
Authentification unique	X	X	X	X	X
Protocole d'affichage RDP					

Tableau 3-1. Fonctionnalités prises en charge par HTML Access (suite)

Fonction	Poste de travail Windows 7	Poste de travail Windows 8.x	Poste de travail Windows 10	Poste de travail Windows Server 2008 R2	Poste de travail Windows Server 2012 R2
Protocole d'affichage PCoIP					
Protocole Blast	X	X	X	X	X
redirection USB					
Audio/Vidéo en temps réel (RTAV)					
Wyse MMR					
Redirection multimédia (MMR) Windows Media					
Impression virtuelle					
Impression basée sur l'emplacement	X	X	X	X	X
Cartes à puce					
Plusieurs écrans					

Pour une description de ces fonctionnalités et de leurs limites, consultez le document *Planification de l'architecture de View*.

Fonctions prises en charge pour les postes de travail basés sur des sessions et les applications hébergées sur les hôtes RDS

Les hôtes RDS sont des ordinateurs serveurs sur lesquels View Agent et les services Bureau à distance Windows sont installés. Plusieurs utilisateurs peuvent avoir plusieurs sessions d'application et de poste de travail simultanément sur un hôte RDS.

Le tableau suivant décrit les fonctionnalités fournies par les hôtes RDS si vous utilisez HTML Access. Des fonctionnalités supplémentaires sont disponibles si vous utilisez Horizon Client installé en mode natif, comme Horizon Client pour Windows.

Tableau 3-2. Fonctions prises en charge pour HTML Access sur des hôtes RDS si View Agent 6.1.1 ou 6.2 est installé

Fonction	Hôte Windows Server 2008 R2 RDS sur une machine physique	Hôte Windows Server 2008 R2 RDS sur une machine virtuelle	Hôte Windows Server 2012 ou 2012 R2 RDS sur une machine physique	Hôte Windows Server 2012 ou 2012 R2 RDS sur une machine virtuelle
RSA SecurID ou RADIUS		X		X
Authentification unique		X		X
Protocole Blast		X		X
Impression virtuelle				

Tableau 3-2. Fonctions prises en charge pour HTML Access sur des hôtes RDS si View Agent 6.1.1 ou 6.2 est installé (suite)

Fonction	Hôte Windows Server 2008 R2 RDS sur une machine physique	Hôte Windows Server 2008 R2 RDS sur une machine virtuelle	Hôte Windows Server 2012 ou 2012 R2 RDS sur une machine physique	Hôte Windows Server 2012 ou 2012 R2 RDS sur une machine virtuelle
Impression basée sur l'emplacement		X		X
Plusieurs écrans				

IMPORTANT L'hôte RDS doit être installé sur une machine virtuelle. Bien que vous puissiez installer View Agent sur une machine physique, le protocole Blast utilisé avec HTML Access ne peut pas accéder à une machine physique. View Agent doit être installé sur une machine virtuelle.

Pour savoir quelles éditions de chaque système d'exploitation invité et quels Service Packs sont pris en charge, consultez la rubrique « Systèmes d'exploitation pris en charge pour View Agent » dans la documentation d'installation de View 6.x.

Internationalisation

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

Pour plus d'informations concernant les modules de langue que vous devez utiliser dans le système client, navigateur et poste de travail distant, consultez « [Claviers internationaux](#) », page 40.

Connexion à une application ou un poste de travail distant

Utilisez vos informations d'identification Active Directory pour vous connecter aux applications et postes de travail distants que vous êtes autorisé à utiliser.

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 NETBIOS pour ouvrir une session. Utilisez par exemple `monentreprise` plutôt que `monentreprise.com`.

Procédure

- 1 Ouvrez un navigateur et entrez l'URL de l'instance du Serveur de connexion View.

Dans l'URL, utilisez **https** et le nom de domaine complet ; par exemple : `https://view.company.com`.

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

Le portail Web de VMware Horizon s'affiche. Par défaut, cette page affiche à la fois une icône pour télécharger et installer Horizon Client natif et une icône pour se connecter via HTML Access.

- 2 Cliquez sur l'icône **VMware Horizon HTML Access**.

- 3 Dans la boîte de dialogue Connexion, 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**.

Le code secret peut comporter un code PIN et le numéro généré sur le jeton.

- 4 Si un message demande une seconde fois les informations d'identification RSA SecurID ou les informations d'identification pour l'authentification RADIUS, entrez le numéro généré suivant dans le jeton.

Ne saisissez pas votre code PIN ni le même numéro généré saisi précédemment. Si besoin, attendez qu'un autre numéro soit généré.

Cette étape n'est requise qu'en cas de mauvaise saisie du premier code secret ou lorsque les paramètres de configuration du serveur RSA changent.

- 5 Dans la boîte de dialogue Connexion, entrez votre nom d'utilisateur et votre mot de passe Active Directory, sélectionnez un nom de domaine et cliquez sur **Connexion**.
- 6 (Facultatif) Sur l'écran de sélection des postes de travail et applications, avant de sélectionner l'élément auquel vous voulez accéder, cliquez sur l'étoile grise dans l'icône de l'application ou du poste de travail pour marquer une application ou un poste de travail distant comme favori.

L'icône d'étoile grise devient jaune. Lors de votre prochaine connexion, vous pourrez cliquer sur l'icône d'étoile dans le coin supérieur droit de la fenêtre du navigateur pour afficher uniquement les favoris.

- 7 Cliquez sur l'icône de l'application ou du poste de travail distant auquel vous voulez accéder.

L'application ou le poste de travail distant est affiché dans votre navigateur. Une barre latérale de navigation est également disponible. Vous pouvez cliquer sur l'onglet sur le côté gauche de la fenêtre du navigateur pour afficher la barre latérale. Vous pouvez utiliser la barre latérale pour accéder à d'autres applications ou postes de travail distants, afficher la fenêtre Paramètres, copier et coller du texte, etc.

Suivant

Si, peu après vous être connecté à une application ou un poste de travail, vous êtes déconnecté et une invite vous demande de cliquer sur un lien pour accepter le certificat de sécurité, vous pouvez indiquer si vous approuvez le certificat. Reportez-vous à la section « [Faire confiance à un certificat racine auto-signé](#) », page 36.

Faire confiance à un certificat racine auto-signé

Dans certains cas, lors de votre première connexion à une application ou un poste de travail distant, vous pouvez être invité par le navigateur à accepter le certificat auto-signé utilisé par la machine distante. Vous devez approuver le certificat pour que la connexion puisse être établie avec l'application ou le poste de travail distant.

La plupart des navigateurs vous permettent d'approuver de façon permanente le certificat auto-signé. Si vous choisissez de ne pas approuver le certificat de façon permanente, vous devez vérifier le certificat à chaque fois que vous redémarrez le navigateur. Si vous utilisez un navigateur Safari, vous devez approuver de façon permanente le certificat de sécurité pour établir la connexion.

Procédure

- 1 Si votre navigateur présente un avertissement de certificat non approuvé ou un avertissement que votre connexion n'est pas privée, examinez le certificat pour vérifier qu'il correspond au certificat utilisé par votre entreprise.

Vous pouvez demander de l'aide à votre administrateur View. Par exemple, dans un navigateur Chrome, vous pouvez utiliser la procédure suivante.

- a Cliquez sur l'icône de verrou dans la barre d'adresse.
- b Cliquez sur le lien **Informations sur le certificat**.
- c Vérifiez que le certificat correspond au certificat utilisé par votre entreprise.

Vous pouvez demander de l'aide à votre administrateur View.

- 2 Acceptez le certificat de sécurité.

Chaque navigateur a ses propres invites spécifiques du navigateur pour accepter ou toujours approuver un certificat. Par exemple, dans un navigateur Chrome, vous pouvez cliquer sur le lien **Avancé** sur la page du navigateur, puis cliquer sur **Continuer vers le site *nom-serveur* (non sécurisé)**.

Dans un navigateur Safari, utilisez la procédure suivante pour approuver de façon permanente le certificat.

- a Cliquez sur le bouton **Afficher le certificat** lorsque la boîte de dialogue du certificat non approuvé s'affiche.
- b Cochez la case **Toujours approuver** et cliquez sur **Continuer**.
- c Lorsque vous y êtes invité, saisissez votre mot de passe et cliquez sur **Mettre les paramètres à jour**.

L'application ou le poste de travail distant est lancé.

Combinaisons de touches de raccourci

Indépendamment de la langue utilisée, certaines combinaisons de touches ne peuvent pas être envoyées à une application ou un poste de travail distant.

Les navigateurs Web permettent à certaines touches et combinaisons de touches d'être envoyées au client et au système de destination. Pour les autres touches et combinaisons de touches, l'entrée est traitée localement et n'est pas envoyée au système de destination. Les combinaisons de touches qui fonctionnent sur votre système dépendent du logiciel de navigation, du système d'exploitation client et des paramètres de langue.

REMARQUE Si vous utilisez un Mac, vous pouvez mapper la touche Commande sur la touche Ctrl de Windows lorsque vous utilisez les combinaisons de touches pour sélectionner, copier et coller du texte. Pour activer cette fonction, vous pouvez cliquer sur le bouton de la barre d'outils **Ouvrir la fenêtre des paramètres** sur la barre latérale et activer **Activer Commande-A, Commande-C, Commande-V et Commande-X**. (Cette option apparaît dans la fenêtre Paramètres uniquement si vous utilisez un Mac.)

Les touches et les combinaisons de touches suivantes ne fonctionnent pas toujours sur les postes de travail distants :

- Ctrl+T
- Ctrl+W
- Ctrl+N
- Touche de commande
- Alt+Entrer

- Ctrl+Alt+*any_key*

IMPORTANT Pour entrer Ctrl+Alt+Delete, utilisez le bouton de la barre d'outils **Envoyer Ctrl+Alt+Delete** situé en haut de la barre latérale.

- Verrouillage majuscule+*modifier_key* (telle que Alt ou Shift)
- Touches de fonction, si vous utilisez un Chromebook.
- Combinaisons de touches Windows

Les combinaisons de touches Windows suivantes fonctionnent sur les postes de travail distants si vous activez la touche Windows pour les postes de travail. Pour activer cette touche, vous pouvez cliquer sur le bouton de la barre d'outils **Ouvrir la fenêtre des paramètres** sur la barre latérale et activer **Activer la touche Windows pour les postes de travail**.

IMPORTANT Après avoir activé **Activer la touche Windows pour les postes de travail**, vous devez appuyer sur Ctrl+Win (sur les systèmes Windows), sur Ctrl+Commande (sur les Mac) ou Ctrl+Recherche (sur les Chromebook) pour simuler l'appui sur la touche Windows.

Ces combinaisons de touches ne fonctionnent pas pour les applications distantes fournies par les hôtes RDS. Elles fonctionnent comme indiqué pour les postes de travail mono-utilisateur et les postes de travail basés sur des sessions Windows Server 2008 R2 et Windows Server 2012 R2 fournis par un hôte RDS.

Certaines combinaisons de touches fonctionnant sur des postes de travail distants avec un système d'exploitation Windows 8.x ou Windows Server 2012 R2 ne fonctionnent pas sur les postes de travail avec un système d'exploitation Windows 7, Windows Server 2008 R2 ou Windows 10.

Tableau 3-3. Raccourcis de touche Windows pour les postes de travail distants Windows 10

Clés	Action	Limites
Touche Windows	Ouvrir ou fermer le menu Démarrer.	
Win+A	Ouvrir le centre de notifications.	
Win+E	Ouvrir l'Explorateur de fichiers.	
Win+G	Ouvrir la barre de jeux quand un jeu est ouvert.	
Win+H	Ouvrir l'icône Partager.	
Win+I	Ouvrir l'icône Paramètres.	
Win+K	Ouvrir Connexion Action rapide.	
Win+M	Réduire toutes les fenêtres.	
Win+R	Ouvrir la boîte de dialogue Exécuter.	
Win+S	Ouvrir une recherche.	
Win+X	Ouvrir le menu Lien rapide .	
Win+, (virgule)	Afficher temporairement le poste de travail.	
Win+Pause	Afficher la boîte de dialogue Propriétés système.	Il n'y a pas de touche Pause sur les Chromebook et les Mac.
Win+Maj+M	Restaurer les fenêtres réduites sur le poste de travail.	Ne fonctionne pas dans les navigateurs Safari.
Win+Alt+Num	Ouvrir le poste de travail et ouvrir la liste de raccourcis de l'application épinglée sur la barre des tâches à la position indiquée par le chiffre.	Ne fonctionne pas sur un Chromebook.
Win+Entrée	Ouvrir le Narrateur.	

Tableau 3-4. Raccourcis de touche Windows pour les postes de travail distants Windows 8.x et Windows Server 2012 R2

Clés	Action	Limites
Win+F1	Ouvrir Aide et support Windows.	Ne fonctionne pas dans les navigateurs Safari.
Touche Windows	Afficher ou masquer l'écran Démarrer.	
Win+B	Sélectionner la zone de notification.	
Win+C	Ouvrir le volet Icônes.	
Win+D	Afficher et masquer le poste de travail.	Ne fonctionne pas dans les navigateurs Safari. Solution : appuyez sur Commande-D sur les Mac.
Win+E	Ouvrir l'Explorateur de fichiers.	
Win+H	Ouvrir l'icône Partager.	
Win+I	Ouvrir l'icône Paramètres.	
Win+K	Ouvrir l'icône Périphériques.	
Win+M	Réduire toutes les fenêtres.	
Win+Q	Ouvrir l'icône Rechercher pour rechercher partout ou dans l'application ouverte, si l'application prend en charge la recherche d'application.	
Win+R	Ouvrir la boîte de dialogue Exécuter.	
Win+S	Ouvrir l'icône Rechercher pour effectuer une recherche dans Windows et sur le Web.	
Win+X	Ouvrir le menu Lien rapide .	
Win+Z	Afficher les commandes disponibles dans l'application.	
Win+, (virgule)	Afficher temporairement le poste de travail, tant que vous continuez à appuyer sur les touches.	REMARQUE Ne fonctionne pas sur les systèmes d'exploitation Windows 2012 R2.
Win+Pause	Afficher la boîte de dialogue Propriétés système.	Il n'y a pas de touche Pause sur les Chromebook et les Mac.
Win+Maj+M	Restaurer les fenêtres réduites sur le poste de travail.	Ne fonctionne pas dans les navigateurs Safari. Solution : appuyez sur Commande-D sur les Mac.
Win+Alt+Num	Ouvrir le poste de travail et ouvrir la liste de raccourcis de l'application épinglée sur la barre des tâches à la position indiquée par le chiffre.	Ne fonctionne pas sur un Chromebook.
Win+Flèche vers le haut	Agrandir la fenêtre.	Ne fonctionne pas sur un Chromebook.
Win+Flèche vers le bas	Supprimer l'application actuelle de l'écran ou réduire la fenêtre de poste de travail.	Ne fonctionne pas sur un Chromebook.
Win+Flèche gauche	Agrandir la fenêtre de l'application ou du poste de travail vers le côté gauche de l'écran.	Ne fonctionne pas sur un Chromebook.
Win+Flèche droite	Agrandir la fenêtre de l'application ou du poste de travail vers le côté droit de l'écran.	Ne fonctionne pas sur un Chromebook.
Win+Origine	Réduire tout, sauf la fenêtre de poste de travail active (restaure toutes les fenêtres lorsque vous appuyez sur Win+Origine une seconde fois).	Ne fonctionne pas dans les navigateurs Safari.

Tableau 3-4. Raccourcis de touche Windows pour les postes de travail distants Windows 8.x et Windows Server 2012 R2 (suite)

Clés	Action	Limites
Win+Maj+Flèche vers le haut	Étirer la fenêtre du poste de travail vers le haut et le bas de l'écran.	Ne fonctionne pas sur un Chromebook.
Win+Maj+Flèche vers le bas	Restaurer la fenêtre du poste de travail verticalement, tout en conservant la largeur, après avoir appuyé sur Win+Maj+Haut pour étirer la fenêtre, ou réduire la fenêtre de poste de travail active.	Ne fonctionne pas sur un Chromebook.
Win+Entrée	Ouvrir le Narrateur.	

Tableau 3-5. Raccourcis de touche Windows pour les postes de travail distants Windows 7 et Windows Server 2008 R2

Clés	Action	Limites
Touche Windows	Ouvrir ou fermer le menu Démarrer.	
Win+Pause	Afficher la boîte de dialogue Propriétés système.	Il n'y a pas de touche Pause sur les Chromebook et les Mac.
Win+D	Afficher et masquer le poste de travail.	Ne fonctionne pas dans les navigateurs Safari. Solution : appuyez sur Commande-D sur les Mac.
Win+M	Réduire toutes les fenêtres.	
Win+E	Ouvrir le dossier Ordinateur.	
Win+R	Ouvrir la boîte de dialogue Exécuter.	
Win+Flèche vers le haut	Agrandir la fenêtre.	Ne fonctionne pas sur un Chromebook.
Win+Flèche vers le bas	Réduire la fenêtre.	Ne fonctionne pas sur un Chromebook.
Win+Flèche gauche	Agrandir la fenêtre de l'application ou du poste de travail vers le côté gauche de l'écran.	Ne fonctionne pas sur un Chromebook.
Win+Flèche droite	Agrandir la fenêtre de l'application ou du poste de travail vers le côté droit de l'écran.	Ne fonctionne pas sur un Chromebook.
Win+Origine	Réduire tout, sauf la fenêtre de poste de travail active.	Ne fonctionne pas dans les navigateurs Safari.
Win+Shift+Flèche vers le haut	Étirer la fenêtre du poste de travail vers le haut et le bas de l'écran.	Ne fonctionne pas sur un Chromebook.
Win+G	Parcourir les gadgets de poste de travail en cours d'exécution.	
Win+U	Ouvrir Gestionnaire d'utilitaires pour les options d'ergonomie.	

Claviers internationaux

Lors de l'utilisation de claviers et de paramètres régionaux non anglais, vous devez configurer certains paramètres de votre système client, navigateur et poste de travail distant. Certaines langues nécessitent l'utilisation d'un IME (éditeur de méthode d'entrée) sur le poste de travail distant.

Avec des paramètres locaux et des méthodes d'entrée installées appropriés, vous pouvez entrer des caractères pour les langues suivantes : Anglais, japonais, français, allemand, chinois simplifié, chinois traditionnel et coréen.

Tableau 3-6. Paramètres de langue d'entrée requis

Langue	Langue d'entrée sur le système client local	IME requis sur le système client local ?	Langue de navigateur et d'entrée sur le poste de travail distant	IME requis sur le poste le travail distant ?
Anglais	Anglais	Non	Anglais	Non
Français	Français	Non	Français	Non
Allemand	Allemand	Non	Allemand	Non
Chinois (simplifié)	Chinois (simplifié)	Mode de saisie en anglais	Chinois (simplifié)	Oui
Chinois (traditionnel)	Chinois (traditionnel)	Mode de saisie en anglais	Chinois (traditionnel)	Oui
Japonais	Japonais	Mode de saisie en anglais	Japonais	Oui
Coréen	Coréen	Mode de saisie en anglais	Coréen	Oui

Résolution de l'écran

Si View Administrator configure un poste de travail distant avec la capacité de mémoire RAM vidéo appropriée, le client Web peut redimensionner un poste de travail distant à la taille de la fenêtre du navigateur. La configuration par défaut est de 36 Mo de RAM vidéo, ce qui est largement suffisant par rapport au minimum requis (16 Mo) si vous n'utilisez pas d'applications 3D.

Si vous utilisez un navigateur ou un périphérique Chrome proposant une densité de pixels élevée, tel qu'un MacBook avec écran Retina ou un Google Chromebook Pixel, vous pouvez définir cette résolution pour l'application ou le poste de travail distant. Activez l'option **Mode haute résolution** dans la fenêtre Paramètres, disponible dans la barre latérale. (Cette option apparaît dans la fenêtre Paramètres uniquement si vous utilisez un écran haute résolution.)

Pour utiliser la fonctionnalité de rendu 3D, vous devez allouer suffisamment de mémoire VRAM à chaque poste de travail distant.

- La fonction graphique accélérée par le logiciel, disponible avec vSphere 5.0 ou version ultérieure, permet d'utiliser des applications 3D telles que les thèmes Windows Aero ou Google Earth. Cette fonctionnalité requiert de 64 Mo à 128 Mo de VRAM.
- La fonction d'affichage graphique accéléré matériellement (vSGA), disponible avec vSphere 5.1 ou version ultérieure, vous permet d'utiliser des applications 3D pour la conception, la modélisation et le multimédia. Cette fonctionnalité requiert de 64 Mo à 512 Mo de VRAM. La valeur par défaut est 96 Mo.
- Disponible dans vSphere 5.5 ou version ultérieure, la fonctionnalité vDGA (Virtual Dedicated Graphics Acceleration) dédie un seul GPU (graphical processing unit) physique sur un seul hôte ESXi à une seule machine virtuelle. Utilisez cette fonctionnalité si vous avez besoin de graphiques de workstation haut de gamme accélérés par le matériel. Cette fonctionnalité requiert de 64 Mo à 512 Mo de VRAM. La valeur par défaut est 96 Mo.

Avec Horizon Client 3.4, lorsque le rendu 3D est activé, le nombre maximal de moniteurs est de 1 et la résolution maximale est 1 920 x 1 200.

Avec Horizon Client 3.5, lorsque le rendu 3D est activé, le nombre maximal de moniteurs est de 1 et la résolution maximale est 3 840 x 2 160.

De la même façon, si vous utilisez un navigateur ou un périphérique proposant une densité de pixels élevée, tel qu'un MacBook avec écran Retina ou un Google Chromebook Pixel, vous devez allouer suffisamment de mémoire VRAM à chaque poste de travail distant.

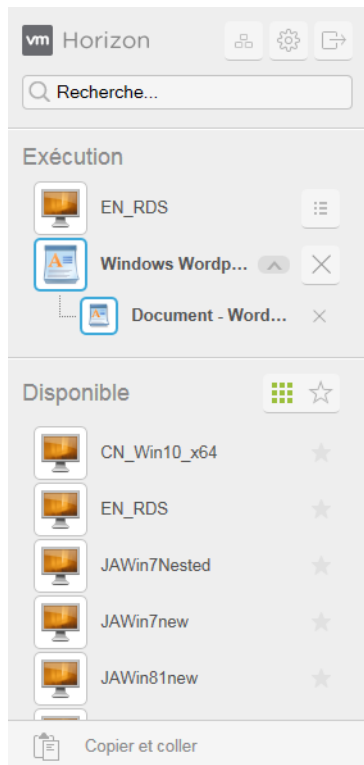
IMPORTANT L'estimation de la quantité de mémoire VRAM requise pour le protocole Blast est semblable à l'estimation de la mémoire VRAM requise pour le protocole d'affichage PCoIP. Pour obtenir les instructions, reportez-vous à la section « Taille de la RAM pour des configurations de moniteur spécifiques 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*.

Utilisation de la barre latérale

Lorsque vous êtes connecté à un poste de travail distant ou à une application hébergée, vous pouvez utiliser la barre latérale pour lancer d'autres applications et postes de travail, basculer entre des postes de travail et des applications en cours d'exécution et exécuter d'autres actions.

Lorsque vous accédez à une application ou un poste de travail distant, la barre latérale s'affiche sur le côté gauche de l'écran. Cliquez sur l'onglet de la barre latérale pour afficher ou masquer la barre latérale. Vous pouvez également faire glisser l'onglet vers le haut et vers le bas.

Figure 3-1. Barre latérale qui apparaît lorsque vous lancez une application ou un poste de travail distant



Cliquez sur la flèche de développement à côté d'une application en cours d'exécution pour voir la liste de documents ouverts de cette application. Toutefois, notez que si vous avez, par exemple, deux documents Excel ouverts dans des programmes Excel distincts hébergés sur deux serveurs différents, l'application Excel est répertoriée deux fois dans la liste **Exécution** dans la barre latérale.

De la barre latérale, vous pouvez exécuter plusieurs actions.

Tableau 3-7. Actions de la barre latérale

Action	Procédure
Afficher la barre latérale	Lorsque vous avez une application ou un poste de travail distant ouvert, cliquez sur l'onglet de la barre latérale. Lorsque la barre latérale est ouverte, vous pouvez toujours effectuer des actions dans la fenêtre de l'application ou du poste de travail.
Masquer la barre latérale	Cliquez sur l'onglet de la barre latérale.
Lancer une application ou un poste de travail distant	Cliquez sur le nom d'une application ou d'un poste de travail sous Disponible dans la barre latérale. Les postes de travail sont répertoriés en premier.
Rechercher une application ou un poste de travail distant	<ul style="list-style-type: none"> ■ Cliquez sur la zone Rechercher et commencez à saisir le nom de l'application ou du poste de travail. ■ Pour lancer une application ou un poste de travail, cliquez sur le nom de l'application ou du poste de travail dans les résultats de la recherche. ■ Pour revenir à l'accueil de la barre latérale, appuyez sur X dans la zone Rechercher.
Créer une liste d'applications et de postes de travail favoris	Cliquez sur l'étoile grise à côté du nom du poste de travail ou de l'application dans la liste Disponible sur la barre latérale. Vous pouvez ensuite cliquer sur le bouton de la barre d'outils Afficher les favoris (icône d'étoile) à côté de Disponible pour afficher une liste des favoris.
Basculer entre des applications ou des postes de travail	Cliquez sur le nom de fichier de l'application ou le nom du poste de travail dans la liste Exécution sur la barre latérale.
Afficher la fenêtre Copier et coller	Cliquez sur le bouton Copier et coller en bas de la barre latérale. Utilisez ce bouton pour copier le texte dans et depuis des applications sur votre système client local. Pour plus d'informations, reportez-vous à la section « Copier et coller du texte », page 44.
Activer Commande-A, Commande-C, Commande-V et Commande-X	Cette option apparaît dans la fenêtre Paramètres uniquement si vous utilisez un Mac. Cliquez sur le bouton de la barre d'outils Ouvrir la fenêtre des paramètres en haut de la barre latérale pour activer cette fonction. Lorsque cette fonction est activée, la touche Commande sur le Mac est mappée sur la touche Ctrl sur l'application ou le poste de travail Windows distant. Par exemple, appuyer sur Commande-A sur un clavier Mac équivaut à appuyer sur Ctrl+A sur l'application ou le poste de travail Windows distant.
Fermer un poste de travail en cours d'exécution	<p>Cliquez sur le bouton Ouvrir le menu à côté du nom de poste de travail dans la liste Exécution sur la barre latérale et sélectionnez l'action de votre choix :</p> <ul style="list-style-type: none"> ■ Sélectionnez Fermer pour vous déconnecter du poste de travail sans fermer votre session sur son système d'exploitation. Toutefois, notez que votre administrateur View peut configurer votre poste de travail pour que la session soit fermée automatiquement lors de la déconnexion. Dans ce cas, les modifications non enregistrées dans les applications ouvertes seront perdues. ■ Sélectionnez Fermer la session pour fermer votre session sur le système d'exploitation et vous déconnecter du poste de travail. Les modifications non enregistrées dans les applications ouvertes seront perdues.
Fermer une application en cours d'exécution	Cliquez sur le X à côté du nom de fichier sous le nom de l'application dans la liste Exécution sur la barre latérale. Cliquez sur le X à côté du nom de l'application pour quitter l'application et fermer tous les fichiers ouverts pour cette application. Vous êtes invité à enregistrer les modifications apportées aux fichiers.
Réinitialiser un poste de travail	Cliquez sur le bouton Ouvrir le menu à côté du nom de poste de travail dans la liste Exécution sur la barre latérale et sélectionnez Réinitialiser . Tous les fichiers ouverts sur le poste de travail distant seront fermés sans être enregistrés. Vous pouvez réinitialiser un poste de travail uniquement si votre administrateur a activé cette fonction.
Réinitialiser toutes les applications en cours d'exécution	Cliquez sur le bouton de la barre d'outils Ouvrir la fenêtre des paramètres en haut de la barre latérale et cliquez sur Réinitialiser . Toutes les modifications non enregistrées sont perdues.

Tableau 3-7. Actions de la barre latérale (suite)

Action	Procédure
Utiliser des combinaisons de touches qui incluent la touche Windows	Cliquez sur le bouton de la barre d'outils Ouvrir la fenêtre des paramètres en haut de la barre latérale et activez Activer la touche Windows pour les postes de travail . Pour plus d'informations, reportez-vous à la section « Combinaisons de touches de raccourci », page 37.
Envoyer la combinaison de touches Ctrl+Alt+Del à l'application ou au poste de travail distant	Cliquez sur le bouton de la barre d'outils Envoyer Ctrl+Alt+Del en haut de la barre latérale.
Se déconnecter du serveur	Cliquez sur le bouton de la barre d'outils Fermer la session de VMware Horizon en haut de la barre latérale.
Utiliser le mode haute résolution sur des machines avec un écran haute résolution (tel que Retina Macbook Pro)	Cliquez sur le bouton de la barre d'outils Ouvrir la fenêtre des paramètres en haut de la barre latérale et activez Mode haute résolution . (Cette option apparaît dans la fenêtre Paramètres uniquement si vous utilisez un écran haute résolution.)
Afficher les rubriques d'aide	Cliquez sur le bouton de la barre d'outils Ouvrir la fenêtre des paramètres en haut de la barre latérale, ou cliquez sur le logo Horizon en haut de la barre latérale, et cliquez sur Aide .
Afficher la zone À propos de VMware Horizon	Cliquez sur le logo Horizon en haut de la barre latérale.

Audio

Vous pouvez lire du son sur vos applications et postes de travail distants, mais certaines limites s'appliquent.

Par défaut, la lecture audio est activée pour les applications et les postes de travail distants, mais votre administrateur View peut définir une stratégie qui la désactive.

Tenez compte des instructions suivantes :

- Pour augmenter le volume, utilisez le contrôle du son à partir du système client et non de l'application ou du poste de travail distant.
- Éventuellement, le son peut être synchronisé avec la vidéo.
- En cas de trafic réseau intense ou si le navigateur exécute un grand nombre de tâches (E/S), la qualité du son peut être médiocre. À cet égard, certains navigateurs fonctionnent mieux que d'autres.

Copier et coller du texte

Il est possible de copier du texte sur et depuis des applications et des postes de travail distants. Votre administrateur View peut définir cette fonctionnalité pour que les opérations copier et coller soient autorisées uniquement depuis votre système client vers une application ou un poste de travail distant ou uniquement depuis une application ou un poste de travail distant vers votre système client, ou les deux, ou aucun.

Les administrateurs configurent la fonctionnalité de copier-coller à l'aide d'objets de stratégie de groupe (GPO) qui appartiennent à View Agent dans des postes de travail distants. Pour plus d'informations, reportez-vous à la section « [Paramètres de stratégie de groupe de HTML Access](#) », page 30.

Vous pouvez copier jusqu'à 1 Mo de texte, y compris des caractères Unicode non-ASCII. Vous pouvez copier du texte depuis votre système client sur une application ou un poste de travail distant, ou l'inverse, mais le texte collé est du texte brut.

Vous ne pouvez pas copier-coller des graphiques. Il est également impossible de copier et coller des fichiers entre un poste de travail distant et le système de fichiers de votre ordinateur client.

Utiliser la fonctionnalité de copier/coller

Pour copier et coller du texte, vous devez utiliser le bouton **Copier et coller** situé en bas de la barre latérale.

Cette procédure décrit comment utiliser la fenêtre Copier et coller pour copier du texte depuis votre système client local sur une application distante ou comment copier du texte depuis une application distante sur votre système client local. Toutefois, si vous copiez et collez du texte entre des applications et des postes de travail distants, vous pouvez simplement copier/coller comme vous le faites normalement. Il n'est pas nécessaire d'utiliser la fenêtre Copier et coller.

La fenêtre Copier et coller, que vous pouvez ouvrir avec le bouton en bas de la barre latérale de HTML Access, est requise uniquement pour synchroniser le presse-papiers de votre système local avec celui sur la machine distante.

Prérequis

Si vous utilisez un Mac, vérifiez que vous avez activé le paramètre pour mapper la touche Commande sur la touche Ctrl de Windows lorsque vous utilisez les combinaisons de touches pour sélectionner, copier et coller du texte. Cliquez sur le bouton de la barre d'outils **Ouvrir la fenêtre des paramètres** sur la barre latérale et activez **Activer Commande-A, Commande-C, Commande-V et Commande-X**. (Cette option apparaît dans la fenêtre Paramètres uniquement si vous utilisez un Mac.)

L'administrateur View doit conserver la stratégie par défaut, ce qui permet aux utilisateurs de copier/coller du texte depuis des systèmes clients sur leurs applications et postes de travail distants, ou configurer une autre stratégie permettant la fonction de copier/coller. Pour plus d'informations, reportez-vous à la section [« Paramètres de stratégie de groupe de HTML Access »](#), page 30.

Procédure

- Pour copier du texte de votre système client sur l'application ou le poste de travail distant :
 - a Copiez le texte dans l'application client locale.

- b Dans votre navigateur, cliquez sur l'onglet de la barre latérale de HTML Access pour ouvrir la barre latérale, puis cliquez sur **Copier et coller** en bas de la barre latérale.

La fenêtre Copier et coller s'affiche. Si du texte copié précédemment apparaît déjà dans la fenêtre, ce texte est remplacé lorsque vous collez le texte que vous venez de copier.

REMARQUE Si la copie est désactivée, un message apparaît en bas de la fenêtre Copier et coller.

- c Appuyez sur Ctrl+V (ou sur Commande-V sur les Mac) pour coller le texte dans la fenêtre Copier et coller.

Le message suivant apparaît brièvement : « Presse-papiers distant synchronisé ».

- d Cliquez sur l'application distante dans laquelle vous voulez coller le texte et appuyez sur Ctrl+V. Le texte est collé dans l'application distante.

- Pour copier du texte de votre application ou poste de travail distant dans votre système client :
 - a Copiez le texte dans votre application distante.

- b Dans votre navigateur, cliquez sur l'onglet de la barre latérale de HTML Access pour ouvrir la barre latérale, puis cliquez sur **Copier et coller** en bas de la barre latérale.

La fenêtre Copier et coller apparaît avec le texte déjà collé. Le message suivant apparaît brièvement : « Presse-papiers distant synchronisé ».

REMARQUE Si la copie est désactivée, un message apparaît en bas de la fenêtre Copier et coller.

- c Cliquez dans la fenêtre Copier et coller et appuyez sur Ctrl+C (ou sur Commande-C sur les Mac) pour copier de nouveau.

Le texte n'est pas sélectionné lorsque vous faites cette action et vous ne pouvez pas sélectionner le texte. Le message suivant apparaît brièvement : « Copié depuis le volet du Presse-papiers ».

- d Sur votre système client, cliquez à l'endroit où vous voulez coller le texte et appuyez sur Ctrl+V.
Le texte est collé dans l'application sur votre système client.

Fermer une session ou se déconnecter

Avec certaines configurations, si vous vous déconnectez d'un poste de travail distant sans fermer votre session, les applications du poste de travail peuvent rester ouvertes. Vous pouvez également vous déconnecter d'un serveur tout en gardant des applications distantes en cours d'exécution.

Procédure

- Fermez la session sur le serveur View et déconnectez-vous (mais ne fermez pas la session) du poste de travail ou quittez l'application hébergée.

Option	Action
Sur l'écran du sélecteur de postes de travail et d'applications, avant de se connecter à une application ou un poste de travail distant	Cliquez sur le bouton de la barre d'outils Fermer la session dans le coin supérieur droit de l'écran.
Depuis la barre latérale lorsque connecté à une application ou un poste de travail distant	Cliquez sur le bouton de la barre d'outils Fermer la session de VMware Horizon en haut de la barre latérale.

- Fermez une application distante.

Option	Action
Depuis l'application	Quittez l'application de la façon habituelle, par exemple en cliquant sur le bouton X (Fermer) dans le coin de la fenêtre d'application.
Depuis la barre latérale	Cliquez sur le X à côté du nom de fichier de l'application dans la liste Exécution sur la barre latérale.

- Fermez une session ou déconnectez-vous 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.
Depuis la barre latérale	<p>Pour fermer la session et vous déconnecter, cliquez sur le bouton de la barre d'outils Ouvrir le menu à côté du nom de poste de travail dans la liste Exécution sur la barre latérale et sélectionnez Fermer la session. Les fichiers ouverts sur le poste de travail distant seront fermés sans être enregistrés.</p> <p>Pour vous déconnecter sans fermer la session, cliquez sur le bouton de la barre d'outils Ouvrir le menu à côté du nom de poste de travail dans la liste Exécution et sélectionnez Fermer.</p> <p>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 fermées.</p>
Utilisation d'un URI	Pour fermer la session, utilisez l'URI <code>https://Connection_Server_name_or_IP_address?desktopId=desktop_name&action=logoff</code> .

Réinitialiser une application ou un poste de travail distant

Vous devez 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 un poste de travail distant uniquement si votre administrateur a activé cette fonction.

Procédure

- ◆ Utilisez la commande **Réinitialiser**.

Option	Action
Réinitialiser des applications depuis l'écran du sélecteur d'applications	Sur l'écran du sélecteur de postes de travail et d'applications, avant de vous connecter à une application ou un poste de travail distant, pour réinitialiser toutes les applications en cours d'exécution, cliquez sur le bouton de la barre d'outils Paramètres dans le coin supérieur droit de l'écran, puis cliquez sur Réinitialiser .
Réinitialiser un poste de travail depuis la barre latérale	Lorsque vous êtes connecté à un poste de travail distant, cliquez sur le bouton de la barre d'outils Ouvrir le menu à côté du nom de poste de travail dans la liste Exécution sur la barre latérale et sélectionnez Réinitialiser .
Réinitialiser des applications depuis la barre latérale	Pour réinitialiser toutes les applications en cours d'exécution, cliquez sur le bouton de la barre d'outils Ouvrir la fenêtre des paramètres en haut de la barre latérale et cliquez sur Réinitialiser .
Réinitialiser un poste de travail à l'aide d'un URI	Pour réinitialiser un poste de travail, utilisez l'URI <code>https://Connection_Server_name_or_IP_address?desktopId=desktop_name&action=reset</code> .

Pour un poste de travail distant, le système d'exploitation du poste de travail distant est redémarré. Le 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.

Index

A

- Agent Blast **12**
- agent HTML Access
 - configuration de certificats SSL **14**
 - importation d'un certificat **15**
- Agent HTML Access, configuration de suites de chiffrement **18**

B

- barre latérale **42**

C

- certificat racine, importation dans le magasin Windows **16**
- certificats, définition de l'empreinte numérique dans le registre Windows **17**
- certificats de sécurité auto-signés **36**
- certificats intermédiaires, importation dans le magasin Windows **16**
- certificats SSL, configuration pour les agents HTML Access **14**
- claviers **37, 40**
- Client Web, Configuration système requise pour HTML Access **7**
- Client Web HTML Access **5**
- collage du texte **44**
- coller du texte **45**
- commande de menu Envoyer Ctrl+Alt+Del **46**
- configuration **7**
- configuration des paramètres **23**
- configuration système, pour HTML Access **7**
- copie du texte **44**
- copier du texte **45**
- Ctrl+Alt+Delete **46**

D

- déconnexion d'un poste de travail distant **46**
- désinstaller HTML Access **20**

E

- exemples d'URI **28**

F

- fermer une session **46**
- Fichiers de modèle d'administration (ADM), HTML Access **30**

H

- Horizon Client, se déconnecter d'un poste de travail **46**
- Horizon View HTML Access **5**
- HTML Access
 - configuration de stratégies de groupe **29**
 - installation d'Horizon Client sur **7**
 - mise à niveau **18**

I

- IME (éditeur de méthode d'entrée) **37, 40**
- installation **7**

L

- lecture du son **44**

M

- magasin de certificats Windows, importation d'un certificat pour l'agent HTML Access **15**
- matrice de prise en charge des fonctions **33**
- MMC, ajout du composant logiciel enfichable Certificat **15**
- moniteurs **41**

O

- ouverture de session **35**

P

- page HTML Access **23**
- portail Web **23**
- ports TCP, HTML Access **11**
- poste de travail
 - fermer une session sur **46**
 - réinitialiser **47**
- poste de travail distant **33**
- programme d'amélioration du produit, données de pool de postes de travail **20**

R

- RAM vidéo **41**
- règles de pare-feu, HTML Access **11**
- réinitialiser le poste de travail **47**
- résolution d'écran **41**

S

- Serveur de connexion View **10**

serveurs de sécurité **10**
stratégies de groupe, configuration pour HTML
Access **29**
suites de chiffrement, configuration pour les
agents HTML Access **18**
syntaxe d'URI pour les clients Web de HTML
Access **26**

T

texte, copie **44**

U

URI (Identifiants uniformes de ressource) **26**