# Utilisation de HTML Access

Mars 2015

VMware Horizon 6

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-001116-06

vmware®

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

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

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

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

docfeedback@vmware.com



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

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

# Table des matières

# Utilisation de 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™ avec View™ 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*.

# 1 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

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 un système client

Les navigateurs Web suivants sont pris en charge.

| | Chrome | Internet Explorer | Safari | Mobile Safari | Firefox |
|---|---|---|---|---|---|
| HTML Access 2.6 | 38 et 39 | 10 et 11 | 6.2, 7 et 8 | iOS 7 ou version ultérieure | 33 |
| HTML Access 2.5 | 35, 36 et 37 | 9 (prise en charge limitée), 10 et 11 | 6.1.3 et 7 | iOS 7 ou version ultérieure | 30 et 31 |
| HTML Access 2.4 | 33 et 34 | 9 (prise en charge limitée), 10 et 11 | 6.1.3 et 7 | iOS 7 ou version ultérieure | 28 et 29 |

### Système d'exploitation client

- Windows XP SP3 (32 bits)
- Windows 7 SP1 ou sans SP (32 ou 64 bits)

- Poste de travail Windows 8.x (32 ou 64 bits)
- Windows Vista SP1 ou SP2 (32 bits)
- Mac OS X Snow Leopard (10.6.8)
- Mac OS X Lion (10.7)
- Mac OS X Mountain Lion (10.8)
- Mac OS X Mavericks (10.9)
- Mac OS X Yosemite (10.10)
- iPad avec iOS 7.0 ou version ultérieure (par conséquent, iPad 1 n'est pas pris en charge)
- Chrome OS 28.*x* ou version ultérieure

**Poste de travail distant**

Les logiciels suivants doivent être installés sur la machine virtuelle accédée par l'utilisateur :

- Systèmes d'exploitation pour postes de travail View mono-utilisateur : si View Agent 6.0.x est installé, Windows XP SP3 (32 bits) et Windows Vista (32 bits) sont pris en charge. Si View Agent 6.0.x ou une version ultérieure est installée, Windows 7 (32 ou 64 bits) et Windows Server 2008 R2 sont également pris en charge. Si View Agent 6.0.1 ou une version ultérieure est installée, Windows 8 (32 ou 64 bits) et Windows 8.1 (32 ou 64 bits) sont également pris en charge. Si View Agent 6.1 ou une version ultérieure est installée, Windows Server 2012 R2 est également pris en charge.
- Systèmes d'exploitation pour postes de travail View basés sur une session sur des hôtes RDS : si View Agent 6.0.2 ou une version ultérieure est installée, Windows Server 2008 R2, Windows Server 2012 et Windows Server 2012 R2 sont pris en charge.
- View Agent : HTML Access 2.6 requiert View Agent 6.1 ou View Agent 6.0.2. HTML Access 2.5 requiert View Agent 6.0.1. HTML Access 2.4 requiert View Agent 6.0.

  Les instructions d'installation sont fournies dans le document *Configuration des postes de travail et applications dans 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 38.
- Le paramètre **HTML Access** doit être activé.

Des instructions de configuration sont fournies dans « Préparer des postes de travail et des pools distants », page 12.

**Serveur de connexion View**

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

- HTML Access 2.6 requiert le Serveur de connexion View 6.1 ou 6.0.x. Si le Serveur de connexion View 6.0.x est installé, vous devez également exécuter le programme d'installation HTML Access distinct sur le serveur.
- HTML Access 2.5 requiert le Serveur de connexion View 6.0.1. Avec cette version du Serveur de connexion View, HTML Access 2.5 est intégré.
- HTML Access 2.4 requiert le Serveur de connexion View 6.0. Avec cette version du Serveur de connexion View, HTML Access 2.4 est intégré.

Par défaut, le composant HTML Access est déjà sélectionné dans le programme d'installation du Serveur de connexion View. Des instructions d'installation sont fournies dans le document *Installation de 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 |
|---|---|---|
| 2.6 | 6.1 | Pas de programme d'installation distinct |
| 2.6 | 6.0.x | Programme d'installation HTML Access distinct |
| 2.5 | 6.0.x | Pas de programme d'installation distinct |
| 2.4 | 6.0 | Pas de programme d'installation 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 Si un programme d'installation HTML Access distinct est requis, depuis l'hôte ou les hôtes d'un groupe répliqué du Serveur de connexion View, téléchargez le programme d'installation HTML Access sur la page de téléchargement View, puis exécutez-le.

   Le nom du programme d'installation est `VMware-Horizon-View-HTML-Access_X64-y.y.y-xxxxxx.exe`, où *y.y.y* est le numéro de version et *xxxxxx* est le numéro de build.

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, assure-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. |

**Tableau 1-2.** Règles de pare-feu pour HTML Access (suite)

| Source | Port source par défaut | Protocole | Cible | Port cible par défaut | Remarques |
|---|---|---|---|---|---|
| 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 et des pools distants

Avant que les utilisateurs finaux puissent accéder à un poste de travail distant, les administrateurs doivent configurer certains paramètres de pool et installer View Agent sur les machines virtuelles de postes de travail distants 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 datacenter.

- Vérifiez que la machine virtuelle que vous prévoyez d'utiliser en tant que source de poste de travail 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 de postes de travail et l'octroi de droits d'utilisation des postes de travail aux utilisateurs. Consultez les rubriques sur la création de pools de postes de travail dans *Configuration de postes de travail et d'applications dans View*.

- Pour vérifier que 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. Sur la machine virtuelle parente que vous prévoyez d'utiliser comme source pour un pool de clones liés ou sur le modèle de machine virtuelle que vous prévoyez d'utiliser comme pool de clones intégraux, installez View Agent.

   Le logiciel View Agent comprend un composant de HTML Access.

2. Si vous créez un pool de clones liés, utilisez vSphere Client pour prendre un snapshot de la machine virtuelle parent.

3. Utilisez View Administrator pour créer un pool à partir de cette machine virtuelle, et activez le paramètre **HTML Access** à la fin de l'assistant d'ajout de pool de postes de travail.

   HTML Access est pris en charge pour les pools de postes de travail de machine virtuelle et, si vous disposez d'HTML Access 2.6, pour les pools de postes de travail basés sur une session sur des hôtes RDS. Les applications distantes et hébergées sur les hôtes RDS ne sont pas prises en charge.

4. Dans les paramètres du pool, vérifiez que la **Résolution maximale de chaque moniteur** est supérieure ou égale à **1 920x1 200**.

5. Octroyez aux utilisateurs le droit d'utiliser ce pool.

6. Utilisez Horizon Client pour vous connecter à un poste de travail de ce pool.

   Avant d'utiliser HTML Access, suivez les étapes ci-dessous pour vérifier que le pool fonctionne correctement.

7. 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.

8. 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.

9. Sur la page de sélection du poste de travail qui s'affiche, cliquez sur une icône de poste de travail.

Vous pouvez à présent accéder à 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.

## 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, car aucune version de maintenance correspondante n'est proposée pour le Serveur de connexion View. 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 |
|---|---|---|
| 2.6 | 6.1 | Pas de programme d'installation distinct |
| 2.6 | 6.0.x | Programme d'installation HTML Access distinct |
| 2.5 | 6.0.x | Pas de programme d'installation distinct |
| 2.4 | 6.0 | Pas de programme d'installation distinct |

Pour effectuer la mise à niveau de HTML Access, vous devez également exécuter le programme d'installation de View Agent sur les machines virtuelles parents correspondantes ou sur les modèles de machines virtuelles de vos pools de postes de travail. La version de View Agent doit correspondre à celle de Serveur de connexion View.

**IMPORTANT** 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.

# 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

1 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.

2 Sélectionnez **VMware Horizon View HTML Access** et cliquez sur **Désinstaller**.

3 (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 |
| Version du produit client | `<client-version>` | Non | 2.6.0-*build_number* |
| Architecture binaire du client | `<client-arch>` | Non | Exemples comprenant les valeurs suivantes :<br>■ navigateur<br>■ arm |
| Architecture native du navigateur | `<browser-arch>` | Non | Exemples comprenant les valeurs suivantes :<br>■ Win32<br>■ Win64<br>■ MacIntel<br>■ iPad |
| Chaîne de l'agent utilisateur du navigateur | `<browser-user-agent>` | Non | Exemples comprenant les valeurs suivantes :<br>■ Mozilla/5.0 (Windows NT 6.1; WOW64)<br>■ AppleWebKit/703.00 (KHTML, like Gecko)<br>■ Chrome/3.0.1750<br>■ Safari/703.00 |
| Chaîne de version interne de navigateur | `<browser-version>` | Non | Exemples comprenant les valeurs suivantes :<br>■ 7.0.3 (pour Safari),<br>■ 29.0 (pour Firefox). |
| Implémentation de base du navigateur | `<browser-core>` | Non | Exemples comprenant les valeurs suivantes :<br>■ Chrome<br>■ Safari<br>■ Firefox<br>■ MSIE (pour Internet Explorer) |
| Si le navigateur tourne sur un périphérique 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

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

| Option | Paramètre propriété |
|---|---|
| **Créer des liens pour des programmes d'installation spécifiques** | 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 `downloads`, situé sous le répertoire `C:\Program Files\VMware\VMware View\Server\broker\webapps\` sur le Serveur de connexion View, comme décrit à l'étape suivante.<br>■ Programme d'installation de Windows 32 bits :<br>`link.win32=https://server/downloads/VMware-Horizon-Client.exe`<br>■ Programme d'installation de Windows 64 bits :<br>`link.win64=https://server/downloads/VMware-Horizon-Client.exe`<br>■ Programme d'installation de Linux :<br>`link.linux=https://server/downloads/VMware-Horizon-Client.tar.gz`<br>■ Programme d'installation de Mac OS X :<br>`link.mac=https://server/downloads/VMware-Horizon-Client.dmg`<br>■ Programme d'installation d'iOS :<br>`link.ios=https://server/downloads/VMware-Horizon-Client-iPhoneOS.zip`<br>■ Programme d'installation d'Android :<br>`link.android=https://server/downloads/VMware-Horizon-Client-AndroidOS.apk` |
| **Modifier l'URL du lien d'aide dans l'écran d'ouverture de session et l'écran du sélecteur de poste de travail** | `link.help`<br>Par défaut, ce lien pointe vers un système d'aide hébergé sur le site Web de VMware. Le lien d'aide s'affiche dans le coin supérieur droit de l'écran. Pour l'écran de connexion à HTML Access et l'écran de sélection de postes de travail, le lien d'aide est une icône en forme de point d'interrogation. |

3 (Facultatif) Changez l'URL du lien de l'aide dans la barre d'outils Horizon Client.

Dès que vous êtes connecté à un poste de travail, le lien d'aide devient une commande **Help** affichée dans le menu déroulant à l'extrémité droite du client. Pour changer l'URL correspondant à ce lien, modifiez la propriété `HELP_URL_VIEW` dans le fichier approprié du dossier approprié.

| Option | Description |
|---|---|
| **Pour HTML Access 2.6** | Sur l'hôte du Serveur de connexion View, le fichier se trouve à l'emplacement suivant :<br>*`ViewConnectionServer-InstallDir`*`\webapps\portal\desktop\locale\` |
| **Pour HTML Access 2.4 et 2.5** | Sur le système d'exploitation du poste de travail distant (sur lequel View Agent est installé), le fichier se trouve à l'emplacement suivant :<br>`C:\Program Files\VMware\VMware Blast\web\locale\` |

Par exemple, si vous utilisez l'anglais, modifiez la propriété `HELP_URL_VIEW` dans le fichier `en.json`.

4 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 dossier `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`*.

5 Redémarrez le service du composant Web View.

# Activer les postes de travail à partir des hôtes RDS

Avec HTML Access 2.6, les administrateurs peuvent configurer le Serveur de connexion View de manière à autoriser un hôte Microsoft RDS (Remote Desktop Session) à fournir des postes de travail distants basés sur des sessions.

### Prérequis

Pour plus d'informations sur l'utilisation de l'utilitaire ADSI Edit sur votre version du système d'exploitation Windows, consultez le site Web Microsoft TechNet. Si vous utilisez un hôte RDS Windows Server 2012, vous devrez peut-être installer les outils AD DS et LDS, sous Outils d'administration de serveur distant, dans **Ajouter des rôles et des fonctionnalités**.

### Procédure

1 Démarrez l'utilitaire ADSI Edit sur votre hôte du Serveur de connexion View.

2 Dans la boîte de dialogue Paramètres de connexion, sélectionnez **DC=vdi,DC=vmware,DC=int** ou connectez-vous à cet objet.

3 Dans le volet Ordinateur, sélectionnez ou tapez **`localhost:389`** ou le nom de domaine complet du Serveur de connexion View, suivi du port 389.

   Par exemple : **`localhost:389`** ou **`mycomputer.mydomain.com:389`**

4 Si le pool a déjà été créé, recherchez son nom sous l'objet **OU=Applications** et ajoutez **BLAST** dans l'attribut **pae-ServerProtocolLevel**.

5 Identifiez le nom de la batterie sous l'objet **OU=Server Groups** et ajoutez **BLAST** dans l'attribut **pae-ServerProtocolLevel**.

Les éléments de la batterie s'affichent désormais dans le client Web HTML Access.

# Utilisation d'URI pour configurer 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://[<varname id="VARNAME_E0F8F9951BC4471D9871655A18782C9E">authority-part</varname>][?
<varname id="VARNAME_217F9AF17A3745369FD8E2154505D735">query-part</varname>]
```

**IMPORTANT** Lors du codage des liens hypertextes HTML ou les boutons contenant l'URI, n'utilisez pas `target='_Blank'` dans le lien. Ce code est utilisé pour ouvrir une nouvelle fenêtre de navigateur, mais entraîne des problèmes avec les navigateurs Internet Explorer 9, 10 et 11. Si vous utilisez ce code dans un `href`, si l'utilisateur sélectionne l'élément du menu **Se déconnecter** une fois le poste de travail déconnecté, le client tente immédiatement de se reconnecter. De plus, les noms d'utilisateur et de domaine ne sont pas définis.

***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 :

```
<varname id="VARNAME_1BAB6153D2834B1490509093A1961D1F">server-
address</varname>:<varname
id="VARNAME_2296A4E54893485C852FFE94067114D7">port-number</varname>
```

***query-part***

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

```
<varname
id="VARNAME_48A6B3A0E1184943BC1206017B78B9D5">query1</varname>=<varna
me
id="VARNAME_9B9916FF3D3540D4AA5622F9C828F072">value1</varname>[&<varn
ame
id="VARNAME_6BCA2912EC454A5683D586754BF89DCE">query2</varname>=<varna
me id="VARNAME_F698C39E83D34D639C943ACDF828BAFE">value2</varname>...]
```

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, consultez le guide *Utilisation de VMware Horizon Client* pour chaque type de système client.

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

**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 |
|---|---|
| `browse` | Affiche une liste des postes de travail disponibles hébergés sur le serveur spécifié. Il ne vous est pas demandé de spécifier un poste de travail pour l'utilisation de cette action. |
| `start-session` | Lance le poste de travail spécifié. Si aucune requête d'action n'est fournie et que le nom du poste de travail est fourni, `start-session` est l'action par défaut. |
| `réinitialiser` | Éteint puis redémarre le poste de travail spécifié. Les données non enregistrées sont perdues. La réinitialisation d'un poste de travail distant équivaut à appuyer sur le bouton Réinitialiser d'un ordinateur physique. |
| `logoff` | 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 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>
```

**Remarque** N'utilisez pas `target='_Blank'` dans le lien, comme, par exemple, dans le code suivant :

```
<a href="https://view.mycompany.com?desktopId=Primary%20Desktop&action=start-session"
target="_Blank">Test Link</a>
```

`target='_Blank'` est utilisé pour ouvrir une nouvelle fenêtre de navigateur, mais entraîne des problèmes avec les navigateurs Internet Explorer 9, 10 et 11. Si vous utilisez ce code dans un `href`, si l'utilisateur sélectionne l'élément du menu **Se déconnecter** une fois le poste de travail déconnecté, le client tente immédiatement de se reconnecter. De plus, les noms d'utilisateur et de domaine ne sont pas définis.

# 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 View Agent 6.0 ou version ultérieure est installé sur vos postes de travail distants. View Agent 6.0 ou version ultérieure inclut un composant HTML Access. Pour les versions antérieures, vous avez dû installer une instance de Remote Experience Agent pour obtenir le composant de HTML Access.
- 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 Horizon 6 à l'adresse http://www.vmware.com/go/downloadview.

   Le fichier se nomme `VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip`, où *x.x.x* est la version et *yyyyyyy* 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 `Blast-enUS.adm`.

3 Sur le serveur Active Directory, modifiez les GPO.

| Option | Description |
|---|---|
| **Windows 2008 ou 2012** | a Sélectionnez **Démarrer > Outils d'administration > Gestion de stratégie de groupe**.<br>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**. |
| **Windows 2003** | a Sélectionnez **Démarrer > Tous les programmes > Outils d'administration > Utilisateurs et ordinateurs Active Directory**.<br>b Cliquez avec le bouton droit sur l'UO qui contient vos postes de travail distants et sélectionnez **Propriétés**.<br>c Sous l'onglet **Stratégie de groupe**, cliquez sur **Ouvrir** pour ouvrir le plug-in Gestion de stratégie de groupe.<br>d Dans le volet de droite, cliquez avec le bouton droit sur le GPO que vous avez créé pour les paramètres de stratégie de groupe et sélectionnez **Edit (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 `Blast-enUS.adm` et cliquez sur **Ouvrir**.

6 Cliquez sur **Close (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, `Blast-enUS.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 | 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.<br>Lorsque ce paramètre est activé ou non configuré, et quelqu'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.<br>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. |
| Nettoyage de la mémoire de session | 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.<br>L'intervalle détermine la fréquence d'exécution du nettoyage de la mémoire. L'intervalle est défini en millisecondes.<br>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. |
| Lecture audio | Permet de contrôler si la lecture audio est autorisée sur le poste de travail distant. Par défaut, ce paramètre est activé. |
| Qualité d'image | 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.<br>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.<br>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.<br>■ **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.<br>■ **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.<br>■ **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 | 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 :<br>■ **Activé du client vers le serveur seulement** (C'està-dire autoriser le copier/coller uniquement du client vers le poste de travail distant.)<br>■ **Désactivé dans les deux sens**<br>■ **Activé dans les deux sens**<br>■ **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.)<br>Ce paramètre s'applique uniquement à View Agent.<br>Pour les postes de travail à distance mono-utilisateur, lorsque ce paramètre est désactivé ou n'est pas configuré, la valeur par défaut est **Activé du client vers le serveur seulement**. Pour les postes de travail à distance basés sur une session sur hôtes RDS (disponible avec HTML Access 2.6), lorsque ce paramètre est désactivé ou n'est pas configuré, la valeur par défaut est **Désactivé dans les deux sens**. |
| Service HTTPS | Permet de changer le port TCP sécurisé (HTTPS) pour Blast Agent service. Le port par défaut est 22443.<br>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). |

# Utilisation d'un poste de travail distant 3

Le client fournit une barre d'outils et un menu déroulants. Vous pouvez donc facilement vous déconnecter d'un poste de travail distant ou utiliser la commande de menu équivalant à la combinaison de touches Ctrl +Alt+Suppr.

Ce chapitre aborde les rubriques suivantes :



## Matrice de prise en charge des fonctions

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

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

| Fonction | Poste de travail distant Windows 8.x | Poste de travail distant Windows 7 | Poste de travail distant Windows XP | Poste de travail distant Windows Vista | Poste de travail Windows Server 2008 R2 |
|---|---|---|---|---|---|
| RSA SecurID ou RADIUS | X | X | X | X | X |
| Single Sing-On | X | X | X | X | X |
| Protocole d'affichage RDP | | | | | |
| Protocole d'affichage PCoIP | | | | | |
| Protocole Blast | X | X | X | X | X |
| Accès USB | | | | | |

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

| Fonction | Poste de travail distant Windows 8.x | Poste de travail distant Windows 7 | Poste de travail distant Windows XP | Poste de travail distant Windows Vista | Poste de travail Windows Server 2008 R2 |
|---|---|---|---|---|---|
| Audio/Vidéo en temps réel (RTAV) | | | | | |
| Wyse MMR | | | | | |
| Redirection multimédia (MMR) Windows 7 | | | | | |
| Impression virtuelle | | | | | |
| Impression basée sur l'emplacement | | | | | |
| Cartes à puce | | | | | |
| Plusieurs écrans | | | | | |

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

## Fonctionnalités prises en charge pour les postes de travail basés sur des sessions 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 de poste de travail simultanément sur un hôte RDS.

Si vous disposez de HTML Access 2.6, vous pouvez également accéder aux postes de travail distants basés sur des sessions sur un hôte Microsoft RDS (Remote Desktop Session). 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.** Fonctionnalités prises en charge pour les hôtes RDS si View Agent 6.0.2 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 RDS sur une machine physique | Hôte Windows Server 2012 RDS sur une machine virtuelle |
|---|---|---|---|---|
| RSA SecurID ou RADIUS | X | X | X | X |
| Single Sing-On | X | X | X | X |
| Protocole Blast | X | X | X | X |
| Impression virtuelle | | | | |
| Impression basée sur l'emplacement | | | | |
| Plusieurs écrans | | | | |

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 37.

# Se connecter à un poste de travail distant

Utilisez vos informations d'identification Active Directory pour vous connecter aux 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 pour ouvrir une session.

### Procédure

1. Si un message demande les informations d'identification RSA SecurID ou les informations d'identification pour l'authentification RADIUS, entrez le nom d'utilisateur et le code secret et cliquez sur **Connexion**.

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

2. 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.

3. Dans la boîte de dialogue Connexion, entrez votre nom d'utilisateur, votre mot de passe et votre nom de domaine Active Directory, puis cliquez sur **Se connecter**.

4. Si plusieurs postes de travail vous ont été octroyés, cliquez sur l'icône du poste de travail distant auquel vous souhaitez accéder.

   Le poste de travail distant est affiché dans votre navigateur.

### Suivant

Si vous utilisez un navigateur Safari et que peu après vous être connecté au poste de travail, vous être 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, lorsque vous vous connectez à un poste de travail distant avec un navigateur Safari, vous êtes déconnecté après quelques minutes et une boîte de dialogue Poste de travail déconnecté apparaît. Vous pouvez utiliser le navigateur pour accepter le certificat de sécurité auto-signé et vous connecter de nouveau au poste de travail distant.

Ce problème peut se produire lorsque Blast Secure Gateway n'est pas utilisé.

#### Procédure

1. Cliquez sur le lien **Cliquez ici pour accepter le certificat de sécurité** dans la boîte de dialogue Poste de travail déconnecté.
2. Cliquez sur le bouton **Afficher le certificat** à la prochaine invite qui s'affiche.
3. Dans le volet Blast qui apparaît, cliquez pour développer la liste déroulante **Approuver/Approbation**.
4. Dans la liste déroulante **Lors de l'utilisation de ce certificat**, sélectionnez **Toujours approuver**, et cliquez sur **Continuer**.
5. Lorsque vous y êtes invité, saisissez votre mot de passe et cliquez sur **Mettre les paramètres à jour**.
6. Dans la fenêtre de sélection du poste de travail, cliquez sur le poste de travail distant.

Vous êtes de nouveau connecté à une session sur le poste de travail distant.

## Limitations du produit

Web client fourni par HTML Access présente des limitations de produit quant à la lecture audio et aux claviers.

- La lecture audio n'est pas prise en charge pour les postes de travail distants Windows XP et Windows Vista.
- Internet Explorer 9 n'est pas pris en charge par HTML Access 2.6. S'agissant d'HTML Access 2.4 et 2.5, Internet Explorer 9 est pris en charge, mais cette version du navigateur ne prend pas en charge nombre de fonctionnalités HTML5 fournies par HTML Access. Parmi les fonctionnalités non prises en charge par Internet Explorer 9 (même avec HTML Access 2.4 ou 2.5), on retrouve la lecture audio, la redirection du presse-papiers, les changements du pointeur de la souris et le mode plein écran.
- Si vous utilisez le navigateur Internet Explorer ou un navigateur installé sur des périphériques de poche tels que les iPad et les tablettes Android, le pointeur de la souris ne change pas de manière dynamique en fonction de son emplacement.

  Parmi ceux-là il y a le curseur occupé, le curseur de déplacement et le curseur de redimensionnement. Par exemple, avec les navigateurs Internet Explorer ou les navigateurs installés sur des périphériques de poche, lorsque vous placez le pointeur de la souris sur un lien d'une page Web dans un poste de travail distant, il ne se transforme pas en icône de main. Si vous déplacez le pointeur de la souris sur le bord d'une fenêtre, le pointeur ne se change pas en flèches de redimensionnement. Si vous modifiez du texte, le pointeur ne se change pas en curseur. Vous pouvez toujours effectuer les actions souhaitées, mais le pointeur reste sous forme de pointeur.
- Certaines touches de modification, touches spéciales et combinaisons de touches ne fonctionnent pas sur un poste de travail distant. Pour plus de précisions et pour obtenir des informations sur l'utilisation des claviers internationaux, reportez-vous à « Limitations de clavier », page 37 et à « Claviers internationaux », page 37.

## Limitations de clavier

Indépendamment de la langue utilisée, certaines combinaisons de touches ne peuvent pas être envoyées à 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.

Les touches et les combinaisons de touches suivantes ne fonctionnent pas toujours :

- Ctrl+T
- Ctrl+W
- Ctrl+N
- Touche Windows
- Touche de commande
- Alt+Entrer
- Ctrl+Alt+*any_key*
- Verrouillage majuscule+*modifier_key* (telle que Alt ou Shift)
- Touches de fonction, si vous utilisez un Chromebook.

**IMPORTANT** Pour entrer Ctrl+Alt+Delete, utilisez **Envoyer Ctrl+Alt+Delete** du menu déroulant situé à droite de la barre de menu client.

## 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 3-3.** 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 le poste de travail distant a été configuré avec la capacité de mémoire RAM vidéo appropriée, le client peut redimensionner un poste de travail distant à la taille de la fenêtre du client. 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.

---

**Important** Pour utiliser la fonctionnalité de rendu 3D, vous devez allouer suffisamment de mémoire VRAM pour chaque poste de travail distant Windows 7 ou version ultérieure.

- 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.

Lorsque le rendu 3D est activé, le nombre maximal de moniteurs est de 1 et la résolution maximale est 1 920 x 1200. 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*.

---

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 le poste de travail distant. Sélectionnez la commande **Mode haute résolution** dans le menu déroulant situé à droite de la barre de menus client. Pour afficher cette barre de menus, cliquez sur la flèche vers le bas dans l'onglet situé en haut de la partie centrale de la fenêtre.

HTML Access propose également une commande **Plein écran** dans le menu déroulant.

---

**Important** Pour utiliser le mode haute résolution en mode plein écran, vous devez allouer suffisamment de mémoire VRAM pour chaque poste de travail distant Windows 7 ou version ultérieure. 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*.

---

## Audio

Si vous utilisez un périphérique Chrome ou un navigateur qui prend en charge WebSocket, vous pouvez avoir le son sur votre poste de travail distant, avec toutefois certaines limites.

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

Tenez compte des instructions suivantes :

- La lecture audio n'est pas prise en charge pour les postes de travail distants Windows XP et Windows Vista.
- Pour augmenter le volume, utilisez le contrôle du son à partir du système client et non 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

Votre administrateur View peut définir cette fonctionnalité pour que les opérations copier et coller soient autorisées uniquement depuis votre système client vers un poste de travail distant ou uniquement depuis un poste de travail distant vers votre système client, ou les deux, ou aucun. Certaines restrictions s'appliquent.

Cette fonctionnalité est disponible si vous utilisez un périphérique Chrome ou un navigateur qui prend en charge WebSocket.

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 du texte brut ou du texte formaté, y compris tout caractère non-ASCII, depuis Horizon Client vers un poste de travail distant, ou l'inverse, mais le texte collé est du texte brut. Vous pouvez copier-coller jusqu'à 5 000 caractères.

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 les commandes **Coller le texte** et **Afficher le texte copié** du menu déroulant situé à droite de la barre de menus du client.

### Prérequis

- L'administrateur View doit conserver la stratégie par défaut, ce qui permet aux utilisateurs de copier/coller du texte depuis des systèmes client sur leur poste de travail virtuel à distance, ou il doit 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.
- Vous devez utiliser un périphérique Chrome ou un navigateur qui prend en charge WebSockets. Les navigateurs qui ne prennent pas en charge cette technologie n'affichent pas les commandes de menu **Coller le texte** et **Afficher le texte copié**.

### Procédure

- Pour copier du texte de votre système client sur le poste de travail distant :

  a Copiez le texte sur votre système client.

  b Sur votre poste de travail distant, cliquez sur la flèche vers le bas dans l'onglet situé en haut de la partie centrale de la fenêtre afin d'afficher la barre de menus.

  c Sélectionnez la commande **Coller le texte** dans le menu déroulant situé à droite de la barre de menus client.

  d Collez le texte dans la boîte de dialogue qui s'affiche.

  e Placez le curseur de la souris dans l'application dans laquelle vous voulez coller le texte.

  f Cliquez sur **Coller** dans la boîte de dialogue correspondante, puis fermez cette dernière.

  Le texte est collé dans l'application.

- Pour copier du texte de votre poste de travail distant dans votre système client :
  a Copiez le texte dans votre poste de travail distant.
  b Sur votre poste de travail distant, cliquez sur la flèche vers le bas dans l'onglet situé en haut de la partie centrale de la fenêtre afin d'afficher la barre de menus.
  c Sélectionnez **Afficher le texte copié** dans le menu déroulant situé à droite de la barre de menus client.

    Si la commande **Afficher le texte copié** ne figure pas dans le menu déroulant, votre navigateur ne prend pas en charge WebSockets ou votre administrateur View n'a pas configuré votre installation pour permettre la copie de texte du poste de travail distant sur le système client, tel qu'indiqué comme conditions préalables au début de cette procédure.
  d Dans la boîte de dialogue Afficher le texte copié, sélectionnez à nouveau le texte et copiez-le.

    Le texte est à présent placé dans le presse-papiers.
  e Sur votre système client, collez le texte selon la procédure habituelle.

# Fermer une session ou se déconnecter

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

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

**Remarque** La combinaison de touches Windows Ctrl+Alt+Suppr n'est pas prise en charge sur les postes de travail distants. Pour utiliser l'équivalent de la combinaison de touches Ctrl+Alt+Suppr, sélectionnez **Envoyer Ctrl+Alt+Suppr** dans le menu déroulant situé dans le côté droit de la barre de menu Client. Pour afficher la barre de menu, cliquez sur la flèche du bas dans l'onglet présent en haut de la partie centrale de la fenêtre.

### Procédure

- Déconnectez-vous du serveur View Server et déconnectez-vous (mais sans fermer la session) du poste de travail.

| Option | Action |
|---|---|
| **À partir du SE du poste de travail** | Sélectionnez **Se déconnecter** dans le menu déroulant situé sur le côté droit de la barre de menus du client, puis cliquez sur le bouton **Fermer la session** dans le coin supérieur droit de l'écran. |
| **Dans l'écran du sélecteur de poste de travail** | Cliquez sur le bouton **Fermer la session** dans le coin supérieur droit de l'écran. |

- Fermez votre session et déconnectez-vous d'un poste de travail en sélectionnant **Fermer la session** dans le menu **Démarrer** du système d'exploitation du poste de travail.

- Déconnectez-vous sans fermer votre session.

| Option | Action |
|---|---|
| **Quittez également le client** | Fermez l'onglet du navigateur. |
| **Choisir un autre poste de travail distant sur le même serveur** | Sélectionnez **Se déconnecter** dans le menu déroulant situé du côté droit de la barre de menus Client, puis sélectionnez un autre poste de travail distant. |
| **Choisir un poste de travail distant sur un autre serveur** | Sélectionnez **Se déconnecter** à partir du menu déroulant puis entrez l'URL de l'autre serveur dans votre navigateur. |

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

- Fermez la session du système d'exploitation de poste de travail lorsqu'aucun poste de travail distant n'est ouvert.

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

  a Dans l'écran du sélecteur de poste de travail, cliquez sur le bouton **Fermer la session** sur l'icône de poste de travail.

  b Si vous y êtes invité, entrez les informations d'identification pour accéder au poste de travail distant.

# Réinitialiser un poste de travail

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

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

### Procédure

- Utilisez la commande **Réinitialiser**.

| Option | Action |
|---|---|
| **À partir de l'OS du poste de travail** | Sélectionner Sélectionnez **Se déconnecter** à partir du menu déroulant situé dans le côté droit de la barre du menu Client, puis cliquez sur **Réinitialiser** sous l'icône du poste de travail. |
| **Dans l'écran du sélecteur de poste de travail** | Cliquez sur **Réinitialiser** sous l'icône du poste de travail. |

Le système d'exploitation du poste de travail distant redémarre. Le client se déconnecte du poste de travail.

### 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

## T



## U