

Guide d'installation et de configuration de VMware Horizon HTML Access

Modifié le 29 mai 2018

VMware Horizon HTML Access 4.8

VMware Horizon 7 7.5



vmware®

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

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

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

Copyright © 2013–2018 VMware, Inc. Tous droits réservés. [Copyright et informations sur les marques.](#)

Table des matières

Guide d'installation et de configuration de VMware Horizon HTML Access 5

1 Configuration et installation 6

- Configuration système requise pour HTML Access 7
- Préparation du Serveur de connexion et des serveurs de sécurité 9
 - Règles de pare-feu pour un accès via un navigateur Web client 10
- Configurer Horizon 7 pour supprimer les informations d'identification du cache 11
- Préparer des postes de travail, des pools et des batteries de serveurs 12
- Configuration requise pour la fonctionnalité de collaboration de session 14
- Configurer les agents HTML Access pour utiliser les nouveaux certificats TLS 15
 - Ajouter le composant logiciel enfichable Certificat à MMC sur un poste de travail distant 16
 - Importer un certificat pour l'agent HTML Access dans un magasin de certificats Windows 17
 - Importer des certificats racine et intermédiaires pour l'agent HTML Access 18
 - Définir l'empreinte numérique de certificat dans le registre Windows 19
- Configurer les agents HTML Access pour utiliser des suites de chiffrement spécifiques 20
- Configuration d'iOS pour utiliser des certificats signés par une autorité de certification 21
- Utilisation d'un certificat signé par une autorité de certification avec Unified Access Gateway 21
- Mise à niveau du logiciel HTML Access 21
- Désinstaller le composant HTML Access du Serveur de connexion 22
- Données collectées par VMware 22

2 Configuration de HTML Access pour les utilisateurs finaux 24

- Configurer la page du portail Web de VMware Horizon pour les utilisateurs finaux 24
- Utiliser des URI pour configurer des clients Web HTML Access 28
 - Syntaxe pour la création d'URI pour HTML Access 29
 - Exemples d'URI 31
- Paramètres de stratégie de groupe de HTML Access 34

3 Utilisation d'une application ou d'un poste de travail distant 35

- Matrice de prise en charge des fonctions 36
- Internationalisation 37
- Connexion à une application ou un poste de travail distant 38
 - Faire confiance à un certificat racine auto-signé 40
- Se connecter à un serveur en mode Workspace ONE 41
- Utiliser l'accès non authentifié pour se connecter à des applications publiées 41
- Combinaisons de touches de raccourci 42
- Claviers internationaux 46
- Résolution de l'écran 47

Autoriser le décodage H.264	48
Définition du fuseau horaire	48
Utilisation de la barre latérale	49
Utiliser plusieurs moniteurs	52
Utilisation de la synchronisation DPI	54
Audio	55
Copier et coller du texte	55
Utiliser la fonctionnalité de copier/coller	56
Transférer des fichiers entre le client et un poste de travail distant	57
Télécharger des fichiers depuis un poste de travail vers le client	58
Charger des fichiers depuis le client vers un poste de travail	59
Utilisation de la fonctionnalité Audio/Vidéo en temps réel pour webcams et microphones	59
Utilisation de la fonctionnalité de collaboration de session	60
Inviter un utilisateur à rejoindre une session de poste de travail distant	60
Gérer une session de collaboration	62
Rejoindre une session de collaboration	63
Fermer une session ou se déconnecter	64
Réinitialiser un poste de travail distant ou des applications publiées	65
Redémarrer un poste de travail distant	66

Guide d'installation et de configuration de VMware Horizon HTML Access

Ce guide, *Guide d'installation et de configuration de VMware Horizon HTML Access*, explique comment installer, configurer et utiliser le logiciel VMware Horizon[®] HTML Access[™] pour vous connecter à des postes de travail virtuels sans devoir 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 VMware Horizon 7 et sur 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'Horizon 7 et de VMware vSphere. Si vous découvrez Horizon 7, 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 Horizon 7* et *Administration de Horizon 7*.

Configuration et installation

La configuration d'un déploiement d'Horizon 7 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](#)
- [Préparation du Serveur de connexion et des serveurs de sécurité](#)
- [Configurer Horizon 7 pour supprimer les informations d'identification du cache](#)
- [Préparer des postes de travail, des pools et des batteries de serveurs](#)
- [Configuration requise pour la fonctionnalité de collaboration de session](#)
- [Configurer les agents HTML Access pour utiliser les nouveaux certificats TLS](#)
- [Configurer les agents HTML Access pour utiliser des suites de chiffrement spécifiques](#)
- [Configuration d'iOS pour utiliser des certificats signés par une autorité de certification](#)
- [Utilisation d'un certificat signé par une autorité de certification avec Unified Access Gateway](#)
- [Mise à niveau du logiciel HTML Access](#)
- [Désinstaller le composant HTML Access du Serveur de connexion](#)
- [Données collectées par VMware](#)

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'Horizon 7 doit respecter certaines exigences logicielles.

Remarque À partir de la version 7.0, View Agent est renommé Horizon Agent.

Navigateurs sur des systèmes clients

Navigateur	Version
Chrome	65, 66
Chrome sur périphérique Android	65 ou version ultérieure
Internet Explorer	11
Safari	11
Safari sur périphérique mobile	iOS 10, iOS 11
Firefox	59, 60
Microsoft Edge	41, 42

Remarque

- Chrome sur un périphérique Android ne prend pas en charge la touche Windows, plusieurs moniteurs, la fonction copier-coller sur le système, le transfert de fichiers, l'impression, le décodage H.264, le nettoyage des informations d'identification et une souris externe. De même, la touche et les combinaisons de touches suivantes ne fonctionnent pas sur le clavier logiciel : Suppr, Ctrl+A, Ctrl+C, Ctrl+V, Ctrl+X, Ctrl+Y, Ctrl+Z.
- Safari sur périphérique mobile ne prend pas en charge une souris externe, la touche Windows, plusieurs moniteurs, la fonction copier et coller vers le système, le transfert de fichiers, l'impression, le décodage H.264 et le nettoyage des informations d'identification.

Système d'exploitation client

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	10.12.x (Sierra)
macOS	10.13.x (High Sierra)
iOS	10, 11
Chrome OS	28.x et versions ultérieures
Android	7, 8

Postes de travail distants

HTML Access requiert Horizon Agent 7.0 ou version ultérieure et prend en charge tous les systèmes d'exploitation de poste de travail pris en charge par Horizon 7.0. Pour plus d'informations, consultez la rubrique « Systèmes d'exploitation pris en charge pour Horizon Agent » dans la version 7.0 ou ultérieure d'*Installation de View*.

Paramètres de pool

HTML Access nécessite les paramètres de pool suivants dans Horizon 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 utilisez des applications 3D ou si des utilisateurs finaux utilisent un MacBook avec écran Retina ou un Google Chromebook Pixel, reportez-vous à la section [Résolution de l'écran](#).

- 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](#).

Serveur de connexion

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

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

La version correspondant à celle du Serveur de connexion doit être installée sur le serveur de sécurité.

Si les systèmes clients se connectent en dehors du pare-feu d'entreprise, utilisez 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 du Serveur de connexion 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
d'Horizon**

VMware Blast

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

Préparation du Serveur de connexion et des serveurs de sécurité

Avant que les utilisateurs finaux puissent se connecter à un serveur et accéder à un poste de travail distant ou à une application publiée, un administrateur Horizon doit installer le Serveur de connexion et des serveurs de sécurité, le cas échéant.

Vous pouvez utiliser des dispositifs Unified Access Gateway, plutôt que des serveurs de sécurité, pour un accès externe sécurisé. Pour plus d'informations, reportez-vous au document *Déploiement et configuration d'Unified Access Gateway*.

Voici la liste de contrôle des tâches qu'un administrateur Horizon doit exécuter pour utiliser HTML Access.

- 1 Installez le Serveur de connexion avec le paramètre **Installer HTML Access** sélectionné sur le ou les serveurs qui composent un groupe répliqué de Serveur de connexion. Ce paramètre installe le composant HTML Access. Ce paramètre est sélectionné dans le programme d'installation par défaut. Pour plus d'informations, reportez-vous au document *Installation d'Horizon 7*.

Pour vérifier que le composant HTML Access est installé, vous pouvez ouvrir l'applet Désinstaller un programme de Windows et rechercher **VMware Horizon 7 HTML Access** dans la liste.
- 2 Si vous utilisez des serveurs de sécurité, installez le serveur de sécurité. La version du serveur de sécurité doit correspondre à celle du Serveur de connexion. Pour les instructions d'installation, reportez-vous au document *Installation d'Horizon 7*.
- 3 Vérifiez que chaque instance du Serveur de connexion ou du serveur de sécurité possède un certificat TLS qui peut être vérifié en utilisant le nom d'hôte que vous entrez dans le navigateur Web. Pour plus d'informations, reportez-vous au document *Installation d'Horizon 7*.

- 4 Pour pouvoir utiliser l'authentification à deux facteurs, telle que l'authentification RSA SecurID ou RADIUS, assurez-vous que cette fonctionnalité est activée sur le Serveur de connexion. Pour plus d'informations, consultez les rubriques concernant l'authentification à deux facteurs dans le document *Administration d'Horizon 7*.

Important Si vous activez le paramètre **Masquer la liste de domaines dans l'interface utilisateur client** et sélectionnez l'authentification à deux facteurs (RSA SecureID ou RADIUS) pour l'instance du Serveur de connexion, n'appliquez pas la correspondance des noms d'utilisateur Windows. L'application de la correspondance des noms d'utilisateur Windows empêche les utilisateurs d'entrer des informations de domaine dans la zone de texte Nom d'utilisateur, et la connexion échoue toujours. Pour plus d'informations, consultez les rubriques concernant l'authentification à deux facteurs dans le document *Administration d'Horizon 7*.

- 5 Si vous utilisez des pare-feu tiers, configurez des règles pour autoriser le trafic entrant sur le port TCP 8443 pour tous les hôtes des serveurs de sécurité et du Serveur de connexion dans un groupe répliqué, et configurez une règle pour autoriser le trafic entrant (à partir des serveurs) sur le port TCP 22443 des machines virtuelles de poste de travail distant et des hôtes RDS du centre de données. Pour plus d'informations, reportez-vous à la section [Règles de pare-feu pour un accès via un navigateur Web client](#).
- 6 Pour autoriser un accès non authentifié aux applications publiées, activez cette fonctionnalité dans le Serveur de connexion. Pour plus d'informations, reportez-vous au document *Administration d'Horizon 7*.

Une fois les serveurs installés, le paramètre **Blast Secure Gateway** est activé sur les instances du Serveur de connexion et les serveurs de sécurité applicables dans Horizon Administrator. De même, le paramètre **URL externe Blast** est configuré pour utiliser Blast Secure Gateway dans les instances du Serveur de connexion et les serveurs de sécurité utilisés. Par défaut, l'URL inclut le nom de domaine complet de l'URL externe du tunnel 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 l'hôte du Serveur de connexion ou l'hôte du serveur de sécurité. Pour plus d'informations, consultez « Définir les URL externes d'une instance du Serveur de connexion » dans le document *Installation d'Horizon 7*.

Remarque Vous pouvez utiliser HTML Access avec VMware Workspace ONE 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 ONE et sa configuration pour l'utiliser avec le Serveur de connexion, consultez la documentation de Workspace ONE. Pour plus d'informations sur le couplage du Serveur de connexion avec un serveur d'authentification SAML, consultez le document *Administration d'Horizon 7*.

Règles de pare-feu pour un accès via un navigateur Web client

Pour autoriser les navigateurs Web clients à effectuer des connexions à des serveurs de sécurité, à des instances du Serveur de connexion, à des postes de travail distants et à des applications publiées, 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 ou un serveur de sécurité, la règle **Serveur de connexion de VMware Horizon View (Blast-In)** est activée sur le pare-feu Windows et ce dernier est configuré pour autoriser le trafic entrant sur le port TCP 8443.

Tableau 1-1. Règles de pare-feu pour un accès via un navigateur client

Source	Port source par défaut	Protocole	Cible	Port cible par défaut	Remarques
Navigateur Web client	Tout port TCP	HTTPS	Serveur de sécurité ou instance du Serveur de connexion	TCP 443	Pour établir la connexion initiale, le navigateur Web d'un périphérique client se connecte à un serveur de sécurité ou à une instance du Serveur de connexion sur le port TCP 443.
Navigateur Web client	Tout port TCP	HTTPS	Blast Secure Gateway	TCP 8443	Une fois la première connexion établie, le navigateur Web sur 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 une instance du Serveur de connexion pour autoriser cette seconde 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 ou une application publiée, Blast Secure Gateway se connecte à l'agent HTML Access sur le port TCP 22443 sur la machine virtuelle de poste de travail distant ou sur l'hôte RDS. Ce composant d'agent est inclus lorsque vous installez Horizon 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 distant ou une application publiée, le navigateur Web sur un périphérique client se connecte directement à l'agent HTML Access sur le port TCP 22443 sur la machine virtuelle de poste de travail distant ou sur l'hôte RDS. Ce composant d'agent est inclus lorsque vous installez Horizon Agent.

Configurer Horizon 7 pour supprimer les informations d'identification du cache

Vous pouvez configurer Horizon 7 pour qu'il supprime les informations d'identification d'un utilisateur du cache lorsque l'utilisateur ferme un onglet qui le connecte à un poste de travail distant ou à une application publiée ou lorsqu'il ferme un onglet qui le connecte à la fenêtre de sélection des postes de travail et applications.

Lorsque cette fonctionnalité est désactivée (paramètre par défaut), les informations d'identification restent dans le cache.

Remarque Lorsque vous activez cette fonctionnalité, les informations d'identification sont également supprimées du cache lorsqu'un utilisateur actualise la page de sélection des postes de travail et applications ou la page de session distante, ou lorsqu'il exécute une commande d'URI dans l'onglet qui contient la session distante. Si le serveur présente un certificat auto-signé, les informations d'identification sont supprimées du cache après qu'un utilisateur démarre un poste de travail distant ou une application publiée et accepte le certificat lorsque l'avertissement de sécurité s'affiche.

Prérequis

Cette fonctionnalité requiert Horizon 7 version 7.0.2 ou ultérieure.

Procédure

- 1 Dans Horizon Administrator, sélectionnez **Configuration de View > Paramètres généraux** et cliquez sur **Modifier** dans le volet Général.
- 2 Cochez la case **Effacer les informations d'identification lorsqu'un onglet est fermé pour HTML Access**.
- 3 Cliquez sur **OK** pour enregistrer les modifications.

Vos modifications prennent effet immédiatement. Vous n'avez pas à redémarrer le Serveur de connexion.

Préparer des postes de travail, des pools et des batteries de serveurs

Avant que les utilisateurs finaux puissent accéder à un poste de travail distant ou à une application publiée, un administrateur Horizon doit configurer certains paramètres de pool et de batterie de serveurs et installer Horizon Agent sur les machines virtuelles de poste de travail 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

- Vérifiez que les composants Horizon respectent la configuration système requise pour HTML Access. Reportez-vous à la section [Configuration système requise pour HTML Access](#).
- Assurez-vous que le composant HTML Access est installé sur l'hôte ou les hôtes du Serveur de connexion, et que les pare-feu Windows sur les instances du Serveur de connexion et les serveurs de sécurité autorisent le trafic entrant sur le port TCP 8443. Reportez-vous à la section [Préparation du Serveur de connexion et des serveurs de sécurité](#).

- Si vous utilisez des pare-feu tiers, ajoutez une règle pour autoriser le trafic entrant à partir de serveurs Horizon Server sur le port TCP 22443 des machines virtuelles de poste de travail et des hôtes RDS dans le centre de données. Reportez-vous à la section [Règles de pare-feu pour un accès via un navigateur Web client](#).
- Vérifiez que la machine virtuelle que vous prévoyez d'utiliser comme source de poste de travail ou l'hôte RDS qui héberge des applications et des postes de travail publiés dispose d'un système d'exploitation pris en charge et de VMware Tools. Reportez-vous à la section [Configuration système requise pour HTML Access](#).
- Familiarisez-vous avec les procédures de création de pools et de batteries de serveurs et d'octroi de droits aux utilisateurs. Consultez les documents *Configuration des postes de travail virtuels dans Horizon 7* et *Configuration d'applications et de postes de travail publiés dans Horizon 7*.
- Pour vérifier que le poste de travail distant ou l'application publiée est accessible aux utilisateurs finaux, installez Horizon Client pour Windows sur un système client. Vous pouvez utiliser Horizon Client pour Windows pour tester la connexion avant de tenter de vous connecter à partir d'un navigateur Web. Pour les instructions d'installation, consultez le document *Guide d'installation et de configuration de VMware Horizon Client pour Windows*.
- Assurez-vous que vous disposez de l'un des navigateurs pris en charge pour accéder à un poste de travail distant ou à une application publiée. Reportez-vous à la section [Configuration système requise pour HTML Access](#).

Procédure

- 1 Pour les applications et les postes de travail publiés, utilisez Horizon 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.
- 2 Pour les pools de postes de travail virtuels, utilisez Horizon 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.
 - b Dans les paramètres du pool, vérifiez que la **Résolution maximale de chaque moniteur** est supérieure ou égale à **1 920x1 200**.
- 3 Une fois les pools créés, recomposés ou mis à niveau pour utiliser Horizon Agent avec l'option **Autoriser l'installation de HTML Access sur les postes de travail et les applications de cette batterie de serveurs** ou **HTML Access**, utilisez Horizon Client pour Windows pour vous connecter au poste de travail distant ou à l'application publiée.

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

- 4 Ouvrez un navigateur compatible et entrez une URL qui pointe vers votre instance du Serveur de connexion.

Par exemple :

```
https://horizon.mycompany.com
```

Vous devez inclure **https** dans l'URL.

- 5 Sur la page Web qui s'affiche, cliquez sur **VMware Horizon HTML Access** et connectez-vous comme vous le faites avec Horizon Client pour Windows.
- 6 Sur la page de sélection des postes de travail et applications qui s'affiche, cliquez sur une icône pour vous connecter.

Vous pouvez maintenant accéder à un poste de travail distant ou à une application publiée à partir d'un navigateur Web.

Suivant

Pour plus de sécurité, si vos stratégies de sécurité nécessitent que l'agent HTML Access du poste de travail distant utilise un certificat TLS d'une autorité de certification, reportez-vous à la section [Configurer les agents HTML Access pour utiliser les nouveaux certificats TLS](#).

Configuration requise pour la fonctionnalité de collaboration de session

Avec la fonctionnalité de collaboration de session, les utilisateurs peuvent inviter d'autres utilisateurs à rejoindre une session de poste de travail distant Windows existante. Pour prendre en charge la fonctionnalité de collaboration de session, votre déploiement d'Horizon doit satisfaire certaines exigences.

Collaborateurs de session

Pour rejoindre une session de collaboration, l'utilisateur doit disposer d'Horizon Client 4.7 ou version ultérieure pour Windows, Mac ou Linux installé sur le système client ou utiliser HTML Access 4.7 ou version ultérieure.

Postes de travail distants Windows

- Horizon Agent 7.4 ou version ultérieure doit être installé sur le poste de travail virtuel ou l'hôte RDS pour les postes de travail publiés.
- La fonctionnalité de collaboration de session doit être activée au niveau du pool de postes de travail ou de la batterie de serveurs. Pour plus d'informations sur l'activation de la fonctionnalité de collaboration de session pour des pools de postes de travail, consultez le document *Configuration des postes de travail virtuels dans Horizon 7*. Pour plus

d'informations sur l'activation de la fonctionnalité de collaboration de session pour une batterie de serveurs, consultez le document *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

Vous pouvez utiliser les paramètres de stratégie de groupe Horizon Agent pour configurer la fonctionnalité de collaboration de session. Pour plus d'informations, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

La fonctionnalité de collaboration de session ne prend pas en charge les sessions de poste de travail distant ou les sessions d'application publiée Linux.

Serveur de connexion La fonctionnalité de collaboration de session requiert que l'instance du Serveur de connexion utilise une licence d'entreprise.

Protocoles d'affichage VMware Blast

Configurer les agents HTML Access pour utiliser les nouveaux certificats TLS

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

Lors de l'installation de l'agent HTML Access sur des postes de travail distants, 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.

Remarque Dans le système d'exploitation invité 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 distant. Vous devez également définir une valeur de registre 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, configurez un certificat unique sur chaque poste de travail distant. 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. Cette approche entraîne des centaines, voire des milliers de postes de travail distants avec des certificats identiques.

Procédure

1 Ajouter le composant logiciel enfichable Certificat à MMC sur un poste de travail distant

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 distants sur lesquels l'agent HTML Access est installé.

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

Pour remplacer le certificat par défaut d'un 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 distant où l'agent HTML Access est installé.

3 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.

4 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 distant 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 distant

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 distants 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 invité Windows sur lequel l'agent HTML Access est installé.

Procédure

- 1 Sur le poste de travail distant, cliquez sur **Démarrer** et entrez `mmc.exe`.
- 2 Dans la fenêtre **MMC**, accédez à **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 **Compte d'ordinateur**, puis 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](#).

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

Pour remplacer le certificat par défaut d'un 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 distant où l'agent HTML Access est installé.

Prérequis

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

Procédure

- 1 Dans la fenêtre MMC sur le poste de travail distant, développez le nœud **Certificats (Ordinateur local)** et sélectionnez le dossier **Personnel**.
- 2 Dans le volet Actions, allez dans **Plus d'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 étendues**.
- 8 Cliquez sur **Suivant** et sur **Terminer**.

Le nouveau certificat s'affiche 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 Dans 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](#).

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](#).

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 distant, 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 racines 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 une autorité de certification intermédiaire a signé votre certificat de serveur, importez tous les certificats intermédiaires 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](#).

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 distant 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](#).

Procédure

- 1 Dans la fenêtre MMC sur le poste de travail distant 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 Windows.

Lorsqu'un utilisateur se connecte à un poste de travail distant 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/manmaster/man1/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.

Configuration d'iOS pour utiliser des certificats signés par une autorité de certification

Pour utiliser HTML Access sur des périphériques iOS, vous devez installer des certificats SSL signés par une autorité de certification plutôt que des certificats SSL par défaut générés par le Serveur de connexion View ou l'agent HTML Access.

Pour obtenir des instructions, consultez la rubrique « Configurer Horizon Client pour qu'iOS approuve les certificats racines et intermédiaires » dans le document *Installation de View*.

Utilisation d'un certificat signé par une autorité de certification avec Unified Access Gateway

Si vous utilisez un dispositif Unified Access Gateway plutôt qu'un Serveur de connexion ou un serveur de sécurité, vous devez installer un certificat signé par une autorité de certification qui a un autre nom de l'objet (SAN) configuré.

Si vous utilisez un certificat auto-signé ou un certificat signé par une autorité de certification qui ne dispose pas d'un SAN configuré, les utilisateurs reçoivent l'erreur « Votre connexion n'est pas privée » et ils ne peuvent pas se connecter avec HTML Access.

Remarque Si vous utilisez une instance du Serveur de connexion ou un serveur de sécurité, les utilisateurs peuvent toujours se connecter en cliquant sur le lien Continuer vers le site *adresse-ip* (non sécurisé).

Pour plus d'informations sur l'installation et la configuration de certificats pour Horizon 7, consultez le document *Installation d'Horizon 7*. Pour plus d'informations sur la configuration d'agents HTML Access pour utiliser des certificats TLS, reportez-vous à la section [Configurer les agents HTML Access pour utiliser les nouveaux certificats TLS](#).

Mise à niveau du logiciel HTML Access

Pour la plupart des versions de HTML Access, la mise à niveau implique simplement de mettre à niveau des Serveurs de connexion et View Agent.

Lorsque vous effectuez la mise à niveau de HTML Access, vérifiez que la version correspondante du Serveur de connexion View est installée sur toutes les instances dans un groupe répliqué.

Lorsque vous mettez à niveau le serveur de connexion, HTML Access est automatiquement installé ou mis à niveau.

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 dans la liste.

Désinstaller le composant HTML Access du Serveur de connexion

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

Procédure

- 1 Sur l'instance du Serveur de connexion sur laquelle HTML Access est installé, ouvrez l'applet Désinstaller un programme du Panneau de configuration Windows.
- 2 Sélectionnez **VMware Horizon 7 HTML Access** et cliquez sur **Désinstaller**.
- 3 (Facultatif) Pour le pare-feu Windows de l'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 l'instance du Serveur de connexion.

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 Horizon 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 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 peut s'inscrire lors de l'exécution de l'Assistant d'installation du Serveur de connexion ou définir une option dans Horizon Administrator après l'installation.

Tableau 1-2. 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	4.8.0-build_number

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

Description	Nom de champ	Ce champ reste-t-il anonyme ?	Exemple
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 ■ Linux armv81 (pour la prise en charge de Chrome pour Android)
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/13.10586
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), ■ 44.0 (pour Firefox) ■ 13.10586 (pour Edge)
Implémentation de base du navigateur	<browser-core>	Non	Exemples comprenant les valeurs suivantes : <ul style="list-style-type: none"> ■ Chrome ■ Safari ■ Firefox ■ 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](#)
- [Utiliser des URI pour configurer des clients Web HTML Access](#)
- [Paramètres de stratégie de groupe de HTML Access](#)

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 du portail Web affiche à la fois une icône pour télécharger et installer le client Horizon Client natif et une icône pour se connecter via HTML Access. Le lien de téléchargement utilisé est déterminé à partir des valeurs par défaut définies dans le fichier `portal-links-html-access.properties`.

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 du portail pour qu'elle pointe vers une URL de téléchargement différente en modifiant le contenu du fichier `portal-links-html-access.properties`. Si ce fichier n'est pas disponible ou s'il est vide, et que le fichier `oslinks.properties` existe, le fichier `oslinks.properties` est utilisé pour déterminer la valeur de lien du fichier du programme d'installation.

Le fichier `oslinks.properties` est installé dans le dossier *répertoire-installation\VMware\VMware View\Server\broker\webapps\portal\WEB-INF*. Si ce fichier est manquant lors de la session HTML Access, le lien de téléchargement dirigera les utilisateurs vers <https://www.vmware.com/go/viewclients> par défaut. Le fichier contient les valeurs par défaut suivantes :

```
link.download=https://www.vmware.com/go/viewclients
# download Links for particular platforms
link.win32=https://www.vmware.com/go/viewclients#win32
link.win64=https://www.vmware.com/go/viewclients#win64
link.linux32=https://www.vmware.com/go/viewclients#linux32
link.linux64=https://www.vmware.com/go/viewclients#linux64
link.mac=https://www.vmware.com/go/viewclients#mac
link.ios=https://itunes.apple.com/us/app/vmware-view-for-ipad/id417993697
link.android=https://play.google.com/store/apps/details?id=com.vmware.view.client.android
link.chromeos=https://chrome.google.com/webstore/detail/vmware-horizonclient/
pckbpdplfajmgaipjlfamclkinbjdnma
link.winmobile=https://www.microsoft.com/en-us/store/p/vmware-horizon-client/9nblggh51p19
```

Vous pouvez créer des liens de programme d'installation pour des systèmes d'exploitation clients spécifiques dans le fichier `portal-links-html-access.properties` ou `oslinks.properties`. 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 ou Linux, vous pouvez créer des liens distincts pour les programmes d'installation 32 et 64 bits.

Important Si vous avez mis à niveau le 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 du Serveur de connexion 6.0 ou version ultérieure. Avec Horizon 6 ou version ultérieure, le composant HTML Access est installé automatiquement pendant une mise à niveau du Serveur de connexion.

Si vous avez déjà installé le composant HTML Access séparément de Horizon 7 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 du Serveur de connexion, 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.

Si le fichier `portal-links-html-access.properties` n'existe pas et que le fichier `oslinks.properties` existe, ouvrez le fichier *<répertoire-installation>\VMware\VMware View\Server\broker\webapps\portal\WEB-INF\oslinks.properties* pour modifier les URL à utiliser pour télécharger des fichiers de programme d'installation spécifiques.

Remarque Pour Horizon 7 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`.

Remarque Le fichier `oslinks.properties` ne peut être utilisé que pour configurer les liens vers les fichiers de programme d'installation spécifiques. Il ne prend pas en charge les autres options répertoriées ci-dessous.

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 downloads, situé sous le répertoire C:\Program Files\VMware\VMware View\Server\broker\webapps\ sur le Serveur de connexion, comme décrit à l'étape suivante.</p> <ul style="list-style-type: none"> ■ Lien général pour télécharger le programme d'installation : <div>link.download=https://server/downloads</div> ■ Programme d'installation de Windows 32 bits : <div>link.win32=https://server/downloads/VMware-Horizon-Client-x86-build#.exe</div> ■ Programme d'installation de Windows 64 bits : <div>link.win64=https://server/downloads/VMware-Horizon-Client-x86_64-build#.exe</div> ■ Programme d'installation de Windows Phone : <div>link.winmobile=https://server/downloads/VMware-Horizon-Client-build#.appx</div> ■ Programme d'installation de Linux 32 bits : <div>link.linux32=https://server/downloads/VMware-Horizon-Client-build#.x86.bundle</div> ■ Programme d'installation de Linux 64 bits : <div>link.linux64=https://server/downloads/VMware-Horizon-Client-build#.x64.bundle</div> ■ Programme d'installation de Mac OS X : <div>link.mac=https://server/downloads/VMware-Horizon-Client-build#.dmg</div> ■ Programme d'installation d'iOS : <div>link.ios=https://server/downloads/VMware-Horizon-Client-iPhoneOS-build#.ipa</div> ■ Programme d'installation d'Android : <div>link.android=https://server/downloads/VMware-Horizon-Client-AndroidOS-build#.apk</div>

Option	Paramètre propriété
	<ul style="list-style-type: none"> Programme d'installation de Chrome OS : <pre>link.chromeos=https://server/downloads/VMware-Horizon-Client-ChromeOS-build#.apk</pre>
Changer l'URL du lien de l'aide sur la page de connexion	<pre>link.help</pre> <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>

- 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` ou `oslinks.properties` à l'étape précédente. Par exemple, pour placer les fichiers dans un répertoire `downloads` sur l'hôte du Serveur de connexion, 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`.

- Redémarrez le service du composant Web Horizon.

Utiliser des URI pour configurer des clients Web HTML Access

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

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

- Adresse du Serveur de connexion View
- Numéro de port pour le Serveur de connexion View
- Nom d'utilisateur Active Directory
- 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 ou de l'application

- 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 un utilisateur, un poste de travail ou une application et des actions ou options de configuration.

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

action

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

Valeur	Description
browse	Affiche une liste des postes de travail et applications disponibles hébergés sur le serveur spécifié. Il ne vous est pas demandé de spécifier un poste de travail ou une application pour l'utilisation de cette action.
start-session	Démarre l'application ou le poste de travail spécifié. Si aucune requête d'action n'est fournie et que le nom du poste de travail ou de l'application est fourni, start-session est l'action par défaut.
reset	Éteint puis redémarre le poste de travail spécifié. Les données non enregistrées sont perdues. La réinitialisation d'un poste de travail distant équivaut à appuyer sur le bouton Réinitialiser d'un ordinateur physique. Cette action n'est pas valide pour une application.
logoff	Déconnecte l'utilisateur du système d'exploitation invité sur le poste de travail distant. Cette action n'est pas valide pour une application.
restart	Arrête et redémarre le poste de travail principal lorsque l'utilisateur confirme la demande d'opération de redémarrage. Cette action n'est pas valide pour une application.

applicationId

Nom affiché de l'application. Le nom complet est celui spécifié dans Horizon Administrator lors de la création du pool d'applications. Si le nom complet contient un espace, le navigateur utilise %20 pour représenter l'espace.

args

Spécifie des arguments de ligne de commande à ajouter au lancement d'applications distantes. Utilisez la syntaxe `args=`*value*, où *value* est une chaîne. Utilisez l'encodage avec pourcentage pour les caractères suivants :

- Pour un deux-points (:), utilisez %3A
- Pour une barre oblique inversée (\), utilisez %5C
- Pour un espace (), utilisez %20

- Pour un guillemet double ("), utilisez %22

Par exemple, pour spécifier le nom de fichier "My new file.txt" pour l'application Notepad++, utilisez %22My%20new%20file.txt%22.

desktopId

Nom affiché du poste de travail. Le nom complet est celui spécifié dans View Administrator lorsque le pool de postes de travail a été créé. Si le nom complet contient un espace, le navigateur utilise %20 pour représenter l'espace.

domainName

Nom de domaine NETBIOS associé à l'utilisateur qui se connecte à l'application ou au poste de travail distant. Utilisez par exemple monentreprise plutôt que monentreprise.com.

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.

userName

Utilisateur Active Directory qui se connecte à l'application ou au poste de travail distant. Le nom d'utilisateur peut utiliser l'un des formats suivants :

- *userName*
- *domainName%5CuserName*
- nom d'utilisateur principal (UPN), c'est-à-dire *userName@domainName*

**unauthenticatedAccess
Enabled**

Si cette option est définie sur **true**, la fonctionnalité Accès non authentifié est activée par défaut. Le HTML Access Web client est lancé et un compte d'utilisateur anonyme s'affiche. Exemple de syntaxe :
unauthenticatedAccessEnabled=true.

**unauthenticatedAccess
Account**

Définit le compte à utiliser si la fonctionnalité Accès non authentifié est activée. Si la fonctionnalité Accès non authentifié est désactivée, cette requête est ignorée. Exemple de syntaxe utilisant le compte d'utilisateur **anonymous1** : **unauthenticatedAccessAccount=anonymous1**

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, ouvrir 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. Les requêtes ne sont pas sensibles à la casse. Par exemple, vous pouvez utiliser **domainName** ou **domainname**.

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

Le HTML Access Web client est lancé et se connecte au serveur `horizon.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://horizon.mycompany.com/?userName=finance%5Cfred`

Le HTML Access Web client est lancé et se connecte au serveur `horizon.mycompany.com`. Dans la boîte de dialogue de connexion, la zone de texte **Nom d'utilisateur** contient le nom **finance\fred**. L'utilisateur doit fournir uniquement un mot de passe.

3 `https://horizon.mycompany.com/?userName=fred@finance`

Le HTML Access Web client est lancé et se connecte au serveur `horizon.mycompany.com`. Dans la boîte de dialogue de connexion, la zone de texte **Nom d'utilisateur** contient le nom **fred@finance**. L'utilisateur doit fournir uniquement un mot de passe.

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

Le HTML Access Web client est lancé et se connecte au serveur `horizon.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.

5 `https://horizon.mycompany.com/?applicationId=Notepad&action=start-session`

Le HTML Access Web client est lancé et se connecte au serveur `horizon.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, l'application Bloc-notes est lancée.

6 `https://horizon.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 le Serveur de connexion. (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.

7

```
https://horizon.mycompany.com/?applicationId=Primary%20Application&desktopId=Primary%20Desktop
```

Cet URI spécifie à la fois une application et un poste de travail. Lorsque vous spécifiez à la fois une application et un poste de travail, seul le poste de travail est lancé.

8

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

Le client Web HTML Access est lancé et se connecte au serveur `horizon.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 Horizon a autorisé les utilisateurs finaux à réinitialiser leurs machines.

9

```
https://horizon.mycompany.com/?My%20Notepad++?args=%22My%20new%20file.txt%22
```

Ouvre My Notepad++ sur le serveur `horizon.mycompany.com` et transmet l'argument `My new file.txt` dans la commande de lancement d'application. Le nom de fichier est entre guillemets, car il contient des espaces.

10

```
https://horizon.mycompany.com/?Notepad++%2012?args=a.txt%20b.txt
```

Ouvre Notepad++ 12 sur le serveur `horizon.mycompany.com` et transmet l'argument `a.txt b.txt` dans la commande de lancement d'application. Comme l'argument n'est pas entre guillemets double, un espace sépare les noms de fichier et les deux fichiers sont ouverts séparément dans Notepad++.

Remarque Les applications peuvent différer dans leur manière d'utiliser des arguments de ligne de commande. Par exemple, si vous transmettez l'argument `a.txt b.txt` à WordPad, WordPad n'ouvre qu'un seul fichier, `a.txt`.

11

```
https://horizon.mycompany.com/?desktopId=Primary%20Desktop&action=restart
```

Le HTML Access Web client est lancé et se connecte au serveur `horizon.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 redémarrage pour Poste de travail principal.

Remarque Cette action n'est disponible que si l'administrateur Horizon a autorisé les utilisateurs finaux à redémarrer leurs machines.

12

```
https://horizon.mycompany.com/?
unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous_user1
```

Le HTML Access Web client est lancé et se connecte au serveur `horizon.mycompany.com` en utilisant le compte **anonymous_user1**

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

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

</body>
</html>
```

Paramètres de stratégie de groupe de HTML Access

HTML Access utilise le protocole VMware Blast. Vous configurez les stratégies de groupe pour HTML Access en configurant les stratégies de groupe pour le protocole VMware Blast.

Pour plus d'informations, consultez les rubriques « Configuration des stratégies pour les pools de postes de travail et d'applications » et « Paramètres de stratégie VMware Blast » dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

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](#)
- [Internationalisation](#)
- [Connexion à une application ou un poste de travail distant](#)
- [Se connecter à un serveur en mode Workspace ONE](#)
- [Utiliser l'accès non authentifié pour se connecter à des applications publiées](#)
- [Combinaisons de touches de raccourci](#)
- [Claviers internationaux](#)
- [Résolution de l'écran](#)
- [Autoriser le décodage H.264](#)
- [Définition du fuseau horaire](#)
- [Utilisation de la barre latérale](#)
- [Utiliser plusieurs moniteurs](#)
- [Utilisation de la synchronisation DPI](#)
- [Audio](#)
- [Copier et coller du texte](#)
- [Transférer des fichiers entre le client et un poste de travail distant](#)
- [Utilisation de la fonctionnalité Audio/Vidéo en temps réel pour webcams et microphones](#)
- [Utilisation de la fonctionnalité de collaboration de session](#)
- [Fermer une session ou se déconnecter](#)
- [Réinitialiser un poste de travail distant ou des applications publiées](#)
- [Redémarrer un poste de travail distant](#)

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	Poste de travail Windows Server 2016
RSA SecurID ou RADIUS	X	X	X	X	X	X
Authentification unique	X	X	X	X	X	X
Protocole d'affichage RDP						
Protocole d'affichage PCoIP						
Protocole d'affichage VMware Blast	X	X	X	X	X	X
redirection USB						
Audio/Vidéo en temps réel (RTAV)	X	X	X	X	X	X
Wyse MMR						
Redirection multimédia (MMR) Windows Media						
Impression virtuelle						
Impression basée sur l'emplacement	X	X	X	X	X	X
Cartes à puce						
Plusieurs écrans	X	X	X	X	X	X

Pour une description de ces fonctionnalités et de leurs limites, consultez le document *Planification de l'architecture de Horizon 7*.

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. Un hôte RDS peut être une machine physique ou une machine virtuelle.

Remarque Le tableau suivant contient des lignes uniquement pour les fonctionnalités disponibles depuis 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 HTML Access sur les hôtes RDS avec View Agent 6.1.1 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure, installé

Fonction	Hôte RDS Windows Server 2008 R2	Hôte RDS Windows Server 2012 ou 2012 R2	Windows Server 2016
RSA SecurID ou RADIUS	X	X	Horizon Agent 7.0.2 et versions ultérieures
Authentification unique	X	X	Horizon Agent 7.0.2 et versions ultérieures
Protocole d'affichage VMware Blast	X	X	Horizon Agent 7.0.2 et versions ultérieures
Impression basée sur l'emplacement	X (machine virtuelle uniquement)	X (machine virtuelle uniquement)	Horizon Agent 7.0.2 et versions ultérieures (machine virtuelle uniquement)
Audio/Vidéo en temps réel (RTAV)	Horizon Agent 7.0.2 et versions ultérieures	Horizon Agent 7.0.2 et versions ultérieures	Horizon Agent 7.0.3 et versions ultérieures
Plusieurs moniteurs (pour les postes de travail basés sur la session uniquement)	X	X	X

Pour savoir quelles éditions de chaque système d'exploitation invité et quels Service Packs sont pris en charge, consultez la section « Systèmes d'exploitation pris en charge pour Horizon Agent » du document *Installation de View*.

Internationalisation

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

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](#).

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

- Procurez-vous des informations d'identification de connexion, 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.

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

Les connexions au Serveur de connexion utilisent toujours SSL. Le port par défaut pour les connexions SSL est 443. Si le Serveur de connexion n'est pas configuré pour utiliser le port par défaut, utilisez le format indiqué dans cet exemple : **horizon.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 (Facultatif) Cochez la case **Cliquez ici pour ignorer cet écran et toujours utiliser HTML Access**.

Votre sélection est stockée dans le stockage local pour le navigateur que vous utilisez actuellement. La prochaine fois que vous entrerez l'URL de l'instance du Serveur de connexion à partir du même navigateur et sur la même machine cliente, vous serez directement dirigé vers l'écran de connexion. Si vous utilisez un autre navigateur sur la même machine cliente ou si vous utilisez le même navigateur sur une autre machine cliente, c'est le portail Web VMware Horizon qui s'affiche. Si vous voulez que le portail Web VMware Horizon s'affiche, effacez le cache de votre navigateur.

- 3 Cliquez sur l'icône **VMware Horizon HTML Access**.
- 4 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.

- 5 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.

- 6 Dans la boîte de dialogue Connexion, entrez vos informations d'identification de connexion.
 - a Dans la zone de texte Nom d'utilisateur, entrez votre nom d'utilisateur Active Directory au format *nomutilisateur*, *domaine\nomutilisateur* ou *nomutilisateur@domaine*.

Si la zone de texte Domaine est désactivée, vous devez utiliser le format *domaine\nomutilisateur* ou *nomutilisateur@domaine*.
 - b Entrez votre mot de passe.
 - c (Facultatif) Si la zone de texte Domaine est activée, sélectionnez un nom de domaine, s'il n'est pas déjà correctement rempli.

Remarque Pour annuler le processus de connexion, cliquez sur **Annuler** avant la fin du processus.

- 7 (Facultatif) Si vous devez définir manuellement le fuseau horaire utilisé dans l'application ou le poste de travail distant, cliquez sur le bouton de la barre d'outils **Paramètres** dans le coin supérieur droit de l'écran du sélecteur de postes de travail et d'applications. Désactivez l'option **Définir le fuseau horaire automatiquement** et sélectionnez l'un des fuseaux horaires dans le menu déroulant. Reportez-vous à [Définition du fuseau horaire](#).
- 8 (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.
- 9 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](#).

Faire confiance à un certificat racine auto-signé

Parfois, lorsque vous vous connectez à un poste de travail distant ou une application pour la première fois, le navigateur peut vous inviter à accepter le certificat auto-signé que la machine distante utilise. Vous devez approuver le certificat pour pouvoir vous connecter au poste de travail distant ou à l'application publiée.

La plupart des navigateurs vous permettent d'approuver de façon permanente le certificat auto-signé. Si vous approuvez 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 le 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 système. Par exemple, dans 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 système.

- 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**.

Le poste de travail distant ou l'application publiée démarre.

Se connecter à un serveur en mode Workspace ONE

À partir d'Horizon 7 version 7.2, un administrateur Horizon peut activer le mode Workspace ONE sur une instance du Serveur de connexion.

Lorsque le mode Workspace ONE est activé, vous pouvez vous connecter au serveur uniquement via le portail Web Workspace ONE. Vous êtes redirigé vers le portail Web Workspace ONE lorsque vous tentez de vous connecter au serveur via HTML Access. Après vous être connecté au serveur via le portail Web Workspace ONE, vous pouvez démarrer des postes de travail distants et des applications publiées uniquement via le portail Web Workspace ONE.

La barre latérale n'affiche pas tous les droits lorsque le mode Workspace ONE est activé. Elle n'affiche que les applications publiées et les postes de travail en cours d'exécution.

Lorsque le mode Workspace ONE est activé, vous pouvez rencontrer les problèmes suivants.

- Impossibilité de vous connecter au serveur via HTML Access. Il est possible que vous ne puissiez pas atteindre le serveur, ou qu'un message s'affiche indiquant que le serveur attend de recevoir vos informations d'identification de connexion en provenance d'un autre serveur ou application.
- Après avoir démarré un poste de travail distant ou une application publiée via le portail Web Workspace ONE, vous ne pouvez pas voir ou démarrer vos postes de travail distants ou vos applications publiées dans HTML Access.

Utiliser l'accès non authentifié pour se connecter à des applications publiées

Un administrateur Horizon peut utiliser la fonctionnalité Accès non authentifié pour créer des utilisateurs avec un accès non authentifié et autoriser ces utilisateurs à accéder à des applications publiées sur une instance du Serveur de connexion. Les utilisateurs disposant d'un accès non authentifié peuvent se connecter au serveur de façon anonyme pour se connecter à leurs applications publiées.

Prérequis

- Effectuez les tâches administratives décrites dans [Préparation du Serveur de connexion et des serveurs de sécurité](#).
- Configurez des utilisateurs avec un accès non authentifié sur l'instance du Serveur de connexion. Pour plus d'informations, consultez « Fournir un accès non authentifié pour des applications publiées » dans le document *Administration d'Horizon 7*.

Procédure

- 1 Pour vous connecter à l'instance du Serveur de connexion sur laquelle vous disposez d'un accès non authentifié à des applications publiées, ouvrez un navigateur et utilisez l'une des syntaxes d'URI suivantes.
 - `https://authority-part?unauthenticatedAccessEnabled=true`

- `https://authority-part?unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous_account`

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*. *anonymous_account* est le compte d'utilisateur Accès non authentifié créé pour vous connecter de façon anonyme.

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

- 2 (Facultatif) Si vous n'avez pas spécifié la requête `unauthenticatedAccessAccount`, sélectionnez un compte d'utilisateur Accès non authentifié dans le menu déroulant **Compte d'utilisateur**, si nécessaire, puis cliquez sur **Envoyer**.

Si un seul compte d'utilisateur Accès non authentifié est disponible, le compte d'utilisateur est sélectionné par défaut.

La fenêtre de sélection des applications s'affiche.

- 3 Cliquez sur l'icône de l'application publiée à laquelle vous voulez accéder.

L'application publiée s'affiche dans votre navigateur. Une barre latérale de navigation est également disponible. Vous pouvez cliquer sur l'onglet sur le côté gauche du navigateur pour afficher la barre latérale. Vous pouvez utiliser la barre latérale pour accéder à d'autres applications publiées, afficher la fenêtre **Paramètres**, copier et coller du texte, etc.

Remarque Vous ne pouvez pas vous reconnecter à des sessions d'application non authentifiées. Lorsque vous vous déconnectez du client, l'hôte RDS ferme la session d'utilisateur local automatiquement.

Combinaisons de touches de raccourci

Certaines combinaisons de touches ne peuvent pas être envoyées à un poste de travail distant ou à une application publiée, indépendamment de la langue que vous utilisez.

Les navigateurs Web permettent à certaines touches et combinaisons de touches d'être envoyées au système 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 fonctionnalité, 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 système client 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** en haut de la barre latérale.

- Verrouillage majuscule+*modifier_key* (telle que Alt ou Shift)
- Touches de fonction sur un Chromebook
- Combinaisons de touches Windows

Si vous activez la touche Windows pour des postes de travail distants, les combinaisons de touches Windows suivantes fonctionnent sur les postes de travail distants. Pour activer cette touche, cliquez sur le bouton de la barre d'outils **Ouvrir la fenêtre des paramètres** sur la barre latérale et activez **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 publiées. Ces combinaisons de touches fonctionnent pour les postes de travail distants et les postes de travail publiés Windows Server 2008 R2, Windows Server 2012 R2 et Windows Server 2016.

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 distants 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 et Windows Server 2016

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.	

Tableau 3-3. Raccourcis de touche Windows pour les postes de travail distants Windows 10 et Windows Server 2016 (suite)

Clés	Action	Limites
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 distant.	
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 distant.	Ne fonctionne pas dans Safari.
Win+Alt+Num	Ouvrir le poste de travail distant 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 Safari.
Touche Windows	Afficher ou masquer la fenêtre Démarrer.	
Win+B	Sélectionner la zone de notification.	
Win+C	Ouvrir le volet Icônes.	
Win+D	Afficher et masquer le poste de travail distant.	Ne fonctionne pas dans Safari. Appuyer sur Commande-D sur un 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	Pour rechercher partout ou dans l'application ouverte, si l'application prend en charge la recherche d'application, ouvrir l'icône Rechercher.	
Win+R	Ouvrir la boîte de dialogue Exécuter.	
Win+S	Pour rechercher dans Windows et sur le Web, ouvrir l'icône Rechercher.	
Win+X	Ouvrir le menu Lien rapide .	
Win+Z	Afficher les commandes disponibles dans l'application.	

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+, (virgule)	Afficher temporairement le poste de travail distant, tant que vous continuez à appuyer sur les touches.	Ne fonctionne pas sur les systèmes d'exploitation Windows 2012 R2.
Win+Pause	Afficher la boîte de dialogue Propriétés système.	Les Chromebook et les Mac n'ont pas de touche Pause.
Win+Maj+M	Restaurer les fenêtres réduites sur le poste de travail distant.	Ne fonctionne pas dans Safari. Appuyer sur Commande-D sur un Mac.
Win+Alt+Num	Ouvrir le poste de travail distant 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 distant.	Ne fonctionne pas sur un Chromebook.
Win+Flèche gauche	Agrandir la fenêtre de l'application ou du poste de travail distant 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 distant vers le côté droit de l'écran.	Ne fonctionne pas sur un Chromebook.
Win+Origine	Réduire tout, sauf la fenêtre de poste de travail distant active (restaure toutes les fenêtres lorsque vous appuyez sur Win+Origine une seconde fois).	Ne fonctionne pas dans les navigateurs Safari.
Win+Maj+Flèche vers le haut	Étirer la fenêtre du poste de travail distant 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 distant 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 distant 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.	Les Chromebook et les Mac n'ont pas de touche Pause.
Win+D	Afficher et masquer le poste de travail distant.	Ne fonctionne pas dans Safari. Appuyer sur Commande-D sur un Mac.
Win+M	Réduire toutes les fenêtres.	
Win+E	Ouvrir le dossier Ordinateur.	

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

Clés	Action	Limites
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 distant vers le côté gauche de la fenêtre.	Ne fonctionne pas sur un Chromebook.
Win+Flèche droite	Agrandir la fenêtre de l'application ou du poste de travail distant vers le côté droit de la fenêtre.	Ne fonctionne pas sur un Chromebook.
Win+Origine	Réduire tout, sauf la fenêtre de poste de travail distant active.	Ne fonctionne pas dans Safari.
Win+Maj+Flèche vers le haut	Étirer la fenêtre du poste de travail distant vers le haut et le bas de l'écran.	Ne fonctionne pas sur un Chromebook.
Win+G	Parcourir les gadgets de poste de travail distant 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.

Lorsque les méthodes d'entrée et les paramètres régionaux corrects sont installés, vous pouvez entrer des caractères pour les langues suivantes : anglais, japonais, français, allemand, chinois simplifié, chinois traditionnel, coréen et espagnol.

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

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

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 de travail distant ?
Coréen	Coréen	Mode de saisie en anglais	Coréen	Oui
Espagnol	Espagnol	Non	Espagnol	Non

Résolution de l'écran

Si Horizon 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 s'affiche uniquement dans la fenêtre Paramètres si vous utilisez un écran haute résolution ou un écran normal qui utilise une échelle supérieure à 100 %.)

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.

Lorsque le rendu 3D est activé, le nombre maximal de moniteurs est de 1 et la résolution maximale est de 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 d'affichage VMware 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 Horizon 7*.

Autoriser le décodage H.264

Lorsque vous utilisez un navigateur Chrome, vous pouvez autoriser le décodage H.264 dans le client pour des sessions de poste de travail distant et d'application publiée.

Lorsque vous autorisez le décodage H.264, le client HTML Access l'utilise si l'agent prend en charge le codage H.264. Si l'agent ne prend pas en charge le codage H.264, le client HTML Access utilise le décodage JPEG/PNG.

Si vous êtes connecté à un poste de travail distant ou à une application publiée, vous pouvez autoriser le décodage H.264 en activant l'option **Autoriser le décodage H.264** dans la fenêtre **Paramètres**, qui est disponible dans la barre latérale. Vous devez vous déconnecter et vous reconnecter au poste de travail distant ou à l'application publiée pour que le nouveau paramètre prenne effet.

Si vous n'êtes pas connecté à un poste de travail distant ou à une application publiée, vous pouvez cliquer sur le bouton de la barre d'outils **Paramètres** dans le coin supérieur droit de la fenêtre de sélection des postes de travail et des applications et activer l'option **Autoriser le décodage H.264** dans la fenêtre **Paramètres**. Le nouveau paramètre prend effet pour toutes les sessions qui sont connectées une fois le paramètre modifié.

Définition du fuseau horaire

Le fuseau horaire qu'utilise un poste de travail distant ou une application publiée est défini automatiquement sur le fuseau horaire de votre système local.

Lorsque vous utilisez le client HTML Access, si le fuseau horaire ne peut pas être déterminé correctement en raison de certaines stratégies d'heure d'été, vous devrez peut-être le définir manuellement.

Pour définir manuellement les informations correctes de fuseau horaire à utiliser avant de vous connecter à un poste de travail distant ou à une application publiée, cliquez sur le bouton de la barre d'outils **Paramètres** dans le coin supérieur droit de la fenêtre de sélection des postes de travail et des applications. Désactivez l'option **Définir le fuseau horaire automatiquement** dans la fenêtre **Paramètres** et sélectionnez l'un des fuseaux horaires dans le menu déroulant.

La valeur sélectionnée est enregistrée comme fuseau horaire préféré à utiliser lors de la connexion à un poste de travail distant ou à une application publiée.

Si vous êtes déjà connecté à un poste de travail distant ou à une application publiée, revenez à la fenêtre de sélection des postes de travail et des applications pour modifier le paramètre de fuseau horaire actuel.

L'option **Définir le fuseau horaire automatiquement** n'est pas disponible dans la fenêtre **Paramètres** accessible depuis la barre latérale.

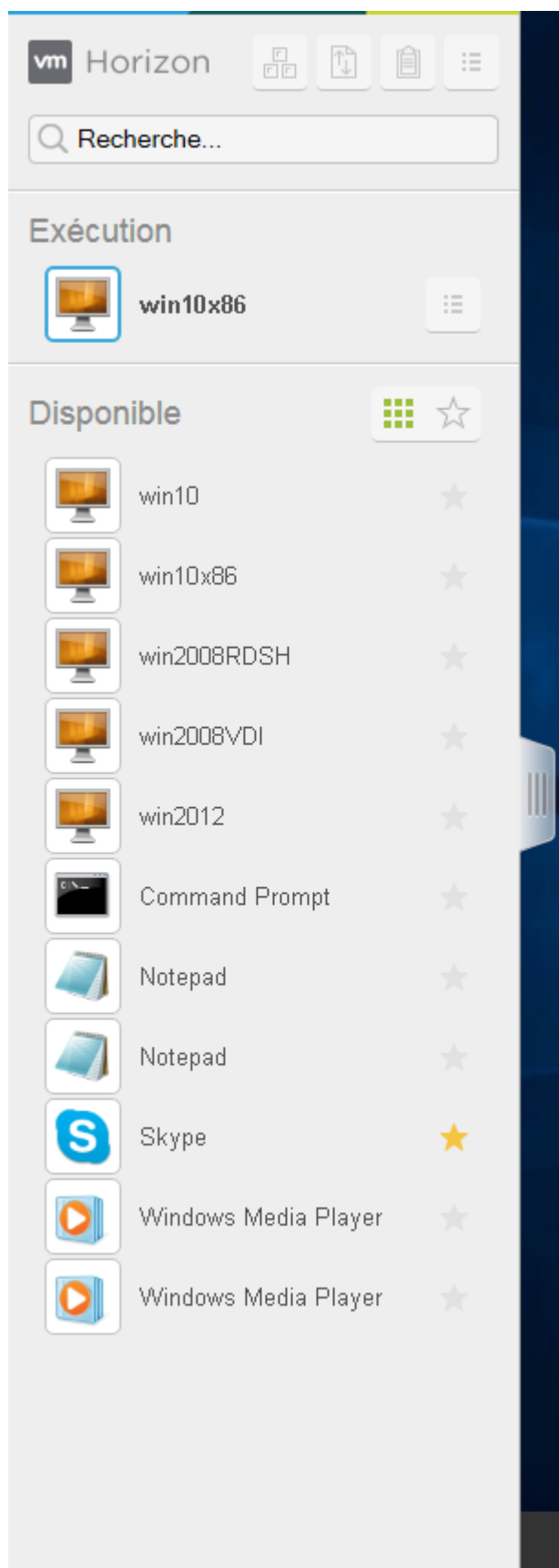
Remarque Lorsque vous utilisez le navigateur Chrome sur un périphérique Android, si l'option **Définir le fuseau horaire automatiquement** est définie sur **true** et que vous modifiez le fuseau horaire du système Android, le nouveau fuseau horaire n'est pas synchronisé automatiquement avec le poste de travail distant. Ce problème est une limite de Chrome sur le système Android. Vous devez redémarrer le périphérique Android et le navigateur Chrome pour synchroniser le fuseau horaire sélectionné.

Utilisation de la barre latérale

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

La barre latérale s'affiche sur le côté gauche de la fenêtre de l'application publiée ou du poste de travail distant. Pour afficher ou masquer la barre latérale, cliquez sur l'onglet de 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 démarrez un poste de travail distant ou une application publiée



Pour afficher la liste des documents ouverts par une application publiée en cours d'exécution, cliquez sur la flèche de développement en regard de l'application publiée dans la liste **Exécution**.

Remarque Si deux documents sont ouverts à partir d'applications publiées semblables, mais distinctes, hébergées sur deux serveurs différents, l'application publiée apparaît deux fois dans la liste **Exécution** dans la barre latérale.

Vous pouvez effectuer de nombreuses actions à partir de la barre latérale.

Tableau 3-7. Actions de la barre latérale

Action	Procédure
Afficher la barre latérale	Lorsqu'une application publiée ou un poste de travail distant est 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 publiée ou du poste de travail distant.
Masquer la barre latérale	Cliquez sur l'onglet de la barre latérale.
Démarrer une application publiée ou un poste de travail distant	Cliquez sur le nom d'une application publiée ou d'un poste de travail distant dans la liste Disponible dans la barre latérale. Les postes de travail distants sont répertoriés en premier.
Rechercher une application publiée 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 publiée ou du poste de travail distant. ■ Pour démarrer une application publiée ou un poste de travail distant, cliquez sur son nom 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 publiées et de postes de travail distants favoris	Cliquez sur l'étoile grise en regard du nom du poste de travail distant ou de l'application publiée 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) en regard de Disponible pour afficher une liste des favoris.
Basculer entre des applications publiées ou des postes de travail distants	Cliquez sur le nom d'une application publiée ou d'un poste de travail distant dans la liste Exécution dans la barre latérale.
Fermer un poste de travail distant en cours d'exécution	<p>Cliquez sur le bouton Ouvrir le menu en regard du nom du poste de travail distant dans la liste Exécution dans la barre latérale, puis sélectionnez une action.</p> <ul style="list-style-type: none"> ■ Sélectionnez Fermer pour vous déconnecter du poste de travail distant sans fermer votre session sur son système d'exploitation. Un administrateur Horizon peut configurer un poste de travail distant pour fermer la session automatiquement lors de la déconnexion. Dans ce cas, les modifications non enregistrées dans les applications ouvertes sont perdues. ■ Sélectionnez Fermer la session pour fermer votre session sur le système d'exploitation et vous déconnecter du poste de travail distant. Les modifications non enregistrées dans les applications ouvertes sont perdues.
Fermer une application publiée en cours d'exécution	<p>Cliquez sur le X en regard du nom de fichier sous le nom de l'application publiée dans la liste Exécution sur la barre latérale. Cliquez sur le X en regard du nom de l'application publiée pour quitter l'application publiée et fermer tous les fichiers ouverts pour cette application.</p> <p>Vous êtes invité à enregistrer les modifications apportées aux fichiers.</p>

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

Action	Procédure
Réinitialiser un poste de travail distant	Cliquez sur le bouton Ouvrir le menu en regard du nom du poste de travail distant dans la liste Exécution dans la barre latérale, puis sélectionnez Réinitialiser . Les fichiers ouverts sur le poste de travail distant sont fermés sans être enregistrés. Vous pouvez réinitialiser un poste de travail distant uniquement si un administrateur Horizon a activé cette fonctionnalité.
Redémarrer un poste de travail distant	Cliquez sur le bouton Ouvrir le menu en regard du nom du poste de travail distant dans la liste Exécution dans la barre latérale, puis sélectionnez Redémarrer . En général, le système d'exploitation du poste de travail distant demande d'enregistrer toutes les données non enregistrées avant de redémarrer. Vous pouvez redémarrer un poste de travail distant uniquement si un administrateur Horizon a activé cette fonctionnalité.
Réinitialiser toutes les applications publiées en cours d'exécution	Cliquez sur le bouton de la barre d'outils Ouvrir le menu en haut de la barre latérale, puis cliquez sur Paramètres et sur Réinitialisez toutes les applications en cours d'exécution . Toutes les modifications non enregistrées sont perdues.
Utiliser des combinaisons de touches qui incluent la touche Windows	Cliquez sur le bouton de la barre d'outils Ouvrir le menu en haut de la barre latérale, cliquez sur Paramètres 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 .
Envoyer Ctrl+Alt+Delete à la zone de travail actuelle	Cliquez sur le bouton de la barre d'outils Envoyer Ctrl+Alt+Del en haut de la barre latérale.
Se déconnecter d'un serveur	Cliquez sur le bouton de la barre d'outils Ouvrir le menu en haut de la barre latérale et cliquez sur Se déconnecter .
Autoriser le décodage H.264	(Chrome uniquement) Cliquez sur le bouton de la barre d'outils Ouvrir le menu en haut de la barre latérale, cliquez sur Paramètres et activez Autoriser le décodage H.264 . Pour plus d'informations, reportez-vous à la section Autoriser le décodage H.264 .
Afficher les rubriques d'aide	Cliquez sur le bouton de la barre d'outils Ouvrir le menu en haut de la barre latérale, puis cliquez sur Paramètres et sur Aide . Vous pouvez également cliquer sur le logo Horizon en haut de la barre latérale et cliquer sur Aide .
Afficher la boîte de dialogue À propos de VMware Horizon Client	Cliquez sur le bouton de la barre d'outils Ouvrir le menu ou sur le logo Horizon en haut de la barre latérale et cliquez sur À propos de . Vous pouvez également cliquer sur le logo Horizon en haut de la barre latérale.

Utiliser plusieurs moniteurs

En utilisant un navigateur Chrome (version 55 ou version ultérieure), vous pouvez utiliser plusieurs moniteurs dans HTML Access Web client pour afficher une fenêtre de poste de travail distante.

Vous pouvez ajouter un moniteur supplémentaire au maximum à votre moniteur principal pour afficher la fenêtre du poste de travail distant actuel auquel vous êtes connecté. Par exemple, si vous disposez de trois moniteurs, vous pouvez spécifier que la fenêtre de poste de travail distant n'apparaît que sur deux de ces moniteurs. Des moniteurs adjacents doivent être sélectionnés pour la configuration de plusieurs moniteurs. Les moniteurs peuvent être placés côte à côte ou l'un au-dessus de l'autre.

À partir de HTML Access Web client 4. 5, la synchronisation DPI par périphérique est appliquée lorsque la fonctionnalité de prise en charge de plusieurs moniteurs est activée. Si vos deux moniteurs ont des paramètres DPI différents, les paramètres DPI de l'agent HTML Access sont définis sur la valeur DPI utilisée par le moniteur de l'ordinateur client qui a été utilisé pour démarrer la session HTML Access Web client.

Procédure

- 1 Démarrez Horizon Client et connectez-vous à un serveur.
- 2 Dans la fenêtre de sélection des postes de travail et applications, cliquez sur l'icône du poste de travail distant auquel vous voulez accéder.
- 3 Pour afficher la barre latérale, cliquez sur l'onglet de la barre latérale.
- 4 Cliquez sur le bouton de la barre d'outils **Ouvrir le menu** en haut de la barre latérale et sélectionnez **Paramètres d'affichage**.
- 5 Dans la boîte de dialogue Paramètres d'affichage, cliquez sur **Ajouter un écran**.

Remarque Si la fenêtre du navigateur Sélecteur d'écran n'apparaît pas, ajoutez l'adresse FQDN de votre Horizon Server dans la section Exceptions liées aux fenêtres contextuelles de la fenêtre **Paramètres de contenu** de votre navigateur.

- 6 Faites glisser la fenêtre Sélecteur d'écran de sorte qu'elle apparaisse sur l'écran de l'autre moniteur que vous voulez utiliser.

Le message dans la fenêtre du navigateur Sélecteur d'écran change et une icône rectangulaire grise est ajoutée.
- 7 Dans la fenêtre du navigateur Sélecteur d'écran, cliquez sur l'icône du moniteur **+** pour confirmer que vous voulez utiliser l'écran du moniteur actuel.

Le message *En attente des autres écrans* s'affiche sur l'écran du moniteur actuel et l'icône de moniteur grise dans la fenêtre Paramètres d'affichage sur votre écran principal devient verte.
- 8 Cliquez sur **OK** dans la fenêtre Paramètres d'affichage lorsque vous avez terminé l'ajout des écrans que vous voulez utiliser pour la session.

La fenêtre Paramètres d'affichage se ferme, le message *En attente des autres écrans* disparaît de l'écran non principal et affiche la fenêtre du poste de travail distant.
- 9 Pour quitter le mode plusieurs écrans, appuyez sur Échap et cliquez sur **Oui** dans la boîte de dialogue **Quitter le mode plusieurs écrans** pour confirmer.

Remarque Chaque fois que vous devez utiliser la touche Échap dans le poste de travail distant, ouvrez l'onglet de la barre latérale, cliquez sur le bouton de la barre d'outils **Ouvrir le menu** en haut de la barre latérale et sélectionnez **Envoyer Échap**.

Utilisation de la synchronisation DPI

La fonctionnalité de synchronisation DPI garantit que le paramètre DPI d'un poste de travail distant ou d'une application publiée correspond au paramètre DPI du système client. Lorsque vous démarrez une nouvelle session distante, Horizon Agent définit pour cette session une valeur DPI qui correspond à la valeur DPI du système client.

La fonctionnalité de synchronisation DPI ne peut pas modifier le paramètre DPI des sessions distantes actives. Si vous vous reconnectez à une session distante existante, la fonctionnalité de mise à l'échelle de l'affichage met à l'échelle le poste de travail distant ou l'application publiée de façon appropriée.

La fonctionnalité de synchronisation DPI est activée lorsque le paramètre Mode Haute résolution est désactivé dans la fenêtre Paramètres. Depuis la version 4.5 de HTML Access, si l'administrateur désactive le paramètre de stratégie de groupe de l'agent **Synchronisation DPI**, la fonctionnalité de synchronisation DPI peut être désactivée, mais pas la fonctionnalité de mise à l'échelle de l'affichage. Vous devez vous déconnecter, puis vous reconnecter pour qu'une modification de configuration prenne effet. Pour plus d'informations sur le paramètre de stratégie de groupe **Synchronisation DPI**, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

La fonctionnalité de synchronisation DPI requiert Windows 7 ou version ultérieure pour les postes de travail à une seule session, Windows Server 2008 R2 ou version ultérieure pour les applications et les postes de travail publiés sur des hôtes RDS, Horizon Agent 7.0.2 ou version ultérieure et HTML Access 4.4 ou version ultérieure.

Ci-dessous figurent les conseils d'utilisation de la fonctionnalité de synchronisation DPI.

- Si vous modifiez le paramètre DPI sur le système client, vous devez vous déconnecter, puis vous reconnecter pour que Horizon Client prenne connaissance du nouveau paramètre DPI sur le système client. Cette exigence s'applique même si le système client exécute Windows 10.
- Si vous démarrez une session distante sur un système client avec un paramètre DPI supérieur à 100 % et que vous utilisez la même session sur un autre système client avec un paramètre DPI différent supérieur à 100 %, vous devez vous déconnecter, puis vous reconnecter sur le deuxième système client pour que la synchronisation DPI fonctionne sur le deuxième système client.
- Même si les systèmes Windows 10 et Windows 8.x prennent en charge différents paramètres DPI sur différents moniteurs, la fonctionnalité de synchronisation DPI utilise la valeur DPI définie sur le moniteur du système client sur lequel se trouve le navigateur Web utilisé pour le lancement de la session du client HTML Access. HTML Access ne prend pas en charge différents paramètres DPI dans différents moniteurs.
- Si vous voulez effectuer une synchronisation avec un autre moniteur avec un paramètre DPI différent, vous devez vous déconnecter du poste de travail distant ou de l'application publiée, faire glisser le navigateur Web utilisé pour lancer la session du client HTML Access sur l'autre moniteur et vous reconnecter au poste de travail distant ou à l'application publiée pour que les paramètres DPI correspondent entre le système client et le poste de travail distant ou l'application publiée.

Audio

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

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

Les limites suivantes s'appliquent à la lecture audio sur des postes de travail distants et des applications publiées.

- 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, la qualité du son peut être médiocre. À cet égard, certains navigateurs fonctionnent mieux que d'autres.

Copier et coller du texte

Vous pouvez copier du texte vers et depuis des applications publiées et des postes de travail. Un administrateur Horizon peut configurer cette fonctionnalité pour que les opérations Copier et Coller soient autorisées uniquement depuis le système client vers un poste de travail distant ou une application publiée, ou uniquement depuis un poste de travail distant ou une application publiée vers le système client, les deux ou aucun.

Les administrateurs Horizon peuvent configurer la fonctionnalité de copier-coller à l'aide de stratégies de groupe qui appartiennent à View Agent ou Horizon Agent dans les postes de travail distants. Pour plus d'informations, reportez-vous à la section [Paramètres de stratégie de groupe de HTML Access](#). Un administrateur Horizon peut également utiliser des stratégies de groupe pour restreindre les formats de Presse-papiers lors des opérations de copier-coller. Étant donné que HTML Access ne prend en charge que le transfert de texte dans le Presse-papiers, seuls les filtres de texte fonctionnent avec le client HTML Access. Pour plus d'informations sur l'utilisation de stratégies de groupe pour filtrer les formats du Presse-papiers, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

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 un poste de travail distant ou une application publiée, 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.

Remarque La fonctionnalité de copier-coller n'est pas prise en charge sur iOS Safari et les périphériques Android.

Utiliser la fonctionnalité de copier/coller

Pour copier et coller du texte, vous devez utiliser le bouton **Copier et coller** en haut 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 et vice versa. 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 haut 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.

Le texte dans la fenêtre Copier et coller affiche l'un des messages suivants pour indiquer dans quel sens l'utilisateur peut copier et coller du contenu.

- Utilisez ce panneau pour copier et coller du contenu entre votre client local et l'application/le poste de travail distant.
- Utilisez ce panneau pour copier et coller du contenu depuis votre client local vers l'application ou le poste de travail distant.
- Utilisez ce panneau pour copier et coller du contenu depuis l'application ou le poste de travail distant vers votre client local.

Remarque Le paramètre de stratégie de groupe de redirection du Presse-papiers par défaut vous permet de copier et coller depuis des systèmes clients vers le poste de travail distant ou l'application uniquement. Le paramètre de stratégie doit être activé dans les deux sens pour pouvoir copier depuis votre application ou poste de travail distant vers votre système client. Contactez votre administrateur Horizon pour obtenir de l'aide.

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 Horizon 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 autorisant les opérations de copier/coller. Pour plus d'informations, reportez-vous à la section [Paramètres de stratégie de groupe de HTML Access](#).

Procédure

- Pour copier du texte depuis votre système client vers 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 haut 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.

- c Pour coller le texte dans la fenêtre Copier et coller, appuyez sur Ctrl+V (ou sur Commande-V sur un Mac).

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 depuis votre application ou poste de travail distant vers 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 haut de la barre latérale.

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

- c Pour copier le texte à nouveau, cliquez dans la fenêtre Copier et coller et appuyez sur Ctrl+C (ou sur Commande-C sur un Mac).

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.

Transférer des fichiers entre le client et un poste de travail distant

Avec la fonctionnalité de transfert de fichiers, vous pouvez transférer (charger et télécharger) des fichiers entre le client et un poste de travail distant. Le transfert de fichiers vers ou depuis des applications publiées n'est pas pris en charge.

Remarque Cette fonctionnalité n'est pas disponible pour une utilisation avec des postes de travail Linux distants, des périphériques Android ou des sessions d'application distantes.

L'administrateur Horizon peut configurer la fonctionnalité d'autorisation, d'interdiction ou d'autorisation dans un seul sens du transfert de fichiers en modifiant le paramètre de stratégie de groupe **Configurer le transfert de fichiers** pour le protocole VMware Blast. La fonctionnalité par défaut est : chargement uniquement. Si la valeur **Désactiver le chargement et le téléchargement** est sélectionnée dans le paramètre de stratégie de groupe **Configurer le transfert de fichiers** pour le protocole VMware Blast, le bouton **Transfert de fichiers** est désactivé. Si la valeur **Activer le chargement de fichiers uniquement** est sélectionnée, seul l'onglet **Chargement** s'affiche dans la fenêtre de dialogue **Transférer des fichiers**. Si la valeur **Activer le téléchargement de fichiers uniquement** est sélectionnée, seul l'onglet **Téléchargement** s'affiche dans la fenêtre de dialogue **Transférer des fichiers**. Pour plus d'informations, reportez-vous à la section [Paramètres de stratégie de groupe de HTML Access](#).

Vous pouvez télécharger un fichier de 500 Mo maximum et charger un fichier de 2 Go maximum. Pour Internet Explorer 11 32 bits, il se peut que le téléchargement d'un fichier plus grand que 300 Mo ne fonctionne pas. Pour résoudre ce problème, exécutez Internet Explorer 11 en mode 64 bits.

Vous ne pouvez pas télécharger ou charger des dossiers ou des fichiers dont la taille est nulle.

Safari sous iOS et Safari 8 ne prennent pas en charge le chargement ou le téléchargement. Safari 9 ou version ultérieure ne prend pas en charge le téléchargement.

Si le transfert de fichiers est en cours dans une session du poste de travail et que l'utilisateur ouvre une connexion sur un deuxième poste de travail, et si un avertissement de sécurité s'affiche (cela peut arriver si aucun certificat valide n'a été installé, par exemple), alors le fait d'ignorer l'avertissement et de continuer la connexion au deuxième poste de travail entraînera l'arrêt du transfert de fichiers dans la session du premier poste de travail. Ce comportement est normal.

Remarque La possibilité de télécharger est affectée par le paramètre de stratégie de groupe pour la redirection du Presse-papiers. Si la redirection du Presse-papiers est désactivée depuis le serveur vers le client, alors le téléchargement du fichier est également désactivé.

Télécharger des fichiers depuis un poste de travail vers le client

Avec Horizon Client, vous pouvez télécharger des fichiers depuis un poste de travail distant et les transférer vers la machine cliente.

Procédure

- 1 Cliquez sur l'icône de transfert de fichiers située en haut de la barre latérale.
La fenêtre **Transférer des fichiers** s'ouvre.
- 2 Cliquez sur **Télécharger**.
- 3 Sélectionnez un ou plusieurs fichiers sur le poste de travail.
- 4 Appuyez sur Ctrl+C pour démarrer le téléchargement.
- 5 Une fois le téléchargement terminé, cliquez sur l'icône de téléchargement pour enregistrer les fichiers sur la machine cliente.

Charger des fichiers depuis le client vers un poste de travail

Avec Horizon Client, vous pouvez charger des fichiers depuis la machine cliente vers un poste de travail distant.

Procédure

- 1 Cliquez sur l'icône de transfert de fichiers située en haut de la barre latérale.

La fenêtre **Transférer des fichiers** s'ouvre.

- 2 Cliquez sur **Charger**.

- 3 Glissez-déposez des fichiers dans la fenêtre **Transfert de fichiers** ou cliquez sur **Choisir des fichiers** pour sélectionner des fichiers.

Les fichiers sélectionnés sont chargés dans le dossier Mes documents.

Avec Internet Explorer 11 et Chrome sur ChromeBook, si vous glissez-déposez des dossiers ou fichiers de taille nulle ou des fichiers plus grands que 2 Go, vous obtiendrez un message d'erreur comme prévu. Après avoir fermé le message d'erreur, vous ne pouvez plus glisser-déposer de fichiers pour les transférer.

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

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

L'Audio/Vidéo en temps réel est pris en charge uniquement dans Chrome, Microsoft Edge et Firefox. La résolution vidéo par défaut est de 320 x 240. Les paramètres d'Audio/Vidéo en temps réel par défaut fonctionnent bien avec la plupart des applications audio et webcam.

Pour plus d'informations sur la modification des paramètres d'Audio/Vidéo en temps réel, consultez « Configuration des paramètres de stratégie de groupe de l'Audio/Vidéo en temps réel » dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Lorsqu'une application publiée ou un poste de travail distant est connecté à la webcam ou au microphone de la machine cliente, le navigateur peut demander une autorisation avant que l'application publiée ou le poste de travail distant puisse utiliser la webcam ou le microphone. Chaque navigateur se comporte différemment.

- Microsoft Edge demande une autorisation à chaque fois. Il n'est pas possible de modifier ce comportement. Pour plus d'informations, reportez-vous à la section <https://blogs.windows.com/msedgedev/2015/05/13/announcing-media-capture-functionality-in-microsoft-edge>.

- Firefox demande une autorisation à chaque fois. Il est possible de modifier ce comportement. Pour plus d'informations, reportez-vous à la section <https://support.mozilla.org/en-US/kb/permissions-manager-give-ability-store-passwords-set-cookies-more?redirectlocale=en-US&redirectslug=how-do-i-manage-website-permissions>.
- Chrome demande une autorisation la première fois. Si vous autorisez l'utilisation du périphérique, Chrome ne redemande pas l'autorisation.

Lorsqu'un poste de travail distant est connecté au microphone ou à la webcam de la machine cliente, une icône pour chaque périphérique s'affiche en haut de la barre latérale. Un point d'interrogation rouge s'affiche sur l'icône de périphérique sur la barre latérale pour indiquer la demande d'autorisation. Si vous autorisez l'utilisation d'un périphérique, le point d'interrogation rouge disparaît. Si vous refusez une demande d'autorisation, l'icône de périphérique disparaît.

Si l'Audio/Vidéo en temps réel est utilisé dans une session d'application publiée ou de poste de travail distant et que vous ouvrez une connexion sur un deuxième poste de travail distant ou application publiée, et si un avertissement de sécurité s'affiche (par exemple, si un certificat valide n'a pas été installé), le fait d'ignorer l'avertissement et de poursuivre la connexion au deuxième poste de travail distant ou application publiée entraîne l'arrêt de l'Audio/Vidéo en temps réel dans la première session.

Utilisation de la fonctionnalité de collaboration de session

Vous pouvez utiliser la fonctionnalité de collaboration de session pour inviter d'autres utilisateurs à rejoindre une session de poste de travail distant existante.

Inviter un utilisateur à rejoindre une session de poste de travail distant

Lorsque la fonctionnalité de collaboration de session est activée pour un poste de travail distant, vous pouvez inviter d'autres utilisateurs à rejoindre une session de poste de travail distant existante.

Par défaut, vous pouvez envoyer des invitations de collaboration de session par e-mail, par messagerie instantanée ou en copiant un lien dans le Presse-papiers et en le transférant aux utilisateurs. Pour utiliser la méthode d'invitation par e-mail, une application de messagerie doit être installée. Pour utiliser la méthode d'invitation par messagerie instantanée, Skype Entreprise doit être installé et configuré. Vous ne pouvez inviter que les utilisateurs qui appartiennent à un domaine que le serveur autorise pour l'authentification. Vous pouvez inviter jusqu'à cinq utilisateurs par défaut.

La fonctionnalité de collaboration de session présente les limitations suivantes.

- Si vous disposez de plusieurs moniteurs, seul le principal est affiché pour les collaborateurs de la session.
- Vous devez sélectionner le protocole d'affichage VMware Blast lorsque vous créez une session de poste de travail distant. La fonctionnalité de collaboration de session ne prend pas en charge les sessions PCoIP ou RDP.
- Le codage matériel H.264 n'est pas pris en charge. Si le propriétaire de la session utilise un codage matériel et qu'un collaborateur rejoint la session, les deux passent au codage logiciel.

- La collaboration anonyme n'est pas prise en charge. Les collaborateurs de la session doivent être identifiables via des mécanismes d'authentification pris en charge par Horizon.
- Les collaborateurs de la session doivent avoir installé Horizon Client 4.7 ou version ultérieure pour Windows, Mac ou Linux ou ils doivent utiliser HTML Access 4.7 ou version ultérieure. Si un collaborateur de la session dispose d'une version non prise en charge d'Horizon Client, un message d'erreur s'affiche lorsque l'utilisateur clique sur un lien de collaboration.
- Vous ne pouvez pas utiliser la fonctionnalité de collaboration de session pour partager des sessions de poste de travail distant ou des sessions d'application publiée Linux.

Prérequis

Pour inviter des utilisateurs à rejoindre une session de poste de travail distant, un administrateur Horizon doit activer la fonctionnalité de collaboration de session.


Cette tâche inclut l'activation de la fonctionnalité de collaboration de session au niveau du pool de postes de travail ou de la batterie de serveurs. Elle peut également inclure l'utilisation de stratégies de groupe pour configurer des fonctionnalités de collaboration de session, telles que les méthodes d'invitation disponibles. Pour plus d'informations sur les exigences, reportez-vous à [Configuration requise pour la fonctionnalité de collaboration de session](#).

Pour plus d'informations sur l'activation de la fonctionnalité de collaboration de session pour des pools de postes de travail, consultez le document *Configuration des postes de travail virtuels dans Horizon 7*. Pour plus d'informations sur l'activation de la fonctionnalité de collaboration de session pour une batterie de serveurs, consultez le document *Configuration d'applications et de postes de travail publiés dans Horizon 7*. Pour plus d'informations sur l'utilisation de paramètres de stratégie de groupe pour configurer la fonctionnalité de collaboration de session, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Procédure

- 1 Connectez-vous à un poste de travail distant pour lequel la fonctionnalité de collaboration de session est activée.

Vous devez utiliser le protocole d'affichage VMware Blast.

- 2 Dans la barre d'état système du poste de travail distant, cliquez sur l'icône VMware Horizon Collaboration, par exemple, .

L'icône de collaboration est différente selon la version du système d'exploitation Windows.

- 3 Lorsque la boîte de dialogue VMware Horizon Collaboration s'ouvre, entrez le nom d'utilisateur (par exemple, **testuser** ou **domain\testuser**) ou l'adresse e-mail de l'utilisateur que vous voulez voir rejoindre la session de poste de travail distant.

La première fois que vous entrez le nom d'utilisateur ou l'adresse e-mail d'un utilisateur particulier, vous devez cliquer sur **Rechercher « utilisateur »**, entrer une virgule (,) ou appuyer sur la touche **Entrée** pour valider l'utilisateur. La fonctionnalité de collaboration de session mémorise l'utilisateur la prochaine fois que vous entrez son nom d'utilisateur ou son adresse e-mail.

Vous pouvez inviter jusqu'à cinq utilisateurs par défaut. Un administrateur Horizon peut modifier le nombre maximal d'utilisateurs que vous pouvez inviter.

- 4 Sélectionnez une méthode d'invitation.

Les méthodes d'invitation suivantes sont disponibles par défaut. Un administrateur Horizon peut désactiver les méthodes d'invitation par e-mail et par messagerie instantanée.

Option	Action
E-mail	Copie l'invitation de collaboration dans le Presse-papiers et ouvre un nouvel e-mail dans l'application de messagerie par défaut. Une application de messagerie doit être installée pour utiliser cette méthode d'invitation.
Messagerie instantanée	Copie l'invitation de collaboration dans le Presse-papiers et ouvre une nouvelle fenêtre dans Skype Entreprise. Appuyez sur Ctrl+V pour coller le lien dans la fenêtre Skype Entreprise. Skype Entreprise doit être installé et configuré pour utiliser cette méthode d'invitation.
Copier le lien	Copie l'invitation de collaboration dans le Presse-papiers. Vous devez ouvrir manuellement une autre application, comme le Bloc-notes, et appuyer sur Ctrl+V pour coller l'invitation.

Une fois l'invitation envoyée, l'icône VMware Horizon Collaboration s'affiche également sur le poste de travail et l'interface utilisateur de la collaboration de session se transforme en tableau de bord qui indique l'état actuel de la session de collaboration et vous permet d'exécuter certaines actions.

Lorsqu'un collaborateur de session accepte votre invitation et rejoint la session, la fonctionnalité de collaboration de session vous avertit et un point rouge s'affiche sur l'icône VMware Horizon Collaboration dans la barre d'état système.

Suivant

Gérez la session de collaboration dans la boîte de dialogue VMware Horizon Collaboration. Reportez-vous à la section [Gérer une session de collaboration](#).

Gérer une session de collaboration

Une fois l'invitation de collaboration de session envoyée, l'interface utilisateur de la collaboration de session se transforme en tableau de bord qui indique l'état actuel de la session de collaboration et vous permet d'exécuter certaines actions.

Prérequis

Démarrez une session de collaboration. Reportez-vous à la section [Inviter un utilisateur à rejoindre une session de poste de travail distant](#).

Procédure

- 1 Dans le poste de travail distant, cliquez sur l'icône VMware Horizon Collaboration dans la barre d'état système ou double-cliquez sur l'icône VMware Horizon Collaboration sur le poste de travail.

Les noms de tous les collaborateurs de session s'affichent dans la colonne Nom et leur état s'affiche dans la colonne État.

- 2 Utilisez le tableau de bord Collaboration de session VMware Horizon pour gérer la session de collaboration.

Option	Action
Révoquer une invitation ou supprimer un collaborateur	Cliquez sur Supprimer dans la colonne État.
Rendre le contrôle à un collaborateur de session	Une fois que le collaborateur de session a rejoint la session, basculez le commutateur dans la colonne Contrôle sur Activé . Pour reprendre le contrôle de la session, double-cliquez ou appuyez sur n'importe quelle touche. Le collaborateur de session peut également rendre le contrôle en basculant le commutateur dans la colonne Contrôle sur Désactivé ou en cliquant sur le bouton Rendre le contrôle .
Ajouter un collaborateur	Cliquez sur Ajouter des collaborateurs .
Mettre fin à la session de collaboration	Cliquez sur Mettre fin à la collaboration . Tous les collaborateurs actifs sont déconnectés. Vous pouvez également mettre fin à la session de collaboration en cliquant sur l'icône Collaboration de session VMware Horizon sur le poste de travail et en cliquant sur le bouton Arrêter .

Rejoindre une session de collaboration

Pour rejoindre une session de collaboration, vous pouvez cliquer sur le lien dans une invitation de collaboration. Le lien peut se trouver dans un e-mail, un message instantané ou dans un document que le propriétaire de la session vous transfère. Vous pouvez également vous connecter au serveur et double-cliquer sur l'icône de la session de collaboration dans la fenêtre de sélection des applications et des postes de travail distants.

Cette procédure décrit la façon de rejoindre une session de collaboration à partir d'une invitation de collaboration.

Remarque Dans un environnement Architecture Cloud Pod, vous ne pouvez pas rejoindre une session de collaboration en vous connectant au serveur, sauf si vous vous connectez à l'espace du propriétaire de la session.

Vous ne pouvez pas utiliser les fonctionnalités suivantes de poste de travail distant dans une session de collaboration.

- Audio/Vidéo en temps réel (RTAV)
- Impression basée sur l'emplacement
- Redirection du Presse-papiers

Vous ne pouvez pas modifier la résolution du poste de travail distant dans une session de collaboration.

Prérequis

Pour rejoindre une session de collaboration, Horizon Client 4.7 pour Windows, Mac ou Linux doit être installé sur le système client ou vous devez utiliser HTML Access 4.7 ou version ultérieure.

Procédure

- 1 Cliquez sur le lien dans l'invitation de collaboration.

Horizon Client s'ouvre sur le système client.

- 2 Entrez vos informations d'identification pour vous connecter à Horizon Client.

Une fois que vous êtes authentifié, la session de collaboration commence et vous pouvez voir le poste de travail distant du propriétaire de la session. Si le propriétaire de la session vous transfère le contrôle de la souris et du clavier, vous pouvez utiliser le poste de travail distant.

- 3 Pour rendre le contrôle de la souris et du clavier au propriétaire de la session, cliquez sur l'icône Collaboration de session VMware Horizon dans la barre d'état système et basculez le commutateur dans la colonne Contrôle sur **Désactivé** ou cliquez sur le bouton **Rendre le contrôle**.
- 4 Pour quitter la session collaborative, cliquez sur **Fermer** dans la barre latérale.

Fermer une session ou se déconnecter

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

Procédure

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

Option	Action
Depuis la fenêtre de sélection des postes de travail et des applications, avant de se connecter à un poste de travail distant ou à une application publiée	Cliquez sur le bouton Fermer la session de la barre d'outils dans le coin supérieur droit de la fenêtre.
Depuis la barre latérale lorsque vous êtes connecté à un poste de travail distant ou à une application publiée	Cliquez sur le bouton de la barre d'outils Fermer la session en haut de la barre latérale.

- Fermer une application publiée.

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

- Fermez une session ou déconnectez-vous d'un poste de travail distant.

Option	Action
Depuis le poste de travail distant	Utilisez le menu Démarrer de Windows pour fermer la session.
Depuis la barre latérale	Pour fermer la session et vous déconnecter, cliquez sur le bouton Ouvrir le menu de la barre d'outils, à côté du nom de poste de travail distant dans la liste Exécution sur la barre latérale, puis sélectionnez Fermer la session . Les fichiers ouverts sur le poste de travail distant sont fermés sans être enregistrés. 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 distant dans la liste Exécution , puis sélectionnez Fermer .

Remarque Un administrateur Horizon peut configurer le poste de travail distant pour fermer la session automatiquement lors de la déconnexion. Dans ce cas, toutes les applications ouvertes sur le poste de travail distant sont fermées.

Réinitialiser un poste de travail distant ou des applications publiées

Vous devez peut-être réinitialiser un poste de travail distant si le système d'exploitation du poste de travail cesse de répondre et que le redémarrage du poste de travail distant ne résout pas le problème. La réinitialisation d'applications publiées entraîne la fermeture de toutes les applications ouvertes.

La réinitialisation d'un poste de travail distant revient 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 sont fermés sans être enregistrés.

La réinitialisation des applications publiées arrête les applications sans enregistrer les données non enregistrées. Toutes les applications publiées ouvertes sont fermées, même celles qui proviennent de batteries de serveurs RDS différentes.

Vous pouvez réinitialiser un poste de travail distant uniquement si un administrateur Horizon a activé la fonctionnalité de réinitialisation pour le poste de travail distant.

Pour plus d'informations sur l'activation de la fonctionnalité de réinitialisation de poste de travail, consultez le document *Configuration des postes de travail virtuels dans Horizon 7* ou *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

Procédure

- ◆ Utilisez la commande **Réinitialiser**.

Option	Action
Réinitialiser des applications publiées depuis la fenêtre de sélection des applications	Depuis la fenêtre de sélection des postes de travail et des applications, avant de vous connecter à un poste de travail distant ou à une application publiée, pour réinitialiser toutes les applications publiées en cours d'exécution, cliquez sur le bouton Paramètres de la barre d'outils, dans le coin supérieur droit de l'écran, puis cliquez sur Réinitialiser .
Réinitialiser un poste de travail distant 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 publiées 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 distant à l'aide d'un URI	Pour réinitialiser un poste de travail distant, utilisez l'URI <code>https://ConnectionServerFQDN?desktopId=desktop_name&action=reset</code> .

Lorsque vous réinitialisez un poste de travail distant, son système d'exploitation redémarre et Horizon Client se déconnecte et ferme la session. Lorsque vous réinitialisez des applications publiées, les applications publiées se ferment.

Suivant

Patiencez jusqu'au redémarrage du système avant de tenter de vous reconnecter au poste de travail distant ou à l'application publiée.

Redémarrer un poste de travail distant

Si le système d'exploitation du poste de travail distant ne répond plus, vous devez redémarrer le poste de travail distant. Le redémarrage d'un poste de travail distant est similaire à la commande de redémarrage du système d'exploitation Windows. En général, le système d'exploitation du poste de travail distant demande d'enregistrer toutes les données non enregistrées avant de redémarrer.

Vous pouvez redémarrer un poste de travail distant uniquement si un administrateur Horizon a activé la fonctionnalité de redémarrage pour le poste de travail distant.

Pour plus d'informations sur l'activation de la fonctionnalité de redémarrage de poste de travail, consultez le document *Configuration des postes de travail virtuels dans Horizon 7* ou *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

Prérequis

Procurez-vous les informations d'identification de connexion, telles que le nom d'utilisateur et le mot de passe Active Directory, le nom d'utilisateur et le mot de passe RSA SecurID ou le nom d'utilisateur et le mot de passe de l'authentification RADIUS.

Procédure

- ◆ Utilisez la commande **Redémarrer**.

Option	Action
Depuis la barre latérale	Lorsque vous êtes connecté à un poste de travail distant, dans la barre d'outils, cliquez sur le bouton Ouvrir le menu à côté du nom du poste de travail distant, dans la liste Exécution sur la barre latérale, puis sélectionnez Redémarrer .
Utilisation d'un URI	Pour redémarrer un poste de travail, utilisez l'URI <code>https://ConnectionServerFQDN?desktopId=desktop_name&action=restart.</code>

Le système d'exploitation du poste de travail distant redémarre, et Horizon Client se déconnecte et ferme la session sur le poste de travail distant.

Suivant

Patientez jusqu'au redémarrage du système avant de tenter de vous reconnecter au poste de travail distant.

Si le redémarrage du poste de travail distant ne résout pas le problème, vous devrez peut-être réinitialiser le poste de travail distant. Reportez-vous à la section [Réinitialiser un poste de travail distant ou des applications publiées](#).