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

Mars 2020

VMware Horizon HTML Access 5.4

VMware Horizon 7 7.12

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

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

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

VMware France SAS.
Tour Franklin
100-101 Terrasse Boieldieu
92042 Paris La Défense 8 Cedex
France
www.vmware.com/fr

Table des matières

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 la documentation *Administration de VMware Horizon Console*.

Configuration et installation

1

La configuration d'un déploiement de Horizon 7 pour HTML Access implique l'installation du composant HTML Access dans le serveur de connexion et l'autorisation du trafic entrant sur certains ports TCP. Pour permettre aux utilisateurs finaux d'utiliser HTML Access pour accéder à des postes de travail publiés et à des applications publiées, vous devez activer HTML Access dans les paramètres de la batterie de serveurs. Pour les postes de travail virtuels, vous devez activer HTML Access dans les paramètres du pool de postes de travail.

Les utilisateurs finaux accèdent à leurs applications publiées et postes de travail distants en ouvrant un navigateur pris en charge et en entrant l'URL d'un serveur. Lorsqu'un utilisateur final se connecte à un serveur, la page du portail Web VMware Horizon s'affiche. Vous pouvez configurer l'apparence de la page du portail Web VMware Horizon et définir des stratégies de groupe pour contrôler la qualité d'image, les ports utilisés et d'autres paramètres.

Ce chapitre contient les rubriques suivantes :

Configuration système requise pour HTML Access

Avec HTML Access, le système client ne requiert aucun autre logiciel à part un navigateur pris en charge. Le déploiement d'Horizon 7 doit respecter certaines exigences logicielles.

Navigateurs sur le système client

Navigateur	Version
Chrome	75, 76
Internet Explorer	11
Safari	12
Firefox	67, 68
Microsoft Edge	42, 44
VMware Workspace ONE Web	Dernière version d'Apple App Store (périphériques iOS) ou de Google Play Store (périphériques Android).

Note

- Sur un périphérique Android, Chrome 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. Les combinaisons de touches Suppr, Ctrl+A, Ctrl+C, Ctrl+V, Ctrl+X, Ctrl+Y, Ctrl+Z ne fonctionnent pas sur le clavier logiciel.
- Sur un périphérique mobile, Safari 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) 8.x (32 et 64 bits) 10 (32 et 64 bits)
macOS	10.14.x (Mojave) 10.13.x (High Sierra)
iOS	10 ou version ultérieure
Chrome OS	28.x ou version ultérieure
Android	7 ou version ultérieure

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 Agent 7.0. Pour plus d'informations, consultez « Systèmes d'exploitation pris en charge pour Horizon Agent » dans la version 7.0 ou ultérieure du document *Installation d'Horizon 7*.

Paramètres de pool

HTML Access requiert les paramètres de pool suivants.

- 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 Définition de la résolution d'écran.

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

Pour obtenir des instructions de configuration, consultez le document Préparer des postes de travail, des pools et des batteries de serveurs.

Serveur de connexion

L'option HTML Access doit être installée sur le Serveur de connexion.

Lorsque vous installez le composant HTML Access, la règle **Serveur de connexion de VMware Horizon View (Blast-In)** est activée sur le Pare-feu Windows. Cette règle configure le pare-feu pour qu'il autorise automatiquement le trafic entrant vers le port TCP 8443.

Serveur de sécurité

Si vous utilisez un serveur de sécurité, la même version que le Serveur de connexion doit être installée sur le serveur de sécurité.

Note Vous pouvez utiliser des dispositifs Unified Access Gateway, plutôt que des serveurs de sécurité, pour un accès externe sécurisé.

Pare-feu tiers

Ajoutez des règles pour permettre le trafic suivant :

- Pour les serveurs (y compris les serveurs de sécurité, les instances du Serveur de connexion et les serveurs de réplica), autorisez le trafic entrant sur le port TCP 8443.
- Pour les machines virtuelles de postes de travail à distance, autorisez le trafic entrant (des serveurs) sur le port TCP 22443.

Protocoles d'affichage

VMware Blast

Lorsque vous utilisez un navigateur Web pour accéder à un poste de travail distant, le protocole d'affichage 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, assure-vous que cette fonctionnalité est activée sur le Serveur de connexion. À partir de Horizon 7 version 7.11, vous pouvez personnaliser les étiquettes sur la page de connexion d'authentification RADIUS. À partir d'Horizon 7 version 7.12, vous pouvez configurer l'authentification à deux facteurs pour qu'elle se produise après l'expiration d'une session distante. Pour plus d'informations, consultez les rubriques concernant l'authentification à deux facteurs dans le document *Administration de VMware Horizon Console*.

5 Pour masquer le menu déroulant **Domaine** dans Horizon Client, activez le paramètre global **Masquer la liste de domaines dans l'interface utilisateur client**. Ce paramètre est disponible dans Horizon 7 version 7.1 et version ultérieure. À partir d'Horizon 7 version 7.8, il est activé par défaut. Pour plus d'informations, reportez-vous au document *Administration de VMware Horizon Console*.

6 Pour envoyer la liste de domaines à Horizon Client, activez-le paramètre global **Envoyer la liste de domaines**. Ce paramètre est disponible dans Horizon 7 version 7.8 et version ultérieure et est désactivé par défaut. Les versions antérieures d'Horizon 7 envoient la liste de domaines. Pour plus d'informations, consultez le document *Administration de VMware Horizon Console* pour Horizon 7 version 7.8 ou version ultérieure.

7 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.

8 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 de VMware Horizon Console*.

Le tableau suivant montre comment les paramètres globaux **Envoyer la liste de domaines** et **Masquer la liste de domaines dans l'interface utilisateur client** déterminent le mode de connexion des utilisateurs au serveur depuis Horizon Client.

Paramètre Envoyer la liste de domaines	Paramètre Masquer la liste de domaines dans l'interface utilisateur client	Mode de connexion des utilisateurs
Désactivé (par défaut)	Activé	Le menu déroulant **Domaine** est masqué. Les utilisateurs doivent entrer l'une des valeurs suivantes dans la zone de texte **Nom d'utilisateur**. ■ Nom d'utilisateur (non autorisé pour plusieurs domaines) ■ *domain\username* ■ *username@domain.com*
Désactivé (par défaut)	Désactivé	Si un domaine par défaut est configuré sur le client, il s'affiche dans le menu déroulant **Domaine**. Si le client ne connaît pas un domaine par défaut, `*DefaultDomain*` s'affiche dans le menu déroulant **Domaine**. Les utilisateurs doivent entrer l'une des valeurs suivantes dans la zone de texte **Nom d'utilisateur**. ■ Nom d'utilisateur (non autorisé pour plusieurs domaines) ■ *domain\username* ■ *username@domain.com*

Paramètre Envoyer la liste de domaines	Paramètre Masquer la liste de domaines dans l'interface utilisateur client	Mode de connexion des utilisateurs
Activé	Activé	Le menu déroulant **Domaine** est masqué. Les utilisateurs doivent entrer l'une des valeurs suivantes dans la zone de texte **Nom d'utilisateur**. ■ Nom d'utilisateur (non autorisé pour plusieurs domaines) ■ *domain\username* ■ *username@domain.com*
Activé	Désactivé	Les utilisateurs peuvent entrer un nom d'utilisateur dans la zone de texte **Nom d'utilisateur** et sélectionner un domaine dans le menu déroulant **Domaine**. Ils peuvent également entrer l'une des valeurs suivantes dans la zone de texte **Nom d'utilisateur**. ■ *domain\username* ■ *username@domain.com*

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 Console. 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*.

Note 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 de VMware Horizon Console*.

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.

Note 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.

Conditions préalables

Cette fonctionnalité requiert Horizon 7 version 7.0.2 ou ultérieure.

Procédure

1. Dans Horizon Console, sélectionnez **Paramètres > Paramètres généraux**, cliquez sur l'onglet **Paramètres généraux**, puis cliquez sur **Modifier**.
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.

Résultats

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.

Horizon Client offre plus de fonctionnalités et de meilleures performances que HTML Access. Par exemple, avec HTML Access, certaines combinaisons de touches ne fonctionnent pas sur le poste de travail distant, mais celles-ci fonctionnent avec Horizon Client. HTML Access représente une bonne alternative lorsque le logiciel Horizon Client n'est pas installé sur le système client.

Conditions préalables

- 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, reportez-vous au 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 Console 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 postes de travail virtuels, utilisez Horizon Console pour 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.

Résultats

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

Étape suivante

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 distante 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 Windows ou sur 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*.

Postes de travail à distance Linux

Pour connaître les exigences des postes de travail distants Linux, consultez le document *Configuration des postes de travail Horizon 7 for 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

La fonctionnalité de collaboration de session ne prend pas en charge les sessions d'application publiée.

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 un poste de travail distant, 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.

Note 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.

Conditions préalables

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**.

Étape suivante

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.

Conditions préalables

- 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`.

Étape suivante

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.

Étape suivante

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.

Conditions préalables

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`

Note 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.

Résultats

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 TLS 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 Sur le poste de travail sur lequel l'agent HTML Access est installé, démarrez l'éditeur du Registre Windows.

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 Pour que vos modifications prennent effet, redémarrez le service VMware Blast.

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

Résultats

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 TLS signés par une autorité de certification. Vous ne pouvez pas utiliser les certificats TLS par défaut générés par le serveur de connexion ou l'agent HTML Access.

Pour obtenir des Informations, consultez la rubrique « Configurer Horizon Client pour qu'iOS approuve les certificats racines et intermédiaires » dans le document *Installation d'Horizon 7*.

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.

Note 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.

Configuration de la lecture automatique dans Chrome et Safari

Lors de l'utilisation de HTML Access dans Safari 12 ou Chrome 71 ou version ultérieure, les utilisateurs peuvent voir la boîte de dialogue `Cliquez pour activer le son` lorsqu'ils démarrent un poste de travail distant ou une application publiée pour la première fois, ou lorsqu'ils actualisent le navigateur alors qu'ils utilisent un poste de travail distant ou une application publiée. Si les utilisateurs cliquent sur **OK** dans cette boîte de dialogue, le son est lu normalement.

Pour empêcher l'affichage de cette boîte de dialogue, configurez la stratégie d'exécution automatique dans le navigateur.

- Dans Safari sur un Mac, sélectionnez **Safari > Réglages pour ce site web**, placez le curseur à droite de **Lecture automatique**, cliquez sur le menu déroulant et sélectionnez **Toujours autoriser la lecture automatique**.
- Dans Chrome, tapez **`chrome://flags/#autoplay-policy`** dans la barre de navigation, faites défiler jusqu'à **Autoplay policy**, puis sélectionnez **No user gesture required** dans le menu déroulant.

Mise à niveau de HTML Access

La mise à niveau de HTML Access implique la mise à niveau du Serveur de connexion et de Horizon Agent.

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

Lorsque vous effectuez la mise à niveau du Serveur de connexion, HTML Access est installé ou mis à niveau automatiquement.

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.

Étape suivante

Interdisez le trafic entrant vers le port TCP 8443 sur le pare-feu Windows des serveurs de sécurité couplés.

Sur les pare-feu tiers, le cas échéant, 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.

Configurer le partage de données d'Horizon Client

Si un administrateur Horizon a choisi de participer au programme d'amélioration du produit (CEIP) de VMware, VMware recueille et reçoit des données anonymes des systèmes clients via le Serveur de connexion. Vous pouvez déterminer si vous souhaitez partager ces données client avec le Serveur de connexion.

Pour plus d'informations sur la configuration d'Horizon afin de participer au programme CEIP, reportez-vous au document *Administration de VMware Horizon Console*.

Le partage de données est activé par défaut dans HTML Access. Vous ne pouvez pas modifier le paramètre de partage de données après vous être connecté à un serveur.

Un administrateur Horizon peut désactiver le partage de données dans HTML Access pour tous les utilisateurs et empêcher les utilisateurs de modifier le paramètre de partage de données dans HTML Access. Pour plus d'informations, reportez-vous à la section Désactivation du partage de données pour tous les utilisateurs de HTML Access.

Procédure

1. Cliquez sur **Paramètres** (icône d'engrenage) sur la page du portail Web de VMware Horizon.
2. Activez ou désactivez l'option **Autoriser le partage de données**.

Désactivation du partage de données pour tous les utilisateurs de HTML Access

Un administrateur Horizon peut désactiver le partage de données pour tous les utilisateurs de HTML Access et empêcher ces derniers de modifier l'option **Autoriser le partage de données** dans HTML Access, en ajoutant le paramètre suivant au fichier `C:\Program Files\VMware\VMware`

`View\Server\broker\webapps\portal\WEB-INF\classes\portal-version.properties` sur l'instance du Serveur de connexion.

```
CEIP.disabled=true
```

Lorsque ce paramètre est défini sur `true`, **Paramètres** (icône d'engrenage) n'apparaît pas sur la page du portail Web de VMware Horizon.

Note Ce paramètre n'a aucun impact sur Horizon Client. Pour plus d'informations sur la désactivation du partage de données dans Horizon Client, consultez le Guide d'installation et de configuration de la plate-forme Horizon Client.

Données collectées par VMware

Si votre entreprise participe au programme d'amélioration du produit (CEIP) de VMware, et que le partage de données est activé sur le client, VMware collecte des données sur le système client.

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 CEIP, VMware collecte des données anonymes sur votre déploiement afin d'améliorer la réponse 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 CEIP, 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 Console après l'installation.

Tableau 1-2. Données client recueillies pour le programme CEIP

Description	Nom de champ	Ce champ reste-t-il anonyme ?	Exemple
Entreprise qui a produit l'application	`<fournisseur_client>`	Non	VMware
Nom du produit	`<produit_client>`	Non	VMware Horizon HTML Access
Version du produit client	`<version_client>`	Non	5.4.0-*build_number*
Architecture binaire du client	`<arch_client>`	Non	Exemples comprenant les valeurs suivantes : ■ navigateur ■ arm

Tableau 1-2. Données client recueillies pour le programme CEIP (suite)

Description	Nom de champ	Ce champ reste-t-il anonyme ?	Exemple
Architecture native du navigateur	<arch_navigateur>	Non	Exemples comprenant les valeurs suivantes : ■ Win32 ■ Win64 ■ MacIntel ■ iPad ■ Linux armv81 (pour la prise en charge de Chrome pour Android)
Chaîne de l'agent utilisateur du navigateur	<agent_utilisateur_navigateur>	Non	Exemples comprenant les valeurs suivantes : ■ 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	<version_navigateur>	Non	Exemples comprenant les valeurs suivantes : ■ 7.0.3 (pour Safari), ■ 44.0 (pour Firefox) ■ 13.10586 (pour Edge)
Implémentation de base du navigateur	<base_navigateur>	Non	Exemples comprenant les valeurs suivantes : ■ Chrome ■ Safari ■ Firefox ■ Internet Explorer ■ Edge
Si le navigateur tourne sur un ordinateur de poche	<navigateur_est_portable>	Non	true

Configuration d'HTML Access pour les utilisateurs finaux

2

Vous pouvez modifier l'apparence de la page du portail Web de VMware Horizon, qui est la page Web que les utilisateurs finaux voient lorsqu'ils entrent l'URL pour HTML Access. Vous pouvez également définir des stratégies de groupe qui contrôlent la qualité de l'image, les ports utilisés ainsi que d'autres paramètres.

Ce chapitre contient les rubriques suivantes :

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

Vous pouvez configurer la page du portail Web VMware Horizon pour afficher ou masquer l'icône de téléchargement d'Horizon Client, l'icône de connexion à un poste de travail distant via HTML Accesset d'autres liens.

Par défaut, la page du portail Web d'VMware Horizon affiche à la fois une icône pour télécharger et installer Horizon Client et une icône pour se connecter via HTML Access. Les valeurs par défaut définies dans le fichier `portal-links-html-access.properties` déterminent le lien de téléchargement qui s'affiche sur la page du portail Web de VMware Horizon.

Parfois, vous voudrez peut-être que les liens sur la page du portail Web de VMware Horizon pointent vers un serveur Web interne ou vous voudrez rendre des versions de client spécifiques disponibles sur votre propre serveur. Vous pouvez reconfigurer la page du portail Web VMware Horizon 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` détermine la valeur de lien du fichier du programme d'installation.

Le fichier `oslinks.properties` est installé dans le répertoire *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 dirige 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/
pckbpdplfajmgaipljfamclkinbjdnma
link.winmobile=https://www.microsoft.com/en-us/store/p/vmware-horizon-client/9nblggh51p19
```

Vous pouvez définir des liens de programme d'installation pour des systèmes d'exploitation clients spécifiques dans le fichier `portal-links-html-access.properties` ou le fichier `oslinks.properties`. Par exemple, si vous accédez à la page du portail Web de VMware Horizon à partir d'un système macOS, le lien du programme d'installation d'Horizon Client pour Mac s'affiche. Pour les clients Windows et Linux, vous pouvez créer des liens distincts pour les programmes d'installation 32 et 64 bits.

Procédure

1. Sur l'hôte du serveur de connexion, utilisez un éditeur de texte pour ouvrir le fichier `portal-links-html-access.properties` *CommonAppDataFolder*`\VMware\VDM\portal\portal-links-html-access.properties` directory.

   Pour les systèmes d'exploitation Windows Server 2012, le dossier *CommonAppDataFolder* est `C:\ProgramData`. Pour afficher le dossier `C:\ProgramData` dans l'Explorateur Windows, utilisez la boîte de dialogue Options des dossiers pour afficher les dossiers cachés.

   Si le fichier `portal-links-html-access.properties` n'existe pas, mais 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.

2 Modifiez les propriétés de configuration.

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`.

Note Le fichier `oslinks.properties` ne peut être utilisé que pour configurer les liens vers les fichiers de programme d'installation spécifiques.

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

Option	Paramètre propriété

Créer des liens pour des programmes d'installation spécifiques	Les exemples suivants montrent des URL complètes. 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 l'hôte du serveur de connexion, vous pouvez utiliser des URL relatives comme décrit à l'étape suivante.
	■ Lien général pour télécharger le programme d'installation :
	`link.download=https://server/downloads`
	■ Programme d'installation de Windows 32 bits :
	`link.win32=https://server/downloads/VMware-Horizon-Client-x86-build#.exe`
	■ Programme d'installation de Windows 64 bits :
	`link.win64=https://server/downloads/VMware-Horizon-Client-x86_64-build#.exe`
	■ Programme d'installation de Windows Phone :
	`link.winmobile=https://server/downloads/VMware-Horizon-Client-build#.appx`
	■ Programme d'installation de Linux 32 bits :
	`link.linux32=https://server/downloads/VMware-Horizon-Client-build#.x86.bundle`
	■ Programme d'installation de Linux 64 bits :
	`link.linux64=https://server/downloads/VMware-Horizon-Client-build#.x64.bundle`
	■ Programme d'installation de Mac OS X :
	`link.mac=https://server/downloads/VMware-Horizon-Client-build#.dmg`
	■ Programme d'installation d'iOS :
	`link.ios=https://server/downloads/VMware-Horizon-Client-iPhoneOS-build#.ipa`
	■ Programme d'installation d'Android :
	`link.android=https://server/downloads/VMware-Horizon-Client-AndroidOS-build#.apk`
	■ Programme d'installation de Chrome OS :
	`link.chromeos=https://server/downloads/VMware-Horizon-Client-ChromeOS-build#.apk`

Changer l'URL du lien de l'aide sur la page de connexion	`link.help` 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.

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

   Cet emplacement doit correspondre aux URL que vous avez spécifiées dans le fichier `portal-links-html-access.properties` ou dans le fichier `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 peuvent alors utiliser des URL relatives au format `/downloads/`*`client-installer-file-name`*.

4 Redémarrez le service du composant Web Horizon.

Utiliser des URI pour configurer des clients Web HTML Access

Vous pouvez utiliser des URI (Uniform Resource Identifiers) pour créer des liens Web ou d'e-mails pour les utilisateurs finaux. Les utilisateurs finaux peuvent cliquer sur ces liens pour démarrer HTML Access, se connecter à un serveur et démarrer un poste de travail distant ou une application publiée avec des options de configuration spécifiques.

Vous pouvez créer ces liens en construisant des URI qui fournissent une partie ou l'intégralité des informations suivantes, afin que les utilisateurs finaux n'aient pas à les fournir.

- Adresse du serveur
- Numéro de port du serveur
- Nom d'utilisateur Active Directory
- Nom d'utilisateur RADIUS ou RSA SecurID, s'il est différent du nom d'utilisateur Active Directory
- Nom de domaine
- Nom d'affichage du poste de travail distant ou de l'application publiée
- Actions incluant la navigation, la réinitialisation, la fermeture 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, éventuellement, une requête pour spécifier un utilisateur, un poste de travail distant ou une application publiée et des actions ou options de configuration.

Spécification d'URI

Utilisez la syntaxe suivante pour créer des URI permettant de démarrer 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 HTML Access. 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 d'installation et de configuration pour chaque type de système client.

action

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

Valeur	Description
`browse`	Affiche la liste des postes de travail distants et applications publiées disponibles hébergés sur le serveur spécifié. Vous ne devez pas spécifier un poste de travail distant ou une application publiée lors de l'utilisation de cette action.
`start-session`	Démarre l'application publiée ou le poste de travail distant spécifié. Si aucune requête d'action n'est fournie et que le nom du poste de travail distant ou de l'application publiée est fourni, `start-session` est l'action par défaut.
`reset`	Éteint puis redémarre le poste de travail distant 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 publiée.
`logoff`	Déconnecte l'utilisateur du système d'exploitation invité sur le poste de travail distant. Cette action n'est pas valide pour une application publiée.
`restart`	Arrête et redémarre le poste de travail distant principal lorsque l'utilisateur confirme la demande d'opération de redémarrage. Cette action n'est pas valide pour une application publiée.

applicationId

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

args

Spécifie les arguments de ligne de commande à ajouter lors du démarrage d'une application publiée. 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 d'affichage du poste de travail distant. Le nom d'affichage est celui qui est spécifié dans Horizon Console lors de la création du pool de postes de travail. Si le nom d'affichage contient un espace, le navigateur utilise **`%20`** pour représenter l'espace.

domainName

Nom de domaine NETBIOS associé à l'utilisateur qui se connecte au poste de travail distant ou à l'application publiée. 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 au poste de travail distant ou à l'application publiée. 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*

unauthenticatedAccessEnabled

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

unauthenticatedAccessAccount

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

Avec un URI, vous pouvez créer des liens hypertextes ou des boutons et inclure ces liens dans un mail ou sur une page Web. Les utilisateurs finaux peuvent cliquer sur ces liens pour ouvrir une application ou un poste de travail distant particulier avec les options de démarrage que vous spécifiez.

Exemples de syntaxe URI

Chacun des exemples d'URI suivants 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`

HTML Access démarre 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`

HTML Access démarre 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`

HTML Access démarre 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`

HTML Access démarre 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 distant dont le nom d'affichage est **Poste de travail principal** et l'utilisateur est connecté au système d'exploitation client.

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

HTML Access démarre 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 s'ouvre.

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. Le port par défaut est 443. Comme un identifiant de poste de travail distant est fourni, le poste de travail distant s'ouvre 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 une application publiée et un poste de travail distant. Lorsque vous spécifiez une application publiée et un poste de travail distant, seul le poste de travail distant démarre.

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

HTML Access démarre 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.

Note Cette action n'est disponible que si un 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.text 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++.

Note Les applications peuvent utiliser les arguments de ligne de commande différemment. 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
```

HTML Access démarre 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.

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

12
```
https://horizon.mycompany.com/?
unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous_user1
```

HTML Access démarre 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 lit **Test Link** et un bouton qui lit **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*.

Gestion des connexions aux postes de travail distants et applications publiées

3

Les utilisateurs finaux peuvent utiliser HTML Access pour se connecter à un serveur et utiliser des postes de travail distants et des applications publiées. À des fins de dépannage, les utilisateurs finaux peuvent réinitialiser les applications publiées et postes de travail distants.

Ce chapitre contient les rubriques suivantes :

Se connecter à un poste de travail distant ou une application publiée

Pour vous connecter à un poste de travail distant ou une application publiée, vous devez fournir le nom d'un serveur et entrer les informations d'identification de votre compte d'utilisateur.

Conditions préalables

- 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 les informations d'identification pour l'authentification RADIUS.
- Obtenez le nom de domaine NETBIOS pour ouvrir une session. Utilisez par exemple `monentreprise` plutôt que `monentreprise.com`.
- Si vous vous trouvez à l'extérieur du réseau de l'entreprise et que vous devez utiliser une connexion VPN pour accéder à des postes de travail distants ou à des applications publiées, vérifiez que le périphérique client est configuré pour utiliser une connexion VPN et activez la connexion.

- Vérifiez que vous disposez du nom de domaine complet (FQDN) du serveur qui fournit l'accès au poste de travail distant ou à l'application publiée. Les traits de soulignement (_) ne sont pas pris en charge dans les noms de serveur. Si le port n'est pas le port 443, vous avez également besoin du numéro de port.

Procédure

1 Si une connexion VPN est requise, activez le VPN.

2 Ouvrez un navigateur et tapez le nom du serveur dans la barre de navigation.

Tapez **`https`** et utilisez le nom de domaine complet du serveur, par exemple, `https://view.company.com`.

Les connexions serveur utilisent toujours TLS. Le port par défaut pour les connexions TLS est 443. Si le serveur n'est pas configuré pour utiliser le port par défaut, utilisez le format **`view.company.com:1443`**.

3 Lorsque la page du portail Web de VMware Horizon s'affiche, sélectionnez l'une des options suivantes.

Le tableau suivant répertorie toutes les options possibles. Les options disponibles dépendent du serveur auquel vous vous connectez et de la manière dont votre environnement est configuré.

Option	Description
Lancer le client natif	(Unified Access Gateway uniquement) Démarre Horizon Client.
Accès au navigateur	(Unified Access Gateway uniquement) Démarre HTML Access.
VMware Horizon HTML Access	Démarre HTML Access.
Installer VMware Horizon Client	Ouvre la page de téléchargement de VMware Horizon Client, où vous pouvez télécharger le programme d'installation d'Horizon Client pour votre système client. **Note** Cette option peut apparaître sous la forme d'un lien plutôt qu'une option.

Vous pouvez également sélectionner une case à cocher pour enregistrer votre sélection et ignorer la page du portail Web de VMware Horizon la prochaine fois que vous entrez le nom du serveur dans le même type de navigateur sur le même système client. Si vous changez d'avis plus tard, vous pouvez utiliser le paramètre **Restaurer la page de lancement par défaut** sur la page Paramètres d'HTML Access pour afficher la page du portail Web de VMware Horizon.

4 Si un message demande les informations d'identification RSA SecurID ou les informations d'identification pour l'authentification RADIUS, entrez-les, 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 Si vous êtes invité à fournir un nom d'utilisateur et un mot de passe, fournissez vos informations d'identification Active Directory.

   a Entrez le nom d'utilisateur et le mot de passe d'un utilisateur autorisé à utiliser au moins un pool de postes de travail ou d'applications.

   b (Facultatif) Sélectionnez un domaine.

      Si vous ne pouvez pas sélectionner un domaine, vous devez entrer le nom d'utilisateur au format *domain**username* ou *username@domain* .

   c Connexion.

7 Pour vous connecter au poste de travail distant ou à l'application publiée, cliquez sur son icône dans la fenêtre de sélection des postes de travail et des applications.

   L'application publiée ou le poste de travail distant s'ouvre dans la fenêtre du navigateur. Pour ouvrir la barre latérale, cliquez sur l'onglet sur le côté gauche de la fenêtre du navigateur. À partir de la barre latérale, vous pouvez ouvrir d'autres postes de travail distants ou applications publiées, configurer des paramètres, copier et coller du texte et effectuer d'autres tâches.

8 (Facultatif) Pour marquer un poste de travail distant ou une application publiée comme favori, sur le poste de travail et l'écran de sélection des postes de travail et applications, cliquez sur l'étoile grise à l'intérieur de l'icône du poste de travail distant ou de l'application publiée.

   L'icône d'étoile grise devient jaune. Lors de votre prochaine connexion, vous pourrez cliquer sur l'icône d'étoile dans la partie supérieure droite de la fenêtre du navigateur pour afficher uniquement les éléments favoris.

Étape suivante

Si, peu après vous être connecté à un poste de travail distant ou à une application publiée, vous êtes déconnecté et une invite vous demande de cliquer sur un lien pour accepter le certificat de sécurité, indiquez si vous approuvez le certificat. Reportez-vous à la section Faire confiance à un certificat racine auto-signé.

Si le fuseau horaire dans le poste de travail distant ou dans l'application publiée n'utilise pas le fuseau horaire défini dans le périphérique client, vous pouvez définir manuellement le fuseau horaire. Reportez-vous à la section Définition du fuseau horaire.

Faire confiance à un certificat racine auto-signé

Parfois, lorsque vous vous connectez à un poste de travail distant ou à une application publiée 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 si un avertissement indique 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 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 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**.

Résultats

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.

Lorsque le mode de Workspace ONE est activé, la barre latérale n'affiche pas tous les postes de travail distants et les applications publiées que vous êtes autorisé à utiliser. Au lieu de cela, il affiche uniquement les postes de travail distants et les applications publiées 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 le poste de travail distants ou l'application publiée dans HTML Access.

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

Si vous disposez d'un compte d'utilisateur Accès non authentifié, vous pouvez vous connecter à un serveur de manière anonyme et vous connecter à vos applications publiées.

Conditions préalables

- 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 de VMware Horizon Console*.

Procédure

1. Pour vous connecter au serveur sur lequel vous disposez d'un accès non authentifié, ouvrez un navigateur et entrez un URI (Uniform Resource Identifier).

   Utilisez l'une des syntaxes d'URI suivantes.

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

authority-part est l'adresse du serveur et, éventuellement, un numéro de port non défini par défaut. Si vous devez spécifier un numéro de port, entrez *adresse-serveur:numéro-port*.

anonymous_account est le compte d'utilisateur Accès non authentifié.

Les connexions utilisent toujours TLS. Le port par défaut pour les connexions TLS est 443. Si le serveur 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 un compte d'utilisateur Accès non authentifié dans l'URI, sélectionnez-en un dans le menu déroulant **Compte d'utilisateur**, si nécessaire, et cliquez sur **Soumettre**.

Si un seul compte d'utilisateur Accès non authentifié est disponible, il 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 de la fenêtre 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.

Note Vous ne pouvez pas vous reconnecter à des sessions d'application non authentifiées. Lorsque vous vous déconnectez du client, vous êtes automatiquement déconnecté de la session d'utilisateur local.

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 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 le fuseau horaire approprié 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.

Pour définir manuellement le fuseau horaire approprié après vous être 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.

Note 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.

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.

H.264 est une norme de l'industrie pour la compression vidéo, qui est le processus de conversion d'une vidéo numérique en un format qui occupe moins de capacité lorsqu'il est stocké ou transmis.

Lorsque vous autorisez le décodage H.264, 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, 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.

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**. **Note** 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.

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

4

HTML Access fournit un environnement de poste de travail et d'application familier et personnalisé. Lorsque vous êtes connecté à un poste de travail distant ou à une application publiée, vous pouvez utiliser une 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.

Vous pouvez copier et coller du texte et transférer des fichiers du périphérique client vers des postes de travail distants et des applications publiées, imprimer à partir d'imprimantes connectées localement dans des postes de travail distants et des applications publiées, utiliser la webcam et le microphone de la machine cliente dans des postes de travail distants et des applications publiées, et partager vos sessions de poste de travail distant avec d'autres utilisateurs.

Ce chapitre contient les rubriques suivantes :

Matrice de prise en charge des fonctionnalités

Lorsque vous planifiez quelles fonctionnalités seront disponibles pour vos utilisateurs finaux, utilisez les informations suivantes pour déterminer quels systèmes d'exploitation invités prennent ces fonctionnalités en charge lorsqu'ils utilisent HTML Access. Des fonctionnalités supplémentaires sont disponibles si les utilisateurs finaux utilisent l'application Horizon Client installée en mode natif, comme Horizon Client pour Windows.

Tableau 4-1. Fonctionnalités prises en charge pour HTML Access sur les postes de travail virtuels Windows

Fonctionnalité	Poste de travail Windows 7	Poste de travail Windows 8.x	Poste de travail Windows 10	Poste de travail Windows Server 2012 R2, Windows Server 2016 ou Windows Server 2019
RSA SecurID ou RADIUS	X	X	X	X
Authentification unique	X	X	X	X
Protocole d'affichage RDP				
Protocole d'affichage PCoIP				
Protocole d'affichage VMware Blast	X	X	X	X
Redirection USB				
Audio/Vidéo en temps réel (RTAV)	X	X	X	X
Redirection multimédia (MMR) Windows Media				
Impression virtuelle				
VMware Integrated Printing			X	Windows Server 2016/2019 uniquement
Impression basée sur l'emplacement	X	X	X	X
Cartes à puce				
Plusieurs écrans	X	X	X	X

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

Fonctionnalités prises en charge pour les postes de travail publiés sur les hôtes RDS

Les hôtes RDS sont des ordinateurs serveurs sur lesquels les services Bureau à distance Windows et Horizon Agent sont installés. Plusieurs utilisateurs peuvent avoir plusieurs sessions simultanées de poste de travail distant sur un hôte RDS. Un hôte RDS peut être une machine physique ou une machine virtuelle.

Tableau 4-2. Fonctionnalités prises en charge pour HTML Access sur les hôtes RDS

Fonctionnalité	Hôte RDS Windows Server 2012 ou 2012 R2	Windows Server 2016	Windows Server 2019
RSA SecurID ou RADIUS	X	Horizon Agent 7.0.2 et versions ultérieures	Horizon Agent 7.7 et versions ultérieures
Authentification unique	X	Horizon Agent 7.0.2 et versions ultérieures	Horizon Agent 7.7 et versions ultérieures
Protocole d'affichage VMware Blast	X	Horizon Agent 7.0.2 et versions ultérieures	Horizon Agent 7.7 et versions ultérieures
VMware Integrated Printing		Horizon Agent 7.12 et versions supérieures	Horizon Agent 7.12 et versions ultérieures
Impression basée sur l'emplacement	X (machine virtuelle uniquement)	Horizon Agent 7.0.2 et versions ultérieures (machine virtuelle uniquement)	Horizon Agent 7.7 et versions ultérieures
Audio/Vidéo en temps réel (RTAV)	Horizon Agent 7.0.2 et versions ultérieures	Horizon Agent 7.0.3 et versions ultérieures	Horizon Agent 7.7 et versions ultérieures
Plusieurs moniteurs (pour les postes de travail basés sur la session uniquement)	X	X	X

Pour plus d'informations sur les éditions de chaque système d'exploitation invité pris en charge, consultez le document *Installation d'Horizon 7*.

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.

Pour afficher une 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**.

Note Si des documents sont ouverts à partir de la même application publiée sur deux serveurs différents, l'application publiée apparaît deux fois dans la liste **Exécution** dans la barre latérale.

Tableau 4-3. Actions de la barre latérale

Action	Procédure
Afficher la barre latérale	Lorsqu'un poste de travail distant ou une application publiée 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 du poste de travail distant ou de l'application publiée.
Masquer la barre latérale	Cliquez sur l'onglet de la barre latérale.
Démarrer un poste de travail distant ou une application publiée	Cliquez sur le nom d'un poste de travail distant ou d'une application publiée dans la liste **Disponible** dans la barre latérale. Les postes de travail distants sont répertoriés en premier.
Rechercher un poste de travail distant ou une application publiée	■ Cliquez sur la zone **Rechercher** et commencez à saisir le nom du poste de travail distant ou de l'application publiée. ■ Pour démarrer un poste de travail distant ou une application publiée, 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 de postes de travail distants ou d'applications publiées 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 postes de travail distants ou des applications publiées	Cliquez sur le nom du poste de travail distant ou de l'application publiée dans la liste **En cours d'exécution** dans la barre latérale.
Activer le mode de sessions multiples pour des applications publiées	Cliquez sur le bouton **Ouvrir le menu** dans la barre latérale, cliquez sur **Paramètres** et faites défiler vers le bas pour atteindre le paramètre **Lancements multiples**. Pour plus d'informations, reportez-vous à la section Utiliser plusieurs sessions d'une application publiée à partir de périphériques clients différents.
Ouvrir le volet Copier et coller	Cliquez sur le bouton **Copier et coller** en haut de la barre latérale. Utilisez ce bouton pour copier le texte dans et depuis des applications sur votre système client local. Pour plus d'informations, reportez-vous à la section Copier et coller du texte. Sous iOS Safari, ce bouton n'est pas disponible, car la fonctionnalité de copier/coller n'est pas prise en charge.
Ouvrir la fenêtre Transfert de fichiers	Pour télécharger des fichiers depuis ou vers un poste de travail distant ou une application publiée, cliquez sur le bouton **Transfert de fichiers** en haut de la barre latérale. Pour plus d'informations, consultez Télécharger des fichiers depuis un poste de travail distant ou une application publiée vers le système client et Charger des fichiers depuis le système client vers un poste de travail distant ou une application publiée.

Tableau 4-3. Actions de la barre latérale (suite)

Action	Procédure
Activer Commande-A, Commande-C, Commande-V et Commande-X	Cette option apparaît dans la fenêtre **Paramètres** uniquement si vous utilisez un Mac. Cliquez sur le bouton de la barre d'outils **Ouvrir le menu** en haut de la barre latérale et cliquez sur **Paramètres**. Lorsque cette fonction est activée, la touche Commande sur le Mac est mappée sur la touche Ctrl sur l'application ou le poste de travail Windows distant. Par exemple, appuyer sur Commande-A sur un clavier Mac équivaut à appuyer sur Ctrl+A sur l'application ou le poste de travail Windows distant.
Fermer un poste de travail distant en cours d'exécution	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. ■ 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	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. Vous êtes invité à enregistrer les modifications apportées aux fichiers.
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**.

Tableau 4-3. Actions de la barre latérale (suite)

Action	Procédure
Utiliser le mode haute résolution sur des machines avec un écran haute résolution, tel que Retina Macbook Pro	Cliquez sur le bouton de la barre d'outils **Ouvrir le menu** en haut de la barre latérale, cliquez sur **Paramètres** et activez **Mode Haute résolution**.
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.
Utiliser plusieurs moniteurs	(Chrome version 55 ou version ultérieure uniquement) Cliquez sur le bouton de la barre d'outils **Ouvrir le menu** en haut de la barre latérale et sélectionnez **Paramètres d'affichage**. Pour plus d'informations, consultez Utiliser plusieurs moniteurs.
Appeler ou fermer le clavier logiciel	(iOS Safari uniquement) Cliquez sur l'icône du clavier en haut de la barre latérale. Vous pouvez également appeler ou fermer le clavier logiciel en appuyant sur l'écran avec trois doigts.
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.
Afficher un poste de travail distant ou une application publiée en mode plein écran	Cliquez sur le bouton de la barre d'outils **Ouvrir le menu** en haut de la barre latérale et cliquez sur **Plein écran**.
Quitter le mode plein écran	Cliquez sur le bouton de la barre d'outils **Ouvrir le menu** en haut de la barre latérale et cliquez sur **Quitter le plein écran**.
Envoyer Échap à un poste de travail distant ou une application publiée qui est en mode plein écran	Cliquez sur le bouton de la barre d'outils **Ouvrir le menu** en haut de la barre latérale et cliquez sur **Envoyer Échap**.

Écrans et résolution d'écran

Vous pouvez étendre un poste de travail distant ou une application publiée sur plusieurs moniteurs. Si vous disposez d'un moniteur haute résolution, vous pouvez afficher l'application publiée ou le poste de travail distant en pleine résolution.

Utiliser plusieurs moniteurs

Vous pouvez utiliser plusieurs moniteurs pour afficher une fenêtre de poste de travail distant. 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. Vous devez sélectionner des moniteurs adjacents pour

la configuration à plusieurs moniteurs. Vous pouvez placer les moniteurs côte à côte ou les empiler verticalement.

Conditions préalables

Vous devez utiliser HTML Access dans Chrome version 55 ou version ultérieure.

Procédure

1. Démarrez HTML Access 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 ouvrir 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 **Plusieurs moniteurs**.
5. Dans la fenêtre **Plusieurs moniteurs**, cliquez sur **Ajouter l'écran**.

   Note Si la fenêtre du navigateur **Sélecteur d'écrans** ne s'affiche pas, ajoutez l'adresse du nom de domaine complet du serveur dans la section Exceptions liées aux fenêtres contextuelles de la fenêtre **Paramètres de contenu** de votre navigateur.
6. Faites glisser la fenêtre de navigateur **Sélecteur d'écrans** de sorte qu'elle s'affiche sur l'écran de l'autre moniteur que vous voulez utiliser.

   Le message dans la fenêtre du navigateur **Sélecteur d'écrans** change et une icône rectangulaire grise apparaît.
7. Pour confirmer que vous souhaitez utiliser l'affichage du moniteur actuel, dans la fenêtre du navigateur **Sélecteur d'écrans**, cliquez sur l'icône de moniteur **+**.

   Le message `En attente des autres écrans` s'affiche sur l'écran du moniteur actuel et l'icône de moniteur grise dans la fenêtre **Plusieurs moniteurs** sur votre écran principal devient verte.
8. Lorsque vous avez terminé d'ajouter les écrans de surveillance que vous souhaitez utiliser pour la session, cliquez sur **OK** dans la fenêtre **Plusieurs moniteurs**.

   La fenêtre **Plusieurs moniteurs** 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.

   Note Pour 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**.

Définition de la résolution d'écran

HTML Access peut redimensionner le poste de travail distant pour qu'il corresponde à la taille de la fenêtre du navigateur. Pour utiliser cette fonctionnalité, un administrateur Horizon doit configurer le poste de travail distant pour qu'il dispose de la quantité de RAM vidéo (VRAM) appropriée. La configuration VRAM par défaut est 36 Mo. Si vous n'utilisez pas d'applications 3D, la configuration minimale de VRAM est de 16 Mo.

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 le poste de travail distant ou l'application publiée afin d'utiliser cette résolution. 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 %.

La fonctionnalité de mode haute résolution ne peut pas modifier la résolution d'une session distante active. Vous devez vous déconnecter, puis vous reconnecter, pour que la fonctionnalité soit appliquée.

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

- La fonctionnalité graphique accélérée par le logiciel, disponible avec vSphere 5.0 ou version ultérieure, vous 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 des instructions, reportez-vous à la section « Estimation de la mémoire requise pour les postes de travail virtuels » dans le document *Planification de l'architecture Horizon 7*.

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.

Si la synchronisation DPI est désactivée, la mise à l'échelle de l'affichage est utilisée. La fonctionnalité de mise à l'échelle de l'affichage met le poste de travail distant ou l'application publiée à l'échelle appropriée.

Pour définir manuellement la résolution, vous pouvez activer le paramètre **Mode Haute résolution**. Pour plus d'informations, reportez-vous à la section Définition de la résolution d'écran.

Le paramètre de stratégie du groupe de l'agent **Synchronisation DPI** détermine si la fonctionnalité de synchronisation DPI est activée ou non. Cette fonctionnalité est activée par défaut. Grâce à la synchronisation DPI, la valeur DPI de la session distante change pour correspondre à la valeur DPI de la machine cliente lorsque vous vous connectez à un poste de travail distant ou à une application publiée. La fonctionnalité de synchronisation DPI requiert Horizon Agent 7.0.2 ou version ultérieure.

Si le paramètre de stratégie du groupe de l'agent **Synchronisation DPI par connexion** est activé, ainsi que le paramètre de stratégie de groupe **Synchronisation DPI**, l'option Synchronisation DPI est prise en charge lorsque vous vous reconnectez à un poste de travail distant. Cette fonctionnalité est désactivée par défaut. La fonctionnalité de synchronisation DPI par connexion requiert Horizon Agent 7.8 ou version ultérieure.

Pour plus d'informations sur les paramètres de stratégie de groupe **Synchronisation DPI** et **Synchronisation DPI par connexion**, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Pour les postes de travail virtuels, la fonctionnalité de synchronisation DPI est prise en charge sur les systèmes d'exploitation invités suivants :

- Windows 7 32 ou 64 bits
- Windows 8.x 32 ou 64 bits
- Windows 10 32 ou 64 bits
- Windows Server 2012 R2 configuré en tant que poste de travail
- Windows Server 2016 configuré en tant que poste de travail
- Windows Server 2019 configuré en tant que poste de travail

Pour les applications et les postes de travail publiés, la fonctionnalité de synchronisation DPI est prise en charge sur les hôtes RDS suivants :

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Pour les postes de travail virtuels, la fonctionnalité de synchronisation DPI par connexion est prise en charge sur les systèmes d'exploitation invités suivants :

- Windows 10 version 1607 et version ultérieure
- Windows Server 2016 et version ultérieure configuré en tant que poste de travail

La fonctionnalité de synchronisation DPI par connexion n'est pas prise en charge pour les postes de travail publiés ou les applications publiées.

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

- Si vous modifiez le paramètre DPI sur le système client, mais que le paramètre DPI ne change pas sur le poste de travail distant, vous aurez peut-être besoin de vous déconnecter et de vous reconnecter afin qu'Horizon Client détecte le nouveau paramètre DPI sur le système client.
- 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 aurez peut-être besoin de vous déconnecter, puis de 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.
- Pour effectuer une synchronisation avec un autre moniteur ayant 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.

Utiliser le mode plein écran

Vous pouvez afficher un poste de travail distant ou une application publiée en mode plein écran.

Vous ne pouvez pas utiliser le mode plein écran dans les situations suivantes.

- Vous utilisez plusieurs moniteurs.
- Le navigateur est en mode plein écran ou est agrandi en faisant glisser la souris.
- Vous utilisez Safari.

Conditions préalables

Connectez-vous au poste de travail distant ou à l'application publiée.

Procédure

- Pour afficher le poste de travail distant ou l'application publiée en mode plein écran, cliquez sur le bouton **Ouvrir le menu** en haut de la barre latérale et cliquez sur **Plein écran**.
- Pour quitter le mode plein écran, cliquez sur le bouton **Ouvrir le menu** en haut de la barre latérale et cliquez sur **Quitter le plein écran**.

  Vous pouvez également appuyer sur la touche Échap du clavier du système client.

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 pixels. 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.

Partage de sessions de poste de travail distant

Avec la fonctionnalité de collaboration de session, vous pouvez inviter des utilisateurs à rejoindre une session de poste de travail distant existante. Une session de poste de travail distant qui est partagée de cette manière est appelée session de collaboration. L'utilisateur qui partage une session avec un autre utilisateur est appelé le propriétaire de la session et l'utilisateur qui rejoint une session partagée est appelé un collaborateur de session.

Un administrateur Horizon doit activer la fonctionnalité de collaboration de session.

Pour les postes de travail Windows, 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 la section 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 postes de travail Windows, 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*.

Pour plus d'informations sur l'activation de la fonctionnalité de collaboration de session pour des postes de travail Linux, consultez le document *Configuration des postes de travail Horizon 7 for Linux*.

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

Avec la fonctionnalité de collaboration de session, vous pouvez inviter des utilisateurs à rejoindre une session de poste de travail distant en envoyant des invitations de collaboration par e-mail,

dans un message instantané (postes de travail distants Windows uniquement) ou en copiant un lien vers le presse-papiers et en transférant le lien aux utilisateurs.

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. Un administrateur Horizon peut modifier le nombre maximal d'utilisateurs que vous pouvez inviter.

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 à partager. 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 d'application publiée.

Conditions préalables

- La fonctionnalité de collaboration de session doit être activée et configurée.
- 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 pour un poste de travail distant Windows, Skype Entreprise doit être installé et configuré.

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 peut être différente selon la version du système d'exploitation.

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. Pour les postes de travail distants Windows, la fonctionnalité de collaboration de session mémorise l'utilisateur la prochaine fois que vous entrez son nom d'utilisateur ou son adresse e-mail.

4 Sélectionnez une méthode d'invitation.

   Toutes les méthodes d'invitation peuvent ne pas être disponibles.

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	(Postes de travail distants Windows uniquement) 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.

Résultats

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 permet d'exécuter certaines actions.

Lorsqu'un collaborateur de session accepte votre invitation à rejoindre une session de poste de travail distant Windows, 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. Lorsqu'un collaborateur de session accepte votre invitation à rejoindre une session de poste de travail distant Linux, une notification s'affiche dans le poste de travail de session principale.

Étape suivante

Gérez la session de poste de travail distant dans la boîte de dialogue VMware Horizon Collaboration. Reportez-vous à la section Gérer une session de poste de travail distant partagée.

Gérer une session de poste de travail distant partagée

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 poste de travail distant partagée et vous permet d'exécuter certaines actions.

Un administrateur Horizon peut empêcher le transfert de contrôle à un collaborateur de session. Pour les postes distants Windows, reportez-vous au paramètre de stratégie de groupe **Autoriser le contrôle de transmission à des collaborateurs** dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*. Pour les postes de travail distants Linux, reportez-vous au paramètre `collaboration.enableControlPassing` du document *Configuration des postes de travail Horizon 7 for Linux*.

Conditions préalables

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.

   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 collaborative.

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. Dans les postes de travail distants Windows, vous pouvez également arrêter la session collaborative en cliquant sur le bouton **Arrêter** en regard de l'icône **Collaboration de session VMware Horizon**. Le bouton **Arrêter** n'est pas disponible dans les postes de travail distants Linux.

Rejoindre une session de poste de travail distant

Avec la fonctionnalité de collaboration de session, vous pouvez cliquer sur le lien dans une invitation de collaboration pour rejoindre une session de poste de travail distant. 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 dans la fenêtre de sélection des applications et des postes de travail distants.

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

Note 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.

Lorsque vous rejoignez une session de poste de travail distant avec la fonctionnalité de collaboration de session, vous ne pouvez pas utiliser les fonctionnalités suivantes dans la session de poste de travail distant.

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

Vous ne pouvez pas non plus modifier la résolution du poste de travail distant dans la session de poste de travail distant.

Conditions préalables

Pour rejoindre une session de poste de travail distant avec la fonctionnalité de collaboration de session, 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 **VMware Horizon Collaboration** 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.

Copier et coller du texte

Vous pouvez copier et coller du texte brut et enrichi au format HTML entre le périphérique client et les postes de travail distants et les applications publiées. 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.

Un administrateur Horizon peut configurer la fonctionnalité de copier-coller à l'aide des paramètres de stratégie de groupe qui concernent Horizon Agent pour les postes de travail distants et les applications publiées. Pour plus d'informations, reportez-vous à la section Paramètres de stratégie de groupe de HTML Access.

Lorsque vous copiez et collez du texte enrichi, les restrictions suivantes s'appliquent.

- Il n'est pas possible de copier-coller des images.
- Si vous copiez du texte enrichi à partir du périphérique client et que la destination est l'application WordPad, seul le texte brut est copié et collé.
- Il n'est pas possible de copier-coller du texte enrichi lorsque vous utilisez HTML Access sur un navigateur Internet Explorer (IE), Microsoft Edge ou Safari. Vous devez utiliser la fenêtre **Copier et coller**. Reportez-vous à la section Utiliser la fenêtre Copier et coller.
- Un administrateur Horizon peut utiliser les paramètres de stratégie 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 du texte dans le Presse-papiers, seuls les filtres de texte sont compatibles avec HTML Access. Pour plus d'informations sur les paramètres de stratégie de filtre du format de Presse-papiers, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Si vous utilisez HTML Access avec un navigateur Chrome ou Firefox, consultez les conseils suivants lors de l'utilisation de la fonctionnalité de Presse-papiers.

- La première fois que vous vous connectez à un poste de travail distant ou à une application publiée, la boîte de dialogue Guide de l'utilisateur du Presse-papiers s'affiche. Pour fermer la boîte de dialogue et ne plus jamais la voir, cliquez sur **OK**.
- Par défaut, l'icône du Presse-papiers sur la barre latérale est sélectionnée et s'affiche en gris.
  - Si l'icône du Presse-papiers est sélectionnée, lorsque vous copiez du texte à partir d'un poste de travail distant ou d'une application publiée, une boîte de dialogue s'affiche pour vous demander de confirmer la copie du texte dans le Presse-papiers du système client local. Cliquez sur **OK**.
  - Si l'icône du Presse-papiers est désélectionnée, la boîte de dialogue de confirmation ne s'affiche pas lorsque vous copiez du texte à partir du poste de travail distant ou de l'application publiée dans le Presse-papiers du système client local.

- Si vous passez votre souris sur l'icône du Presse-papiers sur la barre latérale, une info-bulle explique le fonctionnement de la fonctionnalité du Presse-papiers.

Le Presse-papiers peut stocker 1 Mo de données au maximum pour tous les types opérations de copier-coller. Si les données de texte brut et de texte enrichi utilisent moins de la taille maximale du Presse-papiers, le texte formaté est collé. Il arrive souvent que le texte enrichi ne puisse pas être tronquée. Ainsi, si le texte et le formatage utilisent plus de la taille maximale du Presse-papiers, le texte enrichi est ignoré et le texte brut est collé. Si vous ne pouvez pas coller l'ensemble du texte formaté que vous avez sélectionné en une seule opération, vous devrez peut-être copier et coller de plus petits volumes en plusieurs opérations.

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.

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

Utiliser la fenêtre Copier et coller

Pour copier et coller du texte depuis un navigateur Internet Explorer (IE), Microsoft Edge ou Safari, vous devez utiliser le bouton **Copier et coller** en haut de la barre latérale pour afficher la fenêtre **Copier et coller**.

Cette procédure décrit comment utiliser la fenêtre **Copier et coller** pour copier le texte depuis un navigateur IE, Edge ou Safari sur le système client local vers une application dans un poste de travail distant ou vers une application publiée. Elle indique également comment copier le texte depuis une application dans un poste de travail distant ou une application publiée vers le système client.

Si vous copiez et collez du texte entre des applications publiées ou entre des postes de travail distants, il vous suffit de copier et coller comme vous le faites normalement. Il n'est pas nécessaire d'utiliser la fenêtre **Copier et coller**.

Lorsque vous utilisez un navigateur IE, Edge ou Safari, la fenêtre **Copier et coller** est uniquement requise pour la synchronisation du Presse-papiers sur le système local avec le Presse-papiers dans la machine distante.

Le texte dans la fenêtre **Copier et coller** affiche l'un des messages suivants pour indiquer dans quel sens vous pouvez 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.`

Note Le paramètre de stratégie de groupe de redirection du Presse-papiers par défaut permet de copier et coller uniquement depuis le système client dans un poste de travail distant ou une application publiée. Pour pouvoir copier depuis un poste de travail distant ou une application publiée vers le système client, le paramètre de stratégie de groupe doit être activé dans les deux sens.

Conditions préalables

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**. Si vous utilisez un Mac, cette option s'affiche uniquement dans la fenêtre **Réglages**.

Un administrateur Horizon doit conserver la stratégie par défaut, ce qui permet aux utilisateurs de copier/coller du texte depuis des systèmes clients sur leurs postes de travail distants et applications publiées, 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 le système client vers une application dans un poste de travail distant, ou depuis le système client vers une application publiée, procédez comme suit.
  a. Copiez le texte dans l'application client locale.
  b. Dans HTML Access, ouvrez la barre latérale et 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 sur un système Windows ou sur Commande + V sur un Mac.

     Le message suivant apparaît brièvement : « `Presse-papiers distant synchronisé` ».
  d. Cliquez sur l'application dans laquelle vous voulez coller le texte et appuyez sur Ctrl+V.

     Le texte est collé dans l'application.

- Pour copier du texte depuis une application dans un poste de travail distant vers le système client, ou depuis une application publiée vers le système client, procédez comme suit.
  a Copiez le texte dans l'application.
  b Dans HTML Access, ouvrez la barre latérale et cliquez sur **Copier et coller** en haut de la barre latérale.

    La fenêtre **Copier et coller** apparaît et affiche le texte 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 sur un système Windows 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 le 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 le système client.

Transfert de fichiers entre le client et un poste de travail distant ou une application publiée

À l'aide de la fonctionnalité de transfert de fichiers, vous pouvez transférer des fichiers entre le système client et un poste de travail distant ou une application publiée.

Un 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 VMware Blast. Ce paramètre de stratégie de groupe comprend les valeurs suivantes.

- Si la valeur **Chargement et téléchargement désactivés** est sélectionnée, le bouton **Transfert de fichiers** est désactivé.
- Si la valeur **Chargement de fichiers uniquement activé** est sélectionnée (paramètre par défaut), seul l'onglet **Charger** s'affiche dans la fenêtre **Transférer des fichiers**.
- Si la valeur **Téléchargement de fichiers uniquement activé** est sélectionnée, seul l'onglet **Télécharger** s'affiche dans la fenêtre **Transférer des fichiers**.

Si le paramètre de stratégie de groupe **Configurer la redirection du Presse-papiers** est désactivé du serveur vers le client, le téléchargement de fichiers est également désactivé.

Pour plus d'informations sur ces paramètres de stratégie de groupe, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Cette fonction présente les limites suivantes :

- Vous pouvez télécharger des fichiers ayant une capacité jusqu'à 500 Mo et charger des fichiers ayant une capacité jusqu'à 2 Go.

- 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 et version ultérieure ne prend pas en charge le téléchargement.
- Si un transfert de fichiers est en cours dans une session distante et que vous ouvrez une connexion à une deuxième session distante, et si un avertissement de sécurité s'affiche, le transfert de fichiers de la première session est abandonné si vous ignorez l'avertissement et continuez à vous connecter à la seconde session distante.
- Si vous chargez un fichier à l'aide d'Internet Explorer 11, ou à l'aide de Chrome sur un Chromebook, un message d'erreur s'affiche comme prévu si vous glissez-déposez des dossiers, des fichiers de taille nulle ou des fichiers supérieurs à 2 Go. Après avoir fermé le message d'erreur, vous ne pouvez plus glisser-déposer de fichiers pour les transférer.
- Vous ne pouvez pas utiliser cette fonctionnalité avec des postes de travail Linux distants ou des périphériques Android.

Télécharger des fichiers depuis un poste de travail distant ou une application publiée vers le système client

Vous pouvez télécharger des fichiers à partir d'un poste de travail distant ou d'une application publiée vers le système client.

Un administrateur Horizon peut désactiver cette fonctionnalité. Pour plus d'informations, reportez-vous à la section Transfert de fichiers entre le client et un poste de travail distant ou une application publiée.

Procédure

1. Connectez-vous au poste de travail distant ou à l'application publiée.
2. Pour ouvrir la barre latérale, cliquez sur l'onglet de la barre latérale.
3. Cliquez sur l'icône de transfert de fichiers située en haut de la barre latérale.

   La fenêtre **Transférer des fichiers** s'affiche.
4. Cliquez sur **Télécharger** dans la fenêtre **Transférer des fichiers**.
5. Sélectionnez un ou plusieurs fichiers à télécharger.
6. Pour commencer le transfert de fichiers, appuyez sur Ctrl+C.

   Les fichiers s'affichent dans l'onglet **Télécharger** de la fenêtre **Transférer des fichiers**.

7 Pour télécharger les fichiers sur le système client, cliquez sur l'icône de téléchargement (la flèche vers le bas).

   Les fichiers s'affichent dans le dossier `Téléchargements` sur le système client.

Charger des fichiers depuis le système client vers un poste de travail distant ou une application publiée

Vous pouvez charger des fichiers depuis le système client vers un poste de travail distant ou une application publiée.

Un administrateur Horizon peut désactiver cette fonctionnalité. Pour plus d'informations, reportez-vous à la section Transfert de fichiers entre le client et un poste de travail distant ou une application publiée.

Procédure

1 Connectez-vous au poste de travail distant ou à l'application publiée.

2 Pour ouvrir la barre latérale, cliquez sur l'onglet de la barre latérale.

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

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

4 Pour charger les fichiers, glissez-déposez-les vers l'onglet **Charger** dans la fenêtre **Transférer des fichiers**, ou cliquez sur **Choisir des fichiers** dans l'onglet **Charger** et sélectionnez les fichiers à charger.

   Les fichiers chargés s'affichent dans le dossier `Documents`.

Impression à partir d'un poste de travail distant ou d'une application publiée

Vous pouvez imprimer sur une imprimante réseau ou une imprimante connectée localement à partir d'un poste de travail distant ou d'une application publiée.

Pour utiliser cette fonctionnalité, Horizon Agent 7.12 ou version ultérieure doit être installé sur la machine virtuelle ou sur l'hôte RDS, et l'option VMware Integrated Printing doit être activée pendant l'installation. Pour plus d'informations, reportez-vous au document *Configuration des postes de travail virtuels dans Horizon 7* ou *Configuration de pools de postes de travail et d'applications dans Horizon 7*.

Vous pouvez désactiver la fonctionnalité VMware Integrated Printing pour les utilisateurs HTML Access à l'aide du paramètre de stratégie de groupe **Désactiver la redirection de l'imprimante pour le client externe au bureau**. Pour plus d'informations, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Définir les préférences d'impression de la fonctionnalité de VMware Integrated Printing

Vous pouvez définir des préférences d'impression dans un poste de travail distant pour la fonctionnalité de VMware Integrated Printing. Avec la fonctionnalité de VMware Integrated Printing, vous pouvez utiliser des imprimantes locales ou réseau depuis un poste de travail distant Windows sans avoir à installer d'autres pilotes d'imprimante dans celui-ci. Pour chaque imprimante disponible via cette fonction, vous pouvez définir des préférences pour la compression des données, la qualité d'impression, l'impression recto verso, la couleur et d'autres paramètres.

Conditions préalables

Pour utiliser VMware Integrated Printing, un administrateur Horizon doit activer cette fonctionnalité dans le poste de travail distant. Cette tâche implique l'activation de l'option **VMware Integrated Printing** dans le programme d'installation d'Horizon Agent et la définition des stratégies qui contrôlent le comportement de l'impression virtuelle. Pour plus d'informations sur l'installation d'Horizon Agent, 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*. Pour plus d'informations sur la configuration des stratégies, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Pour déterminer si la fonctionnalité de VMware Integrated Printing est installée dans un poste de travail distant, vérifiez que les fichiers `C:\Program Files\Common Files\VMware\Remote Experience\x64\vmware-print-redir-server.exe` et `C:\Program Files\Common Files\VMware\Remote Experience\x64\vmware-print-redir-service.exe` existent dans le système de fichiers de poste de travail distant.

Cette fonctionnalité requiert Horizon Agent 7.12 ou version ultérieure.

Procédure

1. Dans le poste de travail distant Windows, accédez à **Panneau de configuration > Matériel et audio > Périphériques et imprimantes**.
2. Dans la fenêtre **Périphériques et imprimantes**, cliquez avec le bouton droit sur l'imprimante virtuelle et sélectionnez **Propriétés de l'imprimante** dans le menu contextuel.

   Dans un poste de travail de machine virtuelle mono-utilisateur, chaque imprimante virtuelle apparaît sous la forme *<nom_imprimante>*(*vdi*). Par défaut, dans un poste de travail publié ou une application publiée, chaque imprimante virtuelle apparaît sous la forme *<nom_imprimante>*(v*<ID_session>*).
3. Dans l'onglet **Général**, cliquez sur **Préférences**.
4. Dans la boîte de dialogue Options d'impression, sélectionnez les différents onglets et précisez les paramètres à utiliser.
5. Cliquez sur **OK** pour enregistrer les modifications.

Utiliser plusieurs sessions d'une application publiée à partir de périphériques clients différents

Lorsque le mode de sessions·multiples est activé pour une application publiée, vous pouvez utiliser plusieurs sessions de la même application publiée lorsque vous vous connectez au serveur depuis différents périphériques clients.

Par exemple, si vous ouvrez une application publiée en mode de sessions·multiples sur le client A, puis que vous ouvrez la même application publiée sur le client B, elle reste ouverte sur le client A et une nouvelle session de l'application publiée s'ouvre sur le client B. En comparaison, lorsque le mode de sessions·multiples est désactivé (mode de session unique), la session de l'application publiée sur le client A se déconnecte et se reconnecte sur le client B.

La fonctionnalité de mode de sessions multiples présente les limites suivantes.

- Le mode de sessions multiples ne fonctionne pas pour les applications qui ne prennent pas en charge plusieurs instances, telles que Skype Entreprise.
- Si la session d'application est déconnectée lorsque vous utilisez une application publiée en mode de sessions multiples, vous êtes déconnecté automatiquement et les données non enregistrées sont perdues.

Conditions préalables

Un administrateur Horizon doit activer le mode de sessions multiples pour le pool d'applications. Les utilisateurs ne peuvent pas modifier le mode de sessions multiples pour une application publiée, sauf si un administrateur Horizon l'autorise. Reportez-vous à *Configuration d'applications et de postes de travail publiés dans Horizon 7*. Cette fonctionnalité requiert Horizon 7 7.7 ou version ultérieure.

Procédure

1. Connectez-vous à un serveur.
2. Cliquez sur le bouton **Paramètres** de la barre d'outils dans le coin supérieur droit de la fenêtre de sélection des postes de travail et applications, faites défiler vers le bas pour atteindre le paramètre **Lancements multiples**, puis cliquez sur **Définir**.

   Si vous avez démarré précédemment un poste de travail distant ou une application publiée, vous pouvez également cliquer sur le bouton **Ouvrir le menu** dans la barre latérale, cliquer sur **Paramètres** et faire défiler vers le bas pour atteindre le paramètre **Lancements multiples**. Si aucune application publiée n'est disponible pour une utilisation en mode de sessions multiples, le paramètre **Lancements multiples** est grisé.
3. Sélectionnez les applications publiées que vous voulez utiliser en mode de sessions multiples et cliquez sur **OK**.

   Si un administrateur Horizon a appliqué le mode de sessions multiples pour une application publiée, vous ne pouvez pas modifier ce paramètre.

Réglage du son sur les postes de travail distants et les applications publiées

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

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.

Note 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 Windows), sur Ctrl+Commande (sur Mac) ou Ctrl+Recherche (sur 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 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 ou Windows 10.

Tableau 4-4. 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.	
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.

Tableau 4-4. Raccourcis de touche Windows pour les postes de travail distants Windows 10 et Windows Server 2016 (suite)

Clés	Action	Limites
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 4-5. 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.	
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.

Tableau 4-5. Raccourcis de touche Windows pour les postes de travail distants Windows 8.x et Windows Server 2012 R2 (suite)

Clés	Action	Limites
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 4-6. Raccourcis de touche Windows pour les postes de travail distants Windows 7

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`.	
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.

Tableau 4-6. Raccourcis de touche Windows pour les postes de travail distants Windows 7 (suite)

Clés	Action	Limites
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.	

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.

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 4-7. 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 4-7. 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 le travail distant ?
Coréen	Coréen	Mode de saisie en anglais	Coréen	Oui
Espagnol	Espagnol	Non	Espagnol	Non

Dépannage de Horizon Client

5

Vous pouvez résoudre la plupart des problèmes avec Horizon Client en redémarrant ou en réinitialisant les postes de travail distants ou les applications publiées, ou en réinstallant Horizon Client.

Ce chapitre contient les rubriques suivantes :

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*.

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 `https://`*`ConnectionServerFQDN`*`?desktopId=`*`desktop_name`*`&action=restart`.

Résultats

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.

Étape suivante

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 des postes de travail distants ou des applications publiées.

Réinitialiser des postes de travail distants 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'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 d'applications publiées entraîne la fermeture de toutes les applications ouvertes.

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**.

Option	Action
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 `https://`*`ConnectionServerFQDN`*`?desktopId=`*`desktop_name`*`&action=reset`.

Résultats

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.

Étape suivante

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