Guide d'installation et de configuration de VMware Horizon Client pour Chrome

VMware Horizon Client for Chrome 2103



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

Copyright © 2021 VMware, Inc. Tous droits réservés. Informations relatives aux copyrights et marques commerciales.

Table des matières

Guide d'installation et de configuration de VMware Horizon Client pour Chrome 5

1 Configuration et installation 6
- Configuration système requise 6
- Exigences de l'authentification par carte à puce 7
  - Limitations de l'authentification par carte à puce 8
- Préparation du Serveur de connexion 9
  - Règles de pare-feu pour un accès via un navigateur Web client 11
- Installer ou mettre à niveau Horizon Client pour Chrome 12
- Utilisation de la console d'administration de Google pour configurer des périphériques Chromebook inscrits 13
  - Liste des instances du serveur de connexion 13
  - Instance du serveur de connexion par défaut 14
  - Fonctionnalités du client 14
  - Fonctionnalités du serveur 16
- Configurer les agents HTML Access pour utiliser les nouveaux certificats TLS 18
  - Ajouter le composant logiciel enfichable Certificat à MMC sur un poste de travail distant 19
  - Importer un certificat pour l'agent HTML Access dans un magasin de certificats Windows 19
  - Importer des certificats racine et intermédiaires pour l'agent HTML Access 21
  - Définir l'empreinte numérique de certificat dans le registre Windows 21
- Configurer les agents HTML Access pour utiliser des suites de chiffrement spécifiques 22
- Utilisation d'un certificat signé par une autorité de certification avec Unified Access Gateway 23
- Configurer le partage de données d'Horizon Client 24
  - Données collectées par VMware 24

2 Gestion des connexions aux postes de travail distants et applications publiées 26
- Se connecter à un poste de travail distant ou une application publiée 26
- Utiliser l'accès non authentifié pour se connecter à des applications publiées 29
- Faire confiance à un certificat racine auto-signé 29
- Définition du fuseau horaire 30
- Gérer les raccourcis de serveur 30
- Fermer une session ou se déconnecter 31

3 Utilisation d'un poste de travail distant ou d'une application publiée 33
- Prise en charge des fonctionnalités pour les clients Chrome 34

Mouvements 35
Modifier le mode d'affichage de postes de travail distants 36
Définition de la résolution d'écran 37
Utiliser le mode plein écran 38
Utilisation de la synchronisation DPI 39
Utilisation de la fonctionnalité Audio/Vidéo en temps réel pour webcams et microphones 41
Sélectionner une webcam ou un microphone préféré sur un Chromebook 41
Utilisation de postes de travail distants 42
Utilisation d'applications publiées 43
Utilisation d'applications publiées en mode Kiosque 43
Copier et coller du texte et des images 44
Journalisation des activités copier et coller 45
Transfert de fichiers entre le client et un poste de travail distant ou une application publiée 45
Partager l'accès aux dossiers et lecteurs locaux avec la redirection de lecteur client 46
Utiliser des périphériques USB sur un poste de travail distant 48
Impression à partir d'un poste de travail distant ou d'une application publiée 49
Définir les préférences d'impression de la fonctionnalité de VMware Integrated Printing 50
Utiliser plusieurs sessions d'une application publiée à partir de périphériques clients différents 51
Réglage du son sur les postes de travail distants et les applications publiées 52
Combinaisons de touches de raccourci 52
Internationalisation 55

4 Dépannage 56
Redémarrer un poste de travail distant 56
Réinitialiser des postes de travail distants ou des applications publiées 57
Désinstaller Horizon Client pour Chrome 58
Activer la collecte de journaux 59

Guide d'installation et de configuration de VMware Horizon Client pour Chrome

Ce guide décrit l'installation, la configuration et l'utilisation de VMware Horizon® Client™ pour Chrome sur un Chromebook.

Ces informations sont destinées aux administrateurs qui doivent configurer un déploiement d'Horizon comportant des Chromebooks. Les informations sont destinées aux administrateurs système expérimentés qui connaissent bien le fonctionnement des centres de données et de la technologie des machines virtuelles.

Si vous êtes utilisateur final, reportez-vous au document *Guide de l'utilisateur de VMware Horizon Client pour Chrome* ou affichez l'aide en ligne d'Horizon Client pour Chrome.

Configuration et installation

1

La configuration d'Horizon Client implique l'installation de l'application Horizon Client pour Chrome sur les terminaux clients, la configuration du Serveur de connexion et l'ouverture des ports requis.

Ce chapitre contient les rubriques suivantes :

- Configuration système requise
- Exigences de l'authentification par carte à puce
- Préparation du Serveur de connexion
- Installer ou mettre à niveau Horizon Client pour Chrome
- Utilisation de la console d'administration de Google pour configurer des périphériques Chromebook inscrits
- Configurer les agents HTML Access pour utiliser les nouveaux certificats TLS
- Configurer les agents HTML Access pour utiliser des suites de chiffrement spécifiques
- Utilisation d'un certificat signé par une autorité de certification avec Unified Access Gateway
- Configurer le partage de données d'Horizon Client

Configuration système requise

Le périphérique sur lequel vous utilisez Horizon Client pour Chrome doit répondre à la configuration logicielle requise.

Modèles de périphérique

Chromebook

Systèmes d'exploitation

Chrome OS 75 ou version ultérieure

Architecture du CPU

ARM ou x86

Serveur de connexion et Horizon Agent

Dernière version de maintenance d'Horizon 7 version 7.5.x et versions ultérieures.

Si des systèmes clients se connectent en dehors du pare-feu de l'entreprise, utilisez un dispositif Unified Access Gateway pour que les systèmes clients ne nécessitent pas de connexion VPN. Si votre société dispose d'un réseau interne sans fil afin de permettre un accès routable aux postes de travail distants que des périphériques peuvent utiliser, il n'est pas nécessaire de configurer Unified Access Gateway ou une connexion VPN.

Authentification par carte à puce

Reportez-vous à la section Exigences de l'authentification par carte à puce.

Pare-feu tiers

Les pare-feux doivent autoriser le trafic entrant sur certains ports TCP. Reportez-vous à la section Règles de pare-feu pour un accès via un navigateur Web client.

Protocole d'affichage

VMware Blast

Exigences de l'authentification par carte à puce

Les Chromebooks qui utilisent une carte à puce pour l'authentification utilisateur doivent répondre à certaines exigences.

Exigences logicielles et matérielles du client

Les utilisateurs qui s'authentifient avec des cartes à puce doivent posséder une carte à puce physique et chaque carte à puce doit contenir un certificat utilisateur. Les cartes à puce suivantes sont prises en charge.

- U.S. Department of Defense Common Access Card (CAC)
- U.S. Federal Government Personal Identity Verification (PIV) (également appelée carte à puce FIPS 201)

Chaque Chromebook qui utilise une carte à puce pour l'authentification utilisateur doit disposer des logiciels et matériels suivants.

- Horizon Client pour Chrome
- Un lecteur de carte à puce compatible
- Application Smart Card Connector de Google

  L'application de connecteur fournit une prise en charge de base pour les cartes à puce sur Chrome OS. Vous pouvez télécharger l'application Smart Card Connector sur Chrome Web Store. VMware recommande d'utiliser l'application Smart Card Connector de Google version 1.2.16.1 ou versions ultérieures.
- Application CSSI Smart Card Middleware de Charismathics

L'intergiciel communique avec la carte à puce et autres certificats clients. Vous pouvez télécharger l'application CSSI Smart Card Middleware sur Chrome Web Store.

Vous devrez peut-être installer des certificats racine et intermédiaires sur le Chromebook. Pour plus d'informations, consultez la documentation de Google Chrome OS.

Configuration requise du logiciel de l'agent

Un administrateur Horizon doit installer l'application CSSI Smart Card Middleware de Charismathics sur la machine agent.

Pour les systèmes d'exploitation d'agent pris en charge, reportez-vous à la section Prise en charge des fonctionnalités pour les clients Chrome.

Exigences supplémentaires de l'authentification par carte à puce

Outre le respect des exigences de carte à puce pour les systèmes Horizon Client pour Chrome, les autres composants d'Horizon doivent également respecter certaines exigences de configuration pour prendre en charge les cartes à puce.

Serveur de connexion

Pour plus d'informations sur la configuration du Serveur de connexion pour la prise en charge des cartes à puce, consultez le document*Administration d'Horizon*.

Dispositifs Unified Access Gateway

Unified Access Gateway 3.2 et versions ultérieures.

Pour plus d'informations sur la configuration d'un dispositif Unified Access Gateway pour la prise en charge des cartes à puce, reportez-vous au document *Déploiement et configuration de VMware Unified Access Gateway*.

Active Directory

Pour plus d'informations sur les tâches qu'un administrateur peut effectuer dans Active Directory afin d'implémenter l'authentification par carte à puce, consultez le document *Administration d'Horizon*.

Limitations de l'authentification par carte à puce

Avec l'authentification par carte à puce, vous branchez un lecteur de carte à puce dans le Chromebook, insérez une carte à puce et sélectionnez un serveur dans Horizon Client. Pendant l'étape d'authentification, vous entrez un code PIN au lieu d'un nom d'utilisateur et d'un mot de passe. Après avoir sélectionné un poste de travail distant ou une application publiée, toutes les commandes et réponses de la carte à puce sont redirigées vers le poste de travail distant ou l'application publiée.

L'authentification par carte à puce comporte certaines restrictions lorsqu'elle est utilisée avec Horizon Client pour Chrome.

- La fonctionnalité d'aide-mémoire du nom d'utilisateur de carte à puce du Serveur de connexion et d'Unified Access Gateway n'est pas prise en charge.
- La stratégie de retrait de carte à puce du Serveur de connexion n'est pas prise en charge.
- Single Sign-On n'est pas pris en charge. Lorsque vous vous connectez à un poste de travail distant ou à une application publiée, vous devez entrer à nouveau le code PIN de la carte à puce à l'intérieur de la session distante.
- Après avoir utilisé une carte à puce pour vous authentifier auprès d'un serveur, vous ne pouvez pas basculer vers une autre méthode d'authentification, telle que l'authentification Active Directory. Pour utiliser une autre méthode d'authentification lors de la prochaine connexion à un serveur, vous devez vous déconnecter de Chrome OS ou redémarrer le Chromebook.
- Après avoir sélectionné un certificat et entré votre code PIN, le certificat que vous avez sélectionné est mis en cache sur le Chromebook et est utilisé lors de la prochaine connexion à un serveur. Pour sélectionner un autre certificat lors de la prochaine connexion à un serveur, vous devez redémarrer le Chromebook.

Préparation du Serveur de connexion

Pour 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 et configurer le Serveur de connexion.

Configurer l'URL externe de Blast

Une fois les serveurs installés, le paramètre **Blast Secure Gateway** est activé sur les instances du Serveur de connexion 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 applicables.

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.

Pour plus d'informations, consultez « Définir les URL externes d'une instance du Serveur de connexion Horizon » dans le document *Installation d'Horizon*.

Configurer les règles de pare-feu

Si vous utilisez des pare-feu tiers, configurez des règles pour autoriser le trafic entrant sur le port TCP 8443 pour tous les hôtes du Serveur de connexion dans un groupe répliqué, puis 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.

Configurer l'authentification utilisateur

Utilisez la liste de vérification suivante lors de la configuration de l'authentification utilisateur.

- Vérifiez que chaque instance du Serveur de connexion dispose d'un certificat TLS qui peut être entièrement 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*.
- 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. Vous pouvez personnaliser les étiquettes sur la page de connexion de l'authentification RADIUS. 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 d'Horizon*.
- 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 activé par défaut. Pour plus d'informations, reportez-vous au document *Administration d'Horizon*.
- Pour envoyer la liste de domaines à Horizon Client, activez-le paramètre global **Envoyer la liste de domaines**. Ce paramètre est désactivé par défaut. Pour plus d'informations, reportez-vous au document *Administration d'Horizon*.
- Pour autoriser un accès non authentifié aux applications publiées, activez cette fonctionnalité dans le Serveur de connexion. Pour plus d'informations, reportez-vous au document *Administration d'Horizon*.

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***
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***

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

Pour autoriser les navigateurs Web clients à effectuer des connexions 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 d'Horizon Client pour Chrome doivent utiliser HTTPS. Les connexions HTTP ne sont pas autorisées.

Par défaut, lorsque vous installez une instance du Serveur de connexion, 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	Instance du Serveur de connexion	TCP 443	Pour établir la connexion initiale, le navigateur Web d'un périphérique client se connecte 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 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.

Installer ou mettre à niveau Horizon Client pour Chrome

Horizon Client pour Chrome est une application Chrome, et vous l'installez de la même manière que vous installez d'autres applications Chrome.

Conditions préalables

Vérifiez que le périphérique client répond à la configuration système requise d'Horizon Client pour Chrome. Reportez-vous à la section Configuration système requise.

Procédure

1 Connectez-vous au Chromebook.

2 Téléchargez et installez VMware Horizon Client pour Chrome depuis Chrome Web Store.

Utilisation de la console d'administration de Google pour configurer des périphériques Chromebook inscrits

Vous pouvez utiliser la console d'administration de Google pour configurer les paramètres du Serveur de connexion sur les périphériques Chromebook inscrits.

Vous pouvez configurer une liste d'instances du Serveur de connexion, une instance du Serveur de connexion par défaut et certains serveurs et fonctionnalités client.

Lorsque vous configurez une liste de serveurs, les serveurs s'affichent sous forme de raccourcis dans Horizon Client. Si vous configurez un serveur par défaut, Horizon Client se connecte automatiquement à ce serveur.

Vous configurez ces paramètres dans un fichier de configuration JSON. Un administrateur Chrome doit utiliser la console d'administration de Google pour télécharger le fichier de configuration JSON pour l'application Horizon Client. Pour obtenir des informations détaillées sur l'utilisation de la console d'administration de Google, reportez-vous à l'aide de l'administrateur de G Suite.

Liste des instances du serveur de connexion

Vous pouvez utiliser les propriétés dans la section `server-list` pour configurer une liste de serveurs.

Propriété	Description
`server`	Adresse IP ou nom d'hôte du serveur.
`username`	(Facultatif) Nom d'un utilisateur autorisé à utiliser le serveur.
`domain`	(Facultatif) Domaine de l'utilisateur spécifié dans la propriété `username`.
`description`	(Facultatif) Description du serveur.

L'exemple de fichier de configuration JSON suivant affiche une liste de serveurs.

```
{
  "broker_list": {
    "Value": {
      "settings": {
        "server-list": [{
          "server": "viewserver0.mydomain.com",
          "default": false,
          "description": "View Server 0",
          "username": "User0",
          "desktopId": "RDS2012R2DC",
          "domain": "TestDomain0"
        },{
          "server": "viewserver1.mydomain.com",
          "description": "View Server 1",
          "username": "User1",
          "domain": "TestDomain1",
```

```
          "default": false
        }, {
          "server": "123.456.1.2",
          "description": "View Server 2",
          "username": "User2",
          "default": false,
          "domain": "TestDomain2"
        }, {
          "server": "123.456.1.3",
          "description": "View Server 3",
          "username": "User3",
          "default": false,
          "domain": "TestDomain3"
        }, {
          "server": "viewserver4.mydomain.com",
          "description": "View Server 4",
          "username": "User4",
          "default": false,
          "domain": "TestDomain4"
        }]}
    }
  }
}
```

Instance du serveur de connexion par défaut

Vous pouvez utiliser la propriété `default` pour spécifier un serveur par défaut dans la section `server-list`. Les valeurs valides sont `true` et `false`.

L'exemple de fichier de configuration JSON suivant montre un serveur par défaut.

```
{
  "broker_list": {
    "Value": {
      "settings": {
        "server-list": [{
          "server": "viewserver0.mydomain.com",
          "default": true,
          "description": "View Server 0",
          "username": "User0",
          "desktopId": "RDS2012R2DC",
          "domain": "TestDomain0"
        }]}
    }
  }
}
```

Fonctionnalités du client

Vous pouvez utiliser les paramètres de la section `common-setting` pour configurer certaines fonctionnalités.

Paramètre	Description
`allowDataSharing`	Configure la fonctionnalité Horizon Client le partage de données. La propriété `value` spécifie si la fonctionnalité est activée ou désactivée. La propriété `editable` spécifie si les utilisateurs peuvent modifier le paramètre **Autoriser le partage de données** dans Horizon Client. Les valeurs valides pour les deux propriétés sont `true` et `false`.
`enableAnonymousLogin`	Configure la fonctionnalité d'accès non authentifié. La propriété `value` spécifie si la fonctionnalité est activée ou désactivée. La propriété `editable` spécifie si les utilisateurs peuvent modifier le paramètre **Se connecter de manière anonyme à l'aide de l'accès non authentifié** dans Horizon Client. Les valeurs valides pour les deux propriétés sont `true` et `false`.
`powerSetting`	Empêche le périphérique de passer en mode veille en réponse à l'inactivité de l'utilisateur dans une session distante. Par défaut, le Chromebook passe en mode veille au bout de 10 minutes. Lorsque vous configurez la propriété `powerSetting`, le Chromebook ne passe pas en mode veille jusqu'à la fin de la dernière session distante. La propriété `keepAwakeLevel` spécifie le niveau de stratégie d'alimentation. Vous pouvez définir `keepAwakeLevel` sur l'une des valeurs suivantes : ■ `system`, qui empêche le système de passer en veiller en réponse à l'inactivité de l'utilisateur. Il s'agit de la valeur par défaut. ■ `display`, qui empêche l'affichage de se désactiver ou de s'estomper, ou le système de passer en veille, en réponse à l'inactivité de l'utilisateur.

L'exemple de fichier de configuration JSON suivant illustre les paramètres courants.

```
{
   "broker_list": {
      "settings": {
         "server-list": [{
            "server": "viewserver0.mydomain.com",
            "default": true,
            "description": "View Server 0",
            "username": "User0",
            "domain": "TestDomain0"
         }],
           "common-setting": {
                 "allowDataSharing": false,
                 "enableAnonymousLogin": true,
                 "editable":{
                    "allowDataSharing": true,
                    "enableAnonymousLogin": false
                  },
                  "powerSetting":{
                    "keepAwakeLevel":"display"
```

```
                    }
                }
            }
        }
    }
```

Fonctionnalités du serveur

Vous pouvez utiliser les paramètres de la section `server-list` pour configurer certaines fonctionnalités pour des serveurs spécifiques.

Paramètre	Description
`enableHighResolution`	Configure la fonctionnalité Mode haute résolution. La propriété `value` spécifie si la fonctionnalité est activée ou désactivée. La propriété `editable` spécifie si les utilisateurs peuvent modifier le paramètre **Mode haute résolution** dans Horizon Client. Les valeurs valides pour les deux propriétés sont `true` et `false`.
`enableMultiMonitor`	Configure la fonctionnalité Plusieurs moniteurs. La propriété `value` spécifie si la fonctionnalité est activée ou désactivée. Les valeurs valides sont `true` et `false`. Si la propriété `value` est activée, le paramètre **Affichage** dans Horizon Client est affecté de la manière suivante : ■ Si l'utilisateur a déjà défini un affichage spécifique sur le périphérique, le paramètre **Affichage** est défini sur **Utiliser les affichages sélectionnés**. ■ Si l'utilisateur n'a jamais défini d'affichage spécifique sur le périphérique, le paramètre **Affichage** est défini sur **Utiliser tous les écrans**. Si la propriété `value` est désactivée, le paramètre **Affichage** est défini sur **Utiliser un seul écran**.
`enableWindowsKey`	Active ou désactive la touche Windows pour les postes de travail distants. La propriété `value` spécifie si la fonctionnalité est activée ou désactivée. La propriété `editable` spécifie si les utilisateurs peuvent modifier le paramètre **Activer la touche Windows pour les postes de travail** dans Horizon Client. Les valeurs valides pour les deux propriétés sont `true` et `false`.

Paramètre	Description
`timezoneSync`	Configure le fuseau horaire pour les postes de travail distants et les applications publiées. La propriété `isSync` spécifie s'il faut définir le fuseau horaire automatiquement. La propriété `editable` spécifie si les utilisateurs peuvent modifier le paramètre **Définir le fuseau horaire automatiquement** dans Horizon Client. Les valeurs valides pour les deux propriétés sont `true` et `false`. Si vous définissez `isSync` sur `false`, vous pouvez définir le fuseau horaire manuellement en spécifiant la propriété `timezone`. **Note** Lorsque vous définissez la propriété `isSync` sur `true`, le fuseau horaire du client est toujours cohérent avec celui du système d'exploitation hôte, quelle que soit la valeur de la propriété `timezone`.
`résolution`	Configure la résolution d'écran. La propriété `width` spécifie la largeur de l'écran et la propriété `height` spécifie la hauteur de l'écran. Les deux valeurs doivent être inférieures ou égales à la largeur et la hauteur de la fenêtre Chromebook, sinon Horizon Client utilise la résolution par défaut (largeur et hauteur de la fenêtre Chromebook).
`usbAllowList`	Spécifie les périphériques USB qui sont redirigés. Si un périphérique n'est pas répertorié, il est bloqué. Utilisez la propriété `vid` pour spécifier l'ID du fournisseur et la propriété `pid` pour spécifier l'ID de produit de chaque périphérique. Lorsque ce paramètre est utilisé, le paramètre de stratégie de groupe d'agent équivalent (**Inclure un périphérique Vid/Pid**) est ignoré.
`usbBlockList`	Spécifie les périphériques USB qui ne peuvent pas être redirigés. Utilisez la propriété `vid` pour spécifier l'ID du fournisseur et la propriété `pid` pour spécifier l'ID de produit de chaque périphérique. Lorsque ce paramètre est utilisé, le paramètre de stratégie de groupe d'agent équivalent (**Exclure un périphérique Vid/Pid**) est ignoré. Le paramètre `usbBlockList` a une priorité supérieure que le paramètre `usbAllowList`, ce qui signifie que si un terminal se trouve dans les deux listes, il est bloqué.

L'exemple de fichier de configuration JSON suivant montre les paramètres du serveur.

```
{
  "broker_list": {
    "Value": {
      "settings": {
         "server-list": [{
            "server": "viewserver0.mydomain.com",
            "default": true,
            "description": "View Server 0",
            "username": "User0",
```

```
            "domain": "TestDomain0",
            "settings": {
               "enableHighResolution": false,
               "enableMultiMonitor": false,
               "enableWindowsKey": true,
               "timezoneSync": {
                   "isSync": false,
                   "timezone": "-00:00"
               },
               "resolution": {
                 "width": 600,
                 "height": 800
               },
               "editable": {
                  "enableHighResolution": true,
                  "enableWindowsKey": true,
                  "timezoneSync": false
               },
               "usbAllowList":[{
                  "vid": 1111,
                  "pid": 2222
               },{
                  "vid": 1112,
                  "pid": 2223
               }],
               "usbBlockList":[{
                  "vid": 2222,
                  "pid": 3333
                },{
                  "vid": 2223,
                  "pid": 3334
                }]
              }
           }]
        }
     }
   }
}
```

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 Horizon Client pour Chrome.

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.

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 Horizon Client pour Chrome, 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. Pour afficher le format de la liste de chiffrements, vous pouvez rechercher **`openssl cipher string`** dans un navigateur Web.

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.

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

Si vous utilisez un dispositif Unified Access Gateway vous devez installer un certificat signé par une autorité de certification avec un autre nom de sujet (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 Horizon Client pour Chrome.

Note Si vous utilisez une instance du Serveur de connexion, 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, consultez le document *Installation d'Horizon*. Pour plus d'informations sur l'installation de certificats dans Chrome, consultez la documentation de Google Chrome.

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 d'Horizon*.

Le partage de données est activé par défaut dans Horizon Client. Vous devez configurer le paramètre de partage de données avant de vous connecter à un serveur. Le paramètre est appliqué à tous les serveurs. Vous ne pouvez pas modifier le paramètre de partage de données Horizon Client après vous être connecté à un serveur.

Procédure

1. Cliquez sur **paramètres** (icône d'engrenage) dans la page de sélection du serveur.
2. Appuyez pour activer ou désactiver l'option **Autoriser le partage de données**.

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 Client pour Chrome
Version du produit client	<version_client>	Non	2012-8.1.0-xxxxxxxx
Architecture binaire du client	<arch_client>	Non	navigateur
Architecture native du navigateur	<arch_navigateur>	Non	Chrome OS
Chaîne de l'agent utilisateur du navigateur	<agent_utilisateur_navigateur>	Non	Chrome/3.0.1750
Chaîne de version interne de navigateur	<version_navigateur>	Non	3.0.1750 (pour Chrome)
Implémentation de base du navigateur	<base_navigateur>	Non	Chrome
Si le navigateur tourne sur un ordinateur de poche	<navigateur_est_portable>	Non	true

Gestion des connexions aux postes de travail distants et applications publiées

2

Les utilisateurs finaux peuvent 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
- Utiliser l'accès non authentifié pour se connecter à des applications publiées
- Faire confiance à un certificat racine auto-signé
- Définition du fuseau horaire
- Gérer les raccourcis de serveur
- Fermer une session ou se déconnecter

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.

Avant de laisser vos utilisateurs finaux accéder à leurs applications publiées et postes de travail distants, vérifiez que vous pouvez vous connecter à une application publiée ou à un poste de travail distant à partir d'un périphérique client.

Conditions préalables

- Procurez-vous les informations d'identification de connexion, telles que le nom d'utilisateur et le mot de passe, le nom d'utilisateur et le code secret RSA SecurID, les informations d'identification pour l'authentification RADIUS ou le numéro d'identification personnel (PIN) de carte à puce.
- Obtenez le nom de domaine NETBIOS pour ouvrir une session. Utilisez par exemple monentreprise plutôt que monentreprise.com.

- Si vous utilisez l'authentification par carte à puce, assurez-vous que toutes les exigences de l'authentification par carte à puce sont remplies et que vous connaissez bien les limitations. Pour plus d'informations, reportez-vous à Exigences de l'authentification par carte à puce et à Limitations de l'authentification par carte à puce.
- 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. Connectez-vous au Chromebook.
2. Si une connexion VPN est requise, activez le VPN.
3. Ouvrez l'application VMware Horizon Client.
4. Si vous êtes invité à accorder l'accès à Smart Card Connector, cliquez sur **Autoriser**.

   Cette invite s'affiche au premier de démarrage d'Horizon Client si l'authentification par carte à puce est configurée sur le Chromebook.
5. Connectez-vous à un serveur.

Option	Action
Se connecter à un nouveau serveur	Cliquez sur le signe plus (+), entrez le nom du serveur, entrez une description du serveur (facultative) et cliquez sur **Se connecter**.
Se connecter à un serveur existant	Cliquez sur le raccourci du serveur.

   Les connexions entre Horizon Client et les serveurs 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 : **`view.company.com:1443`**.
6. Si une carte à puce est requise ou facultative, sélectionnez le certificat de la carte à puce à utiliser et entrez votre code PIN.
7. Si vous êtes invité à saisir les informations d'identification pour l'authentification RSA SecurID ou RADIUS, entrez-les, puis cliquez sur **Connexion**.

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

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

   N'entrez pas votre code PIN ni le même numéro généré que vous avez entré 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.

9 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 Sélectionnez un domaine.

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

   c Appuyez sur **Ouverture de session**.

10 (Facultatif) Pour marquer un poste de travail distant ou une application publiée comme favori, 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.

11 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.

12 Si vous utilisez l'authentification par carte à puce, entrez à nouveau le code PIN de la carte à puce dans la session distante.

Résultats

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, définissez manuellement le fuseau horaire. Reportez-vous à la section Définition du fuseau horaire.

Étape suivante

Horizon Client fournit des aides à la navigation pour vous aider à utiliser des postes de travail distants et des applications publiées. Pour plus d'informations, reportez-vous à Utilisation de postes de travail distants et à Utilisation d'applications publiées.

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.
- Configurez des utilisateurs avec un accès non authentifié sur l'instance du Serveur de connexion. Pour plus d'informations, consultez « Fournir un accès non authentifié pour des applications publiées » dans le document *Administration d'Horizon*.

Procédure

1. Cliquez sur le bouton de la barre d'outils **Paramètres** dans le coin supérieur droit de la page de sélection du serveur et activez l'option **Se connecter de manière anonyme à l'aide de l'accès non authentifié**.
2. Connectez-vous à un serveur, entrez un compte d'utilisateur d'accès non authentifié et cliquez sur **Connexion**.

   La fenêtre de sélection des applications s'affiche.
3. Cliquez sur l'icône de l'application publiée à laquelle vous voulez accéder.

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.

Chrome vous permet d'approuver de façon permanente le certificat auto-signé. Si vous n'approuvez pas le certificat de façon permanente, vous devez vérifier le certificat à chaque fois que vous redémarrez le navigateur.

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.

   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)**.

Résultats

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

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 Horizon Client, 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.

Gérer les raccourcis de serveur

Une fois que vous êtes connecté à un serveur, Horizon Client crée un raccourci de serveur. Vous pouvez modifier et supprimer les raccourcis de serveurs.

Horizon Client enregistre le nom du serveur ou l'adresse IP dans un raccourci, même si vous avez tapé une adresse IP ou un nom de serveur incorrect. Vous pouvez supprimer ou modifier ces informations en modifiant le nom du serveur ou l'adresse IP. Si vous n'entrez pas de description de serveur, le nom ou l'adresse IP du serveur devient la description par défaut.

Procédure

1 Cliquez avec le bouton droit sur le raccourci du serveur.

  Un menu contextuel s'affiche.

2 Utilisez le menu contextuel pour supprimer le raccourci du serveur ou modifier le nom ou la description du serveur.

3 Si vous avez modifié le raccourci du serveur, cliquez sur **Terminé** pour enregistrer vos modifications.

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

- Déconnectez-vous d'un poste de travail distant.

Option	Description
Depuis le poste de travail distant	Pointez votre souris en haut de la fenêtre du poste de travail distant jusqu'à ce que la barre de menus s'affiche, puis cliquez sur le bouton **Se déconnecter**. Vous pouvez également cliquer sur le bouton **X** (Fermer) dans le coin supérieur droit de la fenêtre du poste de travail distant.
Depuis le Centre de gestion des sessions	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 applications, ouvrez le Centre de gestion des sessions, sélectionnez la session de poste de travail distant, puis cliquez sur **Se déconnecter**. Vous pouvez également ouvrir le Centre de gestion des sessions en cliquant avec le bouton droit sur l'icône du poste de travail distant sur l'étagère et en cliquant sur **Centre de gestion des sessions**.

- Fermez une session sur un poste de travail distant.

Option	Description
Depuis le poste de travail distant	Pointez votre souris en haut de la fenêtre du poste de travail distant jusqu'à ce que la barre de menus s'affiche, puis cliquez sur le bouton **Fermer la session**.
Depuis le Centre de gestion des sessions	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 applications, ouvrez le Centre de gestion des sessions, sélectionnez la session de poste de travail distant, puis cliquez sur **Fermer la session**. Vous pouvez également ouvrir le Centre de gestion des sessions en cliquant avec le bouton droit sur l'icône du poste de travail distant sur l'étagère et en cliquant sur **Centre de gestion des sessions**.

- Fermer une application publiée.

Option	Description
Depuis l'application publiée	Cliquez sur le bouton **X** (Fermer) dans le coin de la fenêtre de l'application publiée.
Depuis l'étagère	Cliquez avec le bouton droit sur l'icône de l'application publiée dans l'étagère et cliquez sur **Fermer**.

- Pour fermer la session sur un serveur, cliquez sur le bouton **Fermer la session** dans le coin supérieur droit de la fenêtre de sélection des postes de travail et applications.

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

3

Horizon Client fournit un environnement de poste de travail et d'application familier et personnalisé.

Ce chapitre contient les rubriques suivantes :

- Prise en charge des fonctionnalités pour les clients Chrome
- Mouvements
- Modifier le mode d'affichage de postes de travail distants
- Définition de la résolution d'écran
- Utiliser le mode plein écran
- Utilisation de la synchronisation DPI
- Utilisation de la fonctionnalité Audio/Vidéo en temps réel pour webcams et microphones
- Utilisation de postes de travail distants
- Utilisation d'applications publiées
- Utilisation d'applications publiées en mode Kiosque
- Copier et coller du texte et des images
- Transfert de fichiers entre le client et un poste de travail distant ou une application publiée
- Partager l’accès aux dossiers et lecteurs locaux avec la redirection de lecteur client
- Utiliser des périphériques USB sur un poste de travail distant
- Impression à partir d'un poste de travail distant ou d'une application publiée
- Utiliser plusieurs sessions d'une application publiée à partir de périphériques clients différents
- Réglage du son sur les postes de travail distants et les applications publiées
- Combinaisons de touches de raccourci
- Internationalisation

Prise en charge des fonctionnalités pour les clients Chrome

Certains systèmes d'exploitation invités et fonctionnalités de poste de travail distant nécessitent des versions d'Horizon Agent spécifiques. Utilisez ces informations pour planifier les fonctionnalités à mettre à la disposition de vos utilisateurs finaux.

Postes de travail virtuels Windows pris en charge

Les postes de travail virtuels Windows sont des machines virtuelles à session unique.

Cette version d'Horizon Client pour Chrome fonctionne avec les postes de travail virtuels Windows sur lesquels Horizon Agent 7.5 ou version ultérieure est installé. Les systèmes d'exploitation invités pris en charge incluent Windows 7, Windows 8.x, Windows 10, Windows Server 2012 R2, Windows Server 2016 et Windows Server 2019, avec les limitations suivantes :

- Les postes de travail virtuels Windows Server 2019 requièrent Horizon Agent 7.7 ou version ultérieure.
- Les postes de travail virtuels Windows 7 et Windows 8.x ne sont pas pris en charge avec Horizon Agent 2006 et versions ultérieures.
- La fonctionnalité d'impression VMware Integrated Printing fonctionne avec Horizon Agent 7.12 ou version ultérieure sur un poste de travail virtuel Windows 10, Windows Server 2016 ou Windows Server 2019. Elle ne fonctionne pas avec les postes de travail virtuels Windows 7, Windows 8.x et Windows Server 2012 R2.

Postes de travail publiés sur des hôtes RDS pris en charge

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.

Cette version d'Horizon Client pour Chrome fonctionne avec les hôtes RDS sur lesquels Horizon Agent 7.5 ou version ultérieure est installé. Les systèmes d'exploitation invités pris en charge incluent Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 et Windows Server 2019, avec les limitations suivantes :

- Les hôtes RDS Windows Server 2019 requièrent Horizon Agent 7.7 ou version ultérieure.
- Les hôtes RDS de Windows Server 2012 ne sont pas pris en charge avec Horizon Agent 2006 et versions ultérieures.
- La fonctionnalité VMware Integrated Printing fonctionne avec Horizon Agent 7.12 ou version ultérieure sur un hôte RDS Windows Server 2016 ou Windows Server 2019. Elle ne fonctionne pas avec les hôtes RDS Windows Server 2012 et Windows Server 2012 R5.

Postes de travail Linux pris en charge

Pour obtenir la liste des systèmes d'exploitation invités Linux pris en charge et pour plus d'informations sur les fonctionnalités prises en charge, consultez le document *Configuration des postes de travail Linux dans Horizon*.

Mouvements

VMware a créé des aides d'interaction utilisateur pour faciliter la navigation dans les éléments de l'interface utilisateur Windows classique sur un périphérique non-Windows.

Clic

Comme dans les autres applications, vous pouvez appuyer sur votre pavé tactile pour cliquer sur un élément de l'interface utilisateur. Si le Chromebook dispose d'un écran tactile, vous pouvez appuyer dessus pour cliquer sur un élément de l'interface utilisateur. Vous pouvez également utiliser une souris externe.

Clic droit

Les options suivantes sont disponibles pour le clic droit :

- Appuyez avec deux doigts sur le pavé tactile.
- Maintenez la touche Alt enfoncée sur le clavier et appuyez sur le pavé tactile avec un doigt.
- Utilisez une souris externe pour faire un clic droit.
- Si le Chromebook dispose d'un écran tactile, appuyez avec deux doigts pour effectuer un clic avec la bouton droit.

Défilement et barres de défilement

Les options suivantes sont disponibles pour le défilement vertical.

- Appuyez longuement avec votre pouce et faites défiler vers le bas avec un doigt sur le pavé tactile. Vous pouvez également faire défiler avec deux doigts.
- Utilisez une souris externe pour faire défiler.
- Si le Chromebook dispose d'un écran tactile, appuyez avec deux doigts, puis faites glisser pour faire défiler. Le texte sous vos doigts se déplace dans la même direction que vos doigts.

Zoom avant et arrière

Le zoom avant et arrière n'est pas pris en charge.

Redimensionnement de fenêtre

Pour utiliser le pavé tactile pour redimensionner une fenêtre, appuyez avec un doigt dans le coin ou sur le côté de la fenêtre et faites-le glisser pour redimensionner.

Si le Chromebook dispose d'une souris externe, placez le curseur sur le bord de la fenêtre et faites-le glisser pour agrandir ou rétrécir la fenêtre.

Si le Chromebook dispose d'un écran tactile, placez un doigt dans le coin ou sur le côté de la fenêtre et faites-le glisser pour redimensionner.

Son, musique et vidéo

Si le son est activé sur le périphérique, vous pouvez écouter des fichiers audio sur un poste de travail distant.

Limitation de la fonctionnalité Plusieurs moniteurs

Les mouvements tactiles sont désactivés lorsque la fonctionnalité Plusieurs moniteurs est activée. Pour plus d'informations, reportez-vous à la section Modifier le mode d'affichage de postes de travail distants.

Modifier le mode d'affichage de postes de travail distants

Vous pouvez modifier le mode d'affichage pour des postes de travail distants.

Si vous disposez de plusieurs moniteurs, vous pouvez afficher des postes de travail distants sur tous les moniteurs ou sur des moniteurs spécifiques. Vous pouvez sélectionner jusqu'à trois moniteurs.

Conditions préalables

- Cette fonctionnalité requiert Chrome OS 86 ou version ultérieure.
- Cette fonctionnalité n'est pas prise en charge pour les applications publiées.
- Cette fonctionnalité n'est pas prise en charge si le mode Poste de travail unifié est activé pour le périphérique client.

Pour plus d'informations sur la façon dont le paramètre de fichier JSON `enableMultiMonitor` affecte cette fonctionnalité, reportez-vous à la section Fonctionnalités du serveur.

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 **Affichage**, puis cliquez sur **Définir**.

3 Sélectionnez une option d'affichage et cliquez sur **OK**.

Option	Action
Utiliser tous les écrans	Affiche la fenêtre du poste de travail distant sur tous les moniteurs connectés.
Utiliser un seul écran	Affiche le poste de travail distant sur le moniteur principal.
Utiliser les affichages sélectionnés	Affiche le poste de travail distant sur les moniteurs que vous sélectionnez. Vous ne pouvez sélectionner que des moniteurs adjacents. Les miniatures des moniteurs actuellement connectés au système client s'affichent sous **Disposition de l'affichage**. La topologie d'affichage correspond aux paramètres d'affichage sur le système client. Pour sélectionner ou désélectionner un moniteur sur lequel vous souhaitez afficher la fenêtre de poste de travail distant, cliquez sur sa miniature. Lorsque vous cliquez sur une miniature, elle change de couleur.

Étape suivante

Pour quitter le mode multimoniteur, pointez sur le haut de la fenêtre de poste de travail distant jusqu'à ce que la barre de menus s'affiche, puis cliquez sur le bouton **Quitter le mode multimoniteur**.

Définition de la résolution d'écran

Horizon Client 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 périphérique Chrome proposant une densité de pixels élevée, tel qu'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**. 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 % et si un administrateur n'a pas désactivé la fonctionnalité.

Pour plus d'informations sur la désactivation de la fonctionnalité Mode Haute résolution, reportez-vous à la section Utilisation de la console d'administration de Google pour configurer des périphériques Chromebook inscrits.

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.

- Avec la fonctionnalité d'affichage graphique accéléré par le logiciel, vous pouvez utiliser des applications 3D, telles que des thèmes Windows Aero ou Google Earth. Cette fonctionnalité requiert de 64 Mo à 128 Mo de VRAM.
- La fonctionnalité d'affichage graphique accéléré par le matériel (vSGA) partagé, 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 cartes graphiques de poste de travail haut de gamme accélérées 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 périphérique proposant une densité de pixels élevée, tel qu'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.

Utiliser le mode plein écran

Vous pouvez afficher un poste de travail distant en mode plein écran.

Conditions préalables

Connectez-vous au poste de travail distant.

Procédure

- Pour afficher le poste de travail distant en mode plein écran, pointez vers le haut de la fenêtre du poste de travail distant jusqu'à ce que la barre de menus s'affiche, puis cliquez sur le bouton **Plein écran**.
- Pour quitter le mode plein écran, pointez vers le haut de la fenêtre du poste de travail distant jusqu'à ce que la barre de menus s'affiche, puis cliquez sur le bouton **Quitter le plein écran**.

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.

Comme la fonctionnalité de mise à l'échelle de l'affichage, la fonctionnalité de synchronisation DPI peut améliorer la lisibilité du texte et des icônes sur des affichages haute résolution. Contrairement à la fonctionnalité de mise à l'échelle de l'affichage, qui augmente la taille des polices et des images, et qui peut les rendre floues, la fonctionnalité de synchronisation DPI augmente la taille des polices et des images, en les gardant nettes. Pour cette raison, la fonctionnalité de synchronisation DPI est généralement préférée pour une expérience utilisateur optimale.

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.

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.

Comportement de la synchronisation DPI

Le comportement de synchronisation DPI par défaut dépend de la version d'Horizon Agent installée sur la machine agent.

À partir de Horizon Agent 2012, le paramètre DPI par moniteur du client est synchronisé avec l'agent, et, par défaut, les modifications prennent effet immédiatement lors d'une session distante. Cette fonctionnalité est contrôlée par le paramètre de stratégie de groupe de l'agent Synchronisation DPI par moniteur. La fonctionnalité de synchronisation DPI par moniteur est prise en charge par défaut pour les postes de travail virtuels et physiques. Elle n'est pas prise en charge pour les postes de travail publiés.

Avec les versions antérieures d'Horizon Agent, le client ne prend en charge que la synchronisation avec le paramètre DPI système. La synchronisation DPI se produit lors de la connexion initiale. La mise à l'échelle de l'affichage fonctionne alors en cas de reconnexion, si nécessaire. Lorsque la synchronisation DPI fonctionne et que le paramètre DPI du système client correspond au paramètre DPI du poste de travail distant, la mise à l'échelle de l'affichage ne peut pas être appliquée, même si vous sélectionnez l'option Autoriser la mise à l'échelle de l'affichage dans l'interface utilisateur. Windows n'autorise pas les utilisateurs à modifier le paramètre DPI au niveau du système pour la session utilisateur actuelle, et la synchronisation DPI ne se produit que lorsqu'ils se connectent et démarrent une session distante. Si les utilisateurs modifient le paramètre DPI au cours d'une session distante, ils doivent se déconnecter, puis se reconnecter pour que le paramètre DPI du poste de travail distant corresponde au nouveau paramètre DPI du système client.

Le paramètre DPI de l'agent se trouve dans le Registre Windows à l'emplacement `Computer\HKEY_CURRENT_USER\Control Panel\Desktop: logPixels`.

Note Celui-ci doit être différent du paramètre DPI du moniteur principal. Par exemple, si vous fermez le moniteur principal et si le système bascule vers un écran externe qui dispose d'un paramètre DPI différent de celui du moniteur principal, le paramètre DPI système est toujours le même que le paramètre DPI du moniteur principal précédemment fermé.

Cette version du client ne prend pas en charge le paramètre de stratégie de groupe de l'agent Synchronisation DPI par connexion, qui est livré avec Horizon Agent versions 7.8 à 2006.

Pour plus d'informations sur les paramètres de stratégie de groupe de synchronisation DPI, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon* de votre version de Horizon Agent.

Systèmes d'exploitation invités pris en charge pour les postes de travail virtuels

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

Note Pour les machines Windows Server configurées en tant que poste de travail, la fonctionnalité de synchronisation DPI par moniteur n'est pas prise en charge.

Hôtes RDS pris en charge pour les postes de travail publiés et les applications publiées

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

Note Pour les hôtes RDS, la fonctionnalité de synchronisation DPI par moniteur n'est pas prise en charge. Cette limitation ne s'applique pas aux applications publiées qui s'exécutent sur des pools de postes de travail avec la fonctionnalité d'applications hébergées de machine virtuelle

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.

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*.

Lorsqu'une application publiée ou un poste de travail distant est connecté à la webcam ou au microphone de la machine cliente, Chrome demande l'autorisation la première fois avant que l'application publiée ou le poste de travail distant puisse utiliser la webcam ou le microphone. Si vous autorisez l'utilisation du périphérique, Chrome ne redemande pas l'autorisation.

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.

Sélectionner une webcam ou un microphone préféré sur un Chromebook

Avec la fonctionnalité audio/vidéo en temps réel, si plusieurs webcams ou microphones sont connectés au système client local, seul l'un des périphériques est utilisé sur l'application publiée ou le poste de travail distant. Pour spécifier la webcam ou le microphone préféré, vous pouvez configurer les paramètres d'audio/vidéo en temps réel dans Horizon Client pour Chrome.

Si il ou elle est disponible, la webcam ou le microphone préféré(e) est utilisé(e) sur le poste de travail distant ou l'application publiée. Si la webcam ou le microphone préféré(e) n'est pas disponible, une autre webcam ou un autre microphone est utilisé(e).

Conditions préalables

- Assurez-vous qu'une webcam USB ou un microphone USB ou d'un autre type est installé et opérationnel sur le système client local.
- Connectez-vous à un serveur.

Procédure

1. 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 et faites défiler la liste vers le bas jusqu'aux paramètres Audio/Vidéo en temps réel.
2. Dans le menu déroulant **Microphone préféré**, sélectionnez un microphone préféré.
3. Dans le menu déroulant **Webcam préférée**, sélectionner une webcam préférée.

Résultats

Lors du prochain démarrage d'une application publiée ou d'un poste de travail distant, le microphone ou la webcam préféré(e) que vous avez sélectionné(e) est redirigé(e) vers la session à distance.

Utilisation de postes de travail distants

Vous pouvez utiliser la barre de menus supérieure d'une fenêtre de poste de travail distant afin d'effectuer des tâches courantes dans un poste de travail distant.

- Pour ouvrir la barre de menus supérieure d'un poste de travail distant, déplacez votre souris vers le haut de la fenêtre de poste de travail distant jusqu'à ce que la barre s'affiche.
- Pour utiliser le raccourci clavier Ctrl+Alt+Suppr sur un poste de travail distant, cliquez sur le bouton **Envoyer Ctrl+Alt+Delete à la zone de travail actuelle** dans la barre de menus supérieure.
- Pour passer en mode plein écran, cliquez sur le bouton **Plein écran** dans la barre de menus supérieure. Pour quitter le mode plein écran, cliquez sur le bouton **Quitter le plein écran** dans la barre de menus supérieure.
- Pour rediriger des périphériques USB vers le poste de travail distant, cliquez sur le bouton **Redirection de périphérique USB** dans la barre de menus supérieure.
- Pour quitter le mode multimoniteur, cliquez sur le bouton **Quitter le mode multimoniteur** dans la barre de menus supérieure.
- Pour vous déconnecter d'un poste de travail distant, cliquez sur le bouton **Se déconnecter** dans la barre de menus supérieure ou cliquez sur le bouton **X** (Fermer) dans le coin supérieur droit de la fenêtre de poste de travail distant.
- Pour afficher des informations sur Horizon Client, cliquez sur le bouton **À propos de** dans la barre de menus supérieure.

Pour basculer vers un autre poste de travail distant ouvert, cliquez sur cette fenêtre de poste de travail distant. Vous pouvez également parcourir tous les postes de travail distants ouverts (y compris les applications locales et publiées) sur le périphérique client en appuyant sur Alt+Tab. Pour activer un poste de travail distant sélectionné, relâchez la touche Alt.

Pour plus d'informations à propos de la fermeture de session sur un poste de travail distant, reportez-vous à la section Fermer une session ou se déconnecter. Pour plus d'informations sur le redémarrage d'un poste de travail distant, reportez-vous à la section Redémarrer un poste de travail distant. Pour plus d'informations sur la réinitialisation d'un poste de travail distant, reportez-vous à la section Réinitialiser des postes de travail distants ou des applications publiées.

Utilisation d'applications publiées

Horizon Client fournit des aides à la navigation pour vous aider à utiliser des applications publiées.

- Pour agrandir et réduire une application publiée, cliquez sur les boutons **Agrandir** et **Réduire** de la même manière que vous le faites dans n'importe quelle application.
- Pour restaurer une application publiée réduite, cliquez sur son icône d'étagère sur le périphérique client ou sélectionnez la session d'application publiée, puis cliquez sur le bouton **Restaurer** dans la fenêtre du Centre de gestion des sessions. En mode Kiosque, vous devez utiliser le Centre de gestion des sessions pour restaurer une application publiée réduite. Pour plus d'informations, reportez-vous à la section Utilisation d'applications publiées en mode Kiosque.
- Pour réinitialiser une application publiée, reportez-vous à la section Réinitialiser des postes de travail distants ou des applications publiées.

Pour basculer vers une autre application publiée ouverte, cliquez sur la fenêtre de l'application publiée. Vous pouvez également parcourir toutes les applications publiées ouvertes (y compris les applications locales et les postes de travail distants) sur le périphérique client en appuyant sur Alt+Tab. Pour activer une application publiée sélectionnée, relâchez la touche Alt.

Utilisation d'applications publiées en mode Kiosque

Lorsque vous utilisez des applications publiées en mode Kiosque, vous devez utiliser le Centre de gestion des sessions pour effectuer certaines tâches.

- Pour ouvrir la fenêtre du Centre de gestion des sessions, 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 applications, puis cliquez sur **Ouvrir** en regard de **Centre de gestion des sessions**. Si vous avez ouvert une session de poste de travail distant, vous devez la fermer avant de pouvoir accéder à la fenêtre de sélection des postes de travail et applications.
- Pour restaurer une application publiée réduite en mode Kiosque, sélectionnez la session d'application publiée et cliquez sur le bouton **Restaurer** dans la fenêtre du Centre de gestion des sessions.
- Pour basculer des applications publiées en mode Kiosque, sélectionnez la session d'application publiée et cliquez sur le bouton **Restaurer** dans la fenêtre du Centre de gestion de session.

- Pour fermer la fenêtre du Centre de gestion des sessions en mode Kiosque, cliquez sur le bouton Fermer (**X**) dans le coin supérieur droit de la fenêtre du Centre de gestion des sessions.

Copier et coller du texte et des images

Par défaut, vous pouvez copier et coller du texte brut et enrichi au format HTML depuis un périphérique client vers un poste de travail distant ou une application publiée.

Vous pouvez également copier et coller du texte brut et du texte enrichi au format HTML d'un poste de travail distant ou d'une application publiée vers le périphérique client si un administrateur Horizon active cette fonctionnalité.

Un administrateur Horizon peut configurer la fonctionnalité Copier et coller pour que les opérations Copier et Coller soient autorisées uniquement depuis le périphérique client vers un poste de travail distant ou une application publiée, ou uniquement d'un poste de travail distant ou d'une application publiée vers le périphérique client, les deux ou aucun.

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

- Si la source du Presse-papiers est une application Google, telle que Google Docs, vous pouvez copier et coller des images uniquement si le périphérique client peut accéder au site Web de Google.
- Si vous copiez une image et du texte enrichi (ou du texte brut) ensemble à partir du périphérique client, et que la destination est une application qui prend en charge uniquement du texte enrichi, telle que WordPad, l'image est ignorée et seul le texte est copié et collé. Si l'application de destination prend en charge le texte enrichi au format HTML/XML, telle que Microsoft Word, cette restriction ne s'applique pas.
- Un administrateur Horizon peut utiliser des stratégies de groupe afin de limiter les formats de Presse-papiers lors des opérations de copier-coller. Les stratégies de filtre du format de Presse-papiers pour les données de Graphique Microsoft Office et SmartArt et les données Effets du texte Microsoft ne sont pas prises en charge. Pour plus d'informations sur les stratégies de filtre du format de Presse-papiers, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*. L'utilisation de stratégies intelligentes pour contrôler les opérations de copier-coller sur les postes de travail distants n'est pas prise en charge.

Vous pouvez copier un maximum de 64 Ko de données d'un poste de travail distant ou d'une application publiée vers le périphérique client. Le texte brut qui dépasse cette limite est tronqué. Le texte enrichi est converti en texte brut.

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.

Journalisation des activités copier et coller

Lorsque vous activez la fonctionnalité d'audit du Presse-papiers, Horizon Agent enregistre des informations sur les activités copier et coller dans un journal des événements sur la machine agent. La fonctionnalité d'audit du Presse-papiers est désactivée par défaut.

Pour activer la fonctionnalité d'audit du Presse-papiers, vous devez configurer le paramètre de stratégie de groupe **Configurer l'audit du Presse-papiers**.

Vous pouvez éventuellement configurer le paramètre de stratégie de groupe **Bloquer la redirection du Presse-papiers du côté client lorsque le client ne prend pas en charge l'audit** pour indiquez si vous voulez bloquer la redirection du Presse-papiers vers les clients qui ne prennent pas en charge la fonctionnalité d'audit du Presse-papiers.

Pour plus d'informations sur les paramètres de stratégie de groupe pour la redirection du Presse-papiers, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Cette fonctionnalité requiert Horizon Agent 7.7 ou version ultérieure sur la machine agent.

Le journal des événements dans lequel sont enregistrées les informations sur les activités copier et coller se nomme VMware Horizon RX Audit. Pour afficher le journal des événements sur la machine agent, utilisez l'Observateur d'événements de Windows. Pour afficher le journal des événements dans un emplacement centralisé, configurez VMware Log Insight ou le Collecteur d'événements de Windows. Pour plus d'informations sur Log Insight, rendez-vous sur https://docs.vmware.com/fr/vRealize-Log-Insight/index.html. Pour plus d'informations sur le Collecteur d'événements Windows, reportez-vous à la documentation de Microsoft.

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

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

Pour télécharger un fichier, faites glisser le fichier depuis le système client vers la fenêtre du poste de travail distant ou de l'application publiée. Lorsque le téléchargement est terminé, le fichier s'affiche dans le dossier `C:\Users\username\Documents`.

Pour télécharger un fichier, sélectionnez le fichier dans le poste de travail distant ou l'application publiée en appuyant sur Ctrl+C. Une fois que vous avez confirmé le transfert de fichiers, le fichier s'affiche dans le répertoire `Téléchargements` sur le périphérique client.

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, vous ne pouvez pas transférer les fichiers dans l'une ou l'autre direction.
- Si la valeur **Chargement de fichiers uniquement activé** est sélectionnée (paramètre par défaut), vous pouvez uniquement transférer des fichiers depuis le système client vers un poste de travail distant ou une application publiée.
- Si la valeur **Téléchargement de fichiers uniquement activé** est sélectionnée, vous pouvez uniquement transférer des fichiers depuis un poste de travail distant ou une application publiée vers le système client.

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

Partager l’accès aux dossiers et lecteurs locaux avec la redirection de lecteur client

Avec la fonctionnalité de redirection du lecteur client, vous pouvez partager des dossiers ou des lecteurs sur le système client local avec des postes de travail distants et des applications publiées.

Les lecteurs partagés peuvent comporter des lecteurs mappés et des périphériques de stockage USB.

La fonctionnalité de redirection du lecteur client présente les limites suivantes.

- L'utilisation des paramètres de clé de Registre Windows `ForcedByAdmin`, `default shares` et `permissions` pour configurer la redirection du lecteur client n'est pas prise en charge.
- Les canaux latéraux TCP et UDP ne sont pas pris en charge. Si la machine agent est configurée pour utiliser l'un de ces canaux latéraux, vous ne pouvez pas utiliser la fonctionnalité de redirection du lecteur client.
- Les stratégies d'Dynamic Environment Manager ne sont pas prises en charge.
- La récupération du réseau n'est pas prise en charge. Vous ne pouvez pas utiliser la redirection du lecteur client après la reconnexion au réseau, sauf si vous déconnectez la session et la reconnectez.
- Vous pouvez utiliser la fonctionnalité de redirection du lecteur client avec une seule session à distance à la fois. Les sessions multiples à distance ne sont pas prises en charge.
- Vous ne pouvez pas modifier les propriétés des dossiers ou fichiers partagés dans le poste de travail distant.

Conditions préalables

Pour partager des dossiers et des lecteurs avec un poste de travail distant ou une application publiée, l'administrateur Horizon doit activer la fonctionnalité de redirection du lecteur client. Cette tâche implique l'installation d'Horizon Agent et l'activation de l'option **Redirection du lecteur client** de l'agent. Elle peut également inclure la configuration de stratégies pour contrôler le comportement de la redirection du lecteur client. Pour plus d'informations, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Procédure

1. 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 applications et activez l'option **Activer le partage de dossiers** dans la fenêtre Paramètres.
2. Pour sélectionner un dossier ou un lecteur spécifique à partager, cliquez sur **Sélectionner**, sur **Ajouter**, recherchez et sélectionnez le dossier ou le lecteur, puis cliquez sur **OK**.

   Vous pouvez ajouter plusieurs dossiers et lecteurs, mais vous ne pouvez sélectionner qu'un élément à la fois. Vous pouvez supprimer un dossier ou un lecteur en cliquant sur le **X** en regard de son nom dans la boîte de dialogue Partage de dossiers.
3. Pour enregistrer les paramètres, cliquez sur **OK**.

   Les paramètres de partage des dossiers s'appliquent à l'ensemble des postes de travail distants et des applications publiées.

Résultats

Dans un poste de travail distant, un emplacement réseau s'affiche pour chaque dossier et lecteur que vous avez partagé. Par exemple, si vous avez partagé un dossier nommé `test1`, il est possible que l'emplacement réseau `test1(Z:)` s'affiche dans le poste de travail distant. Un périphérique s'affiche également pour chaque dossier et lecteur partagé. Le format de nom de périphérique est *`folder`* `sur Horizon`, par exemple, `test1 sur Horizon`.

Dans une application publiée, vous pouvez sélectionner **Fichier > Ouvrir** ou **Fichier > Enregistrer sous**, le cas échéant, et accéder au dossier ou au lecteur partagé.

Utiliser des périphériques USB sur un poste de travail distant

La fonctionnalité de redirection USB permet d'utiliser certains périphériques USB connectés localement dans un poste de travail distant. Vous pouvez rediriger plusieurs périphériques USB vers un poste de travail distant. Vous ne pouvez pas rediriger des périphériques USB vers des applications publiées et des postes de travail publiés.

En raison des restrictions de Chrome OS, de nombreux périphériques USB ne peuvent pas être redirigés vers un poste de travail distant. Pour cette version, VMware a testé les périphériques USB suivants. Des périphériques supplémentaires peuvent être pris en charge. Si un périphérique USB n'est pas pris en charge, Horizon Client renvoie un message d'erreur lorsque vous essayez de rediriger le périphérique.

- Imprimantes
  - Brother MFC 8710 DW
  - Brother QL-720NW
  - HP LaserJet Pro M201dw
  - HP LaserJet Pro MFP M426dfw
  - HP LaserJet P2055d
  - HP Deskjet 3525
  - HP OfficeJet 200 Mobile
  - Ricoh SP C261SNFw
  - Imprimantes série Samsung C43x
  - Xerox WorkCentre 6515
  - Imprimante Xerox Workcentre 3225/DNI
  - Imprimante Zebra Label GC420-1005G0-000
- Scanners
  - AmbirScanPro 490i

- Périphériques d'interface utilisateur
  - Wacom 520A
  - Wacom 500B

Conditions préalables

- Cette fonctionnalité requiert Chrome OS Version 87 ou version ultérieure.
- Un administrateur Horizon doit configurer la fonctionnalité de redirection USB pour le poste de travail distant.

Pour plus d'informations sur la configuration de la fonctionnalité de redirection USB pour des postes de travail distants, reportez-vous à la section « Configuration de la redirection USB pour les clients Chrome et HTML Access » dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Procédure

1. Connectez le périphérique USB au Chromebook.
2. Démarrez Horizon Client et connectez-vous au poste de travail distant.
3. Déplacez votre souris vers le haut de la fenêtre du poste de travail distant jusqu'à ce que la barre de menus supérieure s'affiche et cliquez sur le bouton **Redirection de périphérique USB**.
4. Cliquez sur **Ajouter un périphérique**.
5. Sélectionnez le périphérique dans la liste des périphériques USB et cliquez sur **Sélectionner**.

   Si le périphérique est pris en charge, il est redirigé vers le poste de travail distant et peut être utilisé dans la session. Dans le cas contraire, un message d'erreur s'affiche.
6. (Facultatif) Cliquez à nouveau sur **Ajouter un périphérique** pour rediriger un autre périphérique USB.
7. Pour libérer un périphérique USB du poste de travail distant, cliquez sur **Libérer**.

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

La fonctionnalité VMware Integrated Printing vous permet d'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, vous devez installer Horizon Agent sur la machine virtuelle ou sur l'hôte RDS avec l'option VMware Integrated Printing activée. Pour plus d'informations, reportez-vous au document *Configuration des postes de travail virtuels dans Horizon* ou *Configuration d'applications et de postes de travail publiés dans Horizon*.

Un administrateur Horizon peut désactiver la fonctionnalité VMware Integrated Printing pour les utilisateurs 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*.

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.

Dans un bureau de machine virtuelle à utilisateur unique, par défaut, chaque imprimante virtuelle apparaît sous la forme *<printer_name>*(*vdi*). Dans un poste de travail publié ou une application publiée, par défaut, chaque imprimante virtuelle apparaît sous la forme *<printer_name>*(v*<session_ID>*).

À partir de Horizon Agent 7.12, vous pouvez utiliser une stratégie de groupe pour modifier la convention d'affectation de noms d'imprimante pour les imprimantes clientes qui sont redirigées. Pour plus d'informations, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon* pour votre version d'Horizon Agent.

Conditions préalables

Pour utiliser VMware Integrated Printing, un administrateur Horizon doit installer cette fonctionnalité sur le poste de travail distant. Cette tâche implique l'activation de l'option **VMware Integrated Printing** dans le programme d'installation d'Horizon Agent. Pour plus d'informations sur l'installation d'Horizon Agent, consultez le document *Configuration des postes de travail virtuels dans Horizon* ou *Configuration d'applications et de postes de travail publiés dans Horizon*. Pour plus d'informations sur la configuration de la fonctionnalité VMware Integrated Printing, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

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.

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*. 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.

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.

Chrome permet 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 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**.

Après avoir activé **Activer la touche Windows pour les postes de travail**, vous devez appuyer sur Ctrl+Recherche 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 3-1. 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**.	

Tableau 3-1. Raccourcis de touche Windows pour les postes de travail distants Windows 10 et Windows Server 2016 (suite)

Clés	Action	Limites
Win+, (virgule)	Afficher temporairement le poste de travail distant.	
Win+Entrée	Ouvrir le Narrateur.	

Tableau 3-2. 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.	
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.	
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+Maj+M	Restaurer les fenêtres réduites sur le poste de travail distant.	
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).	
Win+Entrée	Ouvrir le Narrateur.	

Tableau 3-3. Raccourcis de touche Windows pour les postes de travail distants Windows 7

Clés	Action	Limites
Touche Windows	Ouvrir ou fermer le menu **Démarrer**.	
Win+D	Afficher et masquer le poste de travail distant.	
Win+M	Réduire toutes les fenêtres.	
Win+E	Ouvrir le dossier `Ordinateur`.	
Win+R	Ouvrir la boîte de dialogue Exécuter.	
Win+Origine	Réduire tout, sauf la fenêtre de poste de travail distant active.	
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 d'Horizon Client sont disponibles en anglais, allemand, français, japonais, chinois simplifié, chinois traditionnel, coréen et espagnol. Vous pouvez également entrer des caractères dans ces langues.

Dépannage

4

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
- Réinitialiser des postes de travail distants ou des applications publiées
- Désinstaller Horizon Client pour Chrome
- Activer la collecte de journaux

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* ou *Configuration d'applications et de postes de travail publiés dans Horizon*.

Procédure

- Cliquez sur le bouton de la barre d'outils **Paramètres** dans le coin supérieur droit de l'écran de sélection des postes de travail et applications, ouvrez le Centre de gestion des sessions, sélectionnez la session de poste de travail distant, puis cliquez sur **Redémarrer**.

  Vous pouvez également ouvrir le Centre de gestion des sessions en cliquant avec le bouton droit sur l'icône du poste de travail distant sur l'étagère et en cliquant sur **Centre de gestion des sessions**.

  Note Une session de poste de travail distant n'apparaît pas dans le Centre de gestion des sessions, sauf si vous vous connectez, puis vous déconnectez du poste de travail distant.

Résultats

Le système d'exploitation du poste de travail distant redémarre et le 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.

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'une application publiée arrête l'application sans enregistrer les données non enregistrées. Vous pouvez réinitialiser toutes les applications publiées en cours d'exécution ou vous pouvez réinitialiser des sessions d'applications publiées spécifiques.

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* ou *Configuration d'applications et de postes de travail publiés dans Horizon*.

Procédure

1. Pour réinitialiser toutes les applications publiées en cours d'exécution, cliquez sur le bouton de la barre d'outils **Paramètres** dans le coin supérieur droit de l'écran de sélection des postes de travail et applications, puis faites défiler jusqu'à **Réinitialisez toutes les applications en cours d'exécution** et cliquez sur **Réinitialiser**.
2. Pour réinitialiser une session d'application publiée, cliquez sur le bouton de la barre d'outils **Paramètres** dans le coin supérieur droit de l'écran de sélection des postes de travail et applications, ouvrez le Centre de gestion des sessions, sélectionnez le bouton **Applications distantes** pour la session d'application et cliquez sur **Mettre fin**.

   Vous pouvez également ouvrir le Centre de gestion des sessions en cliquant avec le bouton droit sur l'icône de l'application publiée sur l'étagère et en cliquant sur **Centre de gestion des sessions**.
3. Pour réinitialiser un poste de travail distant, cliquez sur le bouton de la barre d'outils **Paramètres** dans le coin supérieur droit de l'écran de sélection des postes de travail et applications, ouvrez le Centre de gestion des sessions, sélectionnez la session de poste de travail distant, puis cliquez sur **Réinitialiser**.

   Vous pouvez également ouvrir le Centre de gestion des sessions en cliquant avec le bouton droit sur l'icône de l'application publiée sur l'étagère et en cliquant sur **Centre de gestion des sessions**.

Résultats

Lorsque vous réinitialisez un poste de travail distant, son système d'exploitation redémarre et le 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.

Désinstaller Horizon Client pour Chrome

Pour désinstaller l'application VMware Horizon Client pour Chrome, supprimez-la de la même manière que vous supprimez d'autres applications Chromebook.

Procédure

1. Connectez-vous au Chromebook.
2. Cliquez avec le bouton droit sur l'application VMware Horizon Client et sélectionnez **Désinstaller**.

Étape suivante

Pour réinstaller l'application VMware Horizon Client pour Chrome, reportez-vous à la section Installer ou mettre à niveau Horizon Client pour Chrome.

Activer la collecte de journaux

Lorsque vous activez la collecte de journaux, Horizon Client collecte des informations de journaux qui peuvent aider VMware à résoudre les problèmes liés à Horizon Client.

Vous ne pouvez pas activer la collecte de journaux après vous être connecté à un poste de travail distant ou à une application publiée.

Conditions préalables

Connectez-vous à un serveur.

Procédure

1. 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 applications.
2. Pour activer la collecte de journaux, activez l'option **Activer la collecte des journaux** dans la fenêtre **Paramètres** et sélectionnez le niveau de journalisation **Basique**, **Déboguer** ou **Trace**.

   Le chemin d'accès au fichier journal s'affiche sous l'option **Activer la collecte des journaux** dans la fenêtre **Paramètres**.
3. Pour modifier le chemin d'accès au fichier journal, cliquez sur le chemin d'accès par défaut, accédez à un dossier dans lequel enregistrer le fichier journal et sélectionnez-le, puis cliquez sur **Enregistrer**.

   Le nouveau chemin d'accès s'affiche sous l'option **Activer la collecte des journaux** dans la fenêtre **Paramètres**.
4. Pour fermer la fenêtre **Paramètres**, cliquez sur **Fermer**.

Résultats

Horizon Client collecte et enregistre les informations de journalisation sans interruption jusqu'à ce que vous fermiez Horizon Client.