Utilisation de VMware Horizon Client pour iOS

Horizon Client 4.4

Ce document prend en charge la version de chacun des produits répertoriés, ainsi que toutes les versions publiées par la suite jusqu'au remplacement dudit document par une nouvelle édition. Pour rechercher des éditions plus récentes de ce document, rendez-vous sur : http://www.vmware.com/fr/support/pubs.

FR-002432-00

vmware®

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

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

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

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

docfeedback@vmware.com

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

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

Table des matières

Utilisation de VMware Horizon Client pour iOS

Ce guide, intitulé *Utilisation de VMware Horizon Client pour iOS*, fournit des informations concernant l'installation et l'utilisation du logiciel VMware Horizon® Client™ sur un périphérique iOS pour se connecter à une application ou à un poste de travail distant du centre de données.

Les informations de ce document indiquent la configuration système requise et fournissent des instructions d'installation d'Horizon Client. Ce document fournit également à l'utilisateur des conseils pour améliorer l'expérience de navigation et d'utilisation des éléments du poste de travail Windows sur un périphérique iOS tel qu'un iPad.

Ces informations sont destinées aux administrateurs qui doivent configurer un déploiement d'Horizon comportant des périphériques clients iOS. Les informations sont rédigées pour des administrateurs système expérimentés qui connaissent parfaitement la technologie des machines virtuelles et les opérations de datacenter.

Configuration et installation 1

La configuration d'un déploiement d'Horizon pour des clients iOS implique l'utilisation de certains paramètres de configuration du Serveur de connexion, le respect de la configuration système requise pour les serveurs Horizon et les clients iOS, ainsi que l'installation de l'application Horizon Client depuis l'Apple Store. VMware vous recommande également de configurer un serveur de sécurité afin que vos clients iOS n'aient pas besoin d'une connexion VPN.

Ce chapitre aborde les rubriques suivantes :

Configuration système requise

Le périphérique iOS sur lequel vous installez Horizon Client et tous les périphériques qu'il utilise doivent se conformer à une certaine configuration système.

Systèmes d'exploitation	iOS 8.4.1 et versions ultérieures, y compris iOS 9.x et iOS 10
Claviers externes	(Facultatif) Dock avec clavier iPad et clavier sans fil Apple (Bluetooth)
Authentification par carte à puce	Reportez-vous à la section « Exigences de l'authentification par carte à puce », page 9.

Authentification Touch ID	Reportez-vous à la section « Exigences de l'authentification Touch ID », page 11.
Serveur de connexion, serveur de sécurité et View Agent ou Horizon Agent	Dernière version de maintenance de View 5.3.x et versions ultérieures. VMware vous recommande d'utiliser un serveur de sécurité pour que vos clients iOS ne nécessitent pas de connexion VPN. Pour utiliser la fonctionnalité Unity Touch avec des postes de travail View 5.3.x, Remote Experience Agent doit être installé sur les postes de travail. Les applications distantes sont disponibles sur les serveurs Horizon 6.0 avec View et versions ultérieures.
Protocoles d'affichage	■ PCoIP ■ VMware Blast (requiert Horizon Agent 7.0 ou version ultérieure)
Protocoles réseau	■ IPv4 ■ IPv6 (requiert iOS 9.2 ou version ultérieure) Pour plus d'informations sur l'utilisation d'Horizon dans un environnement IPv6, consultez le document *Installation de View*.

Configuration système requise pour l'Audio/Vidéo en temps réel

L'Audio/Vidéo en temps réel fonctionne avec des périphériques audio standard et avec des applications de conférence standard, telles que Skype, WebEx et Google Hangouts. Pour prendre en charge la fonctionnalité Audio/Vidéo en temps réel, votre déploiement d'Horizon doit répondre à certaines exigences matérielles et logicielles.

Important Seule la fonctionnalité d'entrée audio est prise en charge. La fonctionnalité de vidéo n'est pas prise en charge.

Postes de travail distants	View Agent 5.3 ou version ultérieure doit être installé sur les postes de travail. S'agissant des postes de travail View Agent 5.3, la version correspondante de Remote Experience Agent doit également être installée sur les postes de travail. Par exemple, si View Agent 5.3 est installé, vous devez également installer Remote Experience Agent à partir de View 5.3 Feature Pack 1. Consultez le document *Installation et administration de View Feature Pack*. Si vous disposez de View Agent 6.0 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure, aucun Feature Pack n'est requis. Pour utiliser l'Audio/Vidéo en temps réel avec des postes de travail RDS et des applications distantes, vous devez disposer d'Horizon Agent 7.0.2 ou version ultérieure.
Périphérique d'accès client	L'Audio/Vidéo en temps réel est pris en charge sur tous les périphériques iOS qui utilisent Horizon Client pour Windows. Pour plus d'informations, reportez-vous à la section « Configuration système requise », page 7.

Exigences de l'authentification par carte à puce

Les systèmes client qui utilisent une carte à puce pour l'authentification utilisateur doivent satisfaire certaines exigences.

Horizon Client pour iOS prend en charge l'utilisation de cartes à puce avec des postes de travail distants qui disposent des systèmes d'exploitation invités Windows 7, Windows Vista, Windows XP, Windows 8.1, Windows 10 et Windows Server 2008 R2. Pour les applications et les postes de travail basés sur un hôte Microsoft RDS, les systèmes d'exploitation Windows Server 2008 R2 et Windows Server 2012 R2 sont pris en charge. Un système d'exploitation iOS 8.4.1 ou version ultérieure est nécessaire.

Chaque système client qui utilise une carte à puce pour l'authentification utilisateur doit avoir les logiciels et matériels suivants :

- Horizon Client
- Un lecteur de carte à puce compatible
- Des pilotes d'application spécifiques du produit

Vous devez également installer des pilotes d'application spécifiques du produit sur les postes de travail distants ou l'hôte RDS Microsoft.

Les utilisateurs qui s'authentifient avec des cartes à puce doivent posséder une carte à puce et chaque carte à puce doit contenir un certificat utilisateur.

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

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

  Vous devez ajouter tous les certificats d'autorité de certification applicables pour tous les certificats d'utilisateur de confiance à un fichier de magasin d'approbations de serveur sur l'hôte du Serveur de connexion ou du serveur de sécurité. Ces certificats incluent des certificats racines et doivent inclure des certificats intermédiaires si le certificat de carte à puce de l'utilisateur a été délivré par une autorité de certification intermédiaire.

- Pour plus d'informations sur les tâches que vous pouvez effectuer dans Active Directory afin d'implémenter l'authentification par carte à puce, consultez le document *Administration de View*.

Activation du champ Aide-mémoire du nom d'utilisateur dans Horizon Client

Dans certains environnements, les utilisateurs de carte à puce peuvent utiliser un seul certificat de carte à puce pour s'authentifier sur plusieurs comptes d'utilisateur. Les utilisateurs entrent leur nom d'utilisateur dans le champ **Aide-mémoire du nom d'utilisateur** lors de la connexion par carte à puce.

Pour que le champ **Aide-mémoire du nom d'utilisateur** apparaisse dans la boîte de dialogue de connexion d'Horizon Client, vous devez activer la fonctionnalité d'aide-mémoire du nom d'utilisateur de carte à puce pour l'instance du Serveur de connexion dans Horizon Administrator. La fonctionnalité d'aide-mémoire du nom d'utilisateur de carte à puce n'est prise en charge qu'avec les serveurs et les agents Horizon 7 version 7.0.2 et versions ultérieures. Pour plus d'informations sur l'activation de la fonctionnalité d'aide-mémoire du nom d'utilisateur de carte à puce, consultez le document *Administration de View*.

Si votre environnement utilise un dispositif Access Point plutôt qu'un serveur de sécurité pour sécuriser l'accès externe, vous devez configurer le dispositif Access Point pour qu'il prenne en charge la fonctionnalité d'aide-mémoire du nom d'utilisateur de carte à puce. La fonctionnalité d'aide-mémoire du nom d'utilisateur de carte à puce n'est prise en charge qu'avec Access Point 2.7.2 et versions ultérieures. Pour plus d'informations sur l'activation de la fonctionnalité d'aide-mémoire du nom d'utilisateur de carte à puce dans Access Point, consultez le document *Déploiement et configuration d'Access Point*.

Remarque Horizon Client prend toujours en charge les certificats de carte à puce de compte unique lorsque la fonctionnalité d'aide-mémoire du nom d'utilisateur de carte à puce est activée.

Configurer l'authentification par carte à puce

Les tâches de configuration consistent notamment à connecter et à coupler le lecteur de carte à l'appareil, et à définir la stratégie de retrait de la carte à puce.

Prérequis

- Vérifiez que la version du client, de l'agent de poste de travail, du serveur, du système d'exploitation, du lecteur de carte à puce et de la carte à puce que vous utilisez est correcte. Reportez-vous à la section « Exigences de l'authentification par carte à puce », page 9.
- Si ce n'est pas déjà fait, effectuez les tâches décrites dans la rubrique « Préparer Active Directory pour l'authentification par carte à puce » du document *Installation de View*.
- Configurez les serveurs Horizon afin de prendre en charge l'utilisation des cartes à puce. Reportez-vous à la rubrique « Configurer l'authentification par carte à puce » dans le document *Administration de View*.

Procédure

1 Associez l'appareil au lecteur de carte à puce, conformément à la documentation fournie par le fabricant du lecteur de carte.

   Si votre périphérique iOS dispose d'un connecteur à 30 broches, vous pouvez brancher le lecteur de carte à puce sur le connecteur. Pour l'iPad Air et l'iPhone 5S, qui disposent des interfaces Lightning, vous devez utiliser un adaptateur à 30 broches pour brancher le lecteur de carte à puce sur le connecteur à 30 broches du périphérique.

2 Configurez la règle de retrait de carte à puce.

Option	Description
Définir la stratégie sur le serveur	Si vous utilisez Horizon Administrator pour définir une stratégie, vous avez la possibilité de déconnecter les utilisateurs du Serveur de connexion lorsqu'ils retirent leur carte à puce ou de laisser les utilisateurs connectés au Serveur de connexion lorsqu'ils retirent leur carte à puce et les laisser démarrer de nouvelles sessions de poste de travail ou d'application sans s'authentifier de nouveau. a Dans Horizon Administrator, sélectionnez **Configuration de View > Serveurs**. b Dans l'onglet **Serveurs de connexion**, sélectionnez l'instance du Serveur de connexion et cliquez sur **Modifier**. c Dans l'onglet **Authentification**, cochez ou décochez la case **Déconnecter les sessions utilisateur lors du retrait de la carte à puce** pour configurer la stratégie de retrait de la carte à puce. d Cliquez sur **OK** pour enregistrer vos modifications. e Redémarrez le service Serveur de connexion pour que vos modifications prennent effet. Si vous cochez la case **Déconnecter les sessions utilisateur lors du retrait de la carte à puce**, Horizon Client retourne à l'écran **Récent** lorsque les utilisateurs retirent leur carte à puce.
Définir la stratégie sur le poste de travail	Si vous utilisez l'éditeur de stratégie de groupe (`gpedit.msc`), les paramètres suivants sont disponibles : Aucune action, Verrouiller la station de travail, Forcer la fermeture de session ou Déconnecter en cas de session Bureau à distance. Après avoir ouvert `gpedit.msc` dans le système d'exploitation du poste de travail, accédez à **Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Ouverture de session interactive : comportement lorsque la carte à puce est retirée**. Exécutez la commande `gpupdate /force` après avoir modifié la configuration pour forcer une actualisation de la stratégie de groupe.

Exigences de l'authentification Touch ID

Pour utiliser Touch ID pour l'authentification utilisateur dans Horizon Client, vous devez satisfaire certaines exigences.

Modèles d'iPad et d'iPhone	Tout modèle d'iPad ou d'iPhone prenant en charge Touch ID, par exemple, l'iPad Air 2 et l'iPhone 6.
Exigences de système d'exploitation	■ iOS 8 ou version ultérieure. ■ Ajoutez au moins une empreinte digitale dans le paramètre Touch ID et code secret.
Exigences du Serveur de connexion	■ Horizon 6 version 6.2 ou version ultérieure. ■ Activez l'authentification biométrique dans le Serveur de connexion. Pour plus d'informations, consultez « Configurer l'authentification biométrique » dans le document *Administration de View*.

- L'instance du Serveur de connexion doit présenter un certificat signé racine valide à Horizon Client.

Exigences d'Horizon Client

- Définissez le mode de vérification des certificats sur **Ne jamais se connecter aux serveurs non approuvés** ou sur **Avertir avant de se connecter à des serveurs non approuvés**. Pour plus d'informations sur la définition du mode de vérification des certificats, reportez-vous à la section « Définition du mode de vérification de certificats pour Horizon Client », page 30.
- Activez Touch ID en appuyant sur **Activer Touch ID** sur l'écran de connexion du serveur. Une fois que vous êtes connecté, vos informations d'identification Active Directory sont stockées en toute sécurité dans le trousseau de votre périphérique iOS. L'option **Activer Touch ID** est affichée la première fois que vous vous connectez et n'apparaît plus lorsque Touch ID est activé.

Vous pouvez utiliser Touch ID avec l'authentification par carte à puce et dans le cadre de l'authentification à deux facteurs avec l'authentification RSA SecurID et RADIUS. Si vous utilisez Touch ID avec l'authentification par carte à puce, Horizon Client se connecte au serveur une fois que vous avez entré votre code PIN et l'écran de connexion Touch ID ne s'affiche pas.

Systèmes d'exploitation de poste de travail pris en charge

Les administrateurs créent des machines virtuelles avec un système d'exploitation invité et installent le logiciel agent sur le système d'exploitation invité. Les utilisateurs finaux peuvent ouvrir une session sur ces machines virtuelles à partir d'un périphérique client.

Pour obtenir une liste des systèmes d'exploitation invités Windows pris en charge, consultez le document *Installation de View*.

Certains systèmes d'exploitation invités Linux sont également pris en charge si vous possédez View Agent 6.1.1 ou version ultérieure ou Horizon Agent 7.0 ou version ultérieure. Pour plus d'informations sur la configuration système requise, la configuration des machines virtuelles Linux pour les utiliser dans Horizon et obtenir la liste des fonctionnalités prises en charge, consultez *Configuration des postes de travail Horizon 6 for Linux* ou *Configuration des postes de travail Horizon 7 for Linux*.

Préparation du Serveur de connexion pour Horizon Client

Les administrateurs doivent effectuer des tâches spécifiques pour permettre aux utilisateurs finaux de se connecter à des applications ou des postes de travail distants.

Pour que les utilisateurs finaux puissent se connecter au Serveur de connexion ou à un serveur de sécurité et accéder à une application ou à un poste de travail distant, vous devez configurer un certain nombre de paramètres de pool et de sécurité :

- Si vous prévoyez d'utiliser Access Point, configurez le Serveur de connexion pour qu'il fonctionne avec Access Point. Reportez-vous au document *Déploiement et configuration d'Access Point*. Les dispositifs Access Point remplissent le même rôle que celui précédemment joué uniquement par des serveurs de sécurité.
- Si vous utilisez un serveur de sécurité, assurez-vous de disposer des dernières versions de maintenance du Serveur de connexion 5.3.x et du Serveur de sécurité 5.3.x ou versions ultérieures. Pour plus d'informations, reportez-vous au document *Installation de View*.
- Si vous prévoyez d'utiliser une connexion tunnel sécurisée pour des périphériques client et si la connexion sécurisée est configurée avec un nom d'hôte DNS pour le Serveur de connexion ou un serveur de sécurité, vérifiez que le périphérique client peut résoudre ce nom DNS.

Pour activer ou désactiver le tunnel sécurisé, dans Horizon Administrator, accédez à la boîte de dialogue Modifier les paramètres du Serveur de connexion Horizon et cochez la case **Utiliser une connexion par tunnel sécurisé vers le poste de travail**.

- Vérifiez qu'un pool de postes de travail ou d'applications a été créé et que le compte d'utilisateur que vous souhaitez utiliser est autorisé à accéder au pool. Pour plus d'informations, reportez-vous au document *Configuration des postes de travail virtuels dans Horizon 7* ou *Configuration d'applications et de postes de travail publiés dans Horizon 7*.
- Pour pouvoir utiliser une authentification à deux facteurs, telle que l'authentification RSA SecurID ou RADIUS, avec Horizon Client, vous devez activer cette fonctionnalité sur le Serveur de connexion. Pour plus d'informations, consultez les rubriques concernant l'authentification à deux facteurs dans le document *Administration de View*.
- Pour masquer les informations de sécurité dans Horizon Client, notamment les informations d'URL de serveur et le menu déroulant **Domaine**, activez les paramètres **Masquer les informations de serveur dans l'interface utilisateur client** et **Masquer la liste de domaines dans l'interface utilisateur client** dans Horizon Administrator. Ces paramètres globaux sont disponibles dans Horizon 7 versions 7.1 et ultérieures. Pour plus d'informations sur la configuration des paramètres globaux, consultez le document *Administration de View*.

  Pour s'authentifier lorsque le menu déroulant **Domaine** est masqué, les utilisateurs doivent fournir des informations sur le domaine en entrant leur nom d'utilisateur au format ***domaine**nomutilisateur*** ou ***utilisateur*nom@*domaine*** dans la zone de texte **Nom d'utilisateur**.

  Important Si vous activez les paramètres **Masquer les informations de serveur dans l'interface utilisateur client** et **Masquer la liste de domaines dans l'interface utilisateur client** et sélectionnez l'authentification à deux facteurs (RSA SecureID ou RADIUS) pour l'instance du Serveur de connexion, n'appliquez pas la correspondance des noms d'utilisateur Windows. L'application de la correspondance des noms d'utilisateur Windows empêchera les utilisateurs d'entrer des informations sur le domaine dans la zone de texte Nom d'utilisateur et la connexion échouera toujours. Pour plus d'informations, consultez les rubriques concernant l'authentification à deux facteurs dans le document *Administration de View*.
- Pour utiliser l'authentification Touch ID, vous devez activer l'authentification biométrique sur le Serveur de connexion. L'authentification biométrique est prise en charge dans Horizon 6 version 6.2 et ultérieures. Pour plus d'informations, reportez-vous au document *Administration de View*.
- Pour permettre aux utilisateurs finaux d'enregistrer leurs mots de passe sur Horizon Client pour ne pas devoir entrer systématiquement leurs informations d'identification chaque fois qu'ils se connectent à une instance du Serveur de connexion, configurez Horizon LDAP pour cette fonctionnalité sur l'hôte du Serveur de connexion.

  Les utilisateurs peuvent enregistrer leurs mots de passe si Horizon LDAP est configuré pour le permettre, si le mode de vérification des certificats Horizon Client est défini sur **Avertir avant de se connecter à des serveurs non approuvés** ou **Ne jamais se connecter aux serveurs non approuvés**, et si Horizon Client peut entièrement vérifier le certificat de serveur présenté par le Serveur de connexion. Pour obtenir des instructions, reportez-vous au document *Administration de View*.
- Vérifiez que le pool de postes de travail ou d'applications est défini pour utiliser le protocole d'affichage VMware Blast ou PCoIP. Pour plus d'informations, consultez les documents *Configuration des postes de travail virtuels dans Horizon 7* et *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

Installer ou mettre à niveau Horizon Client sur un périphérique iOS

Vous pouvez installer Horizon Client à partir de la page de téléchargements de VMware ou de l'App Store.

Prérequis

- Si vous n'avez pas encore configuré le périphérique iOS, faites-le maintenant. Consultez le guide d'utilisation d'Apple.
- Vérifiez que vous disposez de l'URL d'accès à une page de téléchargement contenant le programme d'installation d'Horizon Client. Il peut s'agir de l'URL de la page de téléchargements de VMware à l'adresse http://www.vmware.com/go/viewclients ou de l'URL d'une instance du Serveur de connexion.

Procédure

1. Sur votre périphérique iOS, Mac ou PC, accédez à l'URL de téléchargement du fichier du programme d'installation ou recherchez l'application Horizon Client dans l'App Store.
2. Téléchargez l'application.
3. Si vous avez téléchargé l'application sur un Mac ou un PC, connectez votre périphérique iOS à l'ordinateur, puis suivez les instructions d'iTunes qui s'affichent à l'écran.
4. Pour voir si l'installation a réussi, vérifiez que l'icône de l'application **Horizon**s'affiche sur le périphérique iOS.

Utilisation de jetons logiciels RSA SecurID intégrés

Si vous créez et distribuez des jetons logiciels RSA SecurID aux utilisateurs finaux, ces derniers doivent entrer uniquement leur code d'identification personnel (PIN) et non pas le code PIN et un code de jeton pour s'authentifier.

Configuration requise

Vous pouvez utiliser le format CTF (Compressed Token Format) ou le provisionnement initial dynamique appelé CT-KIP (Cryptographic Token Key Initialization Protocol), pour configurer un système d'authentification RSA d'utilisation simple. Avec ce système, vous générez une URL à envoyer aux utilisateur finaux. Pour installer le jeton, les utilisateurs finaux collent directement cette URL dans Horizon Client sur leurs périphériques client. La boîte de dialogue permettant de coller l'URL s'affiche lorsque les utilisateurs finaux se connectent au Serveur de connexion avec Horizon Client.

Une fois le jeton logiciel installé, l'utilisateur final entre un code PIN pour s'authentifier. Avec des jetons RSA externes, les utilisateurs finaux doivent entrer un code PIN et le code de jeton généré par un jeton d'authentification matériel ou logiciel.

Les préfixes d'URL suivants sont pris en charge si les utilisateurs finaux font un copier-coller de l'URL dans Horizon Client lorsque Horizon Client est connecté à une instance du Serveur de connexion sur lequel RSA est activé :

- `viewclient-securid://`
- `com.rsa.securid.iphone://`
- `com.rsa.securid://`

Pour les utilisateurs finaux qui installeront le jeton en tapant l'URL, seul le préfixe `viewclient-securid://` est pris en charge.

Pour plus d'informations sur l'utilisation du provisionnement initial dynamique ou le provisionnement (CTF) basé sur un fichier, voir la page Web *Jeton logiciel RSA SecurID pour les périphériques iPhone* sur http://www.rsa.com/node.aspx?id=3652 ou *Jeton logiciel RSA SecurID pour les périphériques Android* sur http://www.rsa.com/node.aspx?id=3832.

Instructions à l'attention des utilisateurs finaux

Lorsque vous créez une URL CTFString ou une URL CT-KIP pour l'envoyer aux utilisateurs finaux, vous pouvez générer une URL avec ou sans mot de passe ou code d'activation. Vous envoyez cette URL aux utilisateurs finaux dans un courrier électronique qui doit contenir les informations suivantes :

- Instructions d'accès à la boîte de dialogue d'installation d'un jeton logiciel.

  Instruction demandant aux utilisateurs finaux d'appuyer sur **Jeton externe** dans la boîte de dialogue Horizon Client qui les invite à entrer les informations d'identification de RSA SecurID lorsqu'ils se connectent à une instance du Serveur de connexion.

- L'URL CTFString ou l'URL CT-KIP en texte brut.

  Si l'URL est formatée, les utilisateurs finaux reçoivent un message d'erreur lorsqu'ils tentent de l'utiliser dans Horizon Client.

- Code d'activation si l'URL CT-KIP que vous créez ne contient pas le code d'activation.

  Les utilisateurs finaux doivent entrer ce code d'activation dans un champ de texte de la boîte de dialogue.

- Si l'URL CT-KIP contient un code d'activation, indiquez aux utilisateurs finaux qu'ils ne doivent rien entrer dans la zone de texte **Mot de passe ou code d'activation** dans la boîte de dialogue d'installation du jeton logiciel.

Configurer des options TLS/SSL avancées

Vous pouvez sélectionner les protocoles de sécurité et les algorithmes de chiffrement qui sont utilisés pour chiffrer les communications entre Horizon Client et les serveurs Horizon et entre Horizon Client et l'agent dans le poste de travail distant.

TLSv1.0, TLSv1.1 et TLSv1.2 sont activés par défaut. SSL v2.0 et 3.0 ne sont pas pris en charge. La chaîne de contrôle de chiffrement par défaut est « !aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA +AESGCM:kECDH+AES:ECDH+AES:RSA+AES ».

Si vous configurez un protocole de sécurité pour Horizon Client qui n'est pas activé sur l'instance d'Horizon Server à laquelle le client se connecte, une erreur TLS/SSL se produit et la connexion échoue.

Pour obtenir des informations sur la configuration des protocoles de sécurité qui sont acceptés par les instances du Serveur de connexion, consultez le document *Sécurité de View*.

Procédure

1. Appuyez sur **Paramètres** en bas de l'écran Horizon Client.
2. Appuyez sur **Options SSL avancées**.
3. Assurez-vous que l'option **Réinitialiser les paramètres par défaut** est définie sur Désactivé.
4. Pour activer ou désactiver un protocole de sécurité, appuyez sur le bouton bascule **Activé** ou **Désactivé** en regard du nom du protocole de sécurité.
5. Pour modifier la chaîne de contrôle de chiffrement, remplacez la chaîne par défaut.
6. (Facultatif) Si vous avez besoin de rétablir les paramètres par défaut, cliquez sur **Réinitialiser** dans le coin supérieur droit de l'écran.

Vos modifications seront appliquées lors de votre prochaine connexion au serveur.

Configurer des options VMware Blast

Vous pouvez configurer des options de décodage H.264 et de condition réseau pour des sessions d'application et de poste de travail distant qui utilisent le protocole d'affichage VMware Blast.

Vous ne pouvez pas modifier l'option de condition réseau après vous être connecté à un serveur. Vous pouvez configurer le décodage H.264 avant ou après vous être connecté à un serveur.

Prérequis

Cette fonctionnalité requiert Horizon Agent 7.0 ou version ultérieure.

Procédure

1 Appuyez sur **Paramètres** en bas de l'écran d'Horizon Client et appuyez sur **VMware Blast**.

Si vous êtes connecté à un serveur, le paramètre **VMware Blast** n'est visible que si VMware Blast est le protocole préféré. Vous ne pouvez pas modifier l'option de condition réseau après vous être connecté à un serveur.

2 Configurez les options de décodage et de condition réseau.

Option	Action
H.264	Configurez cette option, avant ou après la connexion au Serveur de connexion, pour autoriser le décodage H.264 dans Horizon Client. Lorsque cette option est sélectionnée (paramètre par défaut), Horizon Client utilise le décodage H.264 si l'agent prend en charge le codage logiciel ou matériel H.264. Si l'agent ne prend pas en charge le codage logiciel ou matériel H.264, Horizon Client utilise le décodage JPG/PNG. Désélectionnez cette option pour utiliser le décodage JPG/PNG.
Condition réseau	Vous ne pouvez configurer cette option qu'avant la connexion au Serveur de connexion. Sélectionnez l'une des options de condition réseau suivantes : ■ **Excellent** : Horizon Client utilise uniquement la mise en réseau TCP. Cette option est idéale pour un environnement LAN. ■ **Classique (par défaut)** : Horizon Client fonctionne en mode mixte. En mode mixte, Horizon Client utilise la mise en réseau TCP lors de la connexion au serveur et utilise BEAT (Blast Extreme Adaptive Transport) si l'agent et Blast Security Gateway (si activé) prennent en charge la connectivité BEAT. Cette option est le paramètre par défaut. ■ **Faible** : Horizon Client n'utilise la mise en réseau BEAT que si le serveur tunnel BEAT est activé sur le serveur ; sinon il passe en mode mixte. **Remarque** Dans Horizon 7 versions 7.1 et antérieures, les instances du Serveur de connexion et du serveur de sécurité ne prennent pas en charge le serveur tunnel BEAT. VMware Access Point 2.9 et versions ultérieures prennent en charge le serveur tunnel BEAT. Blast Security Gateway pour les instances du Serveur de connexion et du serveur de sécurité ne prend pas en charge la mise en réseau BEAT.

Les modifications de H.264 seront appliquées la prochaine fois qu'un utilisateur se connectera à une application ou un poste de travail distant et qu'il sélectionnera le protocole d'affichage VMware Blast. Vos modifications n'ont pas d'incidence sur les sessions VMware Blast existantes.

Configurer la vue par défaut d' Horizon Client

Vous pouvez configurer si l'écran Récent ou l'écran Serveurs s'affiche lorsque vous lancez Horizon Client.

Procédure

1 Appuyez sur **Paramètres** en bas de l'écran Horizon Client.

2 Appuyez sur **Vue par défaut**.

3 Appuyez sur une option pour sélectionner la vue par défaut.

Option	Description
Récent	L'écran Récent s'affiche lorsque vous lancez Horizon Client. L'écran Récent contient des raccourcis vers des applications et des postes de travail récemment utilisés. Il s'agit du paramètre par défaut.
View	L'écran Serveurs s'affiche lorsque vous lancez Horizon Client. L'écran Serveurs contient des raccourcis vers les serveurs que vous avez ajoutés à Horizon Client.

La vue par défaut que vous avez sélectionnée prend effet immédiatement.

Configurer AirWatch pour fournir Horizon Client aux périphériques iOS

Vous pouvez configurer AirWatch pour fournir Horizon Client aux utilisateurs de périphériques iOS.

Si vous le souhaitez, vous pouvez spécifier une liste par défaut d'instances du Serveur de connexion. Les instances du Serveur de connexion que vous spécifiez s'affichent sous forme de raccourcis dans Horizon Client.

Prérequis

- Installez et déployez AirWatch. Reportez-vous à la page http://www.air-watch.com.
- Familiarisez-vous avec la console AirWatch. Cette procédure suppose que vous savez utiliser la console AirWatch. Pour plus d'informations, reportez-vous à l'aide en ligne ou à la documentation d'AirWatch.

Procédure

1 Connectez-vous à la console AirWatch en tant qu'administrateur.

2 Sélectionnez **Comptes > Utilisateurs > Affichage en liste**, cliquez sur **Ajouter un utilisateur**, puis ajoutez des comptes d'utilisateurs pour les utilisateurs qui exécuteront Horizon Client sur leurs appareils mobiles.

3 Sélectionnez **Comptes > Utilisateurs > Groupes d'utilisateurs**, cliquez sur **Ajouter** et créez un groupe d'utilisateurs pour les comptes d'utilisateurs que vous avez créés.

4 Téléchargez l'application Horizon Client et ajoutez-la à AirWatch.

   a Sélectionnez **Applications et livres > Applications > Affichage en liste** et cliquez sur **Ajouter l'application** dans l'onglet **Public**.

   b Recherchez et sélectionnez VMware Horizon Client pour Apple iOS dans l'App Store.

   c Dans l'onglet **Infos**, tapez un nom d'application et spécifiez les modèles de périphériques iOS pris en charge.

   d Dans l'onglet **Attribution**, attribuez l'application Horizon Client au groupe d'utilisateurs que vous avez créé.

e (Facultatif) Configurez un ou plusieurs serveurs par défaut.

Les serveurs que vous spécifiez s'affichent sous forme de raccourcis dans VMware Horizon Client.

Remarque Cette fonctionnalité est prise en charge uniquement pour les périphériques iOS 7 et versions ultérieures. Vous ne pouvez pas transmettre une liste par défaut du Serveur de connexion à un périphérique iOS 6.

Option	Description
Configurer un serveur, un nom d'utilisateur et des informations de domaine	Dans l'onglet **Déploiement**, sélectionnez un mode de transfert, cochez la case **Envoyer la configuration de l'application**, entrez **broker_list** dans la zone de texte **Clé de configuration**, sélectionnez **Chaîne** dans le menu déroulant **Type de valeur** et entrez une liste de serveurs par défaut dans la zone de texte **Valeur de configuration** au format JSON. Utilisez la propriété **server** pour spécifier l'adresse IP ou le nom d'hôte du serveur, les propriétés **username** et **domain** pour spécifier le nom et le domaine d'un utilisateur autorisé à accéder au serveur et la propriété **description** pour spécifier une description du serveur. L'exemple suivant spécifie quatre serveurs par défaut. `{"settings":{ "server_list":[{"server":"123.456.1.1","description":"View server 1"}, {"server":"123.456.1.2","description":"View server 2"}, {"server":"123.456.1.3","description":"View server 3"}, {"server":"viewserver4.mydomain.com","description":"View server 4","username":"vmware","domain":"view"}]}}`
Configurer uniquement les informations d'un serveur	Dans l'onglet **Déploiement**, sélectionnez un mode de transfert, cochez la case **Envoyer la configuration de l'application**, entrez **servers** dans la zone de texte **Clé de configuration**, sélectionnez **Chaîne** dans le menu déroulant **Type de valeur** et entrez l'adresse IP ou le nom d'hôte d'un serveur dans la zone de texte **Valeur de configuration**. La valeur de clé **servers** est sensible à la casse. Pour spécifier une liste de serveurs, entrez plusieurs adresses IP ou noms d'hôtes, séparés par des virgules, dans la zone de texte **Valeur de la configuration**. L'exemple suivant spécifie trois serveurs par défaut. `123.456.1.1, viewserver4.mydomain.com, 123.456.1.2`

f Publiez l'application Horizon Client.

5 Installez et configurez l'agent AirWatch MDM sur chaque périphérique iOS.

Vous pouvez télécharger l'agent AirWatch MDM à partir d'iTunes.

6 Utilisez la console AirWatch pour installer l'application Horizon Client sur les appareils mobiles.

Vous ne pouvez pas installer l'application Horizon Client avant la date d'effet indiquée dans l'onglet **Déploiement**.

AirWatch fournit Horizon Client aux périphériques iOS dans le groupe d'utilisateurs que vous avez associé à l'application Horizon Client.

Lorsqu'un utilisateur lance Horizon Client, Horizon Client communique avec l'agent AirWatch MDM sur le périphérique. Si vous avez configuré une liste par défaut d'instances du Serveur de connexion, AirWatch transmet les informations du serveur à AirWatch MDM Agent sur le périphérique, et les raccourcis correspondant à ces serveurs s'affichent dans Horizon Client.

Suivant

Vous pouvez utiliser la console AirWatch pour modifier l'application Horizon Client et transmettre ces modifications aux périphériques iOS. Par exemple, vous pouvez ajouter une instance par défaut du Serveur de connexion à la liste de serveurs définie pour l'application Horizon Client.

Données Horizon Client collectées par VMware

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

VMware collecte des données sur les clients afin de hiérarchiser la compatibilité matérielle et logicielle. Si l'administrateur de votre entreprise a choisi de participer au programme d'amélioration du produit, VMware collecte des données anonymes sur votre déploiement afin d'améliorer la réponse de VMware aux exigences des clients. Aucune donnée permettant d'identifier votre organisation n'est collectée. Les informations d'Horizon Client sont envoyées d'abord au Serveur de connexion, puis à VMware, avec des données provenant des instances du Serveur de connexion, des pools de postes de travail et des postes de travail distants.

Bien que les informations soient chiffrées lors de leur transfert au Serveur de connexion, les informations sur le système client sont journalisées non chiffrées dans un répertoire propre à l'utilisateur. Les journaux ne contiennent aucune information d'identification personnelle.

L'administrateur qui installe le Serveur de connexion peut choisir de participer au programme d'amélioration du produit VMware lors de l'exécution de l'assistant d'installation du Serveur de connexion, ou un administrateur peut définir une option dans Horizon Administrator après l'installation.

Tableau 1-1. Données collectées depuis Horizon Client pour le programme d'amélioration du produit

Description	Ce champ reste-t-il anonyme ?	Exemple
Entreprise ayant produit l'application Horizon Client	Non	VMware
Nom du produit	Non	VMware Horizon Client
Version du produit client	Non	(Le format est *x.x.x-yyyyyy*, où *x.x.x* est le numéro de version du client et *yyyyyy* est le numéro de build.)
Architecture binaire du client	Non	Exemples : ■ i386 ■ x86_64 ■ arm
Nom du build du client	Non	Exemples : ■ VMware-Horizon-Client-Win32-Windows ■ VMware-Horizon-Client-Linux ■ VMware-Horizon-Client-iOS ■ VMware-Horizon-Client-Mac ■ VMware-Horizon-Client-Android ■ VMware-Horizon-Client-WinStore
Système d'exploitation hôte	Non	Exemples : ■ Windows 8.1 ■ Windows 7, 64 bits Service Pack 1 (Build 7601) ■ iPhone OS 5.1.1 (9B206) ■ Ubuntu 12.04.4 LTS ■ Mac OS X 10.8.5 (12F45)

Tableau 1-1. Données collectées depuis Horizon Client pour le programme d'amélioration du produit (suite)

Description	Ce champ reste-t-il anonyme ?	Exemple
Noyau du système d'exploitation hôte	Non	Exemples : ■ Windows 6.1.7601 SP1 ■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X ■ Darwin 11.4.2 ■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012 ■ inconnu (pour Windows Store)
Architecture du système d'exploitation hôte	Non	Exemples : ■ x86_64 ■ i386 ■ armv71 ■ ARM
Modèle du système hôte	Non	Exemples : ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision WorkStation T3400 (A04 03/21/2008)
Processeur du système hôte	Non	Exemples : ■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH ■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH ■ inconnu (pour iPad)
Nombre de cœurs dans le processeur du système hôte	Non	Par exemple : 4
Mo de mémoire sur le système hôte	Non	Exemples : ■ 4096 ■ inconnu (pour Windows Store)
Nombre de périphériques USB connectés	Non	2 (la redirection de périphériques USB est prise en charge uniquement pour les clients Linux, Windows et Mac.)
Nombre maximal de connexions de périphériques USB simultanées	Non	2
ID de fournisseur de périphériques USB	Non	Exemples : ■ Kingston ■ NEC ■ Nokia ■ Wacom
ID de produit de périphérique USB	Non	Exemples : ■ DataTraveler ■ Gamepad ■ Disque de stockage ■ Souris sans fil
Famille de périphériques USB	Non	Exemples : ■ Sécurité ■ Périphérique d'interface humaine ■ Imagerie
Nombre d'utilisations du périphérique USB	Non	(Nombre de partages du périphérique)

Utilisation d'URI pour configurer Horizon Client 2

Les URI (Uniform Resource Identifiers) vous permettent de créer une page Web ou un e-mail contenant des liens sur lesquels les utilisateurs finaux peuvent cliquer pour démarrer Horizon Client, se connecter à un serveur et ouvrir un poste de travail ou une application spécifique avec des options de configuration particulières.

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

- Adresse du Serveur de connexion
- Numéro de port du Serveur de connexion
- Nom d'utilisateur Active Directory
- Nom d'utilisateur RADIUS ou RSA SecurID, s'il est différent du nom d'utilisateur Active Directory
- Nom de domaine
- Nom affiché du poste de travail ou de l'application
- Actions incluant la réinitialisation, la déconnexion et le démarrage d'une session

Pour construire un URI, vous pouvez utiliser le schéma d'URI `vmware-view` avec des éléments de chemin et de requête propres à Horizon Client.

Remarque Vous pouvez utiliser les URI pour démarrer Horizon Client uniquement si le logiciel client est déjà installé sur des ordinateurs clients.

Ce chapitre aborde les rubriques suivantes :

Syntaxe pour la création d'URI vmware-view

La syntaxe comprend le schéma d'URI `vmware-view`, un chemin d'accès spécifiant le poste de travail ou l'application et, en option, une requête permettant de spécifier des actions de poste de travail ou d'application, ou des options de configuration.

Spécification d'URI

Utilisez la syntaxe suivante pour créer des URI pour démarrer Horizon Client :

`vmware-view://[`*`authority-part`*`][/`*`path-part`*`][?`*`query-part`*`]`

Le seul élément requis est le schéma d'URI, `vmware-view`. Pour certaines versions de certains systèmes d'exploitation client, le nom du schéma est sensible à la casse. Il faut ainsi utiliser `vmware-view`.

Important Pour tous les éléments, les caractères non ASCII doivent d'abord être encodés en UTF-8 [STD63], puis chaque octet de la séquence UTF-8 correspondante doit être codé en pourcentage pour être représenté en tant que caractères URI.

Pour plus d'informations sur l'encodage de caractères ASCII, consultez la référence d'encodage d'URL sur http://www.utf8-chartable.de/.

authority-part

Spécifie l'adresse du serveur et, éventuellement, un nom d'utilisateur, un numéro de port non défini par défaut, ou bien les deux. Les traits de soulignement (_) ne sont pas pris en charge dans les noms de serveur. Les noms de serveur doivent être conformes à la syntaxe DNS.

Pour spécifier un nom d'utilisateur, utilisez la syntaxe suivante :

`user1@`*`server-address`*

Vous ne pouvez pas spécifier d'adresse UPN, ce qui inclut le domaine. Pour spécifier le domaine, vous pouvez utiliser la partie de requête `domainName` de l'URI.

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

`server-address``:`*`port-number`*

path-part

Spécifie le poste de travail ou l'application. Utilise le nom d'affichage du poste de travail ou de l'application. Ce nom est celui spécifié dans Horizon Administrator lorsque le pool de postes de travail ou d'applications a été créé. Si le nom affiché contient un espace, utilisez le mécanisme de codage **`%20`** pour représenter l'espace.

query-part

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

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

Requêtes prises en charge

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

action

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

Valeur	Description
`browse`	Affiche une liste des postes de travail et applications disponibles hébergés sur le serveur spécifié. Il ne vous est pas demandé de spécifier un poste de travail ou une application pour l'utilisation de cette action. Si vous utilisez l'action `browse` et que vous spécifiez un poste de travail ou une application, ceux-ci sont mis en surbrillance dans la liste des postes de travail ou d'applications disponibles.
`start-session`	Ouvre l'application ou le poste de travail spécifié. Si aucune requête d'action n'est fournie et que le nom du poste de travail ou de l'application est fourni, `start-session` est l'action par défaut.
`reset`	Éteint puis redémarre le poste de travail spécifié ou l'application distante. Les données non enregistrées sont perdues. La réinitialisation d'un poste de travail distant équivaut à appuyer sur le bouton Réinitialiser d'un ordinateur physique.
`restart`	Éteint puis redémarre le poste de travail spécifié. Le redémarrage d'un poste de travail distant équivaut à la commande de redémarrage du système d'exploitation Windows. En général, le système d'exploitation invite l'utilisateur à enregistrer toutes les données non enregistrées avant de redémarrer.
`logoff`	Déconnecte l'utilisateur du système d'exploitation invité sur le poste de travail distant. Si vous spécifiez une application, l'action est ignorée ou l'utilisateur final voit le message d'avertissement « Action d'URI non valide ».

args

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

- Pour un deux-points (:), utilisez **`%3A`**
- Pour une barre oblique inversée (\), utilisez **`%5C`**
- Pour un espace ( ), utilisez **`%20`**
- Pour un guillemet double ("), utilisez **`%22`**

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

appProtocol

Pour les applications distantes, les valeurs valides sont **`PCOIP`** et **`BLAST`**. Par exemple, pour spécifier le protocole PCoIP, utilisez la syntaxe **`appProtocol=PCOIP`**.

defaultLaunchView

Définit la vue de lancement par défaut pour Horizon Client. Les valeurs valides sont **`recent`** et **`servers`**.

desktopProtocol

Pour les postes de travail distants, les valeurs valides sont **`PCOIP`** et **`BLAST`**. Par exemple, pour spécifier le protocole PCoIP, utilisez la syntaxe **`desktopProtocol=PCOIP`**.

domainName	Nom de domaine NETBIOS associé à l'utilisateur qui se connecte à l'application ou au poste de travail distant. Utilisez par exemple `monentreprise` plutôt que `monentreprise.com`.
tokenUserName	Spécifie le nom d'utilisateur RSA ou RADIUS. N'utilisez cette requête que si le nom d'utilisateur RSA ou RADIUS est différent du nom d'utilisateur Active Directory. Si vous ne spécifiez pas cette requête et que l'authentification RSA ou RADIUS est nécessaire, le nom d'utilisateur Windows est utilisé. La syntaxe se présente ainsi : **`tokenUserName=`*`name`***.

Exemples d'URI de vmware-view

Vous pouvez créer des liens hypertextes ou des boutons avec le schéma URI `vmware-view` et inclure ces liens dans des e-mails ou sur une page Web. Vos utilisateurs finaux peuvent cliquer sur ces liens pour, par exemple, ouvrir un poste de travail distant particulier avec les options de démarrage que vous spécifiez.

Exemples de syntaxe URI

Chaque exemple d'URI est suivi d'une description de ce que l'utilisateur final voit après avoir cliqué sur le lien URI.

1 `vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session`

Horizon Client démarre et se connecte au serveur `view.mycompany.com`. La boîte de dialogue de connexion invite l'utilisateur à fournir un nom d'utilisateur, un nom de domaine et un mot de passe. Après l'ouverture de session, le client se connecte au poste de travail dont le nom d'affichage est **Poste de travail principal**, et l'utilisateur voit sa session ouverte sur le système d'exploitation client.

Remarque Le protocole d'affichage et la taille de fenêtre par défaut sont utilisés. Le protocole d'affichage par défaut est PCoIP. La taille de fenêtre par défaut est plein écran.

---

2 `vmware-view://view.mycompany.com:7555/Primary%20Desktop`

Cet URI a le même effet que l'exemple précédent, sauf qu'il utilise le port non défini par défaut 7555 pour le Serveur de connexion. (Le port par défaut est 443.) Comme un identificateur de poste de travail est fourni, le poste de travail s'ouvre même si l'action `start-session` n'est pas incluse dans l'URI.

3 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?desktopProtocol=PCOIP`

Horizon Client démarre et se connecte au serveur `view.mycompany.com`. Dans la boîte de dialogue de connexion, la zone de texte **Nom d'utilisateur** contient le nom **fred**. L'utilisateur doit fournir le nom de domaine et le mot de passe. Après l'ouverture de session, le client se connecte au poste de travail dont le nom d'affichage est **Poste de travail Finance**, et l'utilisateur voit sa session ouverte sur le système d'exploitation client. La connexion utilise le protocole d'affichage PCoIP.

4 `vmware-view://view.mycompany.com/Calculator?action=start-session&appProtocol=BLAST`

Horizon Client démarre et se connecte au serveur `view.mycompany.com`. Dans la boîte de dialogue de connexion, l'utilisateur doit fournir le nom d'utilisateur, le nom de domaine et le mot de passe. Après l'ouverture de session, le client se connecte à l'application dont le nom complet affiché est **Calculatrice**. La connexion utilise le protocole d'affichage VMware Blast.

5 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?domainName=mycompany`

Horizon Client démarre et se connecte au serveur `view.mycompany.com`. Dans la boîte de dialogue de connexion, la zone de texte **Nom d'utilisateur** contient le nom **fred** et la zone de texte **Domaine** contient **mycompany**. L'utilisateur doit fournir uniquement un mot de passe. Après l'ouverture de session, le client se connecte au poste de travail dont le nom d'affichage est **Poste de travail Finance**, et l'utilisateur voit sa session ouverte sur le système d'exploitation client.

6 `vmware-view://view.mycompany.com/`

Horizon Client démarre et l'utilisateur est dirigé vers l'invite d'ouverture de session pour se connecter au serveur `view.mycompany.com`.

7 `vmware-view://view.mycompany.com/Primary%20Desktop?action=reset`

Horizon Client démarre et se connecte au serveur `view.mycompany.com`. La boîte de dialogue de connexion invite l'utilisateur à fournir un nom d'utilisateur, un nom de domaine et un mot de passe. Après l'ouverture de session, Horizon Client affiche une boîte de dialogue qui invite l'utilisateur à confirmer l'opération de réinitialisation pour Poste de travail principal.

Remarque Cette action est uniquement disponible si un administrateur Horizon a activé la fonctionnalité de réinitialisation de poste de travail pour le poste de travail.

8 `vmware-view://view.mycompany.com/Primary%20Desktop?action=restart`

Horizon Client démarre et se connecte au serveur `view.mycompany.com`. La boîte de dialogue de connexion invite l'utilisateur à fournir un nom d'utilisateur, un nom de domaine et un mot de passe. Après l'ouverture de session, Horizon Client affiche une boîte de dialogue qui invite l'utilisateur à confirmer l'opération de redémarrage du poste de travail principal.

Remarque Cette action est uniquement disponible si un administrateur Horizon a activé la fonctionnalité de redémarrage de poste de travail pour le poste de travail.

9 `vmware-view://`

Si le client est déjà en cours d'exécution, l'application Horizon Client passe au premier plan. Si le client n'est pas déjà en cours d'exécution, Horizon Client démarre.

10 `vmware-view://?defaultlaunchview=recent`

Horizon Client démarre et l'utilisateur voit l'écran Récent.

11 `vmware-view://10.10.10.10/My%20Notepad++?args=%22My%20new%20file.txt%22`

Lance My Notepad++ sur le serveur 10.10.10.10 et transmet l'argument `My new file.txt` dans la commande de lancement d'application. Le nom de fichier est entre guillemets, car il contient des espaces.

12 `vmware-view://10.10.10.10/Notepad++%2012?args=a.txt%20b.txt`

Lance Notepad++ 12 sur le serveur 10.10.10.10 et transmet l'argument `a.text b.txt` dans la commande de lancement d'application. Comme l'argument n'est pas entre guillemets, un espace sépare les noms de fichier et les deux fichiers sont ouverts séparément dans Notepad++.

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

Exemples de code HTML

Vous pouvez utiliser des URI pour faire des liens hypertextes et des boutons à inclure dans des e-mails ou sur des pages Web. Les exemples suivants montrent comment utiliser l'URI du premier exemple d'URI pour coder un lien hypertexte qui dit **Test Link** et un bouton qui dit **TestButton**.

```
<html>
<body>

<a href="vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session">Test
Link</a><br>
```

```
<form><input type="button" value="TestButton" onClick="window.location.href=
'vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session'"></form> <br>

</body>
</html>
```

Gestion des connexions aux applications et postes de travail distants

3

Utilisez Horizon Client pour vous connecter à un serveur, pour modifier la liste des serveurs auxquels vous vous connectez, pour ouvrir ou fermer une session sur des postes de travail distants et pour utiliser des applications distantes. À des fins de dépannage, il vous permet également de réinitialiser les applications et postes de travail distants.

En fonction de la façon dont l'administrateur configure les stratégies de postes de travail distants, les utilisateurs finaux peuvent être en mesure d'exécuter plusieurs opérations sur leurs postes de travail.

Ce chapitre aborde les rubriques suivantes :

Connexion à une application ou un poste de travail distant

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

Pour utiliser les applications distantes, vous devez vous connecter au Serveur de connexion 6.0 ou version ultérieure.

Remarque Avant de laisser vos utilisateurs finaux accéder à leurs postes de travail distants, vérifiez que vous pouvez ouvrir une session sur un poste de travail distant à partir d'un périphérique client.

Prérequis

- Procurez-vous les informations d'identification pour ouvrir une session, telles que le nom d'utilisateur et le mot de passe Active Directory, le nom d'utilisateur et le code secret RSA SecurID ou le nom d'utilisateur et le code secret pour l'authentification RADIUS.

- Obtenez le nom de domaine NETBIOS pour ouvrir une session. Utilisez par exemple `monentreprise` plutôt que `monentreprise.com`.
- Effectuez les tâches administratives décrites dans « Préparation du Serveur de connexion pour Horizon Client », page 12.
- Si vous vous trouvez à l'extérieur du réseau d'entreprise et si vous n'utilisez pas de serveur de sécurité pour accéder au poste de travail distant, vérifiez que votre périphérique client est configuré pour utiliser une connexion VPN et activez cette connexion.

  Important VMware vous recommande d'utiliser un serveur de sécurité plutôt qu'un VPN.

  Si votre entreprise possède un réseau interne sans fil afin de permettre un accès routable aux postes de travail distants et que votre périphérique peut utiliser ce réseau, vous n'avez pas besoin de mettre en place un serveur de sécurité ou une connexion VPN.
- Vérifiez que vous disposez du nom de domaine complet (FQDN) du serveur qui fournit l'accès à l'application ou au poste de travail distant. Les traits de soulignement (_) ne sont pas pris en charge dans les noms de serveur. Vous avez également besoin du numéro de port si le port n'est pas 443.
- Si vous prévoyez d'utiliser un logiciel RSA SecurID intégré, vérifiez que vous disposez de l'URL CT-KIP et du code d'activation corrects. Reportez-vous à la section « Utilisation de jetons logiciels RSA SecurID intégrés », page 14.
- Configurez le mode de vérification des certificats pour le certificat SSL présenté par le Serveur de connexion. Reportez-vous à la section « Définition du mode de vérification de certificats pour Horizon Client », page 30.
- Si vous prévoyez d'utiliser Touch ID pour l'authentification, ajoutez au moins une empreinte digitale dans le paramètre Touch ID et code secret sur votre périphérique iOS. Pour toutes les exigences de l'authentification de Touch ID, reportez-vous à la section « Exigences de l'authentification Touch ID », page 11.

Procédure

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

2 Appuyez sur l'icône de l'application **Horizon** dans l'écran Accueil.

3 Connectez-vous à un serveur.

Option	Action
Se connecter à un nouveau serveur	Entrez le nom d'un serveur, entrez une description (facultative) et appuyez sur **Ajouter un serveur**.
Se connecter à un serveur existant	Appuyez sur l'icône du serveur sur l'onglet Serveurs.

Les connexions entre Horizon Client et les serveurs utilisent toujours SSL. Le port par défaut pour les connexions SSL 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`**.

4 Si une carte à puce est requise ou facultative, sélectionnez le certificat de la carte à puce à utiliser et entrez votre code PIN.

Le certificat est sélectionné automatiquement si la carte à puce n'en a qu'un seul. S'il y a plusieurs certificats, vous pouvez les parcourir si nécessaire.

5 Si un message demande les informations d'identification RSA SecurID ou les informations d'identification pour l'authentification RADIUS, entrez les informations d'identification ou, si vous envisagez d'utiliser un jeton RSA SecurID intégré, installez un jeton intégré.

Option	Action
Jeton existant	Si vous utilisez un jeton d'authentification matériel ou logiciel sur un smartphone, entrez vos nom d'utilisateur et code secret. Le code secret peut comporter un code PIN et le numéro généré sur le jeton.
Installer le jeton logiciel	Cliquez sur **Jeton externe**. Dans la boîte de dialogue Installer le jeton logiciel, collez l'URL CT-KIP ou CTFString que votre administrateur vous a envoyée par e-mail. Si l'URL contient un code d'activation, vous n'avez rien à saisir dans la zone de texte **Mot de passe ou code d'activation**.

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

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

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

7 (Facultatif) Si le paramètre **Activer Touch ID** est disponible, activez-le pour utiliser Touch ID pour l'authentification.

Le paramètre **Activer Touch ID** est disponible uniquement si l'authentification biométrique est activée sur le serveur et que vous ne vous êtes pas authentifié auparavant avec Touch ID.

8 Si vous êtes invité à fournir un nom d'utilisateur et un mot de passe, fournissez des informations d'identification Active Directory.

a Tapez 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 le menu déroulant **Domaine** est masqué, vous devez taper le nom d'utilisateur sous la forme ***nomutilisateur@domaine*** ou ***domaine\nomutilisateur***.

c (Facultatif) Appuyez pour activer l'option **Mémoriser ce mot de passe** si votre administrateur a activé cette fonctionnalité et si le certificat de serveur peut être entièrement vérifié.

d Appuyez sur **Ouverture de session**.

Si Touch ID est activé et que vous vous connectez pour la première fois, vos informations d'identification Active Directory sont stockées en toute sécurité dans le trousseau du périphérique iOS pour une utilisation ultérieure.

9 Si vous êtes invité à vous authentifier avec Touch ID, placez votre doigt sur le bouton **Accueil**.

10 (Facultatif) Appuyez sur **Paramètres** en bas de l'écran Horizon Client et appuyez sur **Protocole préféré :** pour sélectionner le protocole d'affichage à utiliser.

VMware Blast améliore l'autonomie de la batterie. Il s'agit du meilleur protocole pour les utilisateurs de périphériques 3D et mobiles haut de gamme. Le protocole d'affichage par défaut est **PCoIP**.

11 Appuyez sur un poste de travail ou une application pour vous y connecter.

Si vous utilisez l'authentification par carte à puce, on ne vous redemande pas votre code PIN, mais le processus de connexion prend plus de temps que lorsque vous utilisez l'authentification Active Directory.

Si vous vous connectez à un poste de travail publié qui est hébergé sur un hôte RDS Microsoft et si le poste de travail est déjà configuré pour utiliser le protocole d'affichage RDP Microsoft, vous ne pouvez pas vous connecter immédiatement. Vous êtes invité à demander au système de fermer votre session sur le système d'exploitation distant afin qu'une connexion puisse être établie avec le protocole d'affichage PCoIP ou VMware Blast. VMware Blast requiert Horizon Agent 7.0 ou version ultérieure.

Après votre première connexion à une application ou un poste de travail, un raccourci pour le poste de travail ou l'application en question est sauvegardé dans l'écran Récent. La prochaine fois que vous souhaiterez vous connecter à l'application ou au poste de travail distant, il vous suffira d'appuyer sur le raccourci au lieu de taper le nom du serveur.

Définition du mode de vérification de certificats pour Horizon Client

Les administrateurs, et parfois les utilisateurs finaux, peuvent configurer le rejet des connexions client si une ou plusieurs vérifications de certificats de serveur échouent.

La vérification des certificats se produit pour les connexions SSL entre le Serveur de connexion et Horizon Client. La vérification de certificat inclut les vérifications suivantes :

- Le certificat a-t-il un autre but que de vérifier l'identité de l'expéditeur et de chiffrer les communications du serveur ? Autrement dit, s'agit-il du bon type de certificat ?
- Le certificat a-t-il expiré, ou est-il valide uniquement dans le futur ? Autrement dit, le certificat est-il valide en fonction de l'horloge de l'ordinateur ?
- Le nom commun sur le certificat correspond-il au nom d'hôte du serveur qui l'envoie ? Une incompatibilité peut se produire si l'équilibrage de charge redirige Horizon Client vers un serveur disposant d'un certificat qui ne correspond pas au nom d'hôte entré dans Horizon Client. Une incompatibilité peut également se produire si vous entrez une adresse IP plutôt qu'un nom d'hôte dans le client.
- Le certificat est-il signé par une autorité de certification inconnue ou non approuvée ? Les certificats auto-signés sont un type d'autorité de certification non approuvée.

  Pour que cette vérification aboutisse, la chaîne d'approbation du certificat doit être associée à une racine dans le magasin de certificats local.

Important Pour plus d'informations sur la distribution d'un certificat racine auto-signé que les utilisateurs peuvent installer sur leurs périphériques iOS, consultez les instructions sur le site Web d'Apple. Par exemple, pour les iPads, consultez http://www.apple.com/ipad/business/docs/iPad_Certificates.pdf.

Pour définir le mode de vérification des certificats, appuyez sur **Paramètres** en bas de l'écran Horizon Client et appuyez sur **Mode de vérification des certificats de serveur**. Vous avez trois possibilités :

- **Ne jamais se connecter à des serveurs non autorisés**. Si l'une des vérifications de certificat échoue, le client ne peut pas se connecter au serveur. Un message d'erreur répertorie les vérifications qui ont échoué.
- **Signaler avant de se connecter à des serveurs non autorisés**. Si une vérification de certificat échoue car le serveur utilise un certificat auto-signé, vous pouvez cliquer sur **Continuer** pour ignorer l'avertissement. Pour les certificats auto-signés, le nom du certificat ne doit pas nécessairement correspondre au nom du serveur que vous avez entré dans Horizon Client.
- **Ne pas vérifier les certificats d'identité des serveurs**. Ce paramètre signifie qu'aucune vérification des certificats n'a lieu.

Si le mode de vérification des certificats est défini sur **Avertir**, vous pouvez toujours vous connecter à une instance du Serveur de connexion qui utilise un certificat auto-signé.

Si un administrateur installe ultérieurement un certificat de sécurité à partir d'une autorité de certification de confiance, afin que toutes les vérifications de certificat aient lieu lorsque vous vous connectez, cette connexion approuvée est enregistrée pour ce serveur spécifique. À l'avenir, si ce serveur présente de nouveau un certificat auto-signé, la connexion échoue. Après qu'un serveur particulier présente un certificat entièrement vérifiable, il doit toujours faire ainsi.

Gérer les serveurs enregistrés

Lorsque vous vous connectez à un serveur, Horizon Client enregistre le serveur dans l'écran Serveurs. Vous pouvez modifier et supprimer les serveurs enregistrés.

Horizon Client enregistre le serveur, même si une erreur se glisse lors de la saisie du nom ou de l'adresse IP. Vous pouvez supprimer ou modifier ces informations.

Important Appuyez sur un nom de serveur pour vous connecter au serveur.

Procédure

1 Appuyez sur **Serveurs** (icône Cloud) en bas de l'écran pour afficher les serveurs enregistrés.

2 Pour gérer un serveur enregistré, appuyez longuement sur l'icône du serveur jusqu'à ce que le menu contextuel s'affiche.

Option	Action
Modifier le nom d'utilisateur, le domaine, le nom du serveur ou la description	a Appuyez sur **Modifier le serveur** dans le menu contextuel. b Apportez vos modifications sur l'écran Modifier le serveur. c Appuyez sur **Mettre à jour** pour enregistrer vos modifications.
Supprimer un serveur	Appuyez sur **Supprimer le serveur** dans le menu contextuel. Les raccourcis des postes de travail et des applications associés au serveur sont également supprimés.
Oublier un mot de passe enregistré	Appuyez sur **Oublier le mot de passe** dans le menu contextuel. L'option est disponible uniquement si vous avez précédemment enregistré votre mot de passe.
Désactiver Touch ID	Appuyez sur **Se déconnecter**. Cette option est disponible uniquement si vous avez activé précédemment Touch ID.

Sélectionner une application ou un poste de travail distant favori

Vous pouvez sélectionner des postes de travail et des applications distants comme favoris. Les favoris sont identifiés par une étoile. L'étoile vous permet de trouver rapidement vos applications et postes de travail favoris. Vos sélections favorites sont sauvegardées, même après la fermeture de votre session sur le serveur.

Prérequis

Obtenez les informations d'identification dont vous avez besoin pour vous connecter au serveur, telles qu'un nom d'utilisateur et un mot de passe ou un jeton RSA SecurID et un code secret.

Procédure

1 Appuyez sur **Serveurs** (icône Cloud) en bas de l'écran, puis sur l'icône du serveur à connecter au serveur.

2 Si vous y êtes invité, entrez votre nom d'utilisateur et code secret RSA, votre nom d'utilisateur et mot de passe Active Directory, ou les deux.

3 Procédez comme suit pour sélectionner ou désélectionner un poste de travail ou une application comme favori.

Option	Action
Sélectionner un favori	Appuyez longuement sur le nom du poste de travail ou de l'application jusqu'à ce que le menu contextuel s'affiche et appuyez sur **Marquer comme favori**. Une étoile s'affiche dans le coin supérieur droit du nom et le nom s'affiche dans la page Favoris.
Désélectionner un favori	Appuyez longuement sur le nom du poste de travail ou de l'application jusqu'à ce que le menu contextuel s'affiche et appuyez sur **Supprimer des favoris**. Une étoile ne s'affiche plus dans le coin supérieur droit du nom et le nom disparaît de la page Favoris.

4 (Facultatif) Appuyez sur **Favoris** (icône étoile) en bas de l'écran pour afficher uniquement les applications ou les postes de travail favoris.

Vous pouvez appuyer sur **Tout** (icône Cloud) en bas de l'écran pour afficher tous les postes de travail et toutes les applications disponibles.

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

Vous pouvez vous déconnecter d'un poste de travail distant sans fermer votre session afin que les applications restent ouvertes sur le poste de travail distant. Vous pouvez également vous déconnecter d'une application distante de manière que celle-ci reste ouverte.

Lorsque vous avez une session ouverte sur l'application ou le poste de travail distant, vous pouvez vous déconnecter en appuyant sur l'icône du menu circulaire Outils d'Horizon Client, puis sur l'icône **Se déconnecter**.

Remarque Un administrateur Horizon peut configurer votre poste de travail pour que la session soit fermée automatiquement lors de la déconnexion. Dans ce cas, tous les programmes ouverts sur votre poste de travail sont arrêtés.

Fermer une session sur un poste de travail distant

Vous pouvez fermer une session sur un système d'exploitation de poste de travail distant, même si aucun poste de travail n'est ouvert dans Horizon Client.

Si vous êtes actuellement connecté à un poste de travail distant et que vous y avez ouvert une session, vous pouvez utiliser le menu **Démarrer** de Windows pour fermer la session. Après que Windows a fermé votre session, le poste de travail est déconnecté.

Remarque Tous les fichiers non enregistrés qui sont ouverts sur le poste de travail distant sont fermés lors de l'opération de fermeture de session.

Prérequis

- Obtenez les informations d'identification dont vous avez besoin pour ouvrir une session, telles que le nom d'utilisateur et le mot de passe Active Directory, le nom d'utilisateur et le code secret RSA SecurID ou le nom d'utilisateur et le code secret pour l'authentification RADIUS.
- Si vous n'avez encore jamais ouvert de session, familiarisez-vous avec la procédure « Connexion à une application ou un poste de travail distant », page 27.

Procédure

1 Appuyez sur **Serveurs** (icône Cloud) en bas de l'écran, puis sur l'icône du serveur.

2 Si vous y êtes invité, entrez votre nom d'utilisateur et code secret RSA, votre nom d'utilisateur et mot de passe Active Directory, ou les deux.

3 Appuyez longuement sur le nom du poste de travail jusqu'à ce que le menu contextuel s'affiche.

4 Appuyez sur **Fermer la session** dans le menu contextuel.

Suivant

Appuyez sur le bouton **Déconnexion** dans le coin supérieur gauche de l'écran pour vous déconnecter du serveur.

Gérer les raccourcis de poste de travail et d'application

Une fois que vous êtes connecté à une application ou à un poste de travail distant, Horizon Client enregistre un raccourci pour l'application ou le poste de travail récemment utilisé. Vous pouvez réorganiser et supprimer ces raccourcis.

Les raccourcis de postes de travail et d'applications peuvent s'afficher sur plusieurs pages et vous pouvez balayer les pages pour voir d'autres raccourcis. Horizon Client crée de nouvelles pages, si nécessaire, pour recevoir tous vos raccourcis.

Procédure

- Effectuez ces étapes pour supprimer un raccourci de poste de travail ou d'application de l'écran Récent.
  a Appuyez longuement sur le raccourci.
  b Appuyez sur le bouton **X**.
- Pour déplacer un raccourci de poste de travail ou d'application, appuyez longuement sur le raccourci, faites-le glisser vers le nouvel emplacement et appuyez sur **Terminé**.

  Vous ne pouvez faire glisser un raccourci vers une autre page que si cette page existe déjà.

Utilisation de 3D Touch avec Horizon Client

Vous pouvez utiliser les gestes Peek et Pop pour interagir avec Horizon Client sur un iPhone 6s ou un iPhone 6s Plus avec 3D Touch activé.

Utilisation de Peek et Pop avec l'application Horizon sur votre écran d'accueil

Vous pouvez utiliser Peek sur l'application **Horizon** sur votre écran d'accueil pour afficher un menu d'actions rapides. Dans le menu d'actions rapides, vous pouvez appuyer sur l'élément **Se connecter au serveur le plus récent** pour vous connecter rapidement au dernier serveur utilisé. S'il n'existe pas de serveur récent, vous pouvez appuyer sur l'élément **Se connecter au serveur le plus récent** pour ajouter un nouveau serveur.

Lorsque vous êtes connecté à une application ou un poste de travail distant, Horizon Client ajoute un raccourci vers le poste de travail ou l'application au menu d'actions rapides. Par exemple, si vous vous connectez à un poste de travail distant nommé Win7, Horizon Client ajoute **Se connecter à Win7**. Vous pouvez appuyer sur un raccourci pour vous connecter rapidement à une application ou un poste de travail distant. Le menu d'actions rapides de l'icône **Horizon** peut contenir jusqu'à trois raccourcis.

Utilisation de Peek et Pop dans Horizon Client

Sur l'écran de sélection de poste de travail et d'application, vous pouvez utiliser Peek sur une application ou un poste de travail distant pour afficher un menu d'actions rapides. Vous pouvez appuyer sur des éléments dans le menu d'actions rapides pour vous connecter, fermer la session, marquer un favori et exécuter d'autres actions, en fonction de l'application ou du poste de travail distant. Vous pouvez également utiliser Pop dans une application ou un poste de travail distant pour vous y connecter.

Des menus d'actions rapides sont également disponibles sur les écrans Serveurs, Récent et Favoris. Par exemple, sur l'écran Serveurs, vous pouvez utiliser Peek sur un serveur enregistré et appuyer sur des éléments dans le menu d'actions rapides pour modifier un serveur, le supprimer ou vous y connecter. Sur l'écran Récent, vous pouvez utiliser Peek sur le raccourci d'une application ou d'un poste de travail distant et appuyer sur des éléments dans le menu d'actions rapides pour supprimer le raccourci ou pour vous connecter au poste de travail ou à l'application. Vous pouvez également utiliser Pop dans le raccourci d'un serveur enregistré, d'une application ou d'un poste de travail distant pour vous y connecter.

Activation de Peek pour les Outils d' Horizon Client

Par défaut, l'icône du menu circulaire Outils d'Horizon Client s'affiche au milieu de l'écran lorsque vous êtes connecté à une application ou à un poste de travail distant. Vous appuyez sur l'icône du menu circulaire pour agrandir le menu et afficher les icônes de chaque outil, que vous sélectionnez en appuyant dessus. Pour les images de l'icône du menu circulaire et les icônes des outils, reportez-vous à la section Tableau 4-6.

Si vous activez Peek pour les Outils d'Horizon Client, l'icône du menu circulaire Outils d'Horizon Client n'apparaît pas. Pour afficher les icônes de chaque outil, appuyez fortement sur l'écran.

Pour activer Peek pour les Outils d'Horizon Client, appuyez sur **Paramètres** en bas de l'écran d'Horizon Client, appuyez sur **Tactile** et activez le paramètre **Aperçu furtif du menu**. Si vous êtes connecté à une application ou un poste de travail distant, vous pouvez accéder aux paramètres en appuyant sur l'icône **Paramètres** (engrenage) dans le menu circulaire Outils d'Horizon Client.

Utilisation de la recherche Spotlight avec Horizon Client

Vous pouvez utiliser la recherche Spotlight sur des périphériques iOS 9 et versions ultérieures pour rechercher des applications et des postes de travail distants et vous connecter à ceux-ci.

Lorsque vous vous connectez à un serveur dans Horizon Client, les applications et postes de travail distants sur le serveur sont ajoutés à l'index Spotlight. Seuls les applications et postes de travail distants sur le dernier serveur auquel vous vous êtes connecté sont indexés.

Pour utiliser la recherche Spotlight afin de rechercher une application ou un poste de travail distant particulier, tapez son nom ou un nom partiel dans le champ de recherche Spotlight. Par exemple, pour rechercher un poste de travail distant nommé Poste de travail Win 2008 RDS, vous pouvez taper **`Win`** ou **`RDS`**.

Pour utiliser la recherche Spotlight afin de trouver vos applications ou postes de travail distants favoris, tapez **`favori`** dans le champ de recherche Spotlight. Pour rechercher une application ou un poste de travail distant, tapez **`vmware`** ou **`horizon`** dans le champ de recherche Spotlight. Les résultats de la recherche peuvent contenir jusqu'à 10 éléments.

Pour vous connecter à une application ou un poste de travail distant, appuyez sur son nom dans les résultats de la recherche. Si vous n'êtes pas actuellement connecté au serveur, l'écran de connexion d'Horizon Client s'affiche, et vous pouvez vous connecter.

Utilisation de Split View et de Slide Over avec Horizon Client

Vous pouvez utiliser Split View et Slide Over avec Horizon Client sur un modèle d'iPad qui prend en charge Split View et Slide Over et qui exécute iOS 9 ou version ultérieure.

Avec Split View et Slide Over, vous pouvez ouvrir Horizon Client et une autre application en même temps. Vous pouvez exécuter Horizon Client comme l'application principale ou comme l'application secondaire.

Si vous faites pivoter votre périphérique ou faites glisser le séparateur vertical qui sépare les applications principale et secondaire, Horizon Client s'adapte automatiquement à la taille de la fenêtre. Si vous êtes connecté à un poste de travail distant, ce dernier s'adapte automatiquement à la taille de la fenêtre si le paramètre **Résolution** est défini sur **Ajustement automatique**. Pour plus d'informations sur la définition de la résolution pour un poste de travail distant, reportez-vous à la section « Changement des paramètres de la résolution d'écran », page 52.

Remarque Horizon Client ne prend pas en charge Image dans l'image.

Utilisation du widget Horizon Client

Si votre périphérique est équipé du système d'exploitation iOS 10 ou version ultérieure, vous pouvez ajouter le widget Horizon Client à son écran Rechercher.

Pour ajouter le widget Horizon Client à l'écran Rechercher, cliquez sur **Modifier** dans l'écran Rechercher, appuyez sur le bouton Plus (+) vert situé en regard de Horizon Client dans la liste des widgets, puis cliquez sur **Terminé**.

Si vous ne vous êtes jamais connecté à une application ou un poste de travail distant, le widget Horizon Client affiche `Aucun poste de travail/application n'a encore été lancé`. Une fois que vous êtes connecté à une application ou à un poste de travail distant, un raccourci pour l'application ou le poste de travail distant récemment utilisé s'affiche dans le widget. Vous pouvez appuyer sur ce raccourci pour ouvrir l'application ou le poste de travail distant à partir de votre écran Rechercher.

Si vous avez un périphérique activé pour 3D Touch, le widget Horizon Client peut s'afficher dans le menu d'action rapide lorsque vous appuyez sur l'application **Horizon** sur votre écran Accueil.

Utilisation d'une application ou d'un poste de travail Microsoft Windows

4

Sur les périphériques iOS, Horizon Client inclut des fonctions supplémentaires pour faciliter la navigation.

Ce chapitre aborde les rubriques suivantes :

Matrice de prise en charge des fonctionnalités pour iOS

Certaines fonctionnalités sont prises en charge sur un type d'Horizon Client, mais pas sur un autre.

Tableau 4-1. Fonctionnalités prises en charge sur les postes de travail Windows pour Horizon Client pour iOS

Fonction	Poste de travail Windows 10	Poste de travail Windows 8.x	Poste de travail Windows 7	Poste de travail Windows Vista	Poste de travail Windows XP	Poste de travail Windows Server 2008/2012 R2 ou Windows Server 2016
RSA SecurID ou RADIUS	X	X	X	Limité	Limité	X
Authentification unique	X	X	X	Limité	Limité	X
Protocole d'affichage RDP						
Protocole d'affichage PCoIP	X	X	X	Limité	Limité	X
Protocole d'affichage VMware Blast	X	X	X			X
Accès USB						
Audio/Vidéo en temps réel (entrée audio uniquement)	X	X	X			X
Wyse MMR						
Redirection multimédia (MMR) Windows 7						
Impression virtuelle						
Impression basée sur l'emplacement	X	X	X	Limité	Limité	X
Cartes à puce	X	X	X	Limité	Limité	X
Plusieurs écrans						

Les postes de travail Windows 10 requièrent View Agent 6.2 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure. Les postes de travail Windows Server 2012 R2 requièrent View Agent 6.1 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure. Les postes de travail Windows Server 2016 requièrent Horizon Agent 7.0.2 ou version ultérieure.

Important View Agent 6.1 et versions ultérieures et Horizon Agent 7.0 et versions ultérieures ne prennent pas en charge les postes de travail Windows XP et Windows Vista. View Agent 6.0.2 est la dernière version de View qui prend en charge ces systèmes d'exploitation. Les clients qui disposent d'un contrat de support étendu avec Microsoft pour Windows XP et Vista, ainsi qu'un contrat de support étendu avec VMware pour ces systèmes d'exploitation invités, peuvent déployer l'instance de View Agent 6.0.2 de leurs postes de travail Windows XP et Vista avec le Serveur de connexion 6.1.

Pour une description de ces fonctionnalités, consultez le document *Planification de View*.

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

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

Remarque Le tableau suivant contient des lignes uniquement pour les fonctionnalités prises en charge. Lorsque le texte spécifie une version minimale de View Agent, le texte « et versions ultérieures » s'entend « inclure Horizon Agent 7.0.x et versions ultérieures ».

Tableau 4-2. Fonctionnalités prises en charge par les hôtes RDS avec View Agent 6.0.x ou version ultérieure, ou Horizon Agent 7.0.x ou version ultérieure, installé

Fonction	Hôte RDS Windows Server 2008 R2	Hôte RDS Windows Server 2012	Hôte RDS Windows Server 2016
RSA SecurID ou RADIUS	X	X	Horizon Agent 7.0.2 et versions ultérieures
Carte à puce	View Agent 6.1 et versions ultérieures	View Agent 6.1 et versions ultérieures	Horizon Agent 7.0.2 et versions ultérieures
Authentification unique	X	X	Horizon Agent 7.0.2 et versions ultérieures
Protocole d'affichage RDP (pour les clients de poste de travail)	X	X	Horizon Agent 7.0.2 et versions ultérieures
Protocole d'affichage PCoIP	X	X	Horizon Agent 7.0.2 et versions ultérieures
Protocole d'affichage VMware Blast	Horizon Agent 7.0 et version ultérieure	Horizon Agent 7.0 et version ultérieure	Horizon Agent 7.0.2 et versions ultérieures
HTML Access	View Agent 6.0.2 et versions ultérieures (machine virtuelle uniquement)	View Agent 6.0.2 et versions ultérieures (machine virtuelle uniquement)	Horizon Agent 7.0.2 et versions ultérieures
Impression virtuelle (pour clients de poste de travail)	View Agent 6.0.1 et versions ultérieures (machine virtuelle uniquement)	View Agent 6.0.1 et versions ultérieures (machine virtuelle uniquement)	Horizon Agent 7.0.2 et versions ultérieures (machine virtuelle uniquement)
Impression basée sur l'emplacement	View Agent 6.0.1 et versions ultérieures (machine virtuelle uniquement)	View Agent 6.0.1 et versions ultérieures (machine virtuelle uniquement)	Horizon Agent 7.0.2 et versions ultérieures (machine virtuelle uniquement)
Plusieurs moniteurs (pour clients de poste de travail)	X	X	Horizon Agent 7.0.2 et versions ultérieures
Unity Touch (pour les clients Chrome OS et mobiles)	X	X	Horizon Agent 7.0.2 et versions ultérieures
Audio/Vidéo en temps réel (RTAV)	Horizon Agent 7.0.2 et versions ultérieures	Horizon Agent 7.0.2 et versions ultérieures	Horizon Agent 7.0.3 et versions ultérieures

Pour plus d'informations sur les éditions de chaque système d'exploitation invité et les service packs pris en charge, consultez le document *Installation de View*.

Limitations de certaines fonctionnalités

Certaines restrictions s'appliquent à des fonctionnalités spécifiques prises en charge sur des postes de travail Windows pour Horizon Client pour iOS.

Tableau 4-3. Configuration requise pour des fonctionnalités spécifiques

Fonction	Configuration requise
Mode gaucher	Cette fonctionnalité est spécifique à iOS. Si votre poste de travail distant est configuré pour que les boutons de souris principal et secondaire soient permutés, utilisez la fonctionnalité Mode Gaucher. Reportez-vous à la section « Configurer Horizon Client pour la prise en charge des boutons de souris inversés », page 51.
Impression basée sur l'emplacement pour les postes de travail Windows Server 2008 R2, les postes de travail RDS (sur hôtes RDS de machine virtuelle) et les applications distantes	Serveurs Horizon 6.0.1 avec View et versions ultérieures.
Cartes à puce pour postes de travail RDS	View Agent 6.1 et versions ultérieures.
Audio/Vidéo en temps réel (entrée audio uniquement)	Reportez-vous à la section « Configuration système requise pour l'Audio/Vidéo en temps réel », page 8.

Remarque Vous pouvez également utiliser Horizon Client pour accéder en toute sécurité aux applications Windows distantes, en plus des postes de travail distants. La sélection d'une application dans Horizon Client ouvre une fenêtre pour cette application sur le périphérique client local et l'application se présente et se comporte comme si elle était installée localement.

Vous ne pouvez utiliser des applications distantes que si vous êtes connecté à un Serveur de connexion 6.0 ou version ultérieure. Pour plus d'informations sur les systèmes d'exploitation pris en charge par l'hôte RDS qui fournit des applications et des postes de travail publiés, consultez le document *Installation de View*.

Fonctions prises en charge pour les postes de travail Linux

Certains systèmes d'exploitation invités Linux sont pris en charge si vous possédez View Agent 6.1.1 ou version ultérieure ou Horizon Agent 7.0 ou version ultérieure. Pour obtenir une liste des systèmes d'exploitation Linux pris en charge ainsi que des informations sur les fonctionnalités prises en charge, consultez le document *Configuration des postes de travail Horizon 6 for Linux* ou *Configuration des postes de travail Horizon 7 for Linux*.

Claviers externes et périphériques d'entrée

Horizon Client prend en charge les claviers externes suivants : le Dock avec clavier iPad et le clavier sans fil Apple (Bluetooth). Horizon Client prend en charge Apple Pencil comme dispositif de pointage sur iPad Pro et la souris Swiftpoint GT sur tous les périphériques iOS qu'elle prend en charge.

Utilisation d'un clavier externe

Horizon Client détecte automatiquement le clavier externe Dock avec clavier iPad. Pour utiliser le clavier sans fil Apple (Bluetooth) avec une application ou un poste de travail distant, vous devez tout d'abord associer le clavier au périphérique client. Après avoir appairé le clavier avec l'iPad, assurez-vous que le clavier à l'écran n'est pas en mode de clavier divisé lorsque vous demandez à l'iPad de détecter le clavier Bluetooth. Pour faire en sorte que le périphérique client détecte le clavier sans fil, appuyez sur l'écran avec trois doigts simultanément ou appuyez sur le bouton **Clavier** dans les Outils d'Horizon Client.

En revanche, lorsque vous utilisez le clavier sans fil Apple (Bluetooth), après la détection du clavier externe, vous ne pouvez ni utiliser les Outils d'Horizon Client ni appuyer avec trois doigts pour afficher le clavier à l'écran. Vous devez d'abord désactiver le clavier externe en appuyant sur sa touche Eject (Éjecter).

Remarque Le clavier sans fil Apple (Bluetooth) ne permet pas d'entrer correctement le caractère tilde japonais pleine chasse sur les postes de travail distants.

Utilisation de la souris Swiftpoint GT

Horizon Client détecte automatiquement la souris SwiftPoint GT. Pour utiliser la souris Swiftpoint GT avec une application ou un poste de travail distant, vous devez tout d'abord associer la souris au périphérique client. Une fois que vous avez associé la souris au périphérique, les actions de la souris sont redirigées vers les applications et les postes de travail distants que vous ouvrez avec Horizon Client.

Claviers internationaux

Vous pouvez saisir des caractères en anglais, japonais, français, allemand, chinois simplifié, chinois traditionnel, coréen et espagnol.

Utilisez un clavier anglais sur votre appareil iOS avec un poste de travail distant qui utilise le mode IME (éditeur de méthode d'entrée) coréen ou japonais. Si vous utilisez un clavier coréen ou japonais sur votre appareil iOS et que vous vous connectez à un poste de travail distant qui utilise un IME coréen ou japonais, le mode IME Windows anglais/coréen ou anglais/japonais n'est pas synchronisé avec les paramètres régionaux du clavier iOS.

Activer la disposition du clavier japonais 106/109

Si vous vous êtes connecté à un poste de travail Windows XP, vous pouvez configurer Horizon Client pour utiliser la disposition de clavier 106/109 japonaise.

Prérequis

Utilisez Horizon Client pour vous connecter à un poste de travail Windows XP sur lequel la disposition du clavier japonais est activée.

Procédure

1 Utilisez les Outils d'Horizon Client pour afficher la boîte de dialogue Options.

2 Appuyez pour activer l'option **Clavier japonais 106/109**.

Ce paramètre est désactivé si la disposition du clavier sur le poste de travail Windows XP n'est pas définie sur Japonais. Ce paramètre est masqué si le poste de travail n'exécute pas Windows XP.

3 Appuyez sur **Terminé**.

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

Avec la fonctionnalité Audio/Vidéo en temps réel, vous pouvez utiliser un microphone connecté à votre périphérique mobile sur votre poste de travail distant. L'Audio/Vidéo en temps réel est compatible avec des périphériques audio et des applications de conférence standard telles que Skype, WebEx et Google Hangouts.

L'Audio/Vidéo en temps réel est activé par défaut lorsque vous installez Horizon Client sur votre périphérique.

Remarque Seule la fonctionnalité d'entrée audio est prise en charge. La fonctionnalité de vidéo n'est pas prise en charge.

Pour plus d'informations sur la configuration de la fonctionnalité Audio/Vidéo en temps réel sur un poste de travail distant, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

La première fois que vous utilisez le microphone, Horizon Client vous invite à autoriser son accès. Vous devez accorder une autorisation pour que le microphone fonctionne avec votre poste de travail distant. Vous pouvez activer et désactiver l'accès au microphone en modifiant l'autorisation Microphone pour Horizon Client dans l'application Paramètres iOS.

Utilisation des mouvements du système d'exploitation natif avec redirection tactile

Vous pouvez utiliser les mouvements natifs du système d'exploitation de votre appareil mobile tactile lorsque vous êtes connecté à un poste de travail distant Windows 8, Windows 10 ou Windows Server 2012 ou à une application distante hébergée sur Windows Server 2012. Par exemple, vous pouvez toucher, maintenir enfoncé et relâcher un élément sur un poste de travail Windows 8 pour afficher le menu contextuel de l'élément.

Lorsque la redirection tactile est activée, vous pouvez utiliser les mouvements tactiles natifs du système d'exploitation uniquement. Les mouvements locaux de Horizon Client, tels que le double-clic et l'écartement/rapprochement des doigts, ne fonctionnent plus. Vous devez faire glisser le bouton de l'onglet Unity Touch pour afficher la barre latérale Unity Touch.

La redirection tactile est activée par défaut lorsque vous vous connectez à un poste de travail distant Windows 8, Windows 10 ou Windows Server 2012 ou à une application distante hébergée sur Windows Server 2012.

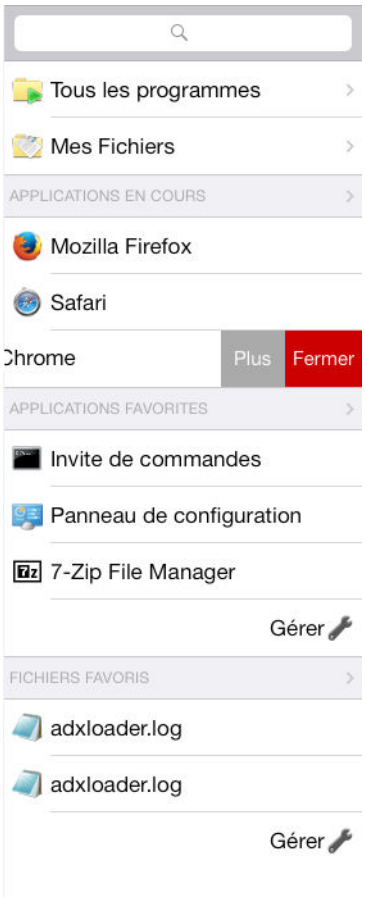
Pour désactiver la redirection tactile, appuyez sur **Paramètres** en bas de l'écran d'Horizon Client, appuyez sur **Tactile** puis désactivez le paramètre **Mouvements tactiles natifs de Windows**. Si vous êtes connecté à une application ou un poste de travail distant, vous pouvez accéder aux paramètres en appuyant sur l'icône **Paramètres** (engrenage) dans le menu circulaire Outils d'Horizon Client.

Utilisation de la barre latérale Unity Touch avec un poste de travail distant

Vous pouvez accéder rapidement à une application ou un fichier de poste de travail distant à partir de la barre latérale Unity Touch. À partir de cette barre latérale, vous pouvez ouvrir des fichiers et des applications, basculer entre des applications en cours d'exécution, et réduire, agrandir, restaurer ou fermer des fenêtres et des applications dans un poste de travail distant.

Si la fonctionnalité Unity Touch est activée, la barre latérale s'affiche sur le côté gauche de l'écran lorsque vous accédez pour la première fois à un poste de travail distant.

Figure 4-1. Barre latérale Unity Touch



Si vous accédez à un poste de travail sur lequel Unity Touch est activé mais que la barre latérale n'est pas affichée, vous pouvez voir un onglet sur le côté gauche de l'écran. En plus de faire glisser cet onglet vers la droite pour ouvrir la barre latérale, vous pouvez le faire glisser vers le haut ou vers le bas.

À partir de cette barre latérale, vous pouvez réaliser plusieurs actions sur un fichier ou une application.

Tableau 4-4. Actions de la barre latérale Unity Touch pour un poste de travail distant

Action	Procédure
Afficher la barre latérale	Faites glisser l'onglet vers la droite. Lorsque la barre latérale est ouverte, vous ne pouvez pas effectuer d'actions sur l'écran du poste de travail ou dans le menu circulaire Outils d'Horizon Client.
Masquer la barre latérale	Faites glisser l'onglet vers la gauche pour fermer la barre latérale. Lorsque la barre latérale est ouverte, vous ne pouvez pas effectuer d'actions sur l'écran du poste de travail ou dans le menu circulaire Outils d'Horizon Client. Vous pouvez également appuyer sur l'écran du poste de travail, notamment le menu circulaire Outils d'Horizon Client, pour masquer la barre latérale.
Accéder à une application	Appuyez sur **Tous les programmes** et accédez à l'application comme vous le feriez à partir du menu Démarrer de Windows.
Accéder à un fichier	Appuyez sur **Mes fichiers** pour accéder au dossier `Utilisateur` et accédez au fichier. **Mes fichiers** contient des dossiers tels que `Mes images`, `Mes documents` et `Téléchargements`. **Mes fichiers** contient les dossiers dans le profil d'utilisateur (répertoire `%USERPROFILE%`). Si vous déplacez le dossier `system` dans le répertoire `%USERPROFILE%`, le menu **Mes fichiers** peut également afficher le contenu du dossier déplacé, qu'il s'agisse d'un dossier déplacé local ou d'un dossier partagé sur un réseau.

Tableau 4-4. Actions de la barre latérale Unity Touch pour un poste de travail distant (suite)

Action	Procédure
Rechercher une application ou un fichier	■ Appuyez dans la zone **Rechercher** et saisissez le nom de l'application ou du fichier. ■ Pour utiliser la dictée vocale, appuyez sur le microphone sur le clavier. ■ Pour lancer une application ou un fichier, appuyez sur le nom de l'application ou du fichier dans les résultats de la recherche. ■ Pour revenir à l'accueil de la barre latérale, appuyez sur **X** pour fermer la zone **Rechercher**.
Ouvrir une application ou un fichier	Appuyez sur le nom du fichier ou de l'application dans la barre latérale. L'application démarre et la barre latérale se ferme.
Basculer entre des applications en cours d'exécution ou ouvrir des fenêtres	Appuyez sur le nom de l'application sous **Applications en cours d'exécution**. Si plusieurs fichiers sont ouverts pour une application, appuyez sur le chevron (>) à côté de l'application pour développer la liste.
Réduire une fenêtre ou une application en cours d'exécution	1 Appuyez sur le nom de l'application sous **Applications en cours d'exécution** et faites-le glisser de droite à gauche. 2 Appuyez sur le bouton **Plus** qui s'affiche. 3 Appuyez sur **Réduire**.
Agrandir une fenêtre ou une application en cours d'exécution	1 Appuyez sur le nom de l'application sous **Applications en cours d'exécution** et faites-le glisser de droite à gauche. 2 Appuyez sur le bouton **Plus** qui s'affiche. 3 Appuyez sur **Agrandir**.
Fermer une application en cours d'exécution ou une fenêtre	Appuyez sur le nom de l'application sous **Applications en cours d'exécution** et faites-le glisser de droite à gauche. Appuyez sur le bouton **Fermer** qui apparaît.
Rétablir une fenêtre ou une application en cours d'exécution à sa taille et sa position précédentes	1 Appuyez sur le nom de l'application sous **Applications en cours d'exécution** et faites-le glisser de droite à gauche. 2 Appuyez sur le bouton **Plus** qui s'affiche. 3 Appuyez sur **Restaurer**.
Créer une liste d'applications ou de fichiers favoris	1 Recherchez l'application ou le fichier, ou appuyez sur **Gérer** sous la liste **Applications favorites** ou **Documents favoris**. Si la barre **Gérer** n'est pas visible, appuyez sur le chevron (>) en regard d'**Applications favorites** ou de **Fichiers favoris**. 2 Appuyez sur la case à cocher en regard des noms de vos favoris dans les résultats de recherche ou dans la liste des applications ou des fichiers disponibles. Le favori que vous ajoutez en dernier s'affiche en haut de la liste des favoris. Vos favoris sont mémorisés sur tous vos appareils mobiles. Ainsi, vous disposez de la même liste, que vous utilisiez votre smartphone ou votre tablette.
Supprimer une application ou un fichier de la liste des favoris	1 Recherchez l'application ou le fichier, ou appuyez sur **Gérer** sous la liste **Applications favorites** ou **Documents favoris**. Si la barre **Gérer** n'est pas visible, appuyez sur le chevron (>) en regard d'**Applications favorites** ou de **Documents favoris**. 2 Appuyez pour supprimer la coche en regard du nom de l'application ou du fichier dans la liste des favoris.
Réorganiser une application ou un fichier dans la liste des favoris	1 Appuyez sur **Gérer** sous la liste **Applications favorites** ou **Documents favoris**. Si la barre **Gérer** n'est pas visible, appuyez sur le chevron (>) en regard d'**Applications favorites** ou de **Documents favoris**. 2 Dans la liste des favoris, appuyez longuement sur la poignée à gauche du nom de l'application ou du fichier, et faites glisser le favori vers le haut ou vers le bas dans la liste.

Remarque Pour utiliser la fonctionnalité Unity Touch avec des postes de travail View 5.3.x, Remote Experience Agent doit être installé sur les postes de travail. Si Remote Experience Agent est installé, mais que vous souhaitez désactiver cette fonctionnalité, vous pouvez définir une valeur de registre sur le poste de travail distant.

Si des utilisateurs ont un poste de travail flottant, leurs applications et fichiers favoris ne peuvent être enregistrés que si des profils d'utilisateur itinérants Windows sont configurés pour le poste de travail. Les administrateurs peuvent créer une liste **Applications favorites** par défaut que les utilisateurs voient la première fois que la barre latérale apparaît.

Utilisation de la barre latérale Unity Touch avec une application distante

Vous pouvez accéder rapidement à une application distante à partir de la barre latérale Unity Touch. À partir de cette barre latérale, vous pouvez lancer des applications, basculer entre des applications en cours d'exécution, et réduire, agrandir, restaurer ou fermer des applications distantes. Vous pouvez également basculer vers un poste de travail distant.

Lorsque vous accédez à une application distante, la barre latérale d'Unity Touch s'affiche sur le côté gauche de l'écran. Si la barre latérale d'Unity Touch est fermée, un onglet s'affiche sur le côté gauche de l'écran. Vous pouvez balayer cet onglet vers la droite pour réouvrir la barre latérale. Vous pouvez également faire glisser l'onglet vers le haut ou vers le bas.

Remarque Vous ne pouvez utiliser des applications distantes que si vous êtes connecté à un Serveur de connexion 6.0 ou version ultérieure.

Figure 4-2. Barre latérale Unity Touch pour une application distante

À partir de la barre latérale Unity Touch, vous pouvez effectuer de nombreuses actions sur une application distante.

Tableau 4-5. Actions de la barre latérale Unity Touch pour une application distante

Action	Procédure
Afficher la barre latérale	Faites glisser l'onglet vers la droite pour ouvrir la barre latérale. Lorsque la barre latérale est ouverte, vous ne pouvez pas effectuer d'actions sur l'écran de l'application.
Masquer la barre latérale	Faites glisser l'onglet vers la gauche pour fermer la barre latérale. Lorsque la barre latérale est ouverte, vous ne pouvez pas effectuer d'actions sur l'écran de l'application. Dans Horizon Client 3.1 et versions ultérieures, vous pouvez également appuyer sur l'écran de l'application, notamment le menu circulaire Outils d'Horizon Client, pour masquer la barre latérale.
Basculer entre des applications en cours d'exécution	Appuyez sur l'application sous **Connexion actuelle**.
Ouvrir une application	Appuyez sur le nom de l'application sous **Applications disponibles** dans la barre latérale. L'application démarre et la barre latérale se ferme.
Fermer une application en cours d'exécution	1 Appuyez sur le nom de l'application sous **Connexion actuelle** et faites-le glisser de droite à gauche. 2 Appuyez sur le bouton **Fermer** qui apparaît.
Réduire une application en cours d'exécution	1 Appuyez sur le nom de l'application sous **Connexion actuelle** et faites-le glisser de droite à gauche. 2 Appuyez sur le bouton **Plus** qui s'affiche. 3 Appuyez sur **Réduire**.
Agrandir une application en cours d'exécution	1 Appuyez sur le nom de l'application sous **Connexion actuelle** et faites-le glisser de droite à gauche. 2 Appuyez sur le bouton **Plus** qui s'affiche. 3 Appuyez sur **Agrandir**.
Restaurer une application en cours d'exécution	1 Appuyez sur le nom de l'application sous **Connexion actuelle** et faites-le glisser de droite à gauche. 2 Appuyez sur le bouton **Plus** qui s'affiche. 3 Appuyez sur **Restaurer**.
Basculer vers un poste de travail distant	Appuyez sur le nom du poste de travail sous **Postes de travail**.

Outils d' Horizon Client sur un périphérique mobile

Sur un périphérique mobile, les Outils d'Horizon Client incluent des boutons pour afficher un clavier à l'écran, le pavé tactile virtuel, des paramètres de configuration et le pavé numérique virtuel pour les touches de navigation et les touches de fonction.

L'icône du menu circulaire d'Horizon Client s'affiche au milieu de l'écran lorsque vous êtes connecté à une application ou à un poste de travail distant. Appuyez sur le menu circulaire pour l'agrandir et afficher les icônes de chaque outil, que vous sélectionnez en appuyant dessus. Appuyez à l'extérieur des icônes d'outil pour réduire les icônes dans l'icône du menu circulaire.

Le menu circulaire comporte plusieurs outils.

Tableau 4-6. Icônes du menu circulaire

Icône	Description
	Menu circulaire Outils d'Horizon Client
	Déconnecter

Tableau 4-6. Icônes du menu circulaire (suite)

Icône	Description
	Clavier à l'écran (bascule pour afficher ou masquer)
	Paramètres
	Touches de navigation
	Pavé tactile virtuel
	Aide relative aux mouvements

Clavier à l'écran

Le clavier à l'écran contient plus de touches que le clavier à l'écran standard, par exemple, les touches de contrôle et les touches de fonction sont disponibles. Pour afficher le clavier à l'écran, appuyez sur l'écran avec trois doigts simultanément ou appuyez sur l'icône **Clavier**.

Vous pouvez également utiliser la fonctionnalité qui affiche le clavier à l'écran à chaque fois que vous appuyez sur un champ de texte, tel qu'une note ou un nouveau contact. Si vous appuyez ensuite sur une zone qui n'est pas un champ de texte, le clavier disparaît.

Important Pour pouvoir appuyer avec trois doigts, assurez-vous que la fonction d'accessibilité d'iOS pour le zoom est désactivée. Lorsque la fonction d'accessibilité du zoom est activée, vous zoomez en tapant deux fois avec trois doigts. Taper une fois avec trois doigts n'a aucun effet.

Même si vous utilisez un clavier externe, un clavier à l'écran d'une ligne peut toujours apparaître et contient des touches de fonction, ainsi que les touches Ctrl, Alt, Win et fléchées. Certains claviers externes n'ont pas toutes ces touches.

Envoi d'une chaîne de caractères

Sur le clavier à l'écran, appuyez sur l'icône stylo à gauche de la touche Ctrl pour afficher la mémoire tampon d'entrée locale. Le texte que vous saisissez dans cette zone de texte n'est pas envoyé à une application tant que vous n'appuyez pas sur **Envoyer.** Par exemple, si vous ouvrez une application comme le Bloc-notes et que vous appuyez sur l'icône stylo, le texte que vous saisissez n'apparaît pas dans l'application Bloc-notes tant que vous n'appuyez pas sur **Envoyer**.

Utilisez cette fonction si votre connexion réseau est mauvaise. Autrement dit, utilisez cette fonction si, lorsque vous saisissez un caractère, celui-ci n'apparaît pas immédiatement dans l'application. Avec cette fonction, vous pouvez saisir rapidement jusqu'à 1 000 caractères puis appuyer sur **Envoyer** ou sur **Retour** pour que les 1 000 caractères apparaissent en même temps dans l'application.

Touches de navigation

Appuyez sur l'icône **Ctrl/Page** dans les Outils d'Horizon Client ou sur le clavier à l'écran pour afficher les touches de navigation. Ces touches incluent les touches Page précédente, Page suivante, les touches fléchées, les touches de fonction et d'autres touches que vous utilisez souvent dans des environnements Windows, telles que Alt, Suppr, Maj, Ctrl, Win et Échap. Vous pouvez appuyer et maintenir enfoncées des touches fléchées pour effectuer des frappes continues. Le tableau en début de cette rubrique illustre l'image de l'icône Ctrl/Page.

Utilisez la touche Maj sur ce clavier lorsque vous devez utiliser des combinaisons de touches comprenant la touche Maj, telles que Ctrl+Maj. Pour effectuer une combinaison de ces touches, comme Ctrl+Alt+Maj, appuyez d'abord sur la touche Ctrl à l'écran. Une fois que la touche Ctrl est bleue, appuyez sur la touche Alt à l'écran. Une fois que la touche Alt est bleue, appuyez sur la touche Maj à l'écran. Une seule touche à l'écran est fournie pour la combinaison de touches Ctrl+Alt+Suppr.

Pavé tactile à l'écran et Pavé tactile en plein écran

Le pavé tactile virtuel peut être de taille normale, pour avoir l'apparence d'un pavé tactile d'ordinateur portable, ou en mode plein écran, pour que tout l'écran soit un pavé tactile.

Par défaut, lorsque vous appuyez sur l'icône du pavé tactile, vous pouvez appuyer n'importe où sur l'écran pour déplacer le pointeur de la souris. L'écran se transforme en pavé tactile en plein écran.

- Lorsque vous déplacez le doigt autour du pavé tactile, cela crée un pointeur de souris qui se déplace dans l'application ou le poste de travail distant.
- Vous pouvez utiliser le pavé tactile virtuel de taille normale ou en plein écran pour un clic simple ou un double-clic.
- Le pavé tactile normal contient également des boutons pour clic gauche et clic droit.
- Pour simuler une pression continue sur le bouton pour clic gauche lors du déplacement, appuyez deux fois avec un doigt puis faites-le glisser.

  Pour activer cette fonctionnalité, utilisez les Outils d'Horizon Client pour afficher la boîte de dialogue Options et cliquez pour activer l'option **Toucher-Glisser du pavé tactile**.
- Vous pouvez appuyer avec deux doigts puis les faire glisser pour défiler verticalement.

Vous pouvez faire glisser le pavé tactile virtuel de taille normale vers le côté du périphérique afin d'utiliser le pavé tactile avec le pouce pendant que vous tenez le périphérique.

Vous pouvez donner au pavé tactile virtuel l'apparence du pavé tactile d'un ordinateur portable, qui comporte les boutons pour clic droit et pour clic gauche. Appuyez sur l'icône du menu circulaire Outils d'Horizon Client pour la développer, appuyez sur l'icône **Paramètres** (engrenage), appuyez sur **Tactile**, puis désactivez le paramètre **Mode Pavé tactile en plein écran**.

Pour régler la vitesse de déplacement du pointeur lorsque vous utilisez le pavé tactile, appuyez sur l'icône du menu circulaire Outils d'Horizon Client pour la développer, appuyez sur l'icône **Paramètres** (engrenage), appuyez sur **Tactile**, puis faites glisser le curseur dans l'option **Sensibilité du pavé tactile**.

Vous pouvez également définir les paramètres **Mode Pavé tactile en plein écran** et **Sensibilité du pavé tactile** dans l'écran Paramètres d'Horizon Client. Appuyez sur **Paramètres** en bas de l'écran d'Horizon Client et appuyez sur **Tactile** pour afficher les paramètres du pavé tactile.

Lorsque vous êtes connecté à un poste de travail distant et que vous modifiez les paramètres du pavé tactile, ceux-ci sont conservés jusqu'à votre prochaine connexion à l'application ou au poste de travail distant à partir du même périphérique iOS.

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 appuyez sur un élément de l'interface utilisateur pour exécuter un clic sur l'élément.

Dans un poste de travail distant, si vous appuyez pendant une seconde, une loupe apparaît, ainsi qu'un pointeur de souris, pour un placement précis. Cette fonction est particulièrement utile lorsque vous voulez redimensionner une fenêtre.

Remarque Si le poste de travail distant est configuré pour un gaucher, reportez-vous à « Configurer Horizon Client pour la prise en charge des boutons de souris inversés », page 51.

Clic droit

Les options suivantes sont disponibles pour le clic droit :

- Utilisez les Outils d'Horizon Client pour afficher le pavé tactile virtuel normal et utilisez le bouton pour clic droit du pavé tactile.
- Sur un écran tactile, appuyez avec deux doigts à peu près en même temps. Le clic droit se produit à l'endroit où le premier doigt a exercé une pression.

Défilement et barres de défilement

Les options suivantes sont disponibles pour le défilement vertical.

- Sur un écran tactile, appuyez avec un ou deux doigts, puis faites glisser pour faire défiler les informations. Le texte sous vos doigts se déplace dans la même direction que vos doigts.

  Important Le défilement avec un doigt présente les limites suivantes : il ne fonctionne pas si vous avez effectué un zoom avant, lorsque le clavier à l'écran est affiché ou lorsque vous utilisez le pavé tactile en plein écran.

- Utilisez les Outils d'Horizon Client pour afficher le pavé tactile, appuyez sur le pavé tactile avec deux doigts, puis faites glisser pour faire défiler les informations.
- Utilisez le pavé tactile à l'écran pour déplacer le pointeur de la souris et cliquer sur les barres de défilement.

Zoom avant et arrière

Comme dans les autres applications, vous pouvez rapprocher ou écarter vos doigts pour effectuer un zoom avant ou arrière sur un écran tactile.

Redimensionnement de fenêtre

Si vous utilisez le pavé tactile en plein écran pour redimensionner une fenêtre, appuyez avec un doigt dans le coin ou sur le côté de la fenêtre et faites-le glisser pour redimensionner, ou appuyez deux fois avec un doigt et faites-le glisser.

Si vous utilisez le pavé tactile virtuel de taille normale, pour simuler une pression continue sur le bouton pour clic gauche lors du déplacement du coin ou du côté d'une fenêtre, appuyez deux fois avec un doigt puis faites-le glisser.

Si vous n'utilisez pas le pavé tactile virtuel, appuyez jusqu'à ce que la loupe apparaisse dans le coin ou sur le côté de la fenêtre. Déplacez votre doigt autour jusqu'à ce que des flèches de redimensionnement apparaissent. Retirez votre doigt de l'écran. La loupe est remplacée par un cercle de redimensionnement. Appuyez sur ce cercle de redimensionnement et faites-le glisser pour redimensionner la fenêtre.

Son, musique et vidéo

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

Multitâche

Vous pouvez basculer entre Horizon Client et d'autres applications sans perdre la connexion avec l'application ou le poste de travail distant.

Sur un réseau WiFi, Horizon Client s'exécute par défaut en arrière-plan pendant trois minutes maximum sur les périphériques iOS 7.0 et versions ultérieures. Dans un réseau 3G, Horizon Client interrompt la transmission des données lorsque vous basculez vers une autre application. La transmission des données reprend lorsque vous revenez à Horizon Client.

Copier et coller du texte et des images

Par défaut, vous pouvez copier et coller du texte à partir de votre périphérique iOS vers une application ou un poste de travail distant. Si un administrateur Horizon active la fonctionnalité, vous pouvez également copier et coller le texte à partir d'une application ou d'un poste de travail distant vers votre périphérique iOS ou entre deux applications ou postes de travail distants. Les formats de fichier pris en charge incluent le texte brut, les images et le format RTF (Rich Text Format). Certaines restrictions s'appliquent.

Un administrateur Horizon peut définir cette fonctionnalité pour que les opérations Copier et Coller soient autorisées uniquement depuis votre périphérique iOS vers une application ou un poste de travail distant ou uniquement depuis une application ou un poste de travail distant vers votre périphérique iOS, ou les deux, ou aucun.

Les données que vous copiez vers le Presse-papiers sont copiées automatiquement vers le Presse-papiers du poste de travail distant lorsque vous ouvrez une session sur le poste de travail distant. Si vous êtes connecté à un poste de travail distant, les données que vous copiez vers son Presse-papiers sont automatiquement copiées sur le Presse-papiers de votre périphérique iOS. Si les données RTF (Rich Text Format) contiennent des images, ces dernières sont perdues lorsque Horizon Client synchronise les données RTF du Presse-papiers du poste de travail distant avec celles du Presse-papiers de votre périphérique iOS.

Les administrateurs Horizon configurent la capacité de copier et coller en configurant des paramètres de stratégie de groupe qui dépendent d'Horizon Agent. En fonction de la version d'Horizon Server et d'Horizon Agent, les administrateurs peuvent également être en mesure d'utiliser des stratégies de groupe afin de limiter les formats de Presse-papiers lors des opérations Copier et Coller ou d'utiliser des stratégies de carte à puce pour contrôler le comportement copier-coller sur des postes de travail distants. Pour plus d'informations, consultez le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Le Presse-papiers peut stocker 1 Mo de données au maximum pour des opérations de copier-coller. Si le texte et les données RTF prennent moins de la taille maximale du Presse-papiers, le texte formaté est collé. Il arrive souvent que les données RTF ne peuvent être tronquées. Ainsi, si le texte et le formatage prennent plus de la taille maximale du Presse-papiers, les données RTF sont ignorées 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.

Enregistrement de documents dans une application distante

Vous pouvez créer et enregistrer des documents avec certaines applications distantes, telles que Microsoft Word ou WordPad. L'emplacement dans lequel vous enregistrez ces documents dépend de l'environnement réseau de votre société. Par exemple, vos documents peuvent être enregistrés sur un partage d'accueil de votre ordinateur local.

Les administrateurs peuvent utiliser un fichier de modèle ADMX pour définir une stratégie de groupe qui spécifie à quel endroit les documents sont enregistrés. Cette stratégie se nomme **Définir le répertoire de base de l'utilisateur des services Bureau à distance**. Pour plus d'informations, reportez-vous au document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Configurer Horizon Client pour la prise en charge des boutons de souris inversés

Vous pouvez utiliser l'option **Mode Gaucher** si les boutons de souris principal et secondaire sont permutés sur votre poste de travail distant.

Si vous définissez les propriétés de la souris sur votre poste de travail distant de manière que le bouton principal de la souris soit celui qui se trouve du côté droit, ainsi que le font de nombreux gauchers, vous devez activer l'option **Mode Gaucher** dans Horizon Client. Si vous n'activez pas cette option lorsque les boutons de la souris sont inversés, un appui unique sera considéré comme un clic avec le bouton secondaire de la souris. Par exemple, un appui unique peut afficher un menu contextuel plutôt que de sélectionner un élément ou d'insérer un curseur.

Procédure

- Si vous êtes déjà connecté au poste de travail distant, exécutez ces étapes.
  a. Appuyez sur l'icône du menu circulaire Outils d'Horizon Client pour la développer et appuyez sur l'icône **Paramètres** (engrenage) pour ouvrir l'écran Paramètres.
  b. Appuyez sur **Tactile** sur l'écran Paramètres.
  c. Appuyez sur **Mode gaucher** pour activer l'option.
  d. Appuyez sur **Terminé** pour fermer l'écran Paramètres.
- Si vous n'êtes pas connecté au poste de travail distant, exécutez ces étapes.
  a. Appuyez sur **Paramètres** en bas de l'écran Horizon Client.
  b. Appuyez sur **Tactile** sur l'écran Paramètres.
  c. Appuyez sur **Mode gaucher** pour activer l'option.

Un appui unique est désormais considéré comme un clic effectué avec le bouton principal de la souris.

Résolutions d'écran et utilisation d'écrans externes

Vous pouvez utiliser Horizon Client avec des écrans externes et vous pouvez modifier les résolutions d'écran.

Lorsque vous connectez votre périphérique à un écran ou un projecteur externe, Horizon Client prend en charge certaines résolutions d'écran maximales. Vous pouvez changer la résolution d'écran utilisée sur le périphérique pour permettre le défilement de l'écran avec une résolution d'écran plus élevée.

Augmentation de la résolution d'écran pour un poste de travail distant

Par défaut, la résolution d'écran est définie pour afficher l'ensemble du poste de travail Windows sur le périphérique et les icônes du poste de travail et les icônes de la barre des tâches ont une certaine taille. Si vous augmentez la résolution, le poste de travail s'affiche toujours sur le périphérique, mais sa taille et celle des icônes de la barre des tâches sont plus petites.

Écartez les doigts pour zoomer et agrandir le poste de travail en débordant des limites de l'écran du périphérique. Vous pouvez appuyer et faire glisser l'écran pour accéder aux bords du poste de travail.

Changement des paramètres de la résolution d'écran

Pour modifier la résolution depuis une application ou un poste de travail distant, appuyez sur l'icône du menu circulaire Outils d'Horizon Client pour la développer, appuyez sur l'icône **Paramètres** (engrenage), puis sur **Résolution**. Vous pouvez également changer la résolution depuis l'écran Paramètres d'Horizon Client. Appuyez sur **Paramètres** en bas de l'écran d'Horizon Client et appuyez sur **Résolution**.

Remarque Certaines options, notamment Mise à l'échelle aux 3/4 et Pas de mise à l'échelle, ne sont pas disponibles sur l'iPhone 6 lorsque le périphérique est en mode de zoom avant. Pour afficher ces options, vous devez quitter le mode Agrandi.

Utilisation de moniteurs et de projecteurs externes

Le paramètre **Résolution** permet d'augmenter la résolution des moniteurs et des projecteurs externes.

Pour afficher le clavier et un pavé tactile étendu à l'écran sur le périphérique tout en affichant le poste de travail distant sur le projecteur ou un moniteur connecté, activez le paramètre **Mode de présentation**. Le pavé tactile étendu et le clavier apparaissent lorsque vous connectez le périphérique au moniteur externe. Le périphérique détecte la résolution maximale fournie par l'écran externe.

Vous pouvez afficher en miroir le contenu de l'écran du périphérique sur un projecteur ou un moniteur connecté, y compris la barre latérale Unity Touch, en désactivant le paramètre **Mode de présentation**. Si vous êtes connecté à un poste de travail distant et si le paramètre **Mode de présentation** est activé, cliquez sur **Terminé** pour passer en mode Miroir.

Vous pouvez utiliser le paramètre **Maintenir l'écran actif pendant la présentation** pour éviter que l'écran ne s'éteigne après une certaine période d'inactivité en mode présentation.

Vous pouvez configurer ces paramètres depuis une application ou un poste de travail distant en appuyant sur l'icône du menu circulaire Outils d'Horizon Client pour la développer, puis en appuyant sur l'icône **Paramètres** (engrenage). Vous pouvez également configurer ces paramètres en appuyant sur l'icône **Paramètres** (engrenage) en bas de l'écran Horizon Client.

Masquer des informations sensibles sur des écrans externes

Lorsque vous utilisez Horizon Client avec un moniteur ou un projecteur externe, des informations sensibles, telles que les mots de passe et les codes secrets, sont masquées automatiquement pour protéger la sécurité des données utilisateur.

Cache d'images client PCoIP

Le cache d'images client PCoIP stocke le contenu des images sur le client pour éviter la retransmission. Cette fonction réduit la bande passante.

Le cache d'images PCoIP capture la redondance spatiale et temporelle. Par exemple, lorsque vous faites défiler un document PDF, le nouveau contenu apparaît depuis le bas de la fenêtre et le contenu le plus ancien disparaît du haut de la fenêtre. L'autre contenu reste constant et remonte. Le cache d'images PCoIP peut détecter cette redondance spatiale et temporelle.

Comme pendant le défilement, les informations d'écran envoyées au périphérique client sont constituées principalement d'une séquence d'index de cache, l'utilisation du cache d'images permet d'économiser un quantité significative de bande passante. Ce défilement efficace offre des avantages dans un réseau LAN et dans un réseau WAN.

- Dans un réseau LAN, où la bande passante est relativement illimitée, le cache d'image client permet d'économiser une quantité significative de bande passante.
- Dans un réseau WAN, pour rester dans les limites de bande passante disponible, le défilement est dégradé si la mise en cache client n'est pas utilisée. Dans un réseau WAN, la mise en cache client peut économiser la bande passante et permettre de faire défiler les données d'une manière fluide et avec grande réactivité.

Avec la mise en cache client, le client stocke des portions de l'affichage ayant déjà été transmises. La taille du cache est deux fois inférieure à la RAM disponible. Si la quantité de RAM est inférieure à 50 Mo, la taille du cache est de 50 Mo.

Supprimer le message d'avertissement concernant les données cellulaires

Lorsqu'Horizon Client détecte que vous utilisez une connexion de données cellulaires, la boîte de dialogue Utilisation du réseau s'affiche pour vous avertir que votre connexion d'applications ou de postes de travail distants peut utiliser une partie substantielle de votre plan de données.

La boîte de dialogue Utilisation du réseau s'affiche une fois que vous êtes connecté à un serveur et tentez de lancer une application ou un poste de travail distant, lorsque vous appuyez sur un raccourci d'application ou de poste de travail récent, et quand vous êtes connecté à une application distante et tentez de lancer une autre application ou un autre poste de travail distant à partir de la barre latérale d'Unity Touch. La boîte de dialogue Utilisation du réseau ne s'affiche que lorsque vous lancez Horizon Client.

Vous pouvez supprimer la boîte de dialogue Utilisation du réseau après son affichage. Vous pouvez également sélectionner une option afin de toujours supprimer cette boîte de dialogue.

Procédure

- Pour supprimer la boîte de dialogue Utilisation du réseau dès qu'elle s'affiche dans Horizon Client, appuyez sur **Ne jamais me le rappeler** dans la boîte de dialogue Utilisation du réseau.
- Pour définir une option afin de toujours supprimer la boîte de dialogue Utilisation du réseau, appuyez sur **Paramètres** en bas de l'écran d'Horizon Client et désactivez l'option **Avertissement concernant les données cellulaires**.

Internationalisation

L'interface utilisateur et la documentation sont disponibles en anglais, allemand, français, japonais, chinois simplifié, chinois traditionnel, coréen et espagnol. Vous pouvez également entrer des caractères dans ces langues.

Résolution des problèmes d' Horizon Client 5

Vous pouvez résoudre la plupart des problèmes d'Horizon Client en réinitialisant le poste de travail ou en réinstallant l'application.

Vous pouvez également activer la collecte des journaux et envoyer les fichiers journaux à VMware pour dépannage.

Ce chapitre aborde les rubriques suivantes :

Collecte et envoi d'informations de journalisation

Vous pouvez configurer Horizon Client pour collecter les informations de journalisation et envoyer les fichiers journaux à VMware à des fins de dépannage.

Si Horizon Client s'arrête de manière inattendue alors que la collecte des journaux est activée, Horizon Client vous invite à envoyer les journaux à VMware lorsque vous relancez Horizon Client.

Si vous décidez d'envoyer les fichiers journaux à VMware, Horizon Client envoie un message à partir du compte de messagerie configuré sur votre périphérique et joint un fichier GZ qui contient les cinq derniers fichiers journaux. Le nom du fichier contient un horodatage, par exemple `Horizon_View_Client_logs_`*`horodatage`*`.log.gz`.

Vous pouvez également récupérer manuellement les fichiers journaux et les envoyer au moment de votre choix.

Activer la collecte de journaux Horizon Client

Lorsque vous activez la collecte de journaux, Horizon Client crée des fichiers journaux contenant des informations qui peuvent aider VMware à résoudre les problèmes d'Horizon Client.

Dans la mesure où la collecte des journaux affecte les performances d'Horizon Client, activez-la uniquement si vous rencontrez un problème.

Prérequis

Vérifiez qu'un compte de messagerie est configuré sur votre périphérique. Horizon Client utilise ce compte de messagerie pour envoyer les fichiers journaux.

Procédure

1 Si vous êtes déjà connecté à une application ou un poste de travail distant, exécutez ces étapes :

   a Appuyez sur l'icône du menu circulaire Outils d'Horizon Client pour la développer et appuyez sur l'icône **Paramètres** (engrenage) pour ouvrir l'écran Paramètres.

   b Appuyez sur **Collecte des journaux** sur l'écran Paramètres.

   c Appuyez pour basculer l'option **Journalisation** sur Activé.

   d Appuyez sur **Terminé** pour fermer l'écran Paramètres.

2 Si vous n'êtes pas connecté à une application ou un poste de travail distant, exécutez ces étapes :

   a Appuyez sur **Paramètres** en bas de l'écran Horizon Client pour ouvrir l'écran Paramètres.

   b Appuyez sur **Collecte des journaux** sur l'écran Paramètres.

   c Appuyez pour basculer l'option **Journalisation** sur Activé.

Une fois la collecte de journaux activée, Horizon Client génère plusieurs fichiers journaux. Lorsque Horizon Client s'arrête de manière inattendue ou lorsqu'il est arrêté et relancé, les fichiers journaux sont fusionnés et compressés dans un fichier GZ unique. Si vous choisissez d'envoyer le journal, Horizon Client joint le fichier GZ à un e-mail.

Si vous accédez aux paramètres sur un poste de travail en cours d'exécution, activez la collecte de journaux et rebasculez sur le poste de travail, vous devez vous reconnecter au poste de travail pour collecter un fichier journal complet.

Extraire et envoyer manuellement les fichiers journaux d' Horizon Client

Lorsque la collecte des journaux d'Horizon Client est activée sur votre périphérique, vous pouvez à tout moment extraire et envoyer manuellement les fichiers journaux.

Cette procédure explique comment extraire et envoyer des fichiers journaux via Horizon Client. Si votre périphérique est connecté à un PC ou à un Mac, vous pouvez également utiliser iTunes pour extraire les fichiers journaux.

Prérequis

- Vérifiez qu'un compte de messagerie est configuré sur votre périphérique. Horizon Client envoie les fichiers journaux à partir de ce compte de messagerie.
- Activez la collecte de journaux Horizon Client. Reportez-vous à la section « Activer la collecte de journaux Horizon Client », page 55.

Procédure

1 Dans Horizon Client, appuyez sur l'icône de messagerie en haut de l'écran.

2 Tapez l'adresse du destinataire de l'e-mail dans la ligne **À :** et cliquez sur **Envoyer** pour envoyer le message.

   Le compte de messagerie configuré sur votre périphérique s'affiche sur la ligne **De :**.

   Le fichier journal GZ existant est joint au message. Horizon Client enregistre un maximum de cinq fichiers journaux GZ. Il supprime les fichiers les plus anciens lorsque le nombre de fichiers journaux GZ est supérieur à cinq.

Désactiver la collecte de journaux Horizon Client

Dans la mesure où la collecte de journaux affecte les performances d'Horizon Client, désactivez-la si vous n'êtes pas en train de résoudre un problème.

Procédure

1 Si vous êtes déjà connecté à une application ou un poste de travail distant, exécutez ces étapes.

   a Appuyez sur l'icône du menu circulaire Outils d'Horizon Client pour la développer et appuyez sur l'icône **Paramètres** (engrenage) pour ouvrir l'écran Paramètres.

   b Appuyez sur **Collecte des journaux** sur l'écran Paramètres.

   c Appuyez pour basculer l'option **Journalisation** sur Désactivé.

   d Appuyez sur **Terminé** pour fermer l'écran Paramètres.

2 Si vous n'êtes pas connecté à une application ou un poste de travail distant, exécutez ces étapes.

   a Appuyez sur **Paramètres** en bas de l'écran Horizon Client pour ouvrir l'écran Paramètres.

   b Appuyez sur **Collecte des journaux** sur l'écran Paramètres.

   c Appuyez pour basculer l'option **Journalisation** sur Désactivé.

Redémarrer un poste de travail distant

Vous devrez peut-être redémarrer un poste de travail distant si le système d'exploitation du poste de travail cesse de répondre. Le redémarrage d'un poste de travail distant équivaut à la commande de redémarrage du système d'exploitation Windows. En général, le système d'exploitation de poste de travail vous invite à 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 de poste de travail pour le poste de travail.

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

Prérequis

- Procurez-vous les informations d'identification pour ouvrir une session, telles que le nom d'utilisateur et le mot de passe Active Directory, le nom d'utilisateur et le code secret RSA SecurID ou le nom d'utilisateur et le code secret pour l'authentification RADIUS.
- Si vous n'avez encore jamais ouvert de session, familiarisez-vous avec la procédure « Connexion à une application ou un poste de travail distant », page 27.

Procédure

1 Appuyez sur **Serveurs** (icône Cloud) en bas de l'écran, puis sur l'icône du serveur à connecter au serveur.

2 Si vous y êtes invité, entrez votre nom d'utilisateur et code secret RSA, votre nom d'utilisateur et mot de passe Active Directory, ou les deux.

3 Appuyez longuement sur le nom du poste de travail jusqu'à ce que le menu contextuel s'affiche.

4 Appuyez sur **Redémarrer** dans le menu contextuel.

   Redémarrer est disponible uniquement si l'état du poste de travail est tel que l'action peut être effectuée.

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

Suivant

Il convient d'observer un temps d'attente suffisant pour le démarrage du système avant de tenter de se reconnecter au poste de travail distant.

Si le redémarrage du poste de travail distant ne résout pas le problème, vous devrez peut-être réinitialiser le poste de travail distant. Reportez-vous à la section « Réinitialiser un poste de travail distant ou des applications distantes », page 58.

Réinitialiser un poste de travail distant ou des applications distantes

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 des applications distantes ferme toutes les applications ouvertes.

La réinitialisation d'un poste de travail distant équivaut à appuyer sur le bouton Réinitialiser d'un ordinateur physique pour le forcer à redémarrer. Tous les fichiers ouverts sur le poste de travail distant sont fermés sans être enregistrés.

La réinitialisation d'applications distantes équivaut à quitter les applications sans enregistrer les données non enregistrées. Toutes les applications distantes ouvertes sont fermées, même les applications qui proviennent de batteries de serveurs RDS différentes.

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

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

Prérequis

- Procurez-vous les informations d'identification pour ouvrir une session, telles que le nom d'utilisateur et le mot de passe Active Directory, le nom d'utilisateur et le code secret RSA SecurID ou le nom d'utilisateur et le code secret pour l'authentification RADIUS.
- Si vous n'avez encore jamais ouvert de session, familiarisez-vous avec la procédure « Connexion à une application ou un poste de travail distant », page 27.

Procédure

1. Appuyez sur **Serveurs** (icône Cloud) en bas de l'écran, puis sur l'icône du serveur à connecter au serveur.
2. Si vous y êtes invité, entrez votre nom d'utilisateur et code secret RSA, votre nom d'utilisateur et mot de passe Active Directory, ou les deux.
3. Appuyez longuement sur le nom du poste de travail ou de l'application jusqu'à ce que le menu contextuel s'affiche.
4. Appuyez sur **Réinitialiser** dans le menu contextuel.

   Réinitialiser est disponible uniquement si l'état du poste de travail ou de l'application est tel que l'action peut être effectuée.

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

Suivant

Il convient d'observer un temps d'attente suffisant pour le démarrage du système avant de tenter de se reconnecter à l'application ou au poste de travail distant.

Désinstaller Horizon Client

Il est parfois possible de résoudre certains problèmes avec Horizon Client en désinstallant et en réinstallant Horizon Client.

Procédure

1 Si vous disposez de l'application Horizon Client dans iTunes sur votre Mac ou votre PC, recherchez l'application Horizon Client dans la Bibliothèque d'applications et supprimez-la.

   Suivez la même procédure que pour désinstaller n'importe quelle application iTunes.

2 Connectez votre périphérique à votre ordinateur et autorisez le périphérique à se synchroniser avec iTunes sur votre Mac ou votre PC.

3 Si l'application Horizon Client n'a pas été désinstallée de votre périphérique, appuyez longuement sur l'icône de l'application **Horizon** jusqu'à ce qu'elle bouge, puis appuyez sur l'icône **X** pour la supprimer.

Suivant

Réinstallez Horizon Client.

Reportez-vous à la section « Installer ou mettre à niveau Horizon Client sur un périphérique iOS », page 14.

Horizon Client cesse de répondre ou le poste de travail distant se fige

Lorsque l'écran se fige, essayez d'abord de réinitialiser le système d'exploitation du poste de travail distant.

Problème

Horizon Client ne fonctionne pas ou se ferme de façon répétée et inattendue, ou le poste de travail distant se bloque.

Cause

En partant du principe que les serveurs Horizon sont correctement configurés et que les ports corrects sont ouverts sur les pare-feu autour d'eux, les autres problèmes sont généralement liés à Horizon Client sur le périphérique ou au système d'exploitation invité sur le poste de travail distant.

Solution

- Si le système d'exploitation du poste de travail distant se fige, utilisez Horizon Client sur le périphérique pour réinitialiser le poste de travail.

  Cette option n'est disponible que si l'administrateur Horizon a activé cette fonctionnalité.
- Désinstallez et réinstallez l'application sur le périphérique.
- Si la réinitialisation du poste de travail distant et la réinstallation d'Horizon Client ne résolvent pas le problème, vous pouvez réinitialiser le périphérique iOS, comme indiqué dans le guide de l'utilisateur du périphérique Apple.
- Si vous obtenez une erreur de connexion lorsque vous tentez de vous connecter au serveur, vous devez peut-être modifier les paramètres proxy.

Problème lors de l'établissement d'une connexion en utilisant un proxy

Une erreur peut parfois se produire si vous essayez de vous connecter au Serveur de connexion à l'aide d'un proxy alors que vous êtes sur un réseau LAN.

Problème

Si l'environnement Horizon est configuré afin d'utiliser une connexion sécurisée à partir du poste de travail distant vers le Serveur de connexion, et si le périphérique client est configuré afin d'utiliser un proxy HTTP, vous risquez de ne pas pouvoir vous connecter.

Cause

Contrairement à Windows Internet Explorer, le périphérique client ne dispose pas d'une option Internet pour contourner le proxy pour les adresses locales. Lorsqu'un proxy HTTP est utilisé pour parcourir des adresses externes et que vous essayez de vous connecter au Serveur de connexion à l'aide d'une adresse interne, le message `Impossible d'établir une connexion` peut s'afficher.

Solution

- Supprimez les paramètres de proxy, afin que le périphérique n'utilise plus de proxy.

Index