Installation et administration de VMware Horizon View Feature Pack

Horizon View 5.3

Horizon View Feature Pack 6

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

FR-001301-01

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

Installation et administration de VMware Horizon View Feature Pack

Le *Guide d'installation et d'administration de VMware Horizon View Feature Pack* contient des informations sur l'installation et la configuration des composants de VMware® Horizon View™ Feature Pack.

Les informations contenues dans ce document incluent les configurations système requises et des instructions pour l'installation de Remote Experience Agent sur des postes de travail Horizon View et du programme d'installation de HTML Access sur des instances de serveur de connexion View. Les tâches de configuration post-installation y sont également décrites.

Public visé

Ce document s'adresse aux administrateurs chargés d'installer et de configurer Feature Pack dans le cadre d'un déploiement d'Horizon View. Les informations sont rédigées pour des administrateurs système expérimentés qui connaissent parfaitement la technologie des machines virtuelles et les opérations de datacenter. Si vous découvrez Horizon View, nous vous recommandons de suivre les instructions pas à pas pour réaliser les procédures de base dans les documents *Installation de VMware Horizon View* et *Administration de VMware Horizon View*.

Composants de VMware Horizon View Feature Pack

VMware Horizon View Feature Pack comprend deux programmes d'installation qui fournissent des composants Horizon View dans un environnement Horizon View. Le programme d'installation de Remote Experience Agent configure les composants sur des postes de travail Horizon View. Le programme d'installation de HTML Access configure le serveur de connexion View pour permettre l'accès aux postes de travail via HTML Access.

Programme d'installation de Remote Experience Agent

Remote Experience Agent installe les composants Feature Pack sur des postes de travail Horizon View, ce qui améliore l'expérience d'utilisation des postes de travail distants fournie par View Agent 5.3. Ce programme installe les composants suivants :

- Agent HTML Access
- Redirection d'URL Flash
- Audio/Vidéo en temps réel
- Unity Touch
- Redirection multimédia Windows 7 (MMR)

Les composants Feature Pack permettent aux utilisateurs de bénéficier de plusieurs nouvelles fonctionnalités sur le poste de travail.

Agent HTML Access

L'agent HTML Access permet aux utilisateurs de se connecter à des postes de travail Horizon View en utilisant HTML Access. L'agent HTML Access doit être en cours d'exécution sur un poste de travail pour activer HTML Access sur ce poste de travail.

Ainsi, pour utiliser HTML Access, vous devez installer Remote Experience Agent avec HTML Access.

Redirection d'URL Flash

La redirection d'URL Flash intercepte et redirige le fichier Shockwave Flash (SWF) du poste de travail distant au point de terminaison client. Sans cette fonctionnalité, les données vidéo de multidiffusion ou de monodiffusion sont diffusées à partir d'Adobe Media Server vers les postes de travail virtuels fonctionnant sur des hôtes ESXi. Les données sont ensuite renvoyées à des sessions PCoIP différentes à partir de chaque poste de travail virtuel vers chaque point de terminaison client.

La redirection d'URL Flash permet à des contenus Flash d'Adobe Media Server d''être diffusés directement vers des points de terminaison clients tout en contournant l'infrastructure de poste de travail virtuel. Les contenus Flash peuvent être affichés à l'aide des lecteurs multimédias flash locaux des clients.

La diffusion de contenus Flash directement à partir d'Adobe Media Server vers les points de terminaison client soulage l'hôte ESXi du datacenter, supprime les routages supplémentaires via le datacenter et réduit la bande passante nécessaire pour écouter simultanément un contenu Flash sur plusieurs points de terminaison client.

Audio/Vidéo en temps réel

L'Audio/Vidéo en temps réel permet aux utilisateurs Horizon View d'exécuter Skype, Webex, Google Hangouts et d'autres applications de conférence en ligne sur leurs postes de travail virtuels. Avec l'Audio/Vidéo en temps réel, les webcams et les périphériques audio qui sont connectés localement au système client sont redirigés vers le poste de travail distant. Cette fonctionnalité redirige les données vidéo et audio vers le poste de travail avec une bande passante beaucoup plus faible que celle utilisée par la redirection USB.

L'Audio/Vidéo en temps réel est compatible avec les applications de conférence standard et prend en charge les webcams, les périphériques audio USB standard et l'entrée audio analogique.

Cette fonctionnalité installe une webcam virtuelle et un microphone virtuel VMware sur le système d'exploitation du poste de travail. Lorsqu'une application de conférence est lancée, elle affiche et utilise ces périphériques virtuels VMware, qui gèrent la redirection audio-vidéo à partir des périphériques connectés localement vers le client. Le microphone virtuel VMware apparaît également dans le Gestionnaire de périphériques sur le système d'exploitation du poste de travail.

Les pilotes des webcams et périphériques audio doivent être installés sur vos systèmes Horizon View Client afin de permettre la redirection.

L’Audio/Vidéo en temps réel n'est pas pris en charge par les postes de travail en mode local.

	Cette fonctionnalité fournit un fichier de modèle d'administration ADM qui vous permet d'installer les paramètres de stratégie de groupe en matière d'audio-vidéo en temps réel sur Active Directory ou sur les postes de travail individuels. Avec ces paramètres, vous pouvez modifier la fréquence et la résolution d'images maximales d'une webcam et vous pouvez également activer/désactiver la fonctionnalité.
Unity Touch	Avec Unity Touch, les utilisateurs de tablettes et de smartphones peuvent facilement parcourir, rechercher et ouvrir des applications et des fichiers Windows, choisir des applications et des fichiers préférés et passer d'une application en cours d'exécution à une autre, le tout sans utiliser le menu Démarrer ou la barre des tâches. Les documents de VMware Horizon View Client pour les périphériques iOS et Android offrent plus d'informations sur les fonctions destinées aux utilisateurs d'Unity Touch.
Redirection multimédia Windows 7 (MMR)	Cette fonctionnalité étend la redirection multimédia (MMR) aux postes de travail et clients Windows 7. MMR délivre le flux multimédia directement aux ordinateurs client. Avec MMR, le flux multimédia est traité, c'est-à-dire décodé, sur le système client. Le système client effectue la lecture du contenu multimédia, déchargeant ainsi la demande sur l'hôte ESXi.

Programme d'installation de HTML Access

Le programme d'installation configure les instances du Serveur de connexion View pour permettre aux utilisateurs de sélectionner HTML Access pour se connecter à des postes de travail. Après avoir exécuté le programme d'installation de HTML Access, View Portal affiche une icône HTML Access en plus de l'icône View Client.

Vous devez exécuter ce programme d'installation si vous voulez utiliser HTML Access pour vous connecter à des postes de travail dans un déploiement d'Horizon View. L'exécution de ce programme d'installation est également requise si vos utilisateurs passent par Horizon Workspace et sélectionnent HTML Access pour se connecter à des postes de travail.

Configuration et installation

Pour configurer le Horizon View Feature Pack, vous installez Remote Experience Agent sur des postes de travail Horizon View et le programme d'installation de HTML Access sur des instances de Serveur de connexion View.

Configuration système requise pour Horizon View Feature Pack

Les postes de travail Horizon View et les instances du serveur de connexion View doivent satisfaire certaines exigences logicielles pour pouvoir prendre en charge des composants Feature Pack.

Serveur de connexion View

Serveur de connexion View 5.3

Des instructions d'installation sont fournies dans le document *Installation de VMware Horizon View* .

Poste de travail Horizon View

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

- Systèmes d'exploitation : Windows XP SP3 (32 bits), Windows Vista (32 bits), Windows 7 (32 ou 64 bits), Windows 8 (32 ou 64 bits), Windows 8.1 (32 ou 64 bits) ou Windows Server 2008 R2

  Remarque Certains composants Feature Pack ne sont pris en charge que sur certains des systèmes d'exploitation de poste de travail pris en charge. Reportez-vous à la section Tableau 1.

- View Agent 5.3

  Des instructions d'installation sont fournies dans le document *Administration de VMware Horizon View*.

Tableau 1 présente les systèmes d'exploitation de poste de travail sur lesquels chaque composant Feature Pack est pris en charge.

Tableau 1. Prise en charge du système d'exploitation de poste de travail Horizon View en fonction des composants Feature Pack

Composant Feature Pack	Windows XP SP3 (32 bits)	Windows Vista (32 bits)	Windows 7 (32 ou 64 bits)	Windows 8 ou Windows 8.1 (32 ou 64 bits)	Windows Server 2008 R2
Agent HTML Access	Oui	Oui	Oui	Oui (Tech Preview)	Oui
Redirection d'URL Flash	Non	Non	Oui	Non	Non
Audio/Vidéo en temps réel	Oui	Oui	Oui	Oui	Oui
Unity Touch	Oui	Oui	Oui	Oui	Oui
Redirection multimédia (MMR) Windows 7	Non	Non	Oui	Non	Non

Les composants Feature Pack pris en charge sont installés par défaut lorsque vous exécutez le programme d'installation de Remote Experience Agent. Vous pouvez choisir de ne pas installer un composant en le désélectionnant durant l'installation.

Pour prendre en charge les composants Feature Pack, le déploiement de votre Horizon View doit satisfaire certaines exigences matérielles et logicielles.

Configuration système requise pour HTML Access

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

Navigateurs sur un système client

Les navigateurs Web suivants sont pris en charge :

- Chrome 28 ou supérieur
- Internet Explorer 9 ou supérieur
- Safari 6 ou supérieur
- Mobile Safari sur les périphériques iOS exécutant iOS 6 ou supérieur
- Firefox 21 ou supérieur

Système d'exploitation client

- Windows XP SP3 (32 bits)
- Windows 7 SP1 ou sans SP (32 ou 64 bits)
- Poste de travail Windows 8 (32 ou 64 bits)
- Windows Vista SP1 ou SP2 (32 bits)
- Mac OS X Snow Leopard (10.6.8)
- Mac OS X Lion (10.7)
- Mac OS X Mountain Lion (10.8)
- iPad avec iOS 6.0 ou version ultérieure (par conséquent, iPad 1 n'est pas pris en charge)
- Chrome OS 28.*x* ou version ultérieure

poste de travail View

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

- Systèmes d'exploitation : Windows XP SP3 (32 bits), Windows Vista (32 bits), Windows 7 (32 ou 64 bits) ou Windows Server 2008 R2.

  En outre, HTML Access est disponible sur Windows 8 (32 ou 64 bits) ou Windows 8.1 (32 ou 64 bits) en mode Tech Preview. Vous pouvez essayer HTML Access sur un poste de travail Windows 8 ou Windows 8.1, mais aucune assistance n'est fournie.

- View Agent 5.3

  Des instructions d'installation sont fournies dans le document *Administration de VMware Horizon View*.

Paramètres de pool

HTML Access nécessite les paramètres de pool suivants dans View Administrator :

- Le paramètre **Résolution max. d'un écran** doit avoir une valeur supérieure ou égale à **1 920 x 1 200** afin que le poste de travail View dispose d'au moins 17,58 Mo de RAM vidéo.

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

Des instructions de configuration sont fournies dans la rubrique « Préparer des postes de travail et des pools View pour HTML Access » dans le document *Utilisation de VMware Horizon View HTML Access*.

Serveur de connexion View

Les logiciels suivants doivent être installés sur le serveur qui héberge le Serveur de connexion View :

- Serveur de connexion View 5.3

  Des instructions d'installation sont fournies dans le document *Installation de VMware Horizon View* .

- HTML Access

  Des instructions d'installation sont fournies dans « Installer le logiciel HTML Access sur Serveur de connexion View », page 23.

Lors de l'installation de HTML Access, le pare-feu est automatiquement configuré pour autoriser le trafic entrant sur le port TCP 8443

Serveur de sécurité

Le service Pare-feu Windows ou un autre logiciel de pare-feu doit être configuré pour autoriser le trafic entrant sur le port TCP 8443

Si les systèmes clients se connectent en dehors du pare-feu d'entreprise, VMware recommande d'utiliser un serveur de sécurité. Avec un serveur de sécurité, les systèmes client ne requièrent pas de connexion VPN.

Remarque Un serveur de sécurité unique peut prendre en charge jusqu'à 350 connexions simultanées à des clients Web.

Pare-feu tiers

Ajoutez des règles pour permettre le trafic suivant :

- Serveurs View (y compris des serveurs de sécurité, des instances de Serveur de connexion View et des serveurs de réplica) : trafic entrant sur le port TCP 8443.
- Postes de travail View : trafic entrant (provenant des serveurs View) sur le port TCP 22443.

Protocole d'affichage pour Horizon View

Blast

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

Remarque Vous pouvez utiliser HTML Access avec VMware Horizon Workspace pour permettre aux utilisateurs de se connecter à leur poste de travail à partir d'un navigateur HTML5. Pour plus d'informations sur l'installation d'Horizon Workspace et sa configuration pour l'utiliser avec Serveur de connexion View, consultez la documentation Horizon Workspace. Pour plus d'informations sur le couplage de Serveur de connexion View avec un serveur d'authentification SAML, consultez la documentation *Administration de VMware Horizon View*.

Configuration système requise pour la redirection d'URL flash

Pour prendre en charge la redirection d'URL Flash, le déploiement de votre Horizon View doit répondre à certaines exigences matérielles et logicielles.

Lecteur multimédia flash et ShockWave Flash (SWF)

Vous devez intégrer un lecteur multimédia Flash approprié tel que Strobe Media Playback dans votre site Web. Pour délivrer un contenu multidiffusion, vous pouvez utiliser `multicastplayer.swf` ou `StrobeMediaPlayback.swf` dans vos pages Web. Pour délivrer un contenu monodiffusion, vous devez utiliser `StrobeMediaPlayback.swf`. Vous pouvez également utiliser `StrobeMediaPlayback.swf` pour d'autres fonctionnalités prises en charge telles que la diffusion de flux RTMP et la diffusion dynamique HTTP.

Poste de travail Horizon View

- Les postes de travail doivent tourner sur des systèmes d'exploitation Windows 7, 64 ou 32 bits.
- Les postes de travail doivent avoir View Agent 5.3 installé.
- Internet Explorer 8, 9 et 10, Chrome 29.*x* et Firefox 20.*x* sont parmi les navigateurs de poste de travail pris en charge.

Logiciel Horizon View Client

Les versions suivantes d'Horizon View Client prennent en charge les flux de multidiffusion et de monodiffusion :

- Horizon View Client 2.2 pour Linux ou versions ultérieures
- Horizon View Client 2.2 pour Windows ou versions ultérieures

Les versions suivantes d'Horizon View Client ne prennent en charge que la multidiffusion :

- Horizon View Client 2.0 ou 2.1 pour Linux
- Horizon View Client 5.4 pour Windows

Ordinateur View Client ou périphérique d'accès client

- La redirection d'URL Flash est prise en charge par tous les systèmes d'exploitation qui exécutent Horizon View Client pour Linux sur les périphériques client légers x86. Cette fonctionnalité n'est pas prise en charge par les processeurs ARM.
- La redirection d'URL Flash est prise en charge par tous les systèmes d'exploitation qui exécutent Horizon View Client pour Windows. Pour plus de détails, reportez-vous au document *Utilisation de VMware Horizon View Client pour Windows*.
- Sur les périphériques client Windows, vous devez installer Adobe Flash Player 10.1 ou versions ultérieures pour Internet Explorer.

- Sur les périphériques clients légers Linux, vous devez installer les fichiers `libexpat.so.0` et `libflashplayer.so`. Reportez-vous à la section « Configurer des périphériques client pour la redirection d'URL Flash », page 35.

Remarque Avec la redirection d'URL Flash, le flux de multidiffusion ou de monodiffusion est redirigé vers les périphériques clients qui pourraient être en dehors du pare-feu de votre organisation. Vos clients doivent avoir accès au serveur Web d'Adobe hébergeant le fichier Shockwave Flash (SWF) qui initie les flux de multidiffusion ou de monodiffusion. Si nécessaire, configurez votre pare-feu pour ouvrir les ports appropriés afin de permettre aux périphériques client d'accéder à ce serveur.

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

L'Audio/Vidéo en temps réel fonctionne avec des webcams standard, des périphériques audio USB et analogiques ainsi qu'avec les applications de conférence standard telles que Skype, WebEx et Google Hangouts. Pour prendre en charge l'Audio/Vidéo en temps réel, le déploiement de votre Horizon View doit satisfaire certaines exigences matérielles et logicielles.

Poste de travail Horizon View

Les postes de travail doivent avoir View Agent 5.3 installé. L'Audio/Vidéo en temps réel est pris en charge par tous les systèmes d'exploitation client Windows qui utilisent View Agent 5.3.

Logiciel Horizon View Client

Horizon View Client 5.4 pour Windows

Horizon View Client 2.2 pour Windows ou version ultérieure

Remarque Horizon View Client 2.2 pour Windows est une version postérieure à Horizon View Client 5.4 pour Windows. Le numéro de version pour Windows est à présent cohérent avec les versions d'Horizon View Client sur les autres systèmes d'exploitation et périphériques.

Horizon View Client 2.2 pour Linux ou version ultérieure. Notez que cette fonction n'est accessible qu'avec la version d'Horizon View Client pour Linux fournie par certains partenaires.

Ordinateur View Client ou périphérique d'accès client

- L'Audio/Vidéo en temps réel est pris en charge par tous les systèmes d'exploitation client Windows qui utilisent Horizon View Client pour Windows. Pour plus de détails, reportez-vous au document *Utilisation de VMware Horizon View Client pour Windows*.
- L'Audio/Vidéo en temps réel est pris en charge par tous les systèmes d'exploitation client Windows qui utilisent Horizon View Client pour Linux sur des périphériques x86. Cette fonctionnalité n'est pas prise en charge par les processeurs ARM. Pour plus de détails, reportez-vous au document *Utilisation de VMware Horizon View Client pour Linux*.

- Les pilotes des webcams et des périphériques audio doivent être installés, et la webcam ainsi que le périphérique audio doivent être opérationnels sur l'ordinateur client. Pour utiliser l'Audio/Vidéo en temps réel, vous n'avez pas à installer les pilotes des périphériques sur le système d'exploitation du poste de travail où View Agent est installé.

Protocole d'affichage pour Horizon View

PCoIP

L'Audio/Vidéo en temps réel n'est pas pris en charge par les sessions postes de travail RDP.

Configuration système requise pour Unity Touch

Le logiciel Horizon View Client et les appareils portables sur lesquels il est installé doivent satisfaire certaines exigences de version pour prendre en charge Unity Touch.

Logiciel Horizon View Client

Unity Touch est pris en charge par les versions Horizon View Client suivantes :

- Horizon View Client 2.0 pour iOS ou versions ultérieures
- Horizon View Client 2.0 pour Android ou versions ultérieures

Systèmes d'exploitation des appareils portables

Unity Touch est pris en charge sur les systèmes d'exploitation des appareils portables :

- iOS 5.0 et versions ultérieures
- Android 3 (Honeycomb), Android 4 (Ice Cream Sandwich) et Android 4.1 et 4.2 (Jelly Bean).

Poste de travail Horizon View

Pour prendre en charge Unity Touch, les logiciels suivants doivent être installés sur la machine virtuelle accédée par l'utilisateur :

- Systèmes d'exploitation : Windows XP SP3 (32 bits), Windows Vista (32 bits), Windows 7 (32 ou 64 bits), Windows 8 (32 ou 64 bits), Windows 8.1 (32 ou 64 bits) ou Windows Server 2008 R2
- View Agent 5.3

  Des instructions d'installation sont fournies dans le document *Administration de VMware Horizon View*.

Configuration requise pour la redirection multimédia Windows 7

Pour prendre en charge la redirection multimédia (MMR) Windows 7, le déploiement de votre Horizon View doit répondre à certaines exigences matérielles et logicielles.

Poste de travail Horizon View

- Les postes de travail doivent tourner sur des systèmes d'exploitation Windows 7, 64 ou 32 bits.
- Le **Rendu 3D** doit être activé sur le pool de postes de travail.
- La version du matériel virtuel des machines virtuelles poste de travail doit être 8 ou plus.
- Les utilisateurs doivent effectuer la lecture de leurs vidéos avec Windows Media Player 12 ou version ultérieure.

Logiciel Horizon View Client

Horizon View Client 2.2 pour Windows ou versions ultérieures

Ordinateur View Client ou périphérique d'accès client	■ Les clients doivent tourner sur des systèmes d'exploitation Windows 7 ou Windows 8, 64 ou 32 bits. ■ Les clients doivent disposer de cartes vidéo compatibles DXVA (DirectX Video Acceleration) qui peuvent décoder les vidéos sélectionnées. ■ Windows Media Player 12 ou version ultérieure doit être installé sur les clients pour permettre la redirection vers le matériel local.
Formats multimédias pris en charge	Les formats multimédias doivent être conformes à la norme de compression vidéo H.264. Les formats de fichiers M4V, MP4 et MOV sont pris en charge. Vos postes de travail virtuels doivent utiliser l'un de ces formats de fichiers et les décodeurs locaux de ces formats doivent exister sur les systèmes client.
Stratégies View	Dans View Administrator, vérifiez que la stratégie **Redirection multimédia (MMR)** est définie sur **Autoriser** (valeur par défaut).
Pare-feu dorsal	Si le déploiement d'Horizon View inclut un pare-feu dorsal entre vos serveurs de sécurité de la zone DMZ et votre réseau interne, assurez-vous que le pare-feu dorsal autorise le trafic vers le port 9427 de vos postes de travail.

Pour une comparaison du composant de redirection multimédia (MMR) Windows 7 et du composant Wyse MMR qui fonctionne sur les postes de travail Windows XP et Windows Vista, reportez-vous à « Prise en charge de la redirection multimédia par les systèmes d'exploitation des postes de travail », page 15.

Prise en charge de la redirection multimédia par les systèmes d'exploitation des postes de travail

La redirection multimédia (MMR) Windows 7est un composant Feature Pack qui est installé avec Remote Experience Agent. Le composant Wyse MMR est installé avec View Agent et fonctionne sur les postes de travail Windows XP et Windows Vista. Quelques caractéristiques et exigences du composant MMR Windows 7 sont légèrement différentes de celles du composant Wyse MMR.

Tableau 2. Prise en charge de la redirection multimédia par les systèmes d'exploitation des postes de travail Horizon View

Système d'exploitation de poste de travail	Exigences de machine virtuelle de poste de travail	Formats multimédias pris en charge	Clients pris en charge	Redirection audio
Windows XP, Windows Vista	Windows Media Player 10 ou une version ultérieure doit être installée.	Plusieurs formats sont pris en charge. Par exemple : MPEG2-1 ; MPEG2 ; MPEG-4 Part 2 ; WMV 7, 8 et 9 ; WMA ; AVI ; ACE ; MPT3 ; WAV	Windows XP, Windows Vista, Windows 7 Windows Media Player 10 ou une version ultérieure doit être installée.	Le flux audio est redirigé vers le système client.
Windows 7	La version du matériel virtuel des postes de travail doit être 8 ou plus. Le **Rendu 3D** doit être activé. Windows Media Player 12 ou une version ultérieure doit être installée.	Compression H.264 standard dans les formats M4V, MP4 ou MOV.	Windows 7, Windows 8 Les clients doivent disposer de cartes vidéo compatibles DXVA (DirectX Video Acceleration) qui peuvent décoder les vidéos sélectionnées. Windows Media Player 12 ou une version ultérieure doit être installée.	Le flux audio n'est pas redirigé. L'audio est livré sur PCoIP à partir du poste de travail distant au système client.
Windows 8	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge

Pour plus d'informations sur la configuration système requise pour MMR sur les clients Horizon View, reportez-vous au document *Utilisation de VMware Horizon View Client pour Windows*.

Installation et déploiement de Remote Experience Agent sur les postes de travail Horizon View

Exécutez le programme d'installation de Remote Experience Agent pour installer les composants Feature Pack sur des postes de travail Horizon View. Vous pouvez utiliser le programme d'installation de Remote Experience Agent en mode interactif ou en mode silencieux à partir de la ligne de commande.

Si vous souhaitez créer un nouveau pool de postes de travail, installez Remote Experience Agent sur une machine virtuelle parent. Prenez un snapshot ou créez un modèle de la machine virtuelle puis créez le pool de postes de travail.

Si vous souhaitez installer les composants Feature Pack sur un pool de postes de travail existant, la méthode à suivre dépend du type de pool de postes de travail. Par exemple, dans le cas d'un pool de clones liés avec des affectations flottantes, vous pouvez exécuter le programme d'installation de Remote Experience Agent sur la machine virtuelle parent puis recomposer les clones liés. Dans le cas d'un pool de clones intégraux ou d'un pool que vous n’allez pas recomposer, vous pouvez installer Remote Experience Agent en mode silencieux sur les postes de travail. Vous pouvez utiliser votre propre script ou un outil de distribution de logiciels pour effectuer l'installation distribuée.

Mise à niveau de Remote Experience Agent

Si une ancienne version de Remote Experience Agent est installée sur vos postes de travail, installez la version actuelle pour obtenir les dernières versions des composants Feature Pack.

Avant d'installer Remote Experience Agent fourni avec Horizon View 5.3 Feature Pack 1, vous devez installer View Agent 5.3 sur vos postes de travail. L'installation de View Agent 5.3 supprime les versions antérieures de Remote Experience Agent et des composants Feature Pack associés. Vous pouvez installer ensuite la version actuelle de Remote Experience Agent, qui procède à une nouvelle installation des composants Feature Pack.

Installer Remote Experience Agent de façon interactive

Le programme d'installation de Remote Experience Agent permet de configurer les composants Feature Pack sur les postes de travail Horizon View.

Le composant Agent HTML Access est nécessaire pour HTML Access. Pour plus d'informations sur la configuration des postes de travail et des pools Horizon View pour HTML Access, reportez-vous à « Préparer des postes de travail et des pools View pour HTML Access » dans le document *Utilisation de VMware Horizon View HTML Access* sur la page de documentation VMware Horizon View Clients.

Important N'installez pas et ne désinstallez pas Remote Experience Agent d'une session de poste de travail View établie via View Client ou HTML Access. Exécutez le programme d'installation directement sur la machine virtuelle. Vous pouvez, par exemple, ouvrir une console sur la machine virtuelle dans vSphere Web Client ou vSphere Client.

Prérequis

- Vérifiez que View Agent 5.3 est installé sur la machine virtuelle.
- Vérifiez que vous disposez des droits d'administration sur la machine virtuelle.
- Vérifiez que le service pare-feu Windows est en cours d'exécution sur la machine virtuelle. L'installation de Remote Experience Agent n'est pas possible si le service pare-feu Windows n'est pas lancé et en cours d'exécution.
- Familiarisez-vous avec les fonctionnalités qui peuvent être installées par Remote Experience Agent. Reportez-vous à la section « Options d'installation de Remote Experience Agent », page 17.
- Vérifiez que vous avez accès au fichier du programme d'installation de Remote Experience Agent sur la page produits VMware à l'adresse http://www.vmware.com/fr/products/.

Procédure

1 Téléchargez le fichier du programme d'installation de Remote Experience Agent sur la page produits VMware.

Sélectionnez le fichier du programme d'installation approprié, où *y.y* est le numéro de version de Feature Pack et *xxxxxx* le numéro de build.

Option	Description
programme d'installation 32 bits	`VMware-Horizon-View-5.3-Remote-Experience-Agent-y.y-xxxxxx.exe`
programme d'installation 64 bits	`VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe`

2 Double-cliquez sur le fichier du programme d'installation pour lancer le programme d'installation de Remote Experience Agent.

3 Acceptez le Contrat de licence d'utilisateur final VMware.

4 Sélectionnez vos options d'installation.

Utilisez le menu déroulant pour une caractéristique particulière pour sélectionner ou désélectionner cette option pour l'installation.

5 Cliquez sur **Installer**.

Le programme affiche le message à la fin de l'installation : `L'installation de VMware Horizon View 5.3 Remote Experience Agent s'est terminée avec succès.`

6 Cliquez sur **Terminer**.

Lorsque l'agent HTML Access est installé sur la machine virtuelle, le port TCP 22443 est ouvert sur le pare-feu Windows. Reportez-vous à la section « Règles de pare-feu pour HTML Access », page 24.

Suivant

Si vous avez installé Remote Experience Agent sur une machine virtuelle parent, prenez un snapshot ou créez un modèle puis créez un pool de postes de travail Horizon View ou recomposez un pool existant.

Options d'installation de Remote Experience Agent

Vous pouvez sélectionner des options d'installation lorsque vous installez Remote Experience Agent sur une machine virtuelle.

Option	Description
HTML Access	Permet aux utilisateurs de se connecter aux postes de travail Horizon View en utilisant HTML Access. L'agent HTML Access doit être installé sur les postes de travail Horizon View pour permettre aux utilisateurs de se connecter avec HTML Access. Cette fonctionnalité est installée par défaut.
Redirection d'URL Flash	La redirection d'URL Flash permet de rediriger les données des flux de multidiffusion ou de monodiffusion des postes de travail virtuels vers des périphériques clients. Cette fonctionnalité permet aux vidéos d'être diffusées directement à partir d'une source de multidiffusion ou de monodiffusion Web sur le matériel client et affichées aux utilisateurs sur les lecteurs multimédias Flash des clients locaux. Cette fonctionnalité est installée par défaut.
Audio/Vidéo en temps réel	Permet de rediriger la webcam et les périphériques audio connectés au système client pour qu'ils puissent être utilisés sur le poste de travail distant. Cette fonctionnalité est installée par défaut.
Unity Touch	Offre aux utilisateurs des smartphones et des tablettes une barre latérale tactile qu'ils peuvent utiliser pour naviguer, rechercher, ouvrir et fermer des applications et fichiers Windows et passer d'une application active à l'autre. Cette fonctionnalité est installée par défaut.
Redirection multimédia Win7	Permet d'étendre la redirection multimédia pour les postes de travail Windows 7 et postes de travail client. Cette fonctionnalité délivre le flux multimédia directement aux ordinateurs client, permettant au flux multimédia d'être traité sur le matériel client plutôt que sur l'hôte ESXi distant. Cette fonctionnalité est installée par défaut.

Installer Remote Experience Agent en mode silencieux

Vous pouvez utiliser l'option d'installation silencieuse de Microsoft Windows Installer (MSI) pour installer Remote Experience Agent sur plusieurs machines virtuelles Windows. Dans une installation silencieuse, vous utilisez la ligne de commande et n'avez pas à répondre à des invites d'assistant.

Le programme d'installation de Remote Experience Agent permet de configurer les composants Feature Pack sur les postes de travail Horizon View.

Important N'installez pas et ne désinstallez pas Remote Experience Agent d'une session de poste de travail View établie via View Client ou HTML Access. Exécutez la commande d'installation directement sur la machine virtuelle. Vous pouvez, par exemple, ouvrir une console sur la machine virtuelle dans vSphere Web Client ou vSphere Client.

Prérequis

- Vérifiez que View Agent 5,3 est installé sur la machine virtuelle.
- Vérifiez que vous disposez des droits d'administration sur la machine virtuelle.
- Vérifiez que le service pare-feu Windows est en cours d'exécution sur la machine virtuelle. L'installation de Remote Experience Agent n'est pas possible si le service pare-feu Windows n'est pas lancé et en cours d'exécution.
- Vérifiez que vous avez accès au fichier du programme d'installation de Remote Experience Agent sur la page produits VMware à l'adresse http://www.vmware.com/fr/products/.
- Familiarisez-vous avec les propriétés de l'installation silencieuse disponibles avec Remote Experience Agent. Reportez-vous à la section « Propriétés de l'installation silencieuse pour Remote Experience Agent », page 19.
- Familiarisez-vous avec les options de ligne de commande du programme d'installation MSI. Reportez-vous à la section « Options de la ligne de commande MSI pour le programme d'installation de Remote Experience Agent », page 19.

Procédure

1 Téléchargez le fichier du programme d'installation de Remote Experience Agent sur la page produits VMware.

Sélectionnez le fichier du programme d'installation approprié, où *y.y* est le numéro de version de Feature Pack et *xxxxxx* le numéro de build.

Option	Description
programme d'installation 32 bits	`VMware-Horizon-View-5,3-Remote-Experience-Agent-`*`y.y-xxxxxx`*`.exe`
programme d'installation 64 bits	`VMware-Horizon-View-5,3-Remote-Experience-Agent-x64-`*`y.y-xxxxxx`*`.exe`

2 Ouvrez une invite de commande de Windows sur la machine virtuelle.

3 Saisissez la commande d'installation sur une ligne.

Voici un exemple d'installation de Remote Experience Agent sur une machine virtuelle. Le programme d'installation configure toutes les options d'installation de Remote Experience Agent et enregistre des journaux dans le fichier `install.log`.

```
VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s /v"/qn /l*v
""C:\myfolder\install.log"""
```

Remarque L'exemple précédent montre comment installer toutes les fonctionnalités qui sont disponibles publiquement. Pour installer les fonctionnalités sélectionnées, utilisez l'option `ADDLOCAL=` et listez les propriétés d'installation silencieuse dans une liste séparée par des virgules. Par exemple : `ADDLOCAL=Core,HTMLAccess,UnityTouch,FlashURLRedirection,RTAV,MMR`. La propriété `Core` est requise lorsque vous utilisez `ADDLOCAL=` pour spécifier les fonctionnalités sélectionnées.

Lorsque l'agent HTML Access est installé sur la machine virtuelle, le port TCP 22443 est ouvert sur le pare-feu Windows. Reportez-vous à la section « Règles de pare-feu pour HTML Access », page 24.

Suivant

Si vous avez installé Remote Experience Agent sur une machine virtuelle parent, prenez un snapshot ou créez un modèle puis créez un pool de postes de travail Horizon View ou recomposez un pool existant.

Propriétés de l'installation silencieuse pour Remote Experience Agent

Dans une commande d'installation silencieuse, vous pouvez utiliser la propriété MSI `ADDLOCAL=` pour spécifier les composants Feature Pack à configurer par le programme d'installation de Remote Experience Agent. Chaque fonctionnalité de l'installation silencieuse correspond à une option d'installation que vous pouvez sélectionner au cours d'une installation interactive.

Pour plus d'informations sur ces fonctionnalités, reportez-vous à « Options d'installation de Remote Experience Agent », page 17.

Tableau 3. Caractéristiques de l'installation silencieuse de Remote Experience Agent et options de l'installation interactive

Caractéristiques de l'installation silencieuse	Options d'installation d'une installation interactive
HTML Access	HTML Access Agent
Redirection d'URL Flash	Redirection d'URL Flash
Audio/Vidéo en temps réel (RTAV)	Audio/Vidéo en temps réel
UnityTouch	Unity Touch
Redirection multimédia (MMR)	Redirection multimédia (MMR) Win7

Options de la ligne de commande MSI pour le programme d'installation de Remote Experience Agent

Pour installer Remote Experience Agent de façon silencieuse, vous devez utiliser les options et les propriétés de la ligne de commande Microsoft Windows Installer (MSI). Le programme d'installation est un programme MSI qui utilise des fonctionnalités MSI standard.

Pour plus d'informations sur MSI, rendez-vous sur le site Web de Microsoft. Pour plus d'informations sur les options de la ligne de commande MSI, rendez-vous sur le site Web de la bibliothèque MSDN (Microsoft Developer Network). Pour voir comment utiliser la ligne de commande MSI, vous pouvez ouvrir une invite de commande sur la machine virtuelle où vous effectuez l'installation et entrer `msiexec /?`.

Remarque L'option `INSTALLDIR` n'est pas disponible pour le programme d'installation de Remote Experience Agent. Vous ne pouvez pas changer le dossier d'installation.

Pour exécuter un programme d'installation de façon silencieuse, vous devez d'abord désactiver le programme de démarrage qui effectue l'extraction du programme d'installation dans un dossier temporaire et démarre une installation interactive.

Vous devez entrer sur la ligne de commande les options qui contrôlent le programme de démarrage du programme d'installation.

Tableau 4. Options de la ligne de commande du programme de démarrage du programme d'installation

Option	Description
`/s`	Désactive l'écran de démarrage et la boîte de dialogue d'extraction du programme de démarrage, qui empêche l'affichage de boîtes de dialogue interactives. Par exemple : `VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s` L'option `/s` est obligatoire pour que l'installation soit silencieuse.
`/v" MSI_command_line_options"`	Demande au programme d'installation de transmettre à MSI la chaîne de caractères comprise entre guillemets, que vous avez entrée sur la ligne de commande comme un ensemble d'options à interpréter. Vous devez délimiter votre chaîne de caractères de la ligne de commande par des guillemets. Placez un guillemet après `/v` et à la fin de la ligne de commande. Par exemple : `VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s /v"command_line_options"` L'option `/v"command_line_options"` est obligatoire pour exécuter une installation silencieuse.

Le contrôle de la suite de l'installation silencieuse se fait en transmettant les options de la ligne de commande et les valeurs de propriété MSI au programme d'installation MSI, `msiexec.exe`. Le programme d'installation MSI utilise les valeurs et les options que vous entrez sur la ligne de commande pour interpréter les options d'installation qui sont spécifiques au programme d'installation de Remote Experience Agent.

Tableau 5. Options de la ligne de commande et propriétés MSI

Option ou propriété MSI	Description
`/qn`	Demande au programme d'installation MSI de ne pas afficher les pages de l'assistant d'installation. Par exemple, vous pourriez installer Remote Experience Agent de façon silencieuse et n'utiliser que des options et des fonctionnalités d'installation par défaut : `VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s /v"/qn"` Vous pouvez également utiliser l'option `/qb` pour afficher les pages de l'assistant d'installation dans une installation automatique non interactive. Pendant l'installation, les pages de l'assistant d'installation seront affichées, mais vous ne pouvez pas y répondre. L'option `/qn` ou `/qb` est obligatoire pour que l'installation soit silencieuse.
`/x`	Désinstalle Remote Experience Agent. Par exemple : `VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s /v"/qb /x"` Pour obtenir des instructions sur la désinstallation de Remote Experience Agent et la restauration à l'état d'avant l'installation du poste de travail Horizon View, reportez-vous à « Désinstaller Remote Experience Agent », page 21.
UNITY_DEFAULT_APPS	Indique une liste d'applications préférées par défaut qui sont affichées dans la barre latérale d'Unity Touch sur un appareil portable. Cette propriété a été créée pour prendre en charge le composant Unity Touch. Il ne s'agit pas d'une propriété MSI générale. Pour plus d'informations sur la configuration d'une liste d'applications préférées par défaut et sur la syntaxe et le format utilisés avec cette propriété, reportez-vous à « Configurer les applications préférées affichées par Unity Touch », page 30. La propriété `UNITY_DEFAULT_APPS` est facultative.

Tableau 5. Options de la ligne de commande et propriétés MSI (suite)

Option ou propriété MSI	Description
ADDLOCAL	Détermine les fonctionnalités spécifiques du composant à installer. Dans une installation interactive, le programme d'installation affiche les options d'installation à sélectionner. La propriété ADDLOCAL vous permet de spécifier ces options sur la ligne de commande. Les options par défaut seront installées si vous n'utilisez pas la propriété ADDLOCAL. Pour spécifier différentes options d'installation, entrez une liste de noms d'options séparés par des virgules. Ne laissez pas d'espaces entre les noms. Utilisez la forme ADDLOCAL=*valeur*,*valeur*,*valeur*.... Les noms des options sont sensibles à la casse. Pour consulter la liste des options d'installation disponibles, reportez-vous à « Propriétés de l'installation silencieuse pour Remote Experience Agent », page 19. L'exemple suivant montre comment installer l'agent HTML Access, Unity Touch, Redirection d'URL Flash et l'Audio/Vidéo en temps réel. VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-*y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=Core,HTMLAccess,UnityTouch,FlashURLRedirection,RTAV,MMR" L'élément Core est obligatoire lorsque vous utilisez la propriété ADDLOCAL pour spécifier les options d'installation. La propriété ADDLOCAL est facultative.
REBOOT	Vous pouvez utiliser l'option REBOOT=ReallySuppress pour autoriser l'exécution de tâches de configuration système avant le redémarrage du système. Cette propriété MSI est facultative.
REMOVE	Supprime les composants Feature Pack spécifiés (options d'installation) installés par le programme d'installation de Remote Experience Agent. Pour supprimer différentes options d'installation, entrez une liste de noms d'options séparés par des virgules. Ne laissez pas d'espaces entre les noms. Utilisez la forme REMOVE=*valeur*,*valeur*,*valeur*.... Les noms des options sont sensibles à la casse. Pour consulter la liste des options d'installation disponibles, reportez-vous à « Propriétés de l'installation silencieuse pour Remote Experience Agent », page 19. L'exemple suivant montre comment installer l'agent HTML Access, Unity Touch, Redirection d'URL Flash et l'Audio/Vidéo en temps réel. VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-*y.y-xxxxxx*exe /s /v"/qn REMOVE=HTMLAccess,UnityTouch,FlashURLRedirection,RTAV,MMR" La propriété REMOVE est facultative.
/l*v *log_file*	Écrit des informations de journalisation dans le fichier journal spécifié avec une sortie détaillée. Par exemple : /l*v ""%TEMP%\vmmsi.log"" Cet exemple génère un fichier journal détaillé semblable à celui généré lors d'une installation interactive. Vous pouvez utiliser cette option pour enregistrer des fonctions personnalisées qui s'appliquent uniquement à votre installation. Vous pouvez utiliser les informations enregistrées pour spécifier les fonctionnalités d'installation lors d'installations silencieuses ultérieures. L'option /l*v est facultative.

Désinstaller Remote Experience Agent

Vous pouvez supprimer Remote Experience Agent à partir des postes de travail Horizon View en utilisant la même méthode que vous utilisez pour supprimer d'autres logiciels Windows.

Remote Experience Agent touche certains fichiers qui sont installés avec View Agent 5.3. Lorsque vous désinstallez Remote Experience Agent, pour que votre machine virtuelle View Agent retourne à son état d'origine, vous devez soit désinstaller puis réinstaller View Agent, soit réparer View Agent.

Procédure

1 Sur les machines virtuelles où Remote Experience Agent est installé, ouvrez l'applet Supprimer des programmes du panneau de configuration Windows.

2 Sélectionnez **VMware Horizon View 5.3 Remote Experience Agent**, puis cliquez sur **Désinstaller**.

3 Désinstallez puis réinstallez View Agent ou réparez-le.

Option	Description
Désinstallation et réinstallation	a Dans l'applet Windows Désinstaller un programme, sélectionnez **VMware View Agent** et cliquez sur **Désinstaller**. b Lancez le fichier d'installation de VMware View Agent 5.3 pour réinstaller le logiciel.
Réparation	Lancez le fichier d'installation de VMware View Agent 5.3 et sélectionnez l'option **Réparer**.

4 (Facultatif) Dans le Pare-feu Windows de la machine virtuelle, vérifiez que le port TCP 22443 ne permet plus de trafic entrant.

Suivant

Si c'est le cas, changez les règles du pare-feu de votre organisation pour interdire le trafic entrant sur le port TCP 22443 de la machine virtuelle du poste de travail.

Installer le logiciel HTML Access sur Serveur de connexion View

Le programme d'installation de HTML Access permet de configurer la page View Portal sur le serveur de connexion View pour permettre aux utilisateurs de sélectionner HTML Access lorsqu'ils se connectent à leurs postes de travail. Exécutez le programme d'installation sur une instance et sur toutes les instances du serveur de connexion View dans un groupe répliqué.

Par défaut, lorsqu'un utilisateur ouvre un navigateur et entrer l'URL d'une instance du serveur de connexion View, la page View Portal qui apparaît contient des liens vers le site de téléchargement pour télécharger View Client.

Une fois le programme d'installation HTML Access exécuté, la page View Portal affiche une icône de HTML Access en plus de l'icône de View client, permettant ainsi aux utilisateurs de se connecter à leurs postes de travail via HTML Access. Les utilisateurs n'ont pas à installer View Client pour se connecter à leurs postes de travail.

Vous pouvez personnaliser la page View Portal si vous souhaitez désactiver l'icône de téléchargement de View Client ou l'icône de connexion via HTML Access, ou modifier l'URL de la page Web de téléchargement de View Client. Reportez-vous à « Configuration de la page HTML Access pour les utilisateurs finaux » dans le document *Utilisation de VMware Horizon View HTML Access*, sur la page de documentation VMware Horizon View Clients.

Important Si vous aviez modifié la page View Portal proposée avec Horizon View ou la page HTML Access Portal fournie avec Horizon View 5.2 Feature Pack 1, ces personnalisations seront perdues lorsque vous passerez à une version plus récente de HTML Access. Vous pouvez personnaliser la page après la mise à niveau. Si vous aviez modifié la page HTML Access Portal fournie avec Horizon View 5.2 Feature Pack 2 ou version ultérieure, vos personnalisations sont conservées.

Pour avoir un aperçu sur la configuration du serveur de connexion View pour HTML Access, reportez-vous à « Préparer les serveurs de connexion View et de sécurité pour HTML Access » dans le document *Utilisation de VMware Horizon View HTML Access*, sur la page de documentation VMware Horizon View Clients.

Mise à niveau du logiciel HTML Access

Installez la version actuelle de HTML Access pour obtenir les mises à jour et améliorations les plus récentes.

Avant d'installer le logiciel HTML Access fourni avec Horizon View 5.3 Feature Pack 1, vous devez effectuer la mise à niveau de vos instances du Serveur de connexion View vers Horizon View 5.3.

Pour ce faire, exécutez la dernière version du logiciel HTML Access sur les instances du Serveur de connexion View dans un groupe répliqué.

Pour effectuer la mise à niveau de HTML Access, vous devez également exécuter la dernière version du programme d'installation de Remote Experience Agent sur les machines virtuelles parents correspondantes ou sur les modèles de machines virtuelles de vos pools de postes de travail. Reportez-vous à la section « Mise à niveau de Remote Experience Agent », page 16.

Installer le logiciel HTML Access sur Serveur de connexion View

Pour configurer la page View Portal afin d'afficher l'icône HTML Access pour les utilisateurs finaux, exécutez le programme d'installation de l'icône HTML Access sur l'instance ou sur les instances du serveur de connexion View dans un groupe répliqué.

Prérequis

- Vérifiez que le serveur de connexion View est Horizon View 5,3.
- Assurez-vous que vous avez accès au fichier du programme d'installation de HTML Access sur la page produits VMware à l'adresse http://www.vmware.com/fr/products/.

Procédure

1 Téléchargez le fichier du programme d'installation de HTML Access à partir de la page produits VMware.

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

2 Double-cliquez sur le fichier du programme d'installation pour lancer l'installation de HTML Access.

3 Acceptez le Contrat de licence d'utilisateur final VMware.

4 Acceptez ou changez le dossier d'installation.

5 Cliquez sur **Installer**.

6 Cliquez sur **Terminer**.

Suivant

Assurez-vous que le port utilisé par HTML Access pour permettre des connexions à des serveurs de sécurité est ouvert sur le pare-feu Windows. Reportez-vous à la section « Ouvrir le port utilisé par HTML Access sur des serveurs de sécurité », page 24.

Vous pouvez modifier la page View Portal en masquant des utilisateurs l'icône de View Client ou l'icône de HTML Access. Reportez-vous à « Configuration de la page HTML Access pour les utilisateurs finaux » dans le document *Utilisation de VMware Horizon View HTML Access*, sur la page de documentation VMware Horizon View Clients.

Ouvrir le port utilisé par HTML Access sur des serveurs de sécurité

Lorsque vous installez Serveur de connexion View ou un serveur de sécurité, le programme d'installation de View Server crée la règle de Pare-feu Windows pour le port utilisé par HTML Access pour les connexions client, mais il laisse la règle désactivée tant qu'elle n'est pas réellement nécessaire. Lorsque vous installez ultérieurement HTML Access sur une instance de Serveur de connexion View, le programme d'installation HTML Access active automatiquement la règle pour autoriser la communication avec ce port. Toutefois, sur les serveurs de sécurité, vous devez activer manuellement la règle dans le Pare-feu Windows pour autoriser la communication avec le port.

Par défaut, HTML Access utilise le port TCP 8443 pour les connexions client avec Blast Secure Gateway.

Procédure

- Pour ouvrir le port utilisé par HTML Access sur un ordinateur Serveur de connexion View, installez HTML Access sur cet ordinateur.

  Le programme d'installation HTML Access active la règle **Serveur de connexion VMware View (Blast-In)** dans le Pare-feu Windows.

- Pour ouvrir le port pour HTML Access sur un serveur de sécurité, activez manuellement la règle **Serveur de connexion VMware View (Blast-In)** dans le Pare-feu Windows.

Désinstaller HTML Access de Serveur de connexion View

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

Procédure

1. Sur les hôtes de Serveur de connexion View sur lesquels HTML Access est installé, ouvrez l'applet Désinstaller un programme du Panneau de configuration Windows.
2. Sélectionnez HTML Access et cliquez sur **Désinstaller**.
3. (Facultatif) Pour le pare-feu Windows de cet hôte, vérifiez que le port TCP 8443 n'autorise plus le trafic entrant.

Suivant

Interdisez le trafic entrant vers le port TCP 8443 sur le pare-feu Windows des serveurs de sécurité couplés. Le cas échéant, sur les pare-feu tiers, modifiez les règles pour interdire le trafic entrant vers le port TCP 8443 pour tous les serveurs de sécurité couplés et cet hôte de Serveur de connexion View.

Règles de pare-feu pour HTML Access

Pour autoriser les navigateurs Web clients à utiliser HTML Access pour effectuer des connexions à des serveurs de sécurité, à des instances de Serveur de connexion View et à des postes de travail Horizon View, vos pare-feu doivent autoriser le trafic entrant sur certains ports TCP.

Les connexions HTML Access doivent utiliser HTTPS. Les connexions HTTP ne sont pas autorisées.

Pour vérifier que le pare-feu Windows sur des serveurs de sécurité est configuré pour autoriser le trafic sur le port TCP utilisé par HTML Access, reportez-vous à la section « Ouvrir le port utilisé par HTML Access sur des serveurs de sécurité », page 24.

Tableau 6. Règles de pare-feu pour HTML Access

Source	Port source par défaut	Protocole	Cible	Port cible par défaut	Remarques
Navigateur Web client	Tout port TCP	HTTPS	Serveur de sécurité ou instance de Serveur de connexion View	TCP 443	Pour établir une connexion initiale à Horizon View, le navigateur Web d'un périphérique client se connecte à un serveur de sécurité ou à une instance de Serveur de connexion View sur le port TCP 443.
Navigateur Web client	Tout port TCP	HTTPS	Blast Secure Gateway	TCP 8443	Une fois la connexion initiale à Horizon View établie, le navigateur Web d'un périphérique client se connecte à Blast Secure Gateway sur le port TCP 8443. Blast Secure Gateway doit être activé sur un serveur de sécurité ou une instance de Serveur de connexion View pour autoriser cette deuxième connexion. **Remarque** Blast Secure Gateway est installé avec Serveur de connexion View dans Horizon View 5.2 et versions supérieures.
Blast Secure Gateway	Tout port TCP	HTTPS	Agent HTML Access	TCP 22443	Si Blast Secure Gateway est activé, lorsqu'un utilisateur sélectionne un poste de travail Horizon View, Blast Secure Gateway se connecte à l'agent HTML Access sur le port TCP 22443 sur le poste de travail.
Navigateur Web client	Tout port TCP	HTTPS	Agent HTML Access	TCP 22443	Si Blast Secure Gateway n'est pas activé, lorsqu'un utilisateur sélectionne un poste de travail Horizon View, le navigateur Web du périphérique client se connecte directement à l'agent HTML Access sur le port TCP 22443 sur le poste de travail.

Configurer les agents HTML Access pour utiliser les nouveaux certificats SSL

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

Lors de l'installation de l'agent HTML Access sur des postes de travail Horizon View, le service de l'agent HTML Access crée des certificats auto-signés par défaut. Le service présente les certificats par défaut aux navigateurs qui utilisent HTML Access pour se connecter à Horizon View.

Remarque Dans le système d'exploitation client sur la machine virtuelle de poste de travail, ce service s'appelle VMware Blast.

Pour remplacer les certificats par défaut par des certificats signés obtenus auprès d'une autorité de certification, vous devez importer un certificat dans le magasin de certificats de l'ordinateur local Windows sur chaque poste de travail Horizon View. Vous devez également définir une valeur de registre sur chaque poste de travail qui autorise l'agent HTML Access à utiliser le nouveau certificat.

Si vous remplacez les certificats par défaut de l'agent HTML Access par des certificats signés par une autorité de certification, VMware vous recommande de configurer un certificat unique sur chaque poste de travail. Ne configurez pas de certificat signé par une autorité de certification sur une machine virtuelle parente ou sur un modèle utilisé pour créer un pool de postes de travail. Cela aurait pour incidence de voir des centaines ou des milliers de postes de travail avec des certificats identiques.

Procédure

1 Ajouter le composant logiciel enfichable Certificat à MMC sur un poste de travail Horizon View page 26

Avant de pouvoir ajouter des certificats au magasin de certificats de l'ordinateur local Windows, vous devez ajouter le composant logiciel enfichable Certificat à MMC (Microsoft Management Console) sur les postes de travail Horizon View sur lesquels l'agent HTML Access est installé.

2 Importer un certificat pour l'agent HTML Access dans un magasin de certificats Windows page 27

Pour remplacer un certificat par défaut de l'agent HTML Access par un certificat signé par une autorité de certification, vous devez importer ce dernier dans le magasin de certificats de l'ordinateur local Windows. Effectuez cette procédure sur chaque poste de travail où l'agent HTML Access est installé.

3 Importer des certificats racine et intermédiaires pour l'agent HTML Access page 28

Si le certificat racine et les certificats intermédiaires dans la chaîne de certificats ne sont pas importés avec le certificat SSL importé pour l'agent HTML Access, vous devez importer ces certificats dans le magasin de certificats de l'ordinateur local Windows.

4 Définir l'empreinte numérique de certificat dans le registre Windows page 28

Pour permettre à l'agent HTML Access d'utiliser un certificat signé par une autorité de certification importé dans le magasin de certificats Windows, vous devez configurer l'empreinte numérique de certificat dans une clé de registre Windows. Vous devez suivre cette étape sur chaque poste de travail sur lequel vous remplacez le certificat par défaut par un certificat signé par une autorité de certification.

Ajouter le composant logiciel enfichable Certificat à MMC sur un poste de travail Horizon View

Avant de pouvoir ajouter des certificats au magasin de certificats de l'ordinateur local Windows, vous devez ajouter le composant logiciel enfichable Certificat à MMC (Microsoft Management Console) sur les postes de travail Horizon View sur lesquels l'agent HTML Access est installé.

Prérequis

Vérifiez que MMC et le composant logiciel enfichable Certificat sont disponibles sur le système d'exploitation client Windows sur lequel l'agent HTML Access est installé.

Procédure

1 Sur le poste de travail Horizon View, cliquez sur **Démarrer** et entrez **`mmc.exe`**.

2 Dans la fenêtre MMC, sélectionnez **Fichier > Ajouter/Supprimer un composant logiciel enfichable**.

3 Dans la fenêtre Ajouter ou supprimer des composants logiciels enfichables, sélectionnez **Certificats** et cliquez sur **Ajouter**.

4 Dans la fenêtre Composant logiciel enfichable Certificats, sélectionnez **Compte d'ordinateur**, cliquez sur **Suivant**, sélectionnez **Ordinateur local** et cliquez sur **Terminer**.

5 Dans la fenêtre Ajouter ou supprimer des composants logiciels enfichables, cliquez sur **OK**.

Suivant

Importez le certificat SSL dans le magasin de certificats de l'ordinateur local Windows. Reportez-vous à la section « Importer un certificat pour l'agent HTML Access dans un magasin de certificats Windows », page 27.

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

Pour remplacer un certificat par défaut de l'agent HTML Access par un certificat signé par une autorité de certification, vous devez importer ce dernier dans le magasin de certificats de l'ordinateur local Windows. Effectuez cette procédure sur chaque poste de travail où l'agent HTML Access est installé.

Prérequis

- Vérifiez que l'agent HTML Access est installé sur le poste de travail Horizon View.
- Vérifiez que le certificat signé par une autorité de certification a été copié sur le poste de travail.
- Vérifiez que le composant logiciel Certificat a été ajouté à MMC. Reportez-vous à la section « Ajouter le composant logiciel enfichable Certificat à MMC sur un poste de travail Horizon View », page 26.

Procédure

1. Dans la fenêtre MMC sur le poste de travail Horizon View, développez le nœud **Certificats (Ordinateur local)** et sélectionnez le dossier **Personnel**.
2. Dans le volet Actions, allez dans **Autres actions > Toutes les tâches > Importer**.
3. Dans l'assistant Importation de certificat, cliquez sur **Suivant** et accédez à l'emplacement de stockage du certificat.
4. Sélectionnez le fichier du certificat et cliquez sur **Ouvrir**.

   Pour afficher votre type de fichier de certificat, vous pouvez sélectionner son format de fichier dans le menu déroulant **Nom de fichier**.
5. Tapez le mot de passe de la clé privée incluse dans le fichier de certificat.
6. Sélectionnez **Marquer cette clé comme exportable**.
7. Sélectionnez **Inclure toutes les propriétés extensibles**.
8. Cliquez sur **Suivant** et sur **Terminer**.

   Le nouveau certificat apparaît dans le dossier **Certificats (Ordinateur local) > Personnel > Certificats**.
9. Vérifiez que le nouveau certificat contient une clé privée.
   a. Dans le dossier **Certificats (Ordinateur local) > Personnel > Certificats**, double-cliquez sur le nouveau certificat.
   b. Sous l'onglet Général de la boîte de dialogue Informations sur le certificat, vérifiez que la déclaration suivante apparaît : `Vous avez une clé privée qui correspond à ce certificat.`

Suivant

Si nécessaire, importez le certificat racine et les certificats intermédiaires dans le magasin de certificats Windows. Reportez-vous à la section « Importer des certificats racine et intermédiaires pour l'agent HTML Access », page 28.

Configurez la clé de registre appropriée avec l'empreinte numérique de certificat. Reportez-vous à la section « Définir l'empreinte numérique de certificat dans le registre Windows », page 28.

Importer des certificats racine et intermédiaires pour l'agent HTML Access

Si le certificat racine et les certificats intermédiaires dans la chaîne de certificats ne sont pas importés avec le certificat SSL importé pour l'agent HTML Access, vous devez importer ces certificats dans le magasin de certificats de l'ordinateur local Windows.

Procédure

1 Dans la console MMC sur le poste de travail Horizon View, développez le nœud **Certificats (Ordinateur local)** et allez dans le dossier **Autorités de certification racine de confiance > Certificats**.

- Si votre certificat racine se trouve dans ce dossier, et qu'il n'y a pas de certificat intermédiaire dans votre chaîne de certificats, ignorez cette procédure.
- Si votre certificat racine ne se trouve pas dans ce dossier, passez à l'étape 2.

2 Cliquez avec le bouton droit sur le dossier **Autorités de certification racine de confiance > Certificats** et cliquez sur **Toutes les tâches > Importer**.

3 Dans l'assistant Importation de certificat, cliquez sur **Suivant** et allez à l'emplacement de stockage du certificat de l'autorité de certification racine.

4 Sélectionnez le fichier du certificat de l'autorité de certification racine et cliquez sur **Ouvrir**.

5 Cliquez sur **Suivant**, **Suivant** et **Terminer**.

6 Si votre certificat de serveur a été signé par une autorité de certification intermédiaire, importez tous les certificats intermédiaires se trouvant dans la chaîne de certificats dans le magasin de certificats de l'ordinateur local Windows.

a Allez dans le dossier **Certificats (Ordinateur local) > Autorités de certification intermédiaires > Certificats**.

b Répétez les étapes 3 à 6 pour chaque certificat intermédiaire devant être importé.

Suivant

Configurez la clé de registre appropriée avec l'empreinte numérique de certificat. Reportez-vous à la section « Définir l'empreinte numérique de certificat dans le registre Windows », page 28.

Définir l'empreinte numérique de certificat dans le registre Windows

Pour permettre à l'agent HTML Access d'utiliser un certificat signé par une autorité de certification importé dans le magasin de certificats Windows, vous devez configurer l'empreinte numérique de certificat dans une clé de registre Windows. Vous devez suivre cette étape sur chaque poste de travail sur lequel vous remplacez le certificat par défaut par un certificat signé par une autorité de certification.

Prérequis

Vérifiez que le certificat signé par une autorité de certification est importé dans le magasin de certificats Windows. Reportez-vous à la section « Importer un certificat pour l'agent HTML Access dans un magasin de certificats Windows », page 27.

Procédure

1 Dans la fenêtre MMC sur le poste de travail Horizon View où l'agent HTML Access est installé, accédez au dossier **Certificats (Ordinateur local) > Personnel > Certificats**.

2 Double-cliquez sur le certificat signé par une autorité de certification que vous avez importé dans le magasin de certificats Windows.

3 Dans la boîte de dialogue Certificats, cliquez sur l'onglet Détails, faites défiler la liste et sélectionnez l'icône **Empreinte numérique**.

4 Copiez l'empreinte numérique sélectionnée dans un fichier texte.

Par exemple : `31 2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e`

Remarque Lorsque vous copiez l'empreinte numérique, n'incluez pas l'espace de début. Si vous le copiez par inadvertance avec l'empreinte numérique dans la clé de registre (à l'étape 7), le certificat peut ne pas être configuré correctement. Ce problème peut survenir même lorsque l'espace de début ne s'affiche pas dans la zone de texte de la valeur du registre.

5 Démarrez l'éditeur de Registre Windows sur le poste de travail sur lequel l'agent HTML Access est installé.

6 Accédez à la clé de registre `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config`.

7 Modifiez la valeur `SslHash` et collez l'empreinte numérique de certificat dans la zone de texte.

8 Redémarrez le service VMware Blast pour que vos modifications prennent effet.

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

Lorsqu'un utilisateur se connecte à un poste de travail via HTML Access, l'agent HTML Access présente le certificat signé par une autorité de certification au navigateur de l'utilisateur.

Configurer des protocoles de sécurité et des suites de chiffrement pour l'agent HTML Access

À partir de Feature Pack 5 (FP5), vous pouvez configurer les protocoles de sécurité et les suites de chiffrement que l'agent HTML Access utilise en modifiant le registre Windows. Vous pouvez également spécifier les configurations dans un objet de stratégie de groupe (GPO).

Par défaut, l'agent HTML Access FP5 utilise uniquement TLS 1.0, TLS 1.1 et TLS 1.2. Les protocoles autorisés sont, du plus faible au plus élevé, TLS 1.0, TLS 1.1 et TLS 1.2. Les protocoles plus anciens, tels que SSLv3 et version antérieure, ne sont jamais autorisés. Deux valeurs de registre, `SslProtocolLow` et `SslProtocolHigh`, déterminent la plage de protocoles que l'agent HTML Access acceptera. Par exemple, les paramètres `SslProtocolLow=tls_1.0` et `SslProtocolHigh=tls_1.2` forceront l'agent HTML Access à accepter TLS 1.0, TLS 1.1 et TLS 1.2. Les paramètres par défaut sont `SslProtocolLow=tls_1.0` et `SslProtocolHigh=tls_1.2`.

Vous devez spécifier la liste de chiffrements utilisant le format défini dans http://openssl.org/docs/manmaster/apps/ciphers.html, sous la section CIPHER LIST FORMAT (Format de liste de chiffrements). La liste de chiffrements suivante est celle par défaut :

```
ECDHE-RSA-AES256-SHA:AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
```

Procédure

1 Démarrez l'éditeur du Registre Windows.

2 Accédez à la clé de registre `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config`.

3 Ajoutez deux nouvelles valeurs de chaîne (REG_SZ), `SslProtocolLow` et `SslProtocolHigh`, pour spécifier la plage de protocoles.

Les données des valeurs de registre doivent être `tls_1.0`, `tls_1.1` ou `tls_1.2`. Pour activer un seul protocole, spécifiez le même protocole pour les deux valeurs de registre. Si l'une des valeurs de registre n'existe pas ou si ses données ne sont pas définies sur l'un des trois protocoles, les protocoles par défaut seront utilisés.

4 Ajoutez une nouvelle valeur de chaîne (REG_SZ), `SslCiphers`, pour spécifier une liste de suites de chiffrement.

   Saisissez ou collez la liste de suites de chiffrement dans le champ de données de la valeur de registre. Par exemple,

   ```
   ECDHE-RSA-AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
   ```

5 Redémarrez VMware Blast de service Windows.

Pour reprendre l'utilisation de la liste de chiffrements par défaut, supprimez la valeur de registre `SslCiphers` et redémarrez VMware Blast de service Windows. Ne supprimez pas simplement la partie données de la valeur, car l'agent HTML Access traitera alors tous les chiffrements comme étant inacceptables, conformément à la définition de format de la liste de chiffrements OpenSSL.

Lorsque l'agent HTML Access démarre, il écrit les informations sur le protocole et le chiffrement dans son fichier journal. Vous pouvez examiner le fichier journal pour voir les valeurs qui sont appliquées.

Les protocoles et les suites de chiffrement par défaut pourront changer à l'avenir en fonction de l'évolution des meilleures pratiques de VMware concernant la sécurité du réseau.

Configurer Unity Touch

Vous pouvez configurer une liste d'applications favorites par défaut qui apparaît dans la barre latérale d'Unity Touch, et vous pouvez activer ou désactiver la fonction Unity Touch après son installation.

Configurer les applications préférées affichées par Unity Touch

Grâce à la fonctionnalité Unity Touch, les utilisateurs de tablettes et de smartphones peuvent naviguer rapidement vers une application ou un fichier d'un poste de travail Horizon View à partir d'une barre latérale Unity Touch. Même si les utilisateurs peuvent spécifier les applications préférées qui apparaissent dans la barre latérale, pour une utilisation plus aisée, les administrateurs peuvent configurer une liste d'applications préférées par défaut.

Si vous utilisez des pools de postes de travail flottants, les applications et fichiers préférés spécifiés par les utilisateurs seront perdus à chaque déconnexion du poste de travail, sauf si les profils d'utilisateur itinérants sont activés dans Active Directory.

La liste par défaut des applications préférées reste utilisable lorsqu'un utilisateur se connecte pour la première fois à un poste de travail sur lequel Unity Touch est activé. Mais si l'utilisateur configure sa propre liste d'applications préférées, la liste par défaut sera ignorée. La liste d'applications préférées de l'utilisateur est conservée dans le profil itinérant de l'utilisateur et sera disponible lorsque l'utilisateur se connecte à d'autres postes de travail d'un pool flottant ou persistant.

Si vous créez une liste d'applications préférées par défaut et qu'une ou plusieurs applications ne sont pas installées sur le système d'exploitation du poste de travail Horizon View, ou que les chemins de ces applications sont introuvables dans le menu Démarrer, les applications n'apparaissent pas dans la liste des applications préférées. Vous pouvez utiliser ce comportement pour configurer une liste de référence par défaut des applications préférées pouvant être appliquée à plusieurs images de machine virtuelle ayant différents ensembles d'applications installées.

Par exemple, si Microsoft Office 2010 et Microsoft Visio sont installés sur une machine virtuelle, et que Windows Powershell et VMware vSphere Client sont installés sur une deuxième machine virtuelle, vous pouvez créer une liste comprenant les quatre applications. Seules les applications installées apparaissent en tant qu'applications préférées par défaut sur chaque poste de travail.

Il existe d'autres méthodes permettant de spécifier une liste d'applications préférées par défaut :

- Ajouter une valeur au registre Windows sur les machines virtuelles de poste de travail

- Créer un package d'installation administrative à partir du programme d'installation de Remote Experience Agent et distribuer le package sur les machines virtuelles
- Exécuter le programme d'installation de Remote Experience Agent à partir de la ligne de commande sur les machines virtuelles

---

Remarque Unity Touch suppose que les raccourcis des applications sont situés dans le dossier Programmes du menu **Démarrer**. Si un raccourci est situé en dehors du dossier Programmes, ajoutez le préfixe **`Programs`** au chemin du raccourci. Par exemple, `Windows Update.lnk` se trouve dans le dossier `ProgramData\Microsoft\Windows\Menu Démarrer`. Pour publier ce raccourci sous forme d'application préférée par défaut, ajoutez le préfixe **`Programs`** au chemin du raccourci. Par exemple : `"Programs/Windows Update.lnk"`.

Prérequis

- Vérifiez que Remote Experience Agent est installé sur la machine virtuelle.
- Vérifiez que vous disposez des droits d'administration sur la machine virtuelle. Pour cette procédure, vous devrez peut-être modifier un paramètre de registre.
- Si vous disposez de pools de postes de travail flottants, utilisez Active Directory pour configurer les profils d'utilisateur itinérants. Suivez les instructions fournies par Microsoft.

  Les utilisateurs de postes de travail de pools flottants pourront consulter leur liste d'applications et de fichiers préférés à chaque connexion.

Procédure

- (Facultatif) Créez une liste d'applications préférées par défaut en ajoutant une valeur au registre Windows.

  a Ouvrez `regedit` et accédez au paramètre de registre `HKLM\Software\VMware, Inc.\VMware Unity`.

  Sur une machine virtuelle 64 bits, accédez au dossier `HKLM\Software\Wow6432Node\VMware, Inc.\VMware Unity`.

  b Créez une valeur de chaîne appelée `FavAppList`.

  c Spécifiez les applications préférées par défaut.

  Utilisez le format suivant pour spécifier les chemins de raccourci vers les applications utilisées dans le menu Démarrer.

  `path-to-app-1|path-to-app-2|path-to-app-3|…`

  Par exemple :

  ```
  Programs/Accessories/Accessibility/Speech Recognition.lnk|Programs/VMware/VMware vSphere Client.lnk|Programs/Microsoft Office/Microsoft Office 2010 Tools/Microsoft Office 2010 Language Preferences.lnk
  ```

- (Facultatif) Créez une liste d'applications préférées par défaut en créant un package d'installation administrative à partir du programme d'installation de Remote Experience Agent.

  a A partir de la ligne de commande, utilisez le format suivant pour créer le package d'installation administrative.

  ```
  VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s /a /v"/qn
  TARGETDIR=""a network share to store the admin install package""
  UNITY_DEFAULT_APPS=""the list of default favorite apps that should be set in the
  registry"""
  ```

  Par exemple :

  ```
  VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s /a /v"/qn
  TARGETDIR=""\\foo-installer-share\ViewFeaturePack\""
  UNITY_DEFAULT_APPS=""Programs/Accessories/Accessibility/Ease of Access.lnk|
  Programs/Accessories/System Tools/Character Map.lnk|Programs/Accessories/Windows
  PowerShell/Windows PowerShell.lnk|Programs/Internet Explorer (64-bit).lnk|
  Programs/Google Chrome/Google Chrome.lnk|Programs/iTunes/iTunes.lnk|Programs/Microsoft
  Office/Microsoft SharePoint Workspace 2010.lnk|Programs/PuTTY/PuTTY.lnk|
  Programs/Skype/Skype.lnk|Programs/WebEx/Productivity Tools/WebEx Settings.lnk|"""
  ```

  b Distribuez le package d'installation administrative à partir du partage de réseau vers les machines virtuelles de poste de travail à l'aide d'une méthode de déploiement MSI (Microsoft Windows Installer) standard utilisée dans votre organisation.

- (Facultatif) Créez une liste d'applications préférées par défaut en exécutant le programme d'installation de Remote Experience Agent directement sur une ligne de commande d'une machine virtuelle.

  Utilisez le format suivant.

  ```
  VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s /v"/qn
  UNITY_DEFAULT_APPS=""the list of default favorite apps that should be set in the registry"""
  ```

  Remarque La commande précédente combine l'installation de Remote Experience Agent avec la spécification de la liste d'applications préférées par défaut. Vous n'avez pas à installer Remote Experience Agent avant d'exécuter cette commande.

Suivant

Si vous avez effectué cette tâche directement sur une machine virtuelle (en modifiant le registre Windows ou en installant Remote Experience Agent à partir de la ligne de commande), vous devez déployer la machine virtuelle nouvellement configurée. Vous pouvez créer un snapshot ou un modèle et créer un pool de postes de travail Horizon View ou recomposer un pool existant. Vous pouvez également créer une stratégie de groupe Active Directory pour déployer la nouvelle configuration.

Activer/désactiver Unity Touch

Lorsque vous installez Remote Experience Agent, l'option d'installation d'Unity Touch est sélectionnée par défaut et la fonctionnalité est activée. Vous pouvez désactiver ou réactiver la fonctionnalité Unity Touch sur les postes de travail virtuels sélectionnés en définissant une valeur d'une clé de registre Windows sur ces postes de travail.

Vous pouvez utiliser le registre pour activer Unity Touch seulement si elle a été installée par le programme d'installation de Remote Experience Agent, puis désactivée via le registre. Si Unity Touch n'a jamais été installée, c.-à-d., si l'option était désactivée lorsque vous avez installé Remote Experience Agent, puis vous avez défini la valeur de registre pour activer Unity Touch, certaines fonctions d'Unity Touch ne fonctionneront pas correctement.

Procédure

1 Lancez l'éditeur de registre Windows sur le poste de travail virtuel.

2 Accédez à la clé de registre de Windows qui contrôle Unity Touch.

Option	Description
Windows 7 64 bits	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware Unity\enabled = value`
Windows 7 32 bits	`HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware Unity\enabled = value`

3 Entrez la valeur pour activer ou désactiver Unity Touch.

Option	Valeur
Désactivé	`0`
Activé	`1`

Par défaut, cette valeur est `1`.

Configurer la redirection d'URL Flash pour le flux de multidiffusion ou monodiffusion

Les clients peuvent désormais utiliser Adobe Media Server et la multidiffusion ou la monodiffusion pour diffuser des événements vidéo en direct dans un environnement d'infrastructure de poste de travail virtuel (VDI). Pour la multidiffusion ou la monodiffusion vidéo en direct dans un environnement VDI, le flux de données multimédia doit être envoyé directement de la source multimédia aux points de terminaison, en contournant les postes de travail virtuels. La fonction redirection d'URL Flash prend en charge cette fonctionnalité en interceptant et en réorientant le fichier Shockwave Flash (SWF) du poste de travail virtuel au point de terminaison client.

La fonctionnalité de redirection d'URL Flash utilise un JavaScript incorporé dans le HTML d'une page Web par l'administrateur de la page Web. Chaque fois qu'un utilisateur de poste de travail virtuel clique sur le lien de l'URL désigné à partir d'une page Web, JavaScript intercepte et redirige le fichier SWF à partir de la session du poste de travail virtuel au point de terminaison client. Le point de terminaison ouvre alors un projecteur Flash local à l'extérieur de la session de poste de travail virtuel et lance la lecture du flux multimédia en local.

Pour configurer la redirection d'URL Flash, vous devez configurer le HTML de votre page Web et vos périphériques client.

Procédure

1 Vérifier que la fonctionnalité redirection d'URL flash est installée page 34

Avant d'utiliser cette fonctionnalité, vérifiez que Remote Experience Agent avec l'option redirection d'URL Flash est installé et tourne sur vos postes de travail virtuels.

2 Configurer les pages Web qui fournissent des flux de multidiffusion ou de monodiffusion page 34

Pour permettre la redirection d'URL Flash, vous devez inclure une commande JavaScript dans les pages Web MIME HTML (MHTML) qui fournissent les liens vers les flux de multidiffusion ou de monodiffusion. Les utilisateurs peuvent afficher ces pages Web dans les navigateurs de leurs postes de travail virtuels pour accéder aux flux vidéo.

3 Configurer des périphériques client pour la redirection d'URL Flash page 35

La fonctionnalité redirection d'URL Flash redirige le fichier SWF à partir des postes de travail virtuels vers les machines client. Pour que ces périphériques client puissent lire des vidéos Flash à partir d'un flux de multidiffusion ou de monodiffusion, vous devez vérifier qu'Adobe Flash Player est installé sur les périphériques client. Les clients doivent également avoir une connectivité IP vers la source multimédia.

4 Activer/désactiver la redirection d'URL Flash page 35

Cette fonctionnalité est activée lorsque vous installez Remote Experience Agent tout en sélectionnant l'option d'installation de la redirection d'URL Flash. Vous pouvez désactiver ou réactiver la fonctionnalité redirection d'URL Flash sur les postes de travail virtuels sélectionnés en définissant une valeur d'une clé de registre Windows sur ces postes de travail.

Vérifier que la fonctionnalité redirection d'URL flash est installée

Avant d'utiliser cette fonctionnalité, vérifiez que Remote Experience Agent avec l'option redirection d'URL Flash est installé et tourne sur vos postes de travail virtuels.

La fonctionnalité de redirection d'URL Flash doit être présente sur chaque poste de travail avec lequel vous souhaitez prendre en charge la redirection de multidiffusion ou de monodiffusion. Pour les instructions d'installation de Remote Experience Agent, reportez-vous à « Installation et déploiement de Remote Experience Agent sur les postes de travail Horizon View », page 15.

Procédure

1 Démarrez une session de poste de travail virtuel qui utilise PCoIP.

2 Ouvrez le Gestionnaire des tâches.

3 Vérifiez que le processus `ViewMPServer.exe` est en cours d'exécution sur le poste de travail.

Configurer les pages Web qui fournissent des flux de multidiffusion ou de monodiffusion

Pour permettre la redirection d'URL Flash, vous devez inclure une commande JavaScript dans les pages Web MIME HTML (MHTML) qui fournissent les liens vers les flux de multidiffusion ou de monodiffusion. Les utilisateurs peuvent afficher ces pages Web dans les navigateurs de leurs postes de travail virtuels pour accéder aux flux vidéo.

En outre, vous pouvez personnaliser le message d'erreur en anglais que voient les utilisateurs en cas de problème avec la redirection d'URL Flash. Choisissez cette option si vous souhaitez afficher un message d'erreur dans la langue locale pour les utilisateurs finaux. Vous devez incorporer la configuration `var vmwareScriptErroMessage` ainsi que votre chaîne de texte localisé dans la page Web MHTML.

Prérequis

Assure-vous que la bibliothèque `swfobject.js` est importée dans la page Web MHTML.

Procédure

1 Insérez la commande JavaScript `viewmp.js` dans la page Web MHTML.

Par exemple : `<script type="text/javascript" src="http://localhost:33333/viewmp.js"></script>`

2 (Facultatif) Personnalisez le message d'erreur de redirection d'URL Flash envoyé aux utilisateurs finaux.

Par exemple : `"var vmwareScriptErroMessage=`*`message d'erreur localisé`*`"`

3 Veillez à incorporer la commande JavaScript `viewmp.js` et personnalisez éventuellement le message d'erreur de redirection d'URL Flash avant que le fichier ShockWave Flash (SWF) ne soit importé dans la page Web MHTML.

Lorsqu'un utilisateur affiche la page Web dans un poste de travail virtuel, la commande JavaScript `viewmp.js` invoque le mécanisme de redirection d'URL Flash qui redirige le fichier SWF du poste de travail vers le périphérique d'hébergement client.

Configurer des périphériques client pour la redirection d'URL Flash

La fonctionnalité redirection d'URL Flash redirige le fichier SWF à partir des postes de travail virtuels vers les machines client. Pour que ces périphériques client puissent lire des vidéos Flash à partir d'un flux de multidiffusion ou de monodiffusion, vous devez vérifier qu'Adobe Flash Player est installé sur les périphériques client. Les clients doivent également avoir une connectivité IP vers la source multimédia.

Remarque Avec la redirection d'URL Flash, le flux de multidiffusion ou de monodiffusion est redirigé vers les périphériques clients qui pourraient être en dehors du pare-feu de votre organisation. Vos clients doivent avoir accès au serveur Web d'Adobe qui héberge le fichier SWF qui initie les flux de multidiffusion ou de monodiffusion. Si nécessaire, configurez votre pare-feu pour ouvrir les ports appropriés afin de permettre aux périphériques client d'accéder à ce serveur.

Procédure

- Installer Adobe Flash Player sur vos périphériques client.

Système d'exploitation	Action
Windows	Installez Adobe Flash Player 10.1 ou versions ultérieures pour Internet Explorer.
Linux	a Installez le fichier `libexpat.so.0` ou assurez-vous que ce fichier est déjà installé. Vérifiez que le fichier est installé dans le répertoire `/usr/lib` ou `/usr/local/lib`. b Installez le fichier `libflashplayer.so`, ou assurez-vous que ce fichier est déjà installé. Assurez-vous que le fichier est installé dans le répertoire du plug-in Flash approprié de votre système d'exploitation Linux. c Installez le programme `wget`, ou assurez-vous que le fichier de ce programme est déjà installé.

Activer/désactiver la redirection d'URL Flash

Cette fonctionnalité est activée lorsque vous installez Remote Experience Agent tout en sélectionnant l'option d'installation de la redirection d'URL Flash. Vous pouvez désactiver ou réactiver la fonctionnalité redirection d'URL Flash sur les postes de travail virtuels sélectionnés en définissant une valeur d'une clé de registre Windows sur ces postes de travail.

Procédure

1 Lancez l'éditeur de registre Windows sur le poste de travail virtuel.

2 Accédez à la clé de registre de Windows qui contrôle la redirection d'URL Flash.

Option	Description
Windows 7 64 bits	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware ViewMP\enabled = value`
Windows 7 32 bits	`HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware ViewMP\enabled = value`

3 Entrez la valeur pour activer ou désactiver la redirection d'URL Flash.

Option	Valeur
Désactivé	`0`
Activé	`1`

Par défaut, cette valeur est `1`.

Configurer l'Audio/Vidéo en temps réel

Une fois installée, la fonctionnalité Audio/Vidéo en temps réel fonctionne sur vos postes de travail Horizon View sans aucune configuration supplémentaire. Il est recommandé d'utiliser les valeurs par défaut de la fréquence et de la résolution d'images pour la plupart des périphériques et applications courantes.

Vous pouvez configurer les paramètres de stratégie de groupe pour modifier ces valeurs par défaut et les adapter à des applications, webcams ou environnements particuliers. Reportez-vous à la section « Configuration des paramètres de stratégie de groupe de l'Audio/Vidéo en temps réel », page 42.

Si vous disposez de plusieurs webcams et périphériques d'entrée audio intégrés ou connectés à vos ordinateurs client, vous pouvez configurer des webcams et des périphériques d'entrée audio préférés qui seront redirigés vers vos postes de travail. Reportez-vous à la section « Sélection de webcams et microphones préférés », page 37.

Remarque Vous pouvez sélectionner un périphérique audio préféré, mais aucune autre option de configuration audio n'est disponible.

Lorsque les images de la webcam et l'entrée audio sont redirigées vers un poste de travail distant, vous ne pouvez pas accéder à la webcam et aux périphériques audio de l'ordinateur local. Inversement, lorsque ces périphériques sont utilisés sur l'ordinateur local, vous ne pouvez pas y accéder via le poste de travail distant.

L'Audio/Vidéo en temps réel n'est pas pris en charge par les postes de travail en mode local.

Pour plus d'informations sur les applications prises en charge, consultez l'article de la base de connaissances VMware *Directives pour l'utilisation de l'Audio/Vidéo en temps réel avec des applications tierces sur les postes de travail Horizon View*, à l'adresse http://kb.vmware.com/kb/2053754.

Garantir que l'Audio/Vidéo en temps réel est utilisée plutôt que la redirection USB

L'Audio/Vidéo en temps réel prend en charge la redirection de la webcam et de l'entrée audio dans des applications de conférence. La redirection USB qui peut être installée avec View Agent ne prend pas en charge la redirection des webcams. Si vous redirigez périphériques d'entrée audio via la redirection USB, le flux audio n'est pas synchronisé correctement avec la vidéo pendant les sessions d'Audio/Vidéo en temps réel, et vous perdez l'avantage de réduction de la bande passante réseau. Vous pouvez prendre des mesures pour garantir que les webcams et les périphériques d'entrée audio soient redirigés vers vos postes de travail via l'Audio/Vidéo en temps réel et non via la redirection USB.

Si vos postes de travail sont configurés avec la redirection USB, les utilisateurs finaux peuvent se connecter et afficher leurs périphériques USB connectés en local en sélectionnant l'option **Connecter le périphérique USB** dans la barre de menu de VMware Horizon View Client.

Si un utilisateur final sélectionne un périphérique USB dans la liste **Connecter le périphérique USB**, celui-ci devient inutilisable pour la vidéoconférence ou l'audioconférence. Par exemple, si un utilisateur effectue un appel Skype, l'image vidéo peut ne pas apparaître ou le flux audio peut être dégradé. Si un utilisateur sélectionne un périphérique au cours d'une session de conférence, la webcam ou la redirection audio sera perturbée.

Pour masquer ces appareils des utilisateurs finaux et prévenir d'éventuelles perturbations, vous pouvez configurer les paramètres de stratégie de groupe de redirection USB pour désactiver l'affichage des webcams et des périphériques d'entrée audio dans VMware Horizon View Client.

En particulier, vous pouvez créer des règles de filtrage de redirection USB pour Horizon View Agent et spécifier les noms des familles des périphériques `d'entrée audio` et `vidéo` à désactiver. Pour plus d'informations sur la configuration des stratégies de groupe et la définition des règles de filtrage pour la redirection USB, reportez-vous à « Utilisation des stratégies pour contrôler la redirection USB » dans le document *Administration de VMware Horizon View*.

Avertissement Si vous ne configurez pas des règles de filtrage de redirection USB pour désactiver les familles de périphériques USB, il convient d'informer vos utilisateurs finaux qu'ils ne peuvent pas sélectionner des webcams ou des périphériques audio dans la liste **Connecter le périphérique USB** dans la barre de menu de VMware Horizon View Client.

Sélection de webcams et microphones préférés

Si un ordinateur client dispose de plus d'une webcam et d'un microphone, vous pouvez configurer une webcam et un microphone par défaut que la fonctionnalité audio/vidéo en temps réel redirige vers le poste de travail. Ces périphériques peuvent être intégrés ou connectés à l'ordinateur client local.

Sur un ordinateur client Windows, vous sélectionnez une webcam préférée en définissant une clé de registre. Sur un ordinateur client Linux, vous pouvez spécifier une webcam ou un microphone préféré en modifiant un fichier de configuration. La fonctionnalité audio/vidéo en temps réel redirige la webcam préférée si elle est disponible. Autrement, la fonctionnalité audio/vidéo en temps réel utilise la première webcam énumérée par le système.

Pour sélectionner un microphone par défaut, vous pouvez configurer le Contrôle du son dans le système d'exploitation Windows ou Linux de l'ordinateur client.

Sélectionner une webcam préférée sur un système client Windows

Avec la fonctionnalité Audio-vidéo en temps réel, une seule des webcams de votre système client est utilisée sur votre poste de travail View. Vous pouvez définir une valeur de clé de registre pour spécifier la webcam préférée.

La webcam préférée est utilisée sur le poste de travail View si elle est disponible, autrement une autre webcam sera utilisée.

Prérequis

- Assure-vous que vous disposez d'une webcam USB installée et opérationnelle sur votre système client.
- Assure-vous que vous utilisez le protocole d'affichage PCoIP pour votre poste de travail View.

Procédure

1 Connectez la webcam que vous souhaitez utiliser.

2 Démarrez un appel, puis arrêtez l'appel.

Ce processus crée un fichier journal.

3 Ouvrez le fichier journal de débogage avec un éditeur de texte.

Système d'exploitation	Emplacement du fichier journal
Windows XP	`C:\Documents and Settings\username\Local Settings\Application Data\VMware\VDM\Logs\debug-20`*`YY-MM-DD-XXXXXX`*`.txt`
Windows 7 ou Windows 8	`C:\Users\%username%\AppData\Local\VMware\VDM\Logs\debug-20`*`YY-MM-DD-XXXXXX`*`.txt`

Le format du fichier journal est `debug-20`*`AA-MM-JJ-XXXXXX`*`.txt`, où 20 *AA* est l'année, *MM*le mois, *JJ* le jour et *XXXXXX* est un nombre.

4 Recherchez `[ViewMMDevRedir] VideoInputBase::LogDevEnum` dans le fichier journal pour trouver les entrées du fichier journal qui fait référence aux webcams connectées.

Voici un extrait du fichier journal identifiant la webcam Microsoft LifeCam HD-5000 :

```
[ViewMMDevRedir] VideoInputBase::LogDevEnum – 2 Device(s) found

[ViewMMDevRedir] VideoInputBase::LogDevEnum – Index=0 Name=Integrated Webcam
UserId=vid_1bcf&pid_2b83&mi_00#7&1b2e878b&0&0000   SystemId=\\?\usb#vid_1bcf&pid_2b83&mi_00#

[ViewMMDevRedir] VideoInputBase::LogDevEnum – Index=1 Name=Microsoft LifeCam HD-5000
UserId=vid_045e&pid_076d&mi_00#8&11811f49&0&0000  SystemId=\\?\usb#vid_045e&pid_076d&mi_00#
```

5 Copiez l'identificateur utilisateur de la webcam préférée.

Par exemple, copiez `vid_045e&pid_076d&mi_00#8&11811f49&0&0000` pour définir Microsoft LifeCam HD-5000 comme webcam par défaut.

6 Lancez l'éditeur du registre (`regedit.exe`) et accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\RTAV`.

7 Collez la partie de l'identificateur de la chaîne de caractères dans la valeur **srcWCamId**.

Par exemple, collez `vid_045e&pid_076d&mi_00#8&11811f49&0&0000` dans **srcWCamId**.

8 Enregistrez vos modifications et quittez le registre.

9 Démarrez un nouvel appel.

Sélectionner une webcam ou un microphone préféré sur un système client Linux

Avec la fonctionnalité Audio/Vidéo en temps réel, si vous disposez de plusieurs webcams et microphones sur votre système client, vous ne pouvez en utiliser qu'un seul sur votre poste de travail View. Pour désigner la webcam et le microphone préférés, vous pouvez modifier un fichier de configuration.

Selon sa disponibilité, la webcam ou le microphone préféré est utilisé sur le poste de travail View ; sinon, une autre webcam ou un autre microphone sera utilisé.

Avec la fonctionnalité Audio/Vidéo en temps réel, les webcams, les périphériques d'entrée audio et les périphériques de sortie audio fonctionnent sans nécessiter l'utilisation de la redirection USB, et la bande passante du réseau nécessaire est considérablement réduite. Les périphériques d'entrée audio analogique sont également pris en charge.

Pour définir les propriétés dans le fichier `/etc/vmware/config` et indiquer un périphérique préféré, vous devez déterminer l'ID du périphérique.

- Pour les webcams, affectez à la propriété `rtav.srcWCamId` la valeur de la description de webcam figurant dans le fichier journal, comme indiqué dans la procédure suivante.
- Pour les périphériques audio, affectez à la propriété `rtav.srcAudioInId` la valeur du champ Pulse Audio `device.description`.

  Recherchez cette valeur dans le fichier journal, comme indiqué dans la procédure suivante.

Prérequis

Selon que vous configurez une webcam préférée, un micro préféré ou les deux, exécutez les tâches préalables appropriées :

- Assure-vous que vous disposez d'une webcam USB installée et opérationnelle sur votre système client.
- Assure-vous que vous disposez d'un microphone USB ou un autre type installé et opérationnel sur votre système client.
- Assure-vous que vous utilisez le protocole d'affichage PCoIP pour votre poste de travail View.

Procédure

1 Lancez le client et démarrez une application de webcam ou de microphone pour déclencher une énumération de périphériques vidéo ou audio dans le journal client.

   a Connectez la webcam ou le périphérique audio que vous souhaitez utiliser.

   b Utilisez la commande `vmware-view` pour démarrer View Client.

   c Démarrez un appel, puis arrêtez-le.

   Ce processus crée un fichier journal.

2 Recherchez les entrées relatives à la webcam ou au microphone.

a Ouvrez le fichier journal de débogage avec un éditeur de texte.

Le fichier journal contenant les messages audio-vidéo en temps réel se trouve dans `/tmp/vmware-<username>/vmware-mks-<pid>.log`. Le fichier journal client est situé dans `/tmp/vmware-<username>/vmware-view-<pid>.log`.

b Recherchez dans le fichier journal les entrées qui renvoient aux webcams et aux microphones raccordés.

L'exemple suivant montre un extrait de la sélection de webcams :

```
main| I120: RTAV: static void VideoInputBase::LogDevEnum() – 3 Device(s) found
main| I120: RTAV: static void VideoInputBase::LogDevEnum() – Name=UVC Camera (046d:
0819)   UserId=UVC Camera (046d:0819)#/sys/devices/pci0000:00/0000:00:1a.
7/usb1/1–3/1–3.4/1–3.4.5   SystemId=/dev/video1
main| I120: RTAV: static void VideoInputBase::LogDevEnum() – Name=gspca main driver
UserId=gspca main driver#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1–3/1–3.4/1–3.4.7
SystemId=/dev/video2
main| I120: RTAV: static void VideoInputBase::LogDevEnum() –
Name=Microsoft® LifeCam HD–6000 for Notebooks   UserId=Microsoft® LifeCam HD–6000 for
Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1–3/1–3.6   SystemId=/dev/video0
main| W110: RTAV: static bool AudioCaptureLin::EnumCaptureDevices(MMDev::DeviceList&) –
enumeration data unavailable
```

L'exemple suivant montre un extrait de la sélection de périphériques audio et le niveau sonore actuel de chacun d'entre eux :

```
vthread–18| I120: RTAV: bool AudioCaptureLin::TriggerEnumDevices() – Triggering
enumeration
vthread–18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) – PulseAudio Get Source (idx=1 'alsa_output.usb–
Logitech_Logitech_USB_Headset–00–Headset.analog–stereo.monitor' 'Monitor of Logitech USB
Headset Analog Stereo')

vthread–18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) – channel:0 vol:65536
vthread–18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) – channel:1 vol:65536
vthread–18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) – PulseAudio Get Source (idx=2 'alsa_input.usb–
Logitech_Logitech_USB_Headset–00–Headset.analog–mono' 'Logitech USB Headset Analog Mono')

vthread–18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) – channel:0 vol:98304
vthread–18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) – PulseAudio Get Source (idx=3 'alsa_output.usb–
Microsoft_Microsoft_LifeChat_LX–6000–00–LX6000.analog–stereo.monitor' 'Monitor of
Microsoft LifeChat LX–6000 Analog Stereo')

vthread–18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) – channel:0 vol:65536
```

Des avertissements s'affichent si l'un des niveaux sonores source du périphérique sélectionné ne respecte pas les critères PulseAudio lorsque la source n'est pas définie à 100 % (0 dB) ou si le périphérique source sélectionné est muet :

```
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel volume: 0:  67%
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel is muted
```

3 Copiez la description du périphérique et utilisez-la pour définir la propriété appropriée dans le fichier `/etc/vmware/config`.

Pour un exemple de webcam, copiez `Microsoft® LifeCam HD-6000 for Notebooks` afin de désigner la webcam Microsoft comme webcam préférée et définissez la propriété comme suit :

```
rtav.srcWCamId="Microsoft® LifeCam HD-6000 for Notebooks"
```

Dans cet exemple, vous pourriez aussi définir la propriété sur `rtav.srcWCamId="Microsoft"`.

Pour un exemple de périphérique audio, copiez `Logitech USB Headset Analog Mono` pour désigner le casque Logitech comme périphérique audio préféré et définissez la propriété comme suit :

```
rtav.srcAudioInId="Logitech USB Headset Analog Monoo"
```

4 Enregistrez les modifications et fermez le fichier de configuration `/etc/vmware/config`.

5 Démarrez un nouvel appel.

Sélectionner un microphone par défaut sur un système client Windows

Si plusieurs microphones sont connectés à votre système client, un seul d'entre eux peut être utilisé sur votre poste de travail View. Pour spécifier le microphone par défaut, vous pouvez utiliser le contrôle du son de votre système client.

Avec la fonctionnalité Audio-vidéo en temps réel, les périphériques d'entrée audio et les périphériques de sortie audio fonctionnent sans nécessiter l'utilisation de la redirection USB, et la bande passante du réseau nécessaire est considérablement réduite. Les périphériques d'entrée audio analogique sont également pris en charge.

Important Si vous utilisez un microphone USB, ne pas le connecter via le menu **Connecter un périphérique USB** d'Horizon View Client. L'utilisation de redirection de périphériques USB dégrade les performances de la fonctionnalité Audio/Vidéo en temps réel.

Prérequis

- Assure-vous que vous disposez d'un microphone USB ou un autre type installé et opérationnel sur votre système client.
- Assure-vous que vous utilisez le protocole d'affichage PCoIP pour votre poste de travail View.

Procédure

1 Si vous êtes en cours d'un appel, arrêtez l'appel.

2 Cliquez avec le bouton droit sur l'icône haut-parleur dans votre barre d'état système et sélectionnez **Périphériques d'enregistrement**.

Vous pouvez également ouvrir le Contrôle du son à partir de du Panneau de configuration et cliquer sur l'onglet **Enregistrement**.

3 Dans l'onglet **Enregistrement** de la boîte de dialogue Son, cliquez avec le bouton droit sur le microphone que vous préférez utiliser.

4 Sélectionnez **Définir comme périphérique par défaut** et cliquez sur **OK**.

5 Démarrez un nouvel appel à partir de votre poste de travail View.

Sélectionner un microphone par défaut sur un système client Linux

Si plusieurs microphones sont connectés à votre système client, un seul d'entre eux peut être utilisé sur votre poste de travail View. Pour spécifier le microphone par défaut, vous pouvez utiliser le contrôle du son de votre système client.

Avec la fonctionnalité Audio-vidéo en temps réel, les périphériques d'entrée audio et les périphériques de sortie audio fonctionnent sans nécessiter l'utilisation de la redirection USB, et la bande passante du réseau nécessaire est considérablement réduite. Les périphériques d'entrée audio analogique sont également pris en charge.

Cette procédure explique comment sélectionner un microphone par défaut depuis l'interface utilisateur du système client. Les administrateurs peuvent également configurer un microphone préféré en modifiant un fichier de configuration. Reportez-vous à la section « Sélectionner une webcam ou un microphone préféré sur un système client Linux », page 39.

Prérequis

- Assure-vous que vous disposez d'un microphone USB ou un autre type installé et opérationnel sur votre système client.
- Assure-vous que vous utilisez le protocole d'affichage PCoIP pour votre poste de travail View.

Procédure

1 Dans l'interface graphique Ubuntu, sélectionnez **Système > Préférences > Son**.

Vous pouvez également cliquer sur l'icône **Son** à droite de la barre d'outils en haut de l'écran.

2 Cliquez sur l'onglet **Entrée** dans la boîte de dialogue Préférences de son.

3 Sélectionnez le périphérique préféré et cliquez sur **Fermer**.

Configuration des paramètres de stratégie de groupe de l'Audio/Vidéo en temps réel

Vous pouvez configurer les paramètres de stratégie de groupe qui permettent de contrôler le comportement de l'Audio/Vidéo en temps réel (RTAV) sur vos postes de travail Horizon View. Ces paramètres définissent la fréquence et la résolution d'images maximales d'une webcam virtuelle. Ces paramètres vous permettent de définir la bande passante maximale qu'un utilisateur peut utiliser. Un paramètre supplémentaire permet de désactiver/activer la fonctionnalité Audio/Vidéo en temps réel (RTAV).

Vous n'avez pas à configurer ces paramètres de stratégie. L'Audio/Vidéo en temps réel utilise la fréquence et la résolution d'images qui sont fixées pour la webcam des systèmes client. Les paramètres par défaut sont recommandés pour la plupart des applications webcam et audio.

Pour voir des exemples d'utilisation de bande passante pour l'Audio/Vidéo en temps réel, reportez-vous à « Bande passante de l'Audio/Vidéo en temps réel », page 45.

Ces paramètres de stratégie affectent vos postes de travail Horizon View et non les systèmes client auxquels les périphériques physiques sont connectés. Pour configurer ces paramètres sur vos postes de travail, ajoutez le fichier de modèle d'administration (ADM) de stratégie de groupe pour l'Audio/Vidéo en temps réel (RTAV) dans Active Directory.

Pour plus d'informations sur la configuration des paramètres sur les systèmes clients, consultez l'article de la base de connaissances VMware *Configuration de la fréquence et de la résolution d'images pour l'Audio/Vidéo en temps réel sur les clients Horizon View*, à l'adresse http://kb.vmware.com/kb/2053644.

Ajouter le modèle d'administration (ADM) pour l'Audio/Vidéo en temps réel (RTAV) dans Active Directory et configurer les paramètres

Horizon View fournit un fichier de modèle d'administration (ADM) pour l'Audio/Vidéo en temps réel (RTAV), `vdm_agent_rtav.adm`, sur la page de téléchargement des produits VMware. Vous pouvez ajouter les paramètres de stratégie aux objets de stratégie de groupe (GPO) dans Active Directory dans ce fichier ADM et configurer les paramètres dans l'Éditeur d'objets de stratégie de groupe.

Pour des raisons de simplicité, le fichier RTAV ADM est livré dans un fichier zip avec tous les autres fichiers ADM d'Horizon View.

Le fichier RTAV ADM est nouveau dans cette version Feature Pack. Les autres fichiers ADM sont les mêmes versions que celles installées avec Horizon View 5,3 sur le serveur de connexion View dans le dossier *`install_directory`*`\VMware\VMware View\Server\extras\GroupPolicyFiles`. Vous n'avez pas à réinstaller les autres fichiers ADM si vous les avez déjà ajoutés à Active Directory lors d'installations ou mises à niveau vers Horizon View 5.3.

Prérequis

- Vérifiez que Remote Experience Agent avec l'option RTAV est installé sur vos postes de travail. Les paramètres n'ont aucun effet si RTAV n'est pas installé. Reportez-vous à la section « Installation et déploiement de Remote Experience Agent sur les postes de travail Horizon View », page 15.
- Vérifiez que les objets de stratégie de groupe (GPO) dans Active Directory sont créés pour les paramètres de stratégie de groupe RTAV. Les objets de stratégie de groupe (GPO) doivent être liés à l'unité d'organisation (UO) qui contient vos postes de travail. Pour des informations générales sur la configuration des paramètres de stratégie de groupe dans Active Directory d' Horizon View, reportez-vous à « Configuration des stratégies » dans le document *Administration de VMware Horizon View*.
- Vérifiez que les composants logiciels enfichables Microsoft MMC (Microsoft Management Console) et l'Éditeur d'objets de stratégie de groupe sont disponibles sur votre serveur Active Directory.
- Familiarisez-vous avec les paramètres de stratégie de groupe RTAV. Reportez-vous à la section « Paramètres de stratégie de groupe de l'Audio/Vidéo en temps réel », page 44.

Procédure

1 Téléchargez le fichier zip ADM Horizon View fourni sur la page de téléchargement des produits VMware.

   Le nom du fichier zip est `VMware-Horizon-View-GPO-Bundle-`*`y.y.y-xxxxxx`*`.zip`, où *y.y.y.* est le numéro de version et *xxxxxx* est le numéro de build.

2 Décompressez le fichier zip et copiez le fichier RTAV ADM, `vdm_agent_rtav.adm`, sur votre serveur Active Directory.

3 Sur le serveur Active Directory, modifiez les objets de stratégie de groupe (GPO) en sélectionnant **Démarrer > Outils d'administration > Gestion de stratégie de groupe**, cliquez avec le bouton droit sur GPO et sélectionnez **Édition**.

4 Dans l'Éditeur d'objets de stratégie de groupe, cliquez avec le bouton droit sur le dossier **Configuration de l'ordinateur > Modèles d'administration**, puis sélectionnez **Ajouter/supprimer des modèles**.

5 Cliquez sur **Ajouter**, localisez le fichier `vdm_agent_rtav.adm` et cliquez sur **Ouvrir**.

6 Cliquez sur **Fermer** pour appliquer les paramètres de stratégie dans le fichier de modèle d'administration pour les objets de stratégie de groupe (GPO).

   Les paramètres se trouvent dans le dossier **Configuration de l'ordinateur > Modèles d'administration > Modèles d'administration classiques > Configuration de VMware View Agent > Configuration de RTAV View**.

7 Configurer les paramètres de stratégie de groupe RTAV.

Paramètres de stratégie de groupe de l'Audio/Vidéo en temps réel

Les paramètres de stratégie de groupe de l'Audio/Vidéo en temps réel (RTAV) permettent de contrôler la fréquence et la résolution d'images maximales d'une webcam virtuelle. Un paramètre supplémentaire permet de désactiver/activer la fonctionnalité Audio/Vidéo en temps réel (RTAV). Ces paramètres de stratégie affectent vos postes de travail Horizon View et non les systèmes client auxquels les périphériques physiques sont connectés.

Si vous ne configurer pas les paramètres de stratégie de groupe RTAV, ce sont les valeurs qui sont définies sur les systèmes clients qui seront utilisées par RTAV. Sur les systèmes clients, la fréquence d'images par défaut de la webcam est de 15 images par seconde. La résolution de l'image par défaut de la webcam est de 320x240 pixels.

Les paramètres de stratégie de groupe RTAV déterminent les valeurs maximales pouvant être utilisées. La fréquence et la résolution d'images définies sur les systèmes client sont des valeurs absolues. Par exemple, si vous configurez les paramètres RTAV pour une résolution d'image maximale de 640x480 pixels, la webcam utilise une résolution définie dans le client, mais ne dépasse pas 640x480 pixels. Si vous fixez la résolution de l'image sur le client à une valeur supérieure à 640x480 pixels, la résolution du client sera plafonnée à 640x480 pixels.

La résolution maximale de 1920x1080 à 25 images par seconde, des paramètres stratégie de groupe, ne peut pas être atteinte par toutes les configurations. La fréquence d'images maximale que votre configuration ne peut atteindre pour une résolution donnée dépend de la webcam utilisée, le matériel du système client, le matériel virtuel de View Agent et la bande passante disponible.

Paramètre de stratégie de groupe	Description
Désactiver RTAV	Lorsque ce paramètre est activé, la fonction Audio/vidéo en temps réel est désactivée. Lorsque ce paramètre n'est pas configuré ou désactivé, la fonction Audio/vidéo en temps réel est activée. Ce paramètre se trouve dans le dossier **Configuration RTAV View**.
Fréquence d'images max.	Détermine la fréquence d'images maximale utilisée par la webcam pour capturer des images. Vous pouvez utiliser ce paramètre pour limiter la fréquence d'images de la webcam dans des environnements réseaux à faible bande passante. La valeur minimale est d'une image par seconde. La valeur minimale est de 25 images par seconde. Lorsque ce paramètre n'est pas configuré ou désactivé, aucune fréquence d'images n'est fixée. L'Audio/Vidéo en temps réel utilise la fréquence d'images sélectionnée pour la webcam sur le système client. Par défaut, les webcams client ont une fréquence d'images de 15 images par seconde. Si aucun paramètre n'est configuré sur le système client et le paramètre **Fréquence d'images max.** n'est pas configuré ou désactivé, la webcam capture 15 images par seconde. Ce paramètre se trouve dans le dossier **Configuration RTAV View > Paramètres RTAV Webcam View**.

Paramètre de stratégie de groupe	Description
Résolution - Largeur d'images maximale en pixels	Détermine la largeur maximale, en pixels, des cadres d'images capturés par la webcam. En fixant une faible valeur à la largeur d'image maximale, vous pouvez diminuer la résolution des images capturées, ce qui peut améliorer la qualité d'image dans des environnements réseaux à faible bande passante. Lorsque ce paramètre n'est pas configuré ou désactivé, aucune largeur d'image maximale n'est fixée. RTAV utilise la largeur d'image définie sur le système client. La largeur d'image par défaut de la webcam sur un système client est de 320 pixels. La limite maximale pour toute webcam est 1920x1080 pixels. Si vous fixez ce paramètre à une valeur supérieure à 1920 pixels, la largeur de l'image maximale effective sera de 1920 pixels. Ce paramètre se trouve dans le dossier **Configuration RTAV View > Paramètres RTAV Webcam View**.
Résolution - Hauteur d'images maximale en pixels	Détermine la hauteur maximale, en pixels, des cadres d'images capturés par la webcam. En fixant une faible valeur à la hauteur d'image maximale, vous pouvez diminuer la résolution des images capturées, ce qui peut améliorer la qualité d'image dans des environnements réseaux à faible bande passante. Lorsque ce paramètre n'est pas configuré ou désactivé, aucune hauteur d'image maximale n'est fixée. RTAV utilise la hauteur d'image définie sur le système client. La hauteur d'image par défaut de la webcam sur un système client est de 240 pixels. La limite maximale pour toute webcam est 1920x1080 pixels. Si vous fixez ce paramètre à une valeur supérieure à 1080 pixels, la hauteur de l'image maximale effective sera de 1080 pixels. Ce paramètre se trouve dans le dossier **Configuration RTAV View > Paramètres RTAV Webcam View**.

Bande passante de l'Audio/Vidéo en temps réel

La bande passante de l'Audio/Vidéo en temps réel varie en fonction de la résolution et la fréquence d'images de la webcam, et de l'image et des données audio capturées.

Les exemples d'essais présentés dans Tableau 7 mesurent de la bande passante que l'Audio/Vidéo en temps réel utilise dans un environnement Horizon View avec webcam et périphériques d'entrée audio standard. Les essais mesurent la bande passante pour envoyer des données audio et vidéo à partir de Horizon View versHorizon View Agent. La bande passante totale nécessaire pour prendre en charge une session de poste de travail à partir de View Client peut être supérieure à ces valeurs. Dans ces essais, la webcam capture des images à 15 images par seconde pour chaque résolution d'image.

Tableau 7. Exemples de résultats de bande passante pour l'envoi de données Audio/Vidéo en temps réel à partir de Horizon View Client vers Horizon View Agent

Résolution de l'image (largeur x hauteur)	Bande passante utilisée (Kbps)
160 x 120	225
320 x 240	320
640 x 480	600

Gestion de l'accès à la redirection multimédia (MMR) Windows 7

Vous pouvez faire en sorte que la redirection multimédia (MMR) Windows 7 ne soit accessible qu'aux systèmes View Client qui disposent des ressources appropriées et qui sont connectés à Horizon View sur un réseau sécurisé.

Les données MMR sont envoyées sur le réseau sans cryptage au niveau de l'application et peuvent contenir des éléments sensibles, selon le contenu redirigé. Pour éviter que ces données ne soient surveillées sur le réseau, utilisez la fonctionnalité de redirection multimédia uniquement sur un réseau sécurisé.

Vous pouvez désactiver la redirection multimédia si les systèmes clients n'ont pas les ressources suffisantes pour gérer le décodage multimédia local ou si vous souhaitez restreindre l'accès à la redirection multimédia aux seuls systèmes clients fonctionnant sur un réseau sécurisé. Vous pouvez ajouter une stratégie dans View Administrator, **Redirection multimédia (MMR)**, qui vous permet d'activer/désactiver MMR pour les

systèmes clients. Vous pouvez définir la stratégie au niveau global, pour des pools de postes de travail spécifiques ou pour des utilisateurs spécifiques. La stratégie est activée par défaut. La stratégie affecte la MMR des postes de travail Windows 7, Windows XP et Windows Vista. Pour plus de précisions, reportez-vous à « Configuration des stratégies » dans le document *Administration de VMware Horizon View*.

Vérifier que les clients peuvent lancer Windows 7 MMR

Windows 7 MMR utilise l'établissement d'une liaison entre le système Horizon View Client et le poste de travail pour valider les demandes de redirection multimédia. Lorsque certaines conditions réseau sont réunies, cet établissement de liaison peut prendre du temps, ce qui empêche le lancement de la fonction MMR. Pour garantir que Windows 7 MMR puisse être lancé, vous pouvez configurer une clé de registre Windows sur le poste de travail afin d'augmenter le délai accordé pour l'établissement de liaison de validation.

La clé de registre Windows contrôle la valeur TTL (Time to Live) de l'établissement de liaison, définie en millisecondes. La clé est au format REG_DWORD (hex). La valeur par défaut est de 5 000 millisecondes (cinq secondes).

Avant de déployer Windows 7 MMR pour les utilisateurs d'Horizon View, testez quelques systèmes clients pour vérifier si le délai par défaut accordé pour effectuer l'établissement de liaison est adapté à votre environnement. Si vos conditions réseau exigent un délai d'établissement de liaison supérieur à cinq secondes, augmentez la valeur TTL.

Procédure

1 Lancez l'éditeur de registre Windows sur le poste de travail virtuel.

2 Accédez à la clé de registre de Windows qui contrôle l'établissement de liaison de validation MMR.

Option	Description
Windows 7 64 bits	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware VDPService\handshakeTTL`
Windows 7 32 bits	`HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware VDPService\handshakeTTL`

3 Augmentez la valeur `handshakeTTL` en indiquant un nombre supérieur à 5 000.

4 Redémarrez Windows Media Player sur le poste de travail pour que la valeur mise à jour entre en vigueur.

Index