Installation und Verwaltung von VMware Horizon View Feature Pack

Horizon View 5.3
Horizon View Feature Pack 6

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter http://www.vmware.com/de/support/pubs.

DE-001301-01

vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

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

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

Installation und Verwaltung von VMware Horizon View Feature Pack

Das Dokument *Installation und Verwaltung von VMware Horizon View Feature Pack* stellt Informationen zu Installation und Konfiguration der VMware® Horizon View™ Feature Pack-Komponenten bereit.

Das vorliegende Dokument liefert Informationen zu Systemanforderungen sowie Anweisungen zur Installation des Remote Experience Agent auf Horizon View-Desktops und dem HTML-Zugriff-Installationsprogramm auf View-Verbindungsserverinstanzen. Darüber hinaus werden nach der Installation ausgeführte Konfigurationsaufgaben beschrieben.

Zielgruppe

Das vorliegende Dokument richtet sich an Administratoren, die das Feature Pack in einer Horizon View-Bereitstellung installieren und konfigurieren. Die Informationen wurden für erfahrene Systemadministratoren verfasst, die mit der Technologie virtueller Maschinen sowie mit Vorgängen in Rechenzentren vertraut sind. Wenn Sie bisher nicht mit Horizon View gearbeitet haben, müssen Sie zur Durchführung grundlegender Verfahren möglicherweise auf die Schrittanleitungen zurückgreifen, die im Dokument *Installation von VMware Horizon View-* bzw. im Dokument *Verwaltung von VMware Horizon View-* bereitgestellt werden.

VMware Horizon View Feature Pack -Komponenten

Das VMware Horizon View Feature Pack umfasst zwei Installationsprogramme, mit denen die Feature Pack-Komponenten in einer Horizon View-Umgebung bereitgestellt werden. Das Installationsprogramm für den Remote Experience Agent konfiguriert die Komponenten auf Horizon View-Desktops. Das HTML-Zugriff-Installationsprogramm konfiguriert den View-Verbindungsserver, um Desktops den Zugriff über HTML-Zugriff zu ermöglichen.

Installationsprogramm für den Remote Experience Agent

Der Remote Experience Agent installiert Feature Pack-Komponenten auf Horizon View-Desktops und verbessert die Benutzererfahrung für Remote-Desktops mit View Agent 5.3. Dieses Programm installiert die folgenden Komponenten:

- HTML-Zugriff Agent
- Flash URL-Umleitung
- Echtzeit-Audio/Video
- Unity Touch
- Windows 7 Multimedia-Umleitung (MMR)

Die Feature Pack-Komponenten ermöglichen es den Benutzern, mehrere neue Desktop-Funktionen zu nutzen.

HTML-Zugriff Agent

Der HTML-Zugriff Agent ermöglicht dem Benutzer die Verbindungherstellung mit Horizon View-Desktops über HTML-Zugriff. Der HTML-Zugriff Agent muss auf einem Desktop ausgeführt werden, um HTML-Zugriff auf diesem Desktop zu aktivieren.

Sie müssen daher zur Verwendung von HTML-Zugriff den Remote Experience Agent mit der HTML-Zugriff-Funktion installieren.

Flash URL-Umleitung

Bei der Flash-URL-Umleitung wird eine ShockWave Flash-Datei (SWF) vom Remote-Desktop abgefangen und an den Clientendpunkt umgeleitet. Ohne diese Funktion werden Multicast- oder Unicast-Videodaten von einem Adobe Media Server an die virtuellen Desktops gestreamt, die auf ESXi-Hosts ausgeführt werden. Die Daten werden dann erneut und in einzelnen PCoIP-Sitzungen von jedem virtuellen Desktop an jeden Clientendpunkt gesendet.

Bei der Flash-URL-Umleitung können Flash-Inhalte von Adobe Media Server direkt und unter Umgehung der virtuellen Desktop-Infrastruktur an die Clientendpunkte gestreamt werden. Die Flash-Inhalte werden dann mithilfe der lokalen Flash-Medienplayer wiedergegeben.

Durch das direkte Streaming von Flash-Inhalten von Adobe Media Server auf die Clientendpunkte wird die Datenlast auf dem ESXi-Host im Rechenzentrum gesenkt, das zusätzliche Routing über das Rechenzentrum vermieden und die erforderliche Bandbreite zum simultanen Streaming von Flash-Inhalten an mehrere Clientendpunkte verringert.

Echtzeit-Audio/Video

Die Echtzeit-Audio/Video-Funktion ermöglicht es Horizon View-Benutzern, Skype, Webex, Google Hangouts und andere Anwendungen für Onlinekonferenzen auf ihren virtuellen Desktops auszuführen. Mit der Echtzeit-Audio/Video-Funktion werden Webcams und Audiogeräte, die lokal an das Clientsystem angeschlossen sind, an den Remote-Desktop umgeleitet. Diese Funktion leitet Video- und Audio-Daten mit deutlich weniger Bandbreite an den Desktop um, als mit der USB-Umleitung erreicht werden kann.

Echtzeit-Audio/Video ist mit Standard-Konferenzanwendungen kompatibel und unterstützt standardmäßige Webcams, Audio-USB-Geräte und analoge Audioeingänge.

Mit dieser Funktion werden VMware Virtual Webcam und VMware Virtual Microphone auf dem Desktop-Betriebssystem installiert. Beim Start einer Konferenzanwendung werden diese virtuellen VMware-Geräte angezeigt und verwendet und sorgen für die Audio/Video-Umleitung von den lokal angeschlossenen Geräten auf dem Client. Das VMware Virtual Microphone erscheint auch im Geräte-Manager auf dem Desktop-Betriebssystem.

Die Treiber für die Audiogeräte und Webcams müssen auf den Horizon View-Clientsystemen installiert sein, um die Umleitung zu aktivieren.

Echtzeit-Audio/Video wird für Desktops im lokalen Modus nicht unterstützt.

Diese Funktion stellt eine ADM-Vorlagendatei bereit, mit der Sie Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video in Active Directory oder auf einzelnen Desktops installieren können. Mit diesen Einstellungen können Sie die standardmäßige maximale Bildrate und -auflösung für die Webcam ändern oder die Funktion insgesamt deaktivieren oder aktivieren.

Unity Touch

Mit Unity Touch können Tablet- und Smartphone-Benutzer Windows-Anwendungen und -Dateien bequem durchsuchen, suchen und öffnen, Lieblingsanwendungen und -dateien auswählen und bequem zwischen ausgeführten Anwendungen wechseln, ohne das Start-Menü oder die Taskleiste zu verwenden. Die Dokumente zu VMware Horizon View Client für iOS- und Android-Geräte enthalten weitere Informationen zu Endbenutzerfunktionen, die über Unity Touch bereitgestellt werden.

Windows 7 Multimedia-Umleitung (MMR)

Diese Funktion erweitert die Multimedia-Umleitung auf Windows 7-Desktops und -Clients.

MMR stellt den Multimedia-Stream direkt auf den Clientcomputern bereit. Mit MMR wird der Multimediadatenstrom auf dem Clientsystem verarbeitet, d. h. entschlüsselt. Das Clientsystem gibt die Medieninhalte wieder und lagert so die Anforderung vom ESXi-Host aus.

HTML-Zugriff -Installationsprogramm

Dieses Installationsprogramm konfiguriert die View-Verbindungsserverinstanzen so, dass Benutzer HTML-Zugriff für die Verbindungsherstellung mit Desktops auswählen können. Nachdem Sie das HTML-Zugriff-Installationsprogramm ausgeführt haben, zeigt View Portal zusätzlich zum View Client-Symbol ein HTML-Zugriff-Symbol an.

Sie müssen dieses Installationsprogramm ausführen, wenn Sie HTML-Zugriff zur Verbindungsherstellung mit Desktops in einer Horizon View-Bereitstellung nutzen möchten. Die Ausführung dieses Installationsprogramms ist auch erforderlich, wenn Ihre Benutzer Horizon Workspace nutzen und HTML-Zugriff zur Verbindungsherstellung mit Desktops auswählen.

Konfiguration und Installation

Um Horizon View Feature Pack einzurichten, installieren Sie Remote Experience Agent auf Horizon View-Desktops und das HTML-Zugriff-Installationsprogramm auf View-Verbindungsserver-Instanzen.

Systemanforderungen für das Horizon View Feature Pack

Horizon View-Desktops und View-Verbindungsserverinstanzen müssen bestimmte Softwareanforderungen erfüllen, um die Feature Pack-Komponenten zu unterstützen.

View-Verbindungsserver

View-Verbindungsserver 5.3

Installationsanweisungen finden Sie im Dokument *Installation von VMware Horizon View-*.

Horizon View-Desktop

In der virtuellen Maschine, auf die der Endbenutzer zugreift, muss die folgende Software installiert sein:

- Betriebssysteme: Windows XP SP3 (32 Bit), Windows Vista (32 Bit), Windows 7 (32 Bit oder 64 Bit), Windows 8 (32 Bit oder 64 Bit), Windows 8.1 (32 Bit oder 64 Bit) oder Windows Server 2008 R2

  Hinweis Bestimmte einzelne Feature Pack-Komponenten werden nur auf einigen der unterstützten Desktop-Betriebssysteme unterstützt. Siehe Tabelle 1.

- View Agent 5.3

  Installationsanweisungen finden Sie im Dokument *Verwaltung von VMware Horizon View-*.

Tabelle 1 zeigt die Desktop-Betriebssysteme, auf denen jede Feature Pack-Komponente unterstützt wird.

Tabelle 1. Unterstützung des Horizon View Desktop-Betriebssystems für einzelne Feature Pack-Komponenten

Feature Pack-Komponente	Windows XP SP3 (32 Bit)	Windows Vista (32 Bit)	Windows 7 (32 Bit oder 64 Bit)	Windows 8 oder Windows 8.1 (32 Bit oder 64 Bit)	Windows Server 2008 R2
HTML Access Agent	Ja	Ja	Ja	Ja (Tech Preview)	Ja
Flash URL-Umleitung	No (Nein)	No (Nein)	Ja	No (Nein)	No (Nein)
Echtzeit-Audio/Video	Ja	Ja	Ja	Ja	Ja
Unity Touch	Ja	Ja	Ja	Ja	Ja
Windows 7 MMR	No (Nein)	No (Nein)	Ja	No (Nein)	No (Nein)

Die unterstützten Feature Pack-Komponenten werden standardmäßig installiert, wenn Sie das Remote Experience Agent-Installationsprogramm ausführen. Sie können sich dazu entschließen, eine Komponente nicht zu installieren, indem Sie sie während der Installation deaktivieren.

Zur Unterstützung einzelner Feature Pack-Komponenten muss Ihre Horizon View-Bereitstellung zusätzliche Software- und Hardwareanforderungen erfüllen.

Systemanforderungen für HTML-Zugriff

Mit HTML-Zugriff wird für das Clientsystem keine weitere Software als ein unterstützter Browser benötigt. Die Horizon View-Bereitstellung muss bestimmte Softwareanforderungen erfüllen.

Browser auf Clientsystem

Die folgenden Webbrowser werden unterstützt:

- Chrome 28 oder höher
- Internet Explorer 9 oder höher
- Safari 6 oder höher
- Mobile Safari auf iOS-Geräten mit iOS 6 oder höher
- Firefox 21 oder höher

Clientbetriebssysteme:

- Windows XP SP3 (32 Bit)
- Windows 7 SP1 oder kein SP (32 Bit oder 64 Bit)
- Windows 8 Desktop (32 Bit oder 64 Bit)
- Windows Vista SP1 oder SP2 (32 Bit)
- Mac OS X Snow Leopard (10.6.8)
- Mac OS X Lion (10.7)
- Mac OS X Mountain Lion (10.8)
- iPad mit iOS 6.0 oder später (d. h. iPad 1 wird nicht unterstützt)
- Chrome OS 28.*x* oder später

View-Desktop

In der virtuellen Maschine, auf die der Endbenutzer zugreift, muss die folgende Software installiert sein:

- Betriebssysteme: Windows XP SP3 (32 Bit), Windows Vista (32 Bit), Windows 7 (32 Bit oder 64 Bit) oder Windows Server 2008 R2.

  Darüber hinaus ist HTML Access unter Windows 8 (32 oder 64 Bit) oder Windows 8.1 (32 oder 64 Bit) als Tech Preview verfügbar. Sie können HTML Access auf einem Windows 8- oder Windows 8.1-Desktop verwenden, Support wird dafür jedoch nicht angeboten.

- View Agent 5.3

  Installationsanweisungen finden Sie im Dokument *Verwaltung von VMware Horizon View-*.

Pool-Einstellungen

HTML-Zugriff erfordert die folgenden Pool-Einstellungen in View Administrator:

- Die **Maximale Auflösung für alle Monitore** muss auf **1920x1200** oder höher festgelegt sein, damit der View-Desktop über mindestens 17,58MB an Video-RAM verfügt.
- Die Einstellung **HTML Access** muss aktiviert sein.

Konfigurationsanweisungen finden Sie im Thema „Vorbereiten von View-Desktops und -Pools für HTML Access“ im Dokument *Verwenden von VMware Horizon View HTML Access*.

View-Verbindungsserver

Auf dem Server, der den View-Verbindungsserver hostet, muss die folgende Software installiert sein:

- View-Verbindungsserver 5.3

  Installationsanweisungen finden Sie im Dokument *Installation von VMware Horizon View-*.

- HTML-Zugriff

  Installationsanweisungen finden Sie unter „Installieren der HTML-Zugriff-Software auf dem View-Verbindungsserver“, auf Seite 22.

Wenn Sie HTML-Zugriff installiert haben, ist die Firewall automatisch zum Zulassen von eingehendem Datenverkehr auf TCP-Port 8443 konfiguriert.

Sicherheitsserver

Der Windows-Firewalldienst oder andere Firewallsoftware muss so konfiguriert werden, dass eingehender Datenverkehr auf TCP-Port 8443 akzeptiert wird.

Wenn Clientsysteme von außerhalb der firmeneigenen Firewall eine Verbindung herstellen, empfiehlt VMware die Verwendung eines Sicherheitsservers. Mit einem Sicherheitsserver erfordern die Clientsysteme keine VPN-Verbindung.

Hinweis Ein einzelner Sicherheitsserver kann bis zu 350 gleichzeitige Verbindungen mit Webclients unterstützen.

Firewalls von Drittanbietern

Fügen Sie Regeln hinzu, um den folgenden Datenverkehr zuzulassen:

- View-Server (einschließlich Sicherheitsserver, View-Verbindungsserverinstanzen und Replikatserver): eingehender Datenverkehr auf TCP-Port 8443

- View-Desktops: eingehender Datenverkehr (von View-Servern) auf TCP-Port 22443

Anzeigeprotokoll für Horizon View

Blast

Wenn Sie einen Webbrowser für den Zugriff auf einen View-Desktop verwenden, wird anstelle von PCoIP oder Microsoft RDP das Blast-Protokoll verwendet. Blast basiert auf HTTPS (HTTP über SSL/TLS).

Hinweis Sie können HTML-Zugriff zusammen mit VMware Horizon Workspace verwenden, damit Benutzer über einen HTML5-Browser eine Verbindung zu ihren Desktops herstellen können. Informationen zur Installation von Horizon Workspace und der Konfiguration für die Verwendung mit dem View-Verbindungsserver finden Sie in der Horizon Workspace-Dokumentation. Informationen über die Kopplung vom View-Verbindungsserver mit einem SAML Authentifizierungsserver finden Sie in der Dokumentation *Verwaltung von VMware Horizon View-*.

Systemanforderungen für die Flash-URL-Umleitung

Zur Unterstützung der Flash-URL-Umleitung muss Ihre Horizon View-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen.

Flash Media Player und ShockWave Flash (SWF)

Sie müssen einen entsprechenden Flash Media Player wie z. B. Strobe Media Playback in Ihre Website integrieren. Zum Streamen von Multicast-Inhalt können Sie `multicastplayer.swf` oder `StrobeMediaPlayback.swf` in Ihren Webseiten verwenden. Zum Streamen von Live-Unicast-Inhalt müssen Sie `StrobeMediaPlayback.swf` verwenden. Sie können `StrobeMediaPlayback.swf` auch für andere unterstützte Funktionen wie RTMP-Streaming und dynamisches HTTP-Streaming verwenden.

Horizon View-Desktop

- Auf den Desktops muss ein 64-Bit- oder 32-Bit-Betriebssystem mit Windows 7 ausgeführt werden.
- Auf den Desktops muss View Agent 5.3 installiert sein.
- Zu den unterstützten Desktop-Browsern gehören der Internet Explorer 8, 9 und 10, Chrome 29.*x* sowie Firefox 20.*x*.

Horizon View Client-Software

Die folgenden Horizon View Client-Versionen unterstützen Multicast und Unicast:

- Horizon View Client 2.2 für Linux oder höher
- Horizon View Client 2.2 für Windows oder höher

Die folgenden Horizon View Client-Versionen unterstützen nur Multicast. (Sie bieten keine Unterstützung für Unicast):

- Horizon View Client 2.0 oder 2.1 für Linux
- Horizon View Client 5.4 für Windows

View Client-Computer oder Clientzugriffsgerät

- Die Flash-URL-Umleitung wird auf allen Betriebssystemen unterstützt, die Horizon View Client für Linux auf x86 Thin Client-Geräten ausführen. Auf ARM-Prozessoren wird diese Funktion nicht unterstützt.
- Die Flash-URL-Umleitung wird auf allen Betriebssystemen unterstützt, auf denen Horizon View Client für Windows ausgeführt wird. Weitere Informationen finden Sie im Dokument *Verwendung von VMware Horizon View Client für Windows*.

- Auf Windows-Clientgeräten müssen Sie Adobe Flash Player 10.1 oder höher für Internet Explorer installieren.
- Auf Linux Thin Client-Geräten müssen Sie die Dateien „`libexpat.so.0`“ und „`libflashplayer.so`“ installieren. Siehe „Einrichten von Clientgeräten für die Flash-URL-Umleitung“, auf Seite 34.

Hinweis Bei der Flash-URL-Umleitung wird der Multicast- oder Unicast-Stream an Clientgeräte umgeleitet, die sich möglicherweise außerhalb der Unternehmensfirewall befinden. Ihre Clients müssen auf den Adobe Webserver zugreifen können, auf dem die ShockWave Flash-Datei (SWF) zur Initiierung des Multicast- oder Unicast-Streaming gehostet wird. Falls erforderlich, müssen Sie in Ihrer Firewall die geeigneten Ports öffnen, um Clientgeräten den Zugriff auf diesen Server zu ermöglichen.

Systemanforderungen für Echtzeit-Audio/Video

Echtzeit-Audio/Video arbeitet mit Standardwebcams, USB-Audio- und analogen Audiogeräten und kann mit standardmäßigen Konferenzanwendungen wie z. B. Skype, WebEx und Google Hangouts verwendet werden. Zur Unterstützung von Echtzeit-Audio/Video muss Ihre Horizon View-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen.

Horizon View-Desktop

Auf den Desktops muss View Agent 5.3 installiert sein. Echtzeit-Audio/Video wird auf allen Windows-Gastbetriebssystemen unterstützt, die View Agent 5.3 unterstützen.

Horizon View Client-Software

Horizon View Client 5.4 für Windows

Horizon View Client 2.2 für Windows oder höher

Hinweis Horizon View Client 2.2 für Windows ist eine spätere Version als Horizon View Client 5.4 für Windows. Die Versionsnummer für Windows ist nun konsistent mit den Horizon View Client-Versionen auf anderen Betriebssystemen und Geräten.

Horizon View Client 2.2 für Linux oder höher. Diese Funktion steht nur mit der Version von Horizon View Client für Linux zur Verfügung, die von Drittanbietern bereitgestellt wird.

View Client-Computer oder Clientzugriffsgerät

- Echtzeit-Audio/Video wird auf allen Betriebssystemen unterstützt, auf denen Horizon View Client für Windows ausgeführt wird. Weitere Informationen finden Sie im Dokument *Verwendung von VMware Horizon View Client für Windows*.
- Echtzeit-Audio/Video wird auf allen Betriebssystemen unterstützt, auf denen Horizon View Client für Linux auf x86-Geräten ausgeführt wird. Auf ARM-Prozessoren wird diese Funktion nicht unterstützt. Weitere Informationen finden Sie im Dokument *Verwendung von VMware Horizon View Client für Linux*.

- Auf dem Clientcomputer müssen Treiber für Webcam und Audiogeräte installiert sein, und die Webcam oder das Audiogerät muss betriebsbereit sein. Zur Unterstützung von Echtzeit-Audio/Video ist es nicht erforderlich, die Gerätetreiber auf dem Desktop-Betriebssystem zu installieren, auf dem View Agent installiert ist.

Anzeigeprotokoll für Horizon View

PCoIP

Echtzeit-Audio/Video wird in RDP-Desktop-Sitzungen nicht unterstützt.

Systemanforderungen für Unity Touch

Die Horizon View Client-Software und die mobilen Geräte, auf denen Sie Horizon View Client installieren, müssen zur Unterstützung von Unity Touch bestimmte Versionsanforderungen erfüllen.

Horizon View Client-Software

Unity Touch wird auf den folgenden Horizon View Client-Versionen unterstützt:

- Horizon View Client 2.0 für iOS oder höher
- Horizon View Client 2.0 für Android oder höher

Betriebssysteme für mobile Geräte

Unity Touch wird auf den folgenden Betriebssystemen für mobile Geräte unterstützt:

- iOS 5.0 und höher
- Android 3 (Honeycomb), Android 4 (Ice Cream Sandwich) und Android 4.1 und 4.2 (Jelly Bean)

Horizon View-Desktop

Zur Unterstützung von Unity Touch muss in der virtuellen Maschine, auf die der Endbenutzer zugreift, die folgende Software installiert sein:

- Betriebssysteme: Windows XP SP3 (32 Bit), Windows Vista (32 Bit), Windows 7 (32 Bit oder 64 Bit), Windows 8 (32 Bit oder 64 Bit), Windows 8.1 (32 Bit oder 64 Bit) oder Windows Server 2008 R2
- View Agent 5.3

  Installationsanweisungen finden Sie im Dokument *Verwaltung von VMware Horizon View-*.

Systemanforderungen für die Windows 7 Multimedia-Umleitung

Zur Unterstützung der Windows 7 Multimedia-Umleitung muss Ihre Horizon View-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen.

Horizon View-Desktop

- Auf den Desktops muss ein Windows 7-Betriebssystem mit 64 Bit oder 32 Bit ausgeführt werden.
- Für den Desktop-Pool muss das **3D-Rendering** aktiviert werden.
- Die virtuellen Desktop-Maschinen müssen virtuelle Hardware der Version 8 oder höher verwenden.
- Benutzer müssen Videos mit Windows Media Player 12 oder höher abspielen.

Horizon View Client-Software

Horizon View Client 2.2 für Windows oder höher

View Client-Computer oder Clientzugriffsgerät	■ Auf den Clients muss ein Windows 7- oder Windows 8-Betriebssystem mit 64 Bit oder 32 Bit ausgeführt werden. ■ Die Clients müssen über DVXA-kompatible (DirectX Video Acceleration) Grafikkarten verfügen, die die ausgewählten Videos decodieren können. ■ Auf den Clients muss Windows Media Player 12 oder höher installiert sein, um eine Umleitung zur lokalen Hardware zu unterstützen.
Unterstützte Medienformate	Die Medienformate müssen dem H.264-Standard zur Videokomprimierung entsprechen. Die Dateiformate M4V, MP4 und MOV werden unterstützt. Ihre virtuellen Desktops müssen eines dieser Dateiformate verwenden, und auf den Clientsystemen müssen lokale Decoder für diese Formate vorhanden sein.
View-Richtlinien	Überprüfen Sie in View Administrator, dass die Richtlinie **Multimedia-Umleitung (MMR)** auf den Standardwert **Zulassen** gesetzt ist.
Backend-Firewall	Wenn Ihre Horizon View-Bereitstellung eine Backend-Firewall zwischen Ihren DMZ-basierten Sicherheitsservern und dem internen Netzwerk enthält, stellen Sie sicher, dass die Backend-Firewall den Datenverkehr zu Port 9427 auf Ihren Desktops zulässt.

Einen Vergleich zwischen der Windows 7 MMR-Komponente und der Wyse MMR-Komponente, die auf Windows XP- und Windows Vista-Desktops ausgeführt wird, finden Sie unter „Unterstützung der Multimedia-Umleitung auf Desktop-Betriebssystemen“, auf Seite 14.

Unterstützung der Multimedia-Umleitung auf Desktop-Betriebssystemen

Die Windows 7 Multimedia-Umleitung (MMR) ist eine Feature Pack-Komponente, die mit Remote Experience Agent installiert wird. Eine Wyse MMR-Komponente wird mit View Agent installiert und arbeitet auf Windows XP- und Windows Vista-Desktops. Windows 7 MMR weist leicht unterschiedliche Merkmale und Anforderungen auf im Vergleich zur Wyse-MMR-Komponente.

Tabelle 2. Horizon View Desktop-Betriebssystemunterstützung für die Multimedia-Umleitung

Desktop-Betriebssystem	Anforderungen an die virtuelle Desktop-Maschine	Unterstützte Medienformate	Unterstützte Clients	Audio-Umleitung
Windows XP, Windows Vista	Windows Media Player 10 oder höher muss installiert sein.	Es werden zahlreiche Formate unterstützt. Beispiel: MPEG2-1; MPEG2; MPEG-4 Part 2;WMV 7, 8 und 9; WMA; AVI; ACE; MPT3; WAV	Windows XP, Windows Vista, Windows 7 Windows Media Player 10 oder höher muss installiert sein.	Der Audio-Stream wird an das Clientsystem umgeleitet.
Windows 7	Die Desktops müssen virtuelle Hardware der Version 8 oder höher verwenden. Das **3D-Rendering** muss aktiviert sein. Windows Media Player 12 oder höher muss installiert sein.	H.264-Komprimierungsstandard für M4V-, MP4- oder MOV-Format.	Windows 7, Windows 8 Die Clients müssen über DVXA-kompatible (DirectX Video Acceleration) Grafikkarten verfügen, die die ausgewählten Videos decodieren können. Windows Media Player 12 oder höher muss installiert sein.	Der Audio-Stream wird nicht umgeleitet. Audiodaten werden vom Remote-Desktop über PCoIP für das Clientsystem bereitgestellt.
Windows 8	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

Weitere Informationen zu MMR-Systemanforderungen auf Horizon View-Clients finden Sie im Dokument *Verwendung von VMware Horizon View Client für Windows*.

Installation und Bereitstellung des Remote Experience Agent auf Horizon View - Desktops

Das Remote Experience Agent-Installationsprogramm konfiguriert die Feature Pack-Komponenten auf Horizon View-Desktops. Sie können das interaktive Installationsprogramm für den Remote Experience Agent verwenden oder eine unbeaufsichtigte Installation von der Befehlszeile ausführen.

Wenn Sie einen neuen Desktop-Pool erstellen möchten, installieren Sie den Remote Experience Agent auf einer übergeordneten virtuellen Maschine. Erstellen Sie einen Snapshot oder legen Sie eine Vorlage aus der virtuellen Maschine an und erstellen Sie den Desktop-Pool.

Wenn Sie die Feature Pack-Komponenten in einem vorhandenen Desktop-Pool installieren möchten, richtet sich der verwendete Ansatz nach der Art des Desktop-Pools. Bei einem Linked-Clone-Pool mit dynamischen Zuweisungen können Sie das Remote Experience Agent-Installationsprogramm beispielsweise auf der übergeordneten virtuellen Maschine ausführen und die verknüpften Klone neu zusammenstellen. Bei einem Full-Clone-Pool oder einem Pool, den Sie nicht neu zusammenstellen, können Sie eine unbeaufsichtigte Installation des Remote Experience Agent auf den Desktops durchführen. Sie können ein eigenes Skript oder ein Tool zur Softwaredistribution verwenden, um eine verteilte Installation durchzuführen.

Upgrade des Remote Experience Agent

Wenn eine Vorgängerversion des Remote Experience Agent auf Ihren Desktops installiert ist, müssen Sie die aktuelle Version installieren, um die neuen Versionen der Feature Pack-Komponenten zu installieren.

Bevor Sie das Programm Remote Experience Agent installieren können, das im Lieferumfang von Horizon View 5.3 Feature Pack 1 enthalten ist, müssen Sie auf Ihren Desktops View Agent 5.3 installieren. Bei der Installation von View Agent 5.3 werden alle früheren Versionen von Remote Experience Agent und die zugehörigen Feature Pack-Komponenten entfernt. Dann können Sie die aktuelle Version von Remote Experience Agent installieren, die eine neue Installation der Feature Pack-Komponenten durchführt.

Interaktive Installation des Remote Experience Agent

Installieren Sie den Remote Experience Agent, um die Feature Pack-Komponenten auf Horizon View-Desktops zu konfigurieren.

Die HTML-Zugriff Agent-Komponente ist für HTML-Zugriff erforderlich. Informationen zum Einrichten von Horizon View-Desktops und -Pools für HTML-Zugriff finden Sie unter „Vorbereiten von View-Desktops und -Pools für HTML-Zugriff“ im Dokument *Verwendung von VMware Horizon View HTML Access* auf der Seite mit der VMware Horizon View--Clientdokumentation.

Wichtig Führen Sie eine Installation oder Deinstallation des Remote Experience Agent nicht aus einer View-Desktop-Sitzung aus, die über View Client oder HTML-Zugriff gestartet wurde. Führen Sie die Installation direkt auf der virtuellen Maschine aus. Sie können beispielsweise in vSphere Web Client oder vSphere Client eine Konsole auf der virtuellen Maschine öffnen.

Voraussetzungen

- Stellen Sie sicher, dass View Agent 5.3 auf der virtuellen Maschine installiert ist.
- Vergewissern Sie sich, dass Sie über Administratorrechte für die virtuelle Maschine verfügen.
- Stellen Sie sicher, dass der Windows-Firewalldienst auf der virtuellen Maschine ausgeführt wird. Wenn der Windows-Firewalldienst nicht gestartet wurde und ausgeführt wird, kann der Remote Experience Agent nicht installiert werden.
- Machen Sie sich mit den Funktionen vertraut, die über den Remote Experience Agent installiert werden können. Siehe „Installationsoptionen für den Remote Experience Agent“, auf Seite 16.
- Vergewissern Sie sich, dass Sie auf die Remote Experience Agent-Installationsdatei auf der VMware-Produktseite unter http://www.vmware.com/de/products/ zugreifen können.

Vorgehensweise

1 Laden Sie die Remote Experience Agent-Installationsdatei von der VMware-Produktseite herunter.

  Wählen Sie die entsprechende Installationsdatei aus, wobei *y.y* für die Feature Pack-Versionsnummer und *xxxxxx* für die Buildnummer steht.

Option	Beschreibung
32-Bit-Installationsprogramm	`VMware-Horizon-View-5.3-Remote-Experience-Agent-y.y-xxxxxx.exe`
64-Bit-Installationsprogramm	`VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe`

2 Doppelklicken Sie auf die Installationsdatei, um das Remote Experience Agent-Installationsprogramm zu starten.

3 Stimmen Sie der VMware-Endbenutzerlizenzvereinbarung zu.

4 Wählen Sie die gewünschten Installationsoptionen aus.

   Verwenden Sie das Dropdown-Menü einer Funktion, um diese Funktion auszuwählen oder von der Installation auszuschließen.

5 Klicken Sie auf **Installieren**.

   Nach Abschluss der Installation zeigt der Installer die folgende Meldung an: `Setup hat VMware Horizon View 5.3 Remote Experience Agent erfolgreich installiert`.

6 Klicken Sie auf **Fertig stellen**.

Wenn der HTML-Zugriff-Agent auf der virtuellen Maschine installiert ist, wird in der Windows-Firewall TCP-Port 22443 geöffnet. Siehe „Firewall-Regeln für HTML-Zugriff“, auf Seite 24.

Weiter

Wenn Sie den Remote Experience Agent auf einer übergeordneten virtuellen Maschine installiert haben, erstellen Sie einen Snapshot oder eine Vorlage und legen Sie einen Horizon View-Desktop-Pool an bzw. stellen Sie einen vorhandenen Pool neu zusammen.

Installationsoptionen für den Remote Experience Agent

Wenn Sie den Remote Experience Agent auf einer virtuellen Maschine installieren, können Sie die gewünschten Installationsoptionen auswählen.

Option	Beschreibung
HTML Access	Ermöglicht dem Benutzer die Verbindungherstellung mit Horizon View-Desktops über HTML-Zugriff. Der HTML-Zugriff Agent muss auf Horizon View-Desktops installiert sein, damit Benutzer Verbindungen mit HTML-Zugriff herstellen können. Diese Funktion ist standardmäßig installiert.
Flash URL-Umleitung	Leitet Flash-URL-Multicast- oder -Unicast-Streamingdaten von virtuellen Desktops an Clientgeräte um. Diese Funktion ermöglicht es, Videodaten direkt von einer Multicast- oder Unicast-Webquelle an die Clienthardware zu streamen und Benutzern auf dem lokalen Flash-Medienplayer des Clients anzuzeigen. Diese Funktion ist standardmäßig installiert.
Echtzeit-Audio/Video	Leitet Webcams und Audiogeräte um, die mit dem Clientsystem verbunden sind, sodass diese auf dem Remote-Desktop eingesetzt werden können. Diese Funktion ist standardmäßig installiert.
Unity Touch	Bietet Tablet- und Smartphone-Benutzern eine komfortable Sidebar, mit der über Touch-Funktionen Windows-Anwendungen und -Dateien durchsucht, gesucht, geöffnet und geschlossen werden können. Außerdem ist es möglich, zwischen ausgeführten Anwendungen zu wechseln. Diese Funktion ist standardmäßig installiert.
Win7 Multimedia-Umleitung	Erweitert die Multimedia-Umleitung auf Windows 7-Desktops und -Clients. Diese Funktion leitet einen Multimedia-Stream direkt an den Clientcomputer um, sodass der Multimedia-Stream nicht auf dem Remote-ESXi-Host, sondern auf der Clienthardware verarbeitet wird. Diese Funktion ist standardmäßig installiert.

Unbeaufsichtigte Installation des Remote Experience Agent

Sie können die MSI-Funktion (Microsoft Windows Installer) für die unbeaufsichtigte Installation verwenden, um den Remote Experience Agent auf mehreren virtuellen Windows-Maschinen zu installieren. Bei einer unbeaufsichtigten Installation verwenden Sie die Befehlszeile und müssen nicht auf Eingabeaufforderungen des Assistenten reagieren.

Das Remote Experience Agent-Installationsprogramm konfiguriert die Feature Pack-Komponenten auf Horizon View-Desktops.

Wichtig Führen Sie eine Installation oder Deinstallation des Remote Experience Agent nicht aus einer View-Desktop-Sitzung aus, die über View Client oder HTML-Zugriff gestartet wurde. Führen Sie den Installationsbefehl direkt auf der virtuellen Maschine aus. Sie können beispielsweise in vSphere Web Client oder vSphere Client eine Konsole auf der virtuellen Maschine öffnen.

Voraussetzungen

- Stellen Sie sicher, dass View Agent 5.3 auf der virtuellen Maschine installiert ist.
- Vergewissern Sie sich, dass Sie über Administratorrechte für die virtuelle Maschine verfügen.
- Stellen Sie sicher, dass der Windows-Firewalldienst auf der virtuellen Maschine ausgeführt wird. Wenn der Windows-Firewalldienst nicht gestartet wurde und ausgeführt wird, kann der Remote Experience Agent nicht installiert werden.
- Vergewissern Sie sich, dass Sie auf die Remote Experience Agent-Installationsdatei auf der VMware-Produktseite unter http://www.vmware.com/de/products/ zugreifen können.
- Machen Sie sich mit den Eigenschaften vertraut, die für die unbeaufsichtigte Installation des Remote Experience Agent zur Verfügung stehen. Siehe „Eigenschaften für die unbeaufsichtigte Installation von Remote Experience Agent“, auf Seite 18.
- Machen Sie sich mit den MSI-Befehlszeilenoptionen vertraut. Siehe „MSI-Befehlszeilenoptionen für das Remote Experience Agent-Installationsprogramm“, auf Seite 18.

Vorgehensweise

1 Laden Sie die Remote Experience Agent-Installationsdatei von der VMware-Produktseite herunter.

Wählen Sie die entsprechende Installationsdatei aus, wobei *y.y* für die Feature Pack-Versionsnummer und *xxxxxx* für die Buildnummer steht.

Option	Beschreibung
32-Bit-Installationsprogramm	`VMware-Horizon-View-5.3-Remote-Experience-Agent-`*`y.y`*`-`*`xxxxxx`*`.exe`
64-Bit-Installationsprogramm	`VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-`*`y.y`*`-`*`xxxxxx`*`.exe`

2 Öffnen Sie auf der virtuellen Maschine eine Windows-Eingabeaufforderung.

3 Geben Sie den Installationsbefehl in einer Zeile ein.

In diesem Beispiel wird der Remote Experience Agent auf einer virtuellen Maschine installiert. Das Installationsprogramm konfiguriert alle Remote Experience Agent-Installationsoptionen und schreibt Protokolle in die Datei „`install.log`“.

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

Hinweis Im vorstehenden Beispiel werden alle öffentlich verfügbaren Funktionen installiert. Zur Installation ausgewählter Funktionen verwenden Sie die Option `ADDLOCAL=` und geben die Eigenschaften für die unbeaufsichtigte Installation in einer Liste mit Kommatrennung an. Beispiel: `ADDLOCAL=Core,HTMLAccess,UnityTouch,FlashURLRedirection,RTAV,MMR`. Die Eigenschaft `Core` ist erforderlich, wenn Sie `ADDLOCAL=` zur Festlegung ausgewählter Funktionen verwenden.

Wenn der HTML-Zugriff-Agent auf der virtuellen Maschine installiert ist, wird in der Windows-Firewall TCP-Port 22443 geöffnet. Siehe „Firewall-Regeln für HTML-Zugriff“, auf Seite 24.

Weiter

Wenn Sie den Remote Experience Agent auf einer übergeordneten virtuellen Maschine installiert haben, erstellen Sie einen Snapshot oder eine Vorlage und legen Sie einen Horizon View-Desktop-Pool an bzw. stellen Sie einen vorhandenen Pool neu zusammen.

Eigenschaften für die unbeaufsichtigte Installation von Remote Experience Agent

In einem Befehl für die unbeaufsichtigte Installation können Sie die MSI-Eigenschaft `ADDLOCAL=` zum Festlegen von Feature Pack-Komponenten verwenden, die das Installationsprogramm von Remote Experience Agent konfigurieren soll. Jede Funktion einer unbeaufsichtigten Installation entspricht einer Installationsoption, die Sie während einer interaktiven Installation aktivieren oder deaktivieren können.

Weitere Informationen zu diesen Funktionen finden Sie unter „Installationsoptionen für den Remote Experience Agent“, auf Seite 16.

Tabelle 3. Remote Experience Agent-Funktionen für die unbeaufsichtigte und die interaktive Installation

Funktion für die unbeaufsichtigte Installation	Installationsoption in einer interaktiven Installation
HTMLAccess	HTML-Zugriff Agent
FlashURLRedirection	Flash-URL-Umleitung
RTAV	Echtzeit-Audio/Video
UnityTouch	Unity Touch
MMR	Win7 Multimedia-Umleitung (MMR)

MSI-Befehlszeilenoptionen für das Remote Experience Agent-Installationsprogramm

Zur unbeaufsichtigten Installation des Remote Experience Agent müssen Sie MSI-Befehlszeilenoptionen und -Eigenschaften (Microsoft Windows Installer) verwenden. Der Installer ist ein MSI-Programm und verwendet MSI-Standardfunktionen.

Einzelheiten zu MSI finden Sie auf der Website von Microsoft. Informationen zu MSI-Befehlszeilenoptionen finden Sie auf der Website der MSDN-Bibliothek (Microsoft Developer Network), wenn Sie nach MSI-Befehlszeilenoptionen suchen. Wenn Sie Informationen zur Verwendung der MSI-Befehlszeilenoptionen anzeigen möchten, öffnen Sie auf der virtuellen Maschine, auf der Sie die Installation durchführen, eine Eingabeaufforderung und geben Sie `msiexec /?` ein.

Hinweis Die Option `INSTALLDIR` steht für das Remote Experience Agent-Installationsprogramm nicht zur Verfügung. Sie können das Installationsverzeichnis nicht ändern.

Zur Durchführung einer unbeaufsichtigten Installation beginnen Sie mit einer unbeaufsichtigten Ausführung des Bootstrap-Programms, mit dem der Installer in ein temporäres Verzeichnis extrahiert und eine interaktive Installation gestartet wird.

An der Befehlszeile müssen Sie die Befehlszeilenoptionen eingeben, die das Bootstrap-Programm des Installers steuern.

Tabelle 4. Befehlszeilenoptionen für das Bootstrap-Programm eines Installers

Option	Beschreibung
`/s`	Deaktiviert den Bootstrap-Splash-Bildschirm und das Dialogfeld für die Extraktion, wodurch die Anzeige interaktiver Dialogfelder unterbunden wird. Beispiel: `VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s` Die Option `/s` ist erforderlich, um eine unbeaufsichtigte Installation durchzuführen.
`/v"MSI-Befehlszeilenoptionen"`	Weist den Installer an, die in doppelten Anführungszeichen eingeschlossene Zeichenfolge, die Sie an der Befehlszeile eingeben, als Befehlssatz zur Interpretation durch MSI zu übergeben. Sie müssen Ihre Befehlszeileneinträge in doppelte Anführungszeichen einschließen. Geben Sie ein doppeltes Anführungszeichen nach `/v` und am Ende der Befehlszeile ein. Beispiel: `VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s /v"Befehlszeilenoptionen"` Die Option `/v"Befehlszeilenoptionen"` ist erforderlich, um eine unbeaufsichtigte Installation durchzuführen.

Sie steuern die verbleibenden Schritte einer unbeaufsichtigten Installation, indem Sie Befehlszeilenoptionen und MSI-Eigenschaftenwerte an den MSI Installer, `msiexec.exe`, übergeben. Der MSI Installer verwendet die Werte und Optionen, die Sie an der Befehlszeile eingeben, um Installations- und Setup-Optionen zu interpretieren, die für das Remote Experience Agent-Installationsprogramm spezifisch sind.

Tabelle 5. MSI-Befehlszeilenoptionen und MSI-Eigenschaften

MSI-Option oder -Eigenschaft	Beschreibung
`/qn`	Weist den MSI Installer an, keine Seiten des Installations-Assistenten anzuzeigen. Sie können beispielsweise eine unbeaufsichtigte Installation des Remote Experience Agent durchführen und nur standardmäßige Optionen und Funktionen für das Setup verwenden: `VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s /v"/qn"` Alternativ können Sie die Option `/qb` zur Anzeige der Assistentenseiten in einer nicht interaktiven, automatisierten Installation verwenden. Während die Installation durchgeführt wird, werden die Assistentenseiten angezeigt, Sie können jedoch keine Eingaben vornehmen. Die Option `/qn` oder `/qb` ist erforderlich, um eine unbeaufsichtigte Installation durchzuführen.
`/x`	Deinstalliert den Remote Experience Agent. Beispiel: `VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s /v"/qb /x"` Anweisungen zum Deinstallieren des Remote Experience Agent und zum Zurücksetzen eines Horizon View-Desktops in den Zustand vor der Installation finden Sie unter „Deinstallieren des Remote Experience Agent“, auf Seite 21.
UNITY_DEFAULT_APPS	Gibt eine Standardliste mit Favoritenanwendungen an, die in der Unity Touch-Sidebar auf einem mobilen Gerät angezeigt werden. Diese Eigenschaft wurde zur Unterstützung der Unity Touch-Komponente erstellt. Es handelt sich nicht um eine allgemeine MSI-Eigenschaft. Informationen zum Konfigurieren einer Standardliste mit Favoritenanwendungen und zu Syntax und Format dieser Eigenschaft finden Sie unter „Konfigurieren von Favoritenanwendungen durch Unity Touch“, auf Seite 29. Die Eigenschaft `UNITY_DEFAULT_APPS` ist optional.

Tabelle 5. MSI-Befehlszeilenoptionen und MSI-Eigenschaften (Fortsetzung)

MSI-Option oder -Eigenschaft	Beschreibung
ADDLOCAL	Legt die komponentenspezifischen Funktionen fest, die installiert werden sollen. In einer interaktiven Installation zeigt das Installationsprogramm Optionen an, aus denen der Benutzer auswählen kann. Mit der Eigenschaft ADDLOCAL können Sie diese Optionen an der Befehlszeile festlegen. Wenn Sie die Eigenschaft ADDLOCAL nicht verwenden, werden die standardmäßigen Optionen installiert. Zur Festlegung einzelner Installationsoptionen geben Sie eine durch Kommas getrennte Liste mit Optionsnamen ein. Verwenden Sie zwischen den Namen keine Leerzeichen. Verwenden Sie das Format ADDLOCAL=*Wert*,*Wert*,*Wert*.... Bei den Optionsnamen muss die Klein-/Großschreibung beachtet werden. Eine Liste der verfügbaren Installationsoptionen finden Sie unter „Eigenschaften für die unbeaufsichtigte Installation von Remote Experience Agent“, auf Seite 18. Im folgenden Beispiel werden HTML Access-Agent, Unity Touch, Flash-URL-Umleitung und Echtzeit-Audio/Video installiert: `VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,HTMLAccess,UnityTouch,FlashURLRedirection,RTAV,MMR"` Bei Verwendung der Eigenschaft ADDLOCAL zur Festlegung der Installationsoptionen ist die Komponente „Core“ erforderlich. Die Eigenschaft ADDLOCAL ist optional.
REBOOT	Sie können die Option REBOOT=ReallySuppress verwenden, um die Ausführung von Systemkonfigurationsaufgaben zuzulassen, bevor das System neu gestartet wird. Diese MSI-Eigenschaft ist optional.
REMOVE	Entfernt die angegebenen Feature Pack-Komponenten (Installationsoptionen), die über das Remote Experience Agent-Installationsprogramm installiert wurden. Zum Entfernen einzelner Installationsoptionen geben Sie eine durch Kommas getrennte Liste mit Optionsnamen ein. Verwenden Sie zwischen den Namen keine Leerzeichen. Verwenden Sie das Format REMOVE=*Wert*,*Wert*,*Wert*.... Bei den Optionsnamen muss die Klein-/Großschreibung beachtet werden. Eine Liste der verfügbaren Installationsoptionen finden Sie unter „Eigenschaften für die unbeaufsichtigte Installation von Remote Experience Agent“, auf Seite 18. Im folgenden Beispiel werden HTML Access-Agent, Unity Touch, Flash-URL-Umleitung und Echtzeit-Audio/Video entfernt: `VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s /v"/qn REMOVE=HTMLAccess,UnityTouch,FlashURLRedirection,RTAV,MMR"` Die Eigenschaft REMOVE ist optional.
/l*v *Protokolldatei*	Schreibt ausführliche Protokollinformationen in die angegebene Protokolldatei. Beispiel: `/l*v ""%TEMP%\vmmsi.log""` In diesem Beispiel wird eine detaillierte Protokolldatei generiert, die dem Protokoll ähnelt, das während einer interaktiven Installation erstellt wird. Sie können diese Option dazu verwenden, benutzerdefinierte Funktionen aufzuzeichnen, die möglicherweise nur für Ihre Installation gelten. Sie können die aufgezeichneten Informationen dazu verwenden, Installationsfunktionen für unbeaufsichtigte Installationen anzugeben. Die Option /l*v ist optional.

Deinstallieren des Remote Experience Agent

Sie können den Remote Experience Agent auf dieselbe Weise wie Windows-Komponenten von Horizon View-Desktops entfernen.

Der Remote Experience Agent wirkt sich auf bestimmte Dateien aus, die mit View Agent 5.3 installiert werden. Wenn Sie den Remote Experience Agent deinstallieren, müssen Sie View Agent deinstallieren und neu installieren oder View Agent reparieren, um die virtuelle View Agent-Maschine wieder in den Zustand vor der Installation zurückzuversetzen.

Vorgehensweise

1 Öffnen Sie auf virtuellen Maschinen mit Remote Experience Agent in der Windows-Systemsteuerung das Applet zum Deinstallieren von Programmen.

2 Wählen Sie **VMware Horizon View 5.3 Remote Experience Agent** und klicken Sie auf **Deinstallieren**.

3 Deinstallieren und installieren Sie View Agent erneut oder reparieren Sie View Agent.

Option	Beschreibung
Deinstallieren und neu installieren	a Wählen Sie im Windows-Applet „Programm deinstallieren“ **VMware View Agent** und klicken Sie auf **Deinstallieren**. b Starten Sie die VMware View Agent 5.3-Installationsdatei, um die Software neu zu installieren.
Reparieren	Starten Sie die VMware View Agent 5.3-Installationsdatei und wählen Sie die Option **Reparieren**.

4 (Optional) Stellen Sie sicher, dass für die Windows-Firewall auf der virtuellen Maschine der TCP-Port 22443 nicht länger für das Zulassen von eingehendem Datenverkehr konfiguriert ist.

Weiter

Falls erforderlich, ändern Sie die Regeln für Ihre Unternehmensfirewall, um eingehenden Datenverkehr auf TCP-Port 22443 auf der virtuellen Desktop-Maschine zu unterbinden.

Installieren der HTML Access-Software auf dem View-Verbindungsserver

Das HTML-Zugriff-Installationsprogramm konfiguriert die View Portal-Seite auf dem View-Verbindungsserver so, dass Benutzer HTML-Zugriff auswählen können, wenn sie sich mit ihren Desktops verbinden. Führen Sie das Installationsprogramm auf einer View-Verbindungsserverinstanz und auf allen Instanzen in einer replizierten Gruppe aus.

Per Voreinstellung enthält die View Portal-Seite, die erscheint, wenn Sie einen Browser öffnen und die URL einer View-Verbindungsserverinstanz eingeben, Links zur VMware-Download-Website zum Herunterladen des View Client.

Nachdem Sie das HTML-Zugriff-Installationsprogramm ausgeführt haben, zeigt die View Portal-Seite neben dem View Client-Symbol ein HTML-Zugriff-Symbol an, mit dem die Benutzer über HTML-Zugriff eine Verbindung mit ihren Desktops herstellen können. Benutzer müssen View Client nicht installieren, um eine Verbindung mit ihren Desktops herzustellen.

Sie können die View Portal-Seite anpassen, wenn Sie das Symbol für den Download von View Client deaktivieren möchten, das Symbol für die Verbindungsherstellung über HTML-Zugriff deaktivieren oder die URL der Webseite für den Download von View Client ändern. Siehe Abschnitt „Konfigurieren der HTML Access-Seite für Endbenutzer“ im Dokument *Verwendung von VMware Horizon View HTML Access* auf der Seite mit der VMware Horizon View--Clientdokumentation.

Wichtig Wenn Sie die View Portal-Seite von Horizon View oder die HTML Access-Portalseite von Horizon View 5.2 Feature Pack 1 zuvor bearbeitet haben, werden diese Anpassungen verworfen, wenn Sie auf eine neuere Version von HTML Access aktualisieren. Sie können die Seite nach dem Upgrade erneut anpassen. Wenn Sie zuvor die HTML Access-Portalseite von Horizon View 5.2 Feature Pack 2 oder später bearbeitet haben, bleiben Ihre Anpassungen erhalten.

Eine Übersicht zur Einrichtung des View-Verbindungsservers für HTML-Zugriff finden Sie unter „Vorbereiten von View-Verbindungsserver und Sicherheitsservern für HTML-Zugriff“ im Dokument *Verwendung von VMware Horizon View HTML Access* auf der Seite mit der VMware Horizon View--Clientdokumentation.

Upgrade der HTML Access-Software

Installieren Sie die neueste HTML Access-Version, um von den neuesten Updates und Verbesserungen zu profitieren.

Bevor Sie die Software „HTML Access“ installieren können, die im Lieferumfang von Horizon View 5.3 Feature Pack 1 enthalten ist, müssen Sie Ihre View-Verbindungsserverinstanzen auf Horizon View 5.3 aktualisieren.

Bei einem Upgrade wird die neueste Version der HTML Access-Software auf den View-Verbindungsserverinstanzen in einer replizierten Gruppe ausgeführt.

Zum Abschließen des Upgrades von HTML Access müssen Sie außerdem die neueste Version des Remote Experience Agent-Installationsprogramms auf den entsprechenden übergeordneten virtuellen Maschinen oder virtuellen Maschinenvorlagen für Ihre Desktop-Pools ausführen. Siehe „Upgrade des Remote Experience Agent“, auf Seite 15.

Installieren der HTML-Zugriff -Software auf dem View-Verbindungsserver

Wenn Sie die View Portal-Seite so konfigurieren möchten, dass auf ihr das HTML Access-Symbol angezeigt wird, führen Sie das HTML Access-Installationsprogramm auf der View-Verbindungsserverinstanz aus (bzw. auf mehreren Instanzen, wenn diese Teil einer replizierten Gruppe sind).

Voraussetzungen

- Stellen Sie sicher, dass View Connection Server Horizon View 5.3 verwendet wird.
- Vergewissern Sie sich, dass Sie auf die HTML-Zugriff-Installationsdatei auf der VMware-Produktseite unter http://www.vmware.com/de/products/ zugreifen können.

Vorgehensweise

1 Laden Sie die HTML-Zugriff-Installationsdatei von der VMware-Produktseite herunter.

  Der Dateiname des Installationsprogramms lautet: `VMware-Horizon-View-HTML-Access_X64-y.y.y-xxxxxx.exe`. Hierbei steht *xxxxxx* für die Buildnummer und *y.y.y* für die Versionsnummer.

2 Doppelklicken Sie auf die Installationsdatei, um das HTML-Zugriff-Installationsprogramm zu starten.

3 Stimmen Sie der VMware-Endbenutzerlizenzvereinbarung zu.

4 Übernehmen oder ändern Sie den Installationsordner.

5 Klicken Sie auf **Installieren**.

6 Klicken Sie auf **Fertig stellen**.

Weiter

Stellen Sie sicher, dass der von HTML-Zugriff verwendete Port zur Verbindungsherstellung mit Sicherheitsservern in der Windows-Firewall geöffnet ist. Siehe „Öffnen des Ports, der von HTML-Zugriff auf Sicherheitsservern verwendet wird“, auf Seite 23.

Sie können die View Portal-Seite ändern, indem Sie entweder das View Client-Symbol oder das HTML-Zugriff-Symbol für die Benutzer ausblenden. Siehe Abschnitt „Konfigurieren der HTML-Zugriff-Seite für Endbenutzer“ im Dokument *Verwendung von VMware Horizon View HTML Access* auf der Seite mit der VMware Horizon View- Client-Dokumentation.

Öffnen des Ports, der von HTML-Zugriff auf Sicherheitsservern verwendet wird

Wenn Sie View-Verbindungsserver oder Sicherheitsserver installieren, erstellt das View Server-Installationsprogramm die Windows-Firewall-Regel für den Port, der von HTML-Zugriff für Client-Verbindungen verwendet wird. Das Installationsprogramm lässt aber die Regel solange deaktiviert, bis sie tatsächlich benötigt wird. Wenn Sie später HTML-Zugriff auf einer View-Verbindungsserver-Instanz installieren, aktiviert das HTML-Zugriff-Installationsprogramm automatisch die Regel, welche die Kommunikation zu diesem Port erlaubt. Auf Sicherheitsservern müssen Sie die Regel in der Windows-Firewall manuell aktivieren, um die Kommunikation über diesen Port zu ermöglichen.

Standardmäßig benutzt HTML-Zugriff den TCP-Port 8443 für Client-Verbindungen zum Blast Secure Gateway.

Vorgehensweise

- Um den Port von HTML-Zugriff auf einem View-Verbindungsserver-Computer zu öffnen, installieren Sie auf diesem Computer HTML Access.

  Der HTML-Zugriff Installer aktiviert die **VMware View-Verbindungsserver (Blast-In)**-Regel in der Windows-Firewall.

- Um den Port für HTML-Zugriff auf einem Sicherheitsserver zu öffnen, aktivieren Sie die **VMware View-Verbindungsserver (Blast-In)** Regel in der Windows-Firewall.

Deinstallieren von HTML-Zugriff vom View-Verbindungsserver

Sie können HTML-Zugriff mit der gleichen Methode entfernen, mit der Sie andere Windows-Software entfernen.

Vorgehensweise

1. Auf den View-Verbindungsserver-Hosts, wo HTML-Zugriff installiert ist, öffnen Sie in der Windows-Systemsteuerung das Applet-Programm zum Deinstallieren.
2. Wählen Sie HTML-Zugriff und klicken Sie auf **Deinstallieren**.
3. (Optional) Stellen Sie in der Windows-Firewall für diesen Host sicher, dass der TCP-Port 8443 keinen eingehenden Datenverkehr mehr erlaubt.

Weiter

Verhindern Sie eingehenden Datenverkehr an TCP-Port 8443 auf der Windows-Firewall aller gepaarten Sicherheitsserver. Auf Firewalls von Drittanbietern ändern Sie gegebenenfalls die Regeln, um eingehenden Datenverkehr an TCP-Port 8443 für alle gepaarten Sicherheitsserver und diesen View-Verbindungsserver-Host zu verbieten.

Firewall-Regeln für HTML-Zugriff

Um Client-Webbrowsern zu ermöglichen, HTML-Zugriff zur Herstellung einer Verbindung zum Sicherheitsserver, zu View-Verbindungsserver-Instanzen und zu Horizon View-Desktops zu verwenden, müssen Ihre Firewalls eingehenden Datenverkehr auf bestimmten TCP-Ports erlauben.

HTML-Zugriff-Verbindungen müssen HTTPS verwenden. HTTP-Verbindungen sind nicht erlaubt.

Um sicherzustellen, dass die Windows-Firewall auf Sicherheitsservern so konfiguriert ist, dass Datenverkehr zum von HTML-Zugriff verwendeten TCP-Port erlaubt ist, siehe„Öffnen des Ports, der von HTML-Zugriff auf Sicherheitsservern verwendet wird“, auf Seite 23.

Tabelle 6. Firewall-Regeln für HTML-Zugriff

Source	Standard-quell-Port	Protokoll	Target	Standardziel-Port	Notizen
Client-Webbrowser	TCP beliebig	HTTPS	Sicherheitsserver oder View-Verbindungsserver-Instanz	TCP 443	Um die erste Verbindung zu Horizon View herzustellen, verbindet sich der Webbrowser auf einem Client-Gerät an TCP-Port 443 mit einem Sicherheitsserver oder einer View-Verbindungsserver-Instanz.
Client-Webbrowser	TCP beliebig	HTTPS	Blast Secure Gateway	TCP 8443	Nachdem die erste Verbindung zu Horizon View hergestellt ist, verbindet sich der Webbrowser auf einem Client-Gerät an TCP-Port 8443 mit dem Blast Secure Gateway. Das Blast Secure Gateway muss auf einem Sicherheitsserver oder einer View-Verbindungsserver-Instanz aktiviert sein, damit diese zweite Verbindung stattfinden kann. **Hinweis** Das Blast Secure Gateway ist mit dem View-Verbindungsserver in Horizon View 5.2 und späteren Versionen installiert.
Blast Secure Gateway	TCP beliebig	HTTPS	HTML-Zugriff-Agent	TCP 22443	Wenn, nachdem der Benutzer einen Horizon View-Desktop ausgewählt hat, das Blast Secure Gateway aktiviert ist, stellt das Blast Secure Gateway über den TCP-Port 22443 auf dem Desktop eine Verbindung zum HTML-Zugriff-Agent her.
Client-Webbrowser	TCP beliebig	HTTPS	HTML-Zugriff-Agent	TCP 22443	Wenn das Blast Secure Gateway, nachdem der Benutzer einen Horizon View-Desktop gewählt hat, nicht aktiviert ist, erstellt der Webbrowser auf einem Client-Gerät über den TCP-Port 22443 auf dem Desktop eine direkte Verbindung mit dem HTML-Zugriff-Agent.

Konfigurieren von HTML-Zugriff -Agents zur Verwendung von neuen SSL-Zertifikaten

Um Industrie- oder Sicherheitsvorschriften zu entsprechen, ersetzen Sie die Standard-SSL-Zertifikate, die vom HTML-Zugriff-Agent mit Zertifikaten erstellt wurden, die von einer Certificate Authority (CA) signiert wurden.

Wenn Sie den HTML-Zugriff-Agent auf Horizon View-Desktops installieren, erstellt der HTML-Zugriff-Agent-Dienst standardmäßig selbst signierte Zertifikate. Der Dienst liefert die Standardzertifikate an Browser, die HTML-Zugriff zur Herstellung einer Verbindung zu Horizon View verwenden.

Hinweis Im Gast-Betriebssystem auf der virtuellen Desktop-Maschine wird dieser Dienst VMware Blast-Dienst genannt.

Um die Standardzertifikate durch signierte Zertifikate zu ersetzen, die Sie von einer Zertifizierungsstelle erhalten haben, müssen Sie auf jedem Horizon View-Desktop ein Zertifikat in den lokalen Windows-Zertifikatspeicher des Computers importieren. Außerdem müssen Sie auf jedem Desktop einen Registrierungswert festlegen, der es dem HTML-Zugriff-Agent ermöglicht, das neue Zertifikat zu verwenden.

Wenn Sie die standardmäßigen HTML-Zugriff-Agent-Zertifikate durch CA-signierte Zertifikate ersetzt haben, empfiehlt VMware, dass Sie ein eindeutiges Zertifikat auf jedem einzelnen Desktop konfigurieren. Konfigurieren Sie kein CA-Zertifikat auf einer übergeordneten virtuellen Maschine oder Vorlage, die Sie für das Erstellen eines Desktop-Pools verwenden. Dieser Ansatz würde zu Hunderten oder Tausenden Desktops mit identischen Zertifikaten führen.

Vorgehensweise

1 Hinzufügen eines Zertifikats-Snap-In zu MMC auf einem Horizon View-Desktop auf Seite 25

Bevor Sie Zertifikate im lokalen Windows-Zertifikatspeicher des Computers hinzufügen können, müssen Sie das Zertifikats-Snap-In der Microsoft Management Console (MMC) auf den Horizon View-Desktops hinzufügen, auf denen der HTML-Zugriff-Agent installiert ist.

2 Importieren eines Zertifikats für den HTML-Zugriff Agent in den Windows-Zertifikatspeicher auf Seite 26

Um ein standardmäßiges HTML-Zugriff-Agent-Zertifikat durch ein CA-Zertifikat zu ersetzen, müssen Sie das CA-Zertifikat in den lokalen Windows-Zertifikatspeicher des Computers importieren. Führen Sie diese Prozedur auf jedem Desktop durch, auf dem der HTML-Zugriff-Agent installiert ist.

3 Importieren von Stamm- und Zwischenzertifikaten für den HTML-Zugriff-Agent auf Seite 27

Wenn die Stamm- und Zwischenzertifikate in der Zertifikatskette nicht mit dem SSL-Zertifikat importiert werden, das Sie für den HTML-Zugriff-Agent importiert haben, müssen Sie diese Zertifikate in den lokalen Windows-Zertifikatsspeicher des Computers importieren.

4 Einrichten des Zertifikatsfingerabdrucks in der Windows-Registrierung auf Seite 27

Damit der HTML-Zugriff-Agent ein CA-Zertifikat benutzen kann, das in den Windows-Zertifikatspeicher importiert wurde, müssen Sie den Fingerabdruck des Zertifikats in einem Windows-Registrierungsschlüssel konfigurieren. Sie müssen diesen Schritt auf jedem einzelnen Desktop ausführen, auf dem Sie das Standardzertifikat durch ein CA-signiertes Zertifikat ersetzen.

Hinzufügen eines Zertifikats-Snap-In zu MMC auf einem Horizon View-Desktop

Bevor Sie Zertifikate im lokalen Windows-Zertifikatspeicher des Computers hinzufügen können, müssen Sie das Zertifikats-Snap-In der Microsoft Management Console (MMC) auf den Horizon View-Desktops hinzufügen, auf denen der HTML-Zugriff-Agent installiert ist.

Voraussetzungen

Stellen Sie sicher, dass die MMC und das Zertifikats-Snap-In in dem Windows-Gast-Betriebssystem verfügbar ist, in dem der HTML-Zugriff-Agent installiert wurde.

Vorgehensweise

1 Auf dem Horizon View-Desktop klicken Sie auf **Start** und geben Sie **`mmc.exe`** ein.

2 Im Fenster MMC gehen Sie zu **Datei > Snap-In hinzufügen/entfernen**.

3 Im Fenster Snap-In hinzufügen oder entfernen wählen Sie **Zertifikate** und klicken auf **Hinzufügen**.

4 Im Fenster Zertifikate-Snap-In wählen Sie **Computer-Konto** aus. Klicken Sie auf **Weiter**, wählen Sie **Lokaler Computer** und klicken Sie auf **Beenden**.

5 Im Fenster Snap-In hinzufügen oder entfernen klicken Sie auf **OK**.

Weiter

Importieren Sie das SSL-Zertifikat in den Zertifikatsspeicher des lokalen Windows-Computers auf dem View Server-Host. Siehe „Importieren eines Zertifikats für den HTML-Zugriff Agent in den Windows-Zertifikatspeicher“, auf Seite 26.

Importieren eines Zertifikats für den HTML-Zugriff Agent in den Windows-Zertifikatspeicher

Um ein standardmäßiges HTML-Zugriff-Agent-Zertifikat durch ein CA-Zertifikat zu ersetzen, müssen Sie das CA-Zertifikat in den lokalen Windows-Zertifikatspeicher des Computers importieren. Führen Sie diese Prozedur auf jedem Desktop durch, auf dem der HTML-Zugriff-Agent installiert ist.

Voraussetzungen

- Stellen Sie sicher, dass der HTML-Zugriff-Agent auf dem Horizon View-Desktop installiert ist.
- Stellen Sie sicher, dass das CA-Zertifikat auf den Desktop kopiert wurde.
- Überprüfen Sie, ob das Zertifikat-Snap-In der MMC hinzugefügt wurde. Siehe „Hinzufügen eines Zertifikats-Snap-In zu MMC auf einem Horizon View-Desktop“, auf Seite 25.

Vorgehensweise

1. Erweitern Sie im Fenster MMC auf dem Horizon View-Desktop den Knoten **Zertifikate (Lokaler Computer)** und wählen Sie den Ordner **Persönlich**.
2. Wechseln Sie im Bereich „Aktionen“ zu **Weitere Aktionen > Alle Aufgaben > Importieren**.
3. Klicken Sie im Zertifikatsimport-Assistenten auf **Weiter** und navigieren Sie zum Speicherort des Zertifikats.
4. Wählen Sie die Zertifikatsdatei und klicken Sie auf **Öffnen**.

   Um den Typ Ihrer Zertifikatsdatei anzuzeigen, können Sie ihr Dateiformat im Dropdown-Menü **Dateiname** auswählen.
5. Geben Sie das Kennwort für den privaten Schlüssel in der Zertifikatsdatei ein.
6. Aktivieren Sie **Schlüssel als exportierbar markieren**.
7. Aktivieren Sie **Alle erweiterbaren Eigenschaften mit einbeziehen**.
8. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

   Das neue Zertifikat wird im Ordner **Zertifikate (Lokaler Computer) > Persönlich > Zertifikate** angezeigt.
9. Überprüfen Sie, ob das neue Zertifikat einen privaten Schlüssel enthält.
   a. Doppelklicken Sie im Ordner **Zertifikate (Lokaler Computer) > Persönlich > Zertifikate** auf das neue Zertifikat.
   b. Überprüfen Sie, ob im Dialogfeld „Zertifikatinformationen“ auf der Registerkarte „Allgemein“ die folgende Aussage angezeigt wird: `Sie besitzen einen privaten Schlüssel für dieses Zertifikat`.

Weiter

Falls erforderlich, importieren Sie das Stammzertifikat und Zwischenzertifikate in den Windows-Zertifikatsspeicher. Siehe „Importieren von Stamm- und Zwischenzertifikaten für den HTML-Zugriff-Agent“, auf Seite 27.

Konfigurieren Sie die entsprechenden Registrierungsschlüssel mit dem Fingerabdruck des Zertifikats. Siehe „Einrichten des Zertifikatsfingerabdrucks in der Windows-Registrierung“, auf Seite 27.

Importieren von Stamm- und Zwischenzertifikaten für den HTML-Zugriff -Agent

Wenn die Stamm- und Zwischenzertifikate in der Zertifikatskette nicht mit dem SSL-Zertifikat importiert werden, das Sie für den HTML-Zugriff-Agent importiert haben, müssen Sie diese Zertifikate in den lokalen Windows-Zertifikatsspeicher des Computers importieren.

Vorgehensweise

1 Auf der MMC-Konsole auf Horizon View-Desktop erweitern Sie den Knoten **Zertifikate (Lokaler Computer)** und gehen Sie zum Ordner **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.

- Wenn sich Ihr Stammzertifikat in diesem Ordner befindet und Ihre Zertifikatskette keine Zwischenzertifikate enthält, übergehen Sie diese Prozedur.
- Wenn Ihr Stammzertifikat sich nicht in diesem Ordner befindet, fahren Sie mit Schritt 2 fort.

2 Klicken Sie mit der rechten Maustaste auf den Ordner **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate** und klicken Sie auf **Alle Aufgaben > Importieren**.

3 Klicken Sie im Zertifikatsimport-Assistenten auf **Weiter** und navigieren Sie zum Speicherort des Stamm-Zertifizierungsstellenzertifikats.

4 Wählen Sie die Datei mit dem Stamm-Zertifizierungsstellenzertifikat aus und klicken Sie auf **Öffnen**.

5 Klicken Sie auf **Weiter**, klicken Sie auf **Weiter** und klicken Sie auf **Fertigstellen**.

6 Wenn Ihr Serverzertifikat von einer Zwischenzertifizierungsstelle signiert wurde, importieren Sie alle Zwischenzertifikate in der Zertifikatskette in den Zertifikatspeicher des lokalen Windows-Computers.

a Navigieren Sie zum Ordner **Zertifikate (Lokaler Computer) > Zwischenzertifizierungsstellen > Zertifikate**.

b Wiederholen Sie die Schritte 3 bis 6 für jedes zu importierende Zwischenzertifikat.

Weiter

Konfigurieren Sie die entsprechenden Registrierungsschlüssel mit dem Fingerabdruck des Zertifikats. Siehe „Einrichten des Zertifikatsfingerabdrucks in der Windows-Registrierung“, auf Seite 27.

Einrichten des Zertifikatsfingerabdrucks in der Windows-Registrierung

Damit der HTML-Zugriff-Agent ein CA-Zertifikat benutzen kann, das in den Windows-Zertifikatspeicher importiert wurde, müssen Sie den Fingerabdruck des Zertifikats in einem Windows-Registrierungsschlüssel konfigurieren. Sie müssen diesen Schritt auf jedem einzelnen Desktop ausführen, auf dem Sie das Standardzertifikat durch ein CA-signiertes Zertifikat ersetzen.

Voraussetzungen

Stellen Sie sicher, dass das CA-signierte Zertifikat in den Windows-Zertifikatspeicher importiert wurde. Siehe „Importieren eines Zertifikats für den HTML-Zugriff Agent in den Windows-Zertifikatspeicher“, auf Seite 26.

Vorgehensweise

1 Im MMC-Fenster auf dem Horizon View-Desktop, wo der HTML-Zugriff-Agent installiert ist, navigieren Sie zum Ordner **Zertifikate (Lokaler Computer) > Persönliche > Zertifikate**.

2 Doppelklicken Sie auf das CA-Zertifikat, das Sie in den Windows-Zertifikatsspeicher importiert haben.

3 Im Dialogfeld Zertifikate klicken Sie auf die Registerkarte Details. Blättern Sie nach unten und wählen Sie das Symbol **Fingerabdruck**.

4 Kopieren Sie den ausgewählten Fingerabdruck in eine Textdatei.

Beispiel: `31 2a 32 50 1A 0B 34 b1 65 46 13 a8 0A 5E f7 43 6E a9 2C 3E`

Hinweis Wenn Sie den Fingerabdruck kopieren, dürfen Sie das führende Leerzeichen nicht mitkopieren. Wenn Sie versehentlich das führende Leerzeichen mit dem Fingerabdruck zusammen in den Registrierungsschlüssel (in Schritt 7) einfügen, kann es sein, dass das Zertifikat nicht erfolgreich konfiguriert werden kann. Dieses Problem kann auftreten, obwohl das führende Leerzeichen nicht im Textfeld Registrierungswert angezeigt wird.

5 Starten Sie den Windows-Registrierungs-Editor auf dem Desktop, wo der HTML-Zugriff-Agent installiert ist.

6 Navigieren Sie zum Registrierungsschlüssel `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config`.

7 Ändern Sie den `SslHash`-Wert und fügen Sie den Fingerabdruck des Zertifikats in das Textfeld ein.

8 Starten Sie den VMware Blast-Dienst neu, damit Ihre Änderungen wirksam werden.

Im Windows-Gast-Betriebssystem wird der Dienst für den HTML-Zugriff-Agent VMware Blast genannt.

Wenn sich ein Benutzer über HTML-Zugriff mit einem Desktop verbindet, präsentiert der HTML-Zugriff-Agent dem Browser des Benutzers das CA-Zertifikat.

Konfigurieren von Sicherheitsprotokollen und Verschlüsselungssammlungen für HTML Access-Agent

Ab Feature Pack 5 (FP5) können Sie die Sicherheitsprotokolle und Verschlüsselungssammlungen konfigurieren, die HTML-Zugriff Agent verwendet, indem Sie die Windows-Registrierung bearbeiten. Sie können die Konfigurationen auch in einem Gruppenrichtlinienobjekt (GPO) festlegen.

Standardmäßig verwendet der FP5 HTML-Zugriff Agent nur TLS 1.0, TLS 1.1 und TLS 1.2. Die zulässigen Protokolle sind (mit steigender Sicherheit) TLS 1.0, TLS 1.1 und TLS 1.2. Ältere Protokolle wie z. B. SSLv3 und frühere Versionen sind niemals zulässig. Zwei Registrierungswerte, `SslProtocolLow` und `SslProtocolHigh`, legen den Protokollbereich fest, den HTML Access Agent akzeptiert. Zum Beispiel bewirken die Einstellungen `SslProtocolLow=tls_1.0` und `SslProtocolHigh=tls_1.2`, dass HTML-Zugriff Agent TLS 1.0, TLS 1.1 und TLS 1.2 akzeptiert. Die Standardeinstellungen sind `SslProtocolLow=tls_1.0` und `SslProtocolHigh=tls_1.2`.

Sie müssen die Liste der Verschlüsselungen festlegen, und zwar mit dem Format, das in http://openssl.org/docs/manmaster/apps/ciphers.html im Abschnitt FORMAT DER VERSCHLÜSSELUNGSLISTE definiert ist. Die folgende Verschlüsselungsliste wird standardmäßig verwendet:

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

Vorgehensweise

1 Starten Sie den Windows-Registrierungs-Editor.

2 Navigieren Sie zum Registrierungsschlüssel `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config`.

3 Fügen Sie zwei neue Zeichenfolgenwerte (REG_SZ), `SslProtocolLow` und `SslProtocolHigh`, hinzu, um den Protokollbereich anzugeben.

Die Daten für die Registrierungswerte müssen `tls_1.0`, `tls_1.1` oder `tls_1.2` sein. Um nur ein Protokoll zu aktivieren, geben Sie dasselbe Protokoll für beide Registrierungswerte an. Wenn einer der beiden Registrierungswerte nicht vorhanden ist oder wenn seine Daten nicht auf eines der drei Protokolle festgelegt sind, werden die Standardprotokolle verwendet.

4 Fügen Sie einen neuen Zeichenfolgenwert (REG_SZ), `SslCiphers`, hinzu, um einen Liste von Verschlüsselungssammlungen anzugeben.

   Geben Sie die Liste von Verschlüsselungssammlungen in das Datenfeld des Registrierungswerts ein oder fügen Sie sie ein. Beispiel:

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

5 Führen Sie einen Neustart des Windows-Dienstes VMware Blast durch.

Um zur Nutzung der standardmäßigen Verschlüsselungsliste zurückzukehren, löschen Sie den `SslCiphers`-Registrierungswert und starten Sie den Windows-Dienst VMware Blast neu. Löschen Sie nicht einfach den Datenteil des Werts, sonst behandelt der HTML-Zugriff-Agent alle Verschlüsselungsverfahren entsprechend der Formatdefinition für die OpenSSL-Verschlüsselungsliste als inakzeptabel.

Wenn der HTML-Zugriff Agent startet, schreibt er die Protokoll- und Verschlüsselungsinformationen in seine Protokolldatei. Sie können die Protokolldatei überprüfen, um festzustellen, welche Werte in Kraft sind.

Die Standardprotokolle und Verschlüsselungssammlungen können sich auf der Grundlage der von VMware empfohlenen und ständig weiterentwickelten Vorgehensweisen für die Netzwerksicherheit zukünftig ändern.

Konfigurieren von Unity Touch

Sie können eine Standardliste der Favoritenanwendungen konfigurieren, die in der Unity Touch-Sidebar angezeigt werden, und Sie können die Unity Touch-Funktion nach der Installation deaktivieren oder aktivieren.

Konfigurieren von Favoritenanwendungen durch Unity Touch

Mit der Unity Touch-Funktion können Tablet- und Smartphone-Benutzer von einer Unity Touch-Sidebar aus schnell zu einer Horizon View-Desktop-Anwendung oder -Datei navigieren. Wenngleich Endbenutzer festlegen können, welche Favoritenanwendungen in der Sidebar angezeigt werden sollen, können Administratoren zur Verbesserung der Benutzerfreundlichkeit eine Standardliste mit Favoritenanwendungen konfigurieren.

Wenn Sie dynamische Desktop-Pools einsetzen, gehen die von den Endbenutzern festgelegten Favoritenanwendungen und -dateien verloren, wenn sie die Verbindung mit einem Desktop trennen. Dies gilt nicht, wenn Sie in Active Directory die Verwendung von Roamingbenutzerprofilen aktivieren.

Die Standardliste der Favoritenanwendungen bleibt erhalten, wenn sich ein Endbenutzer zum ersten Mal mit einem Desktop verbindet, der für Unity Touch aktiviert ist. Wenn der Benutzer jedoch eigene Favoritenanwendungen konfiguriert, wird die Standardliste ignoriert. Die vom Benutzer definierte Liste der Favoritenanwendungen wird im Roamingbenutzerprofil abgelegt und ist verfügbar, wenn sich der Benutzer in einem dynamischen oder persistenten Pool an anderen Desktops anmeldet.

Wenn Sie eine Standardliste mit Favoritenanwendungen erstellen und mindestens eine der Anwendungen nicht auf dem Horizon View-Desktop-Betriebssystem installiert ist oder die Pfade zu diesen Anwendungen nicht im Startmenü gefunden werden, wird die Anwendung nicht in der Favoritenliste angezeigt. Sie können dieses Verhalten dazu nutzen, um eine Master-Standardliste mit Favoritenanwendungen einzurichten, die anschließend auf mehrere virtuelle Maschinen-Images angewendet werden kann, auf denen unterschiedliche Anwendungen installiert sind.

Wenn beispielsweise Microsoft Office 2010 und Microsoft Visio auf einer virtuellen Maschine installiert sind und Windows Powershell und VMware vSphere Client auf einer zweiten virtuellen Maschine, können Sie eine Liste erstellen, die alle vier Anwendungen enthält. Es werden nur die installierten Anwendungen als standardmäßige Favoritenanwendungen auf den jeweiligen Desktops angezeigt.

Sie können unterschiedliche Methoden zur Festlegung einer Standardliste mit Favoritenanwendungen einsetzen.

- Fügen Sie der Windows-Registrierung auf den virtuellen Desktop-Maschinen einen Wert hinzu.
- Erstellen Sie ein administratives Installationspaket aus dem Remote Experience Agent-Installationsprogramm und verteilen Sie das Paket an die virtuellen Maschinen.
- Führen Sie auf den virtuellen Maschinen das Remote Experience Agent-Installationsprogramm von der Befehlszeile aus.

Hinweis Für Unity Touch wird davon ausgegangen, dass sich Verknüpfungen für Anwendungen im Programmordner des Menüs **Start** befinden. Wenn sich eine Verknüpfung außerhalb des Programmordners befindet, fügen Sie das Präfix **`Programs`** in den Verknüpfungspfad ein. Beispiel: `Windows Update.lnk` befindet sich im Ordner `ProgramData\Microsoft\Windows\Start Menu`. Zur Veröffentlichung dieser Verknüpfung als standardmäßige Favoritenanwendung fügen Sie dem Verknüpfungspfad das Präfix **`Programs`** hinzu. Beispiel: `"Programs/Windows Update.lnk"`.

Voraussetzungen

- Stellen Sie sicher, dass der Remote Experience Agent auf der virtuellen Maschine installiert ist.
- Vergewissern Sie sich, dass Sie über Administratorrechte für die virtuelle Maschine verfügen. Für dieses Verfahren müssen Sie möglicherweise eine Registrierungseinstellung bearbeiten.
- Wenn Sie dynamische Desktop-Pools einsetzen, verwenden Sie Active Directory zum Einrichten von Roamingbenutzerprofilen. Folgen Sie den von Microsoft bereitgestellten Anweisungen.

  Benutzer von dynamischen Pool-Desktops sind in der Lage, ihre Liste mit Favoritenanwendungen und -dateien bei jeder Anmeldung anzuzeigen.

Vorgehensweise

- (Optional) Erstellen Sie eine Standardliste mit Favoritenanwendungen, indem Sie der Windows-Registrierung einen Wert hinzufügen.

  a Öffnen Sie `regedit` und navigieren Sie zur Registrierungseinstellung `HKLM\Software\VMware, Inc.\VMware Unity`.

  Navigieren Sie auf einer virtuellen Maschine mit 64 Bit zum Verzeichnis `HKLM\Software\Wow6432Node\VMware, Inc.\VMware Unity`.

  b Erstellen Sie einen Zeichenfolgenwert mit dem Namen `FavAppList`.

  c Geben Sie die standardmäßigen Favoritenanwendungen an.

  Verwenden Sie das folgende Format, um die Verknüpfungspfade zu den Anwendungen im Startmenü anzugeben.

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

  Beispiel:

  ```
  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
  ```

- (Optional) Erstellen Sie eine Standardliste mit Favoritenanwendungen, indem Sie ein administratives Installationspaket aus dem Remote Experience Agent-Installationsprogramm erstellen.

  a Verwenden Sie an der Befehlszeile das folgende Format, um das administrative Installationspaket zu erstellen.

  ```
  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"""
  ```

  Beispiel:

  ```
  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 Verteilen Sie das administrative Installationspaket von der Netzwerkfreigabe auf den virtuellen Desktop-Maschinen, indem Sie eine standardmäßige MSI-Bereitstellungsmethode (Microsoft Windows Installer) einsetzen, die in Ihrer Organisation verwendet wird.

- (Optional) Erstellen Sie eine Standardliste mit Favoritenanwendungen, indem Sie das Remote Experience Agent-Installationsprogramm an der Befehlszeile einer virtuellen Maschine direkt ausführen.

  Verwenden Sie das folgende Format.

  ```
  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"""
  ```

  Hinweis Der oben gezeigte Befehl kombiniert die Installation des Remote Experience Agent mit der Festlegung einer Standardliste mit Favoritenanwendungen. Sie müssen den Remote Experience Agent nicht installieren, bevor Sie diesen Befehl ausführen.

Weiter

Wenn Sie diese Aufgabe direkt auf einer virtuellen Maschine ausführen (indem Sie die Windows-Registrierung bearbeiten oder den Remote Experience Agent über die Befehlszeile installieren), müssen Sie die neu konfigurierte virtuelle Maschine bereitstellen. Sie können einen Snapshot oder eine Vorlage erstellen und einen Horizon View-Desktop-Pool anlegen oder einen vorhandenen Pool neu zusammenstellen. Alternativ können Sie eine Active Directory-Gruppenrichtlinie zur Bereitstellung der neuen Konfiguration erstellen.

Deaktivieren oder Aktivieren von Unity Touch

Wenn Sie den Remote Experience Agent installieren, ist die Installationsoption für Unity Touch automatisch ausgewählt und die Funktion aktiviert. Sie können die Unity Touch-Funktion für ausgewählte Desktops deaktivieren oder erneut aktivieren, indem Sie einen Windows-Registrierungsschlüssel auf diesen Desktops festlegen.

Sie können die Registrierung nur dann zur Aktivierung von Unity Touch verwenden, wenn Unity Touch über das Remote Experience Agent-Installationsprogramm installiert und dann über die Registrierung deaktiviert wurde. Wenn Unity Touch nicht installiert wurde, d. h. die Option wurde bei der Remote Experience Agent-Installation nicht ausgewählt, und Sie anschließend den Registrierungswert zum Aktivieren von Unity Touch festlegen, arbeiten bestimmte Unity Touch-Funktionen nicht ordnungsgemäß.

Vorgehensweise

1 Starten Sie den Windows-Registrierungs-Editor auf dem virtuellen Desktop.

2 Navigieren Sie zum Windows-Registrierungsschlüssel, der Unity Touch steuert.

Option	Beschreibung
Windows 7, 64 Bit	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware Unity\enabled = Wert`
Windows 7, 32 Bit	`HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware Unity\enabled = Wert`

3 Legen Sie den Wert so fest, dass Unity Touch deaktiviert oder aktiviert wird.

Option	Wert
Deaktiviert	`0`
Aktiviert	`1`

Per Voreinstellung ist der Wert auf `1` festgelegt.

Konfigurieren der Flash-URL-Umleitung für das Multicast- oder Unicast-Streaming

Kunden können ab sofort Adobe Media Server und Multicast oder Unicast zur Bereitstellung von Live-Videoereignissen in einer VDI-Umgebung (Virtual Desktop Infrastructure) nutzen. Zur Bereitstellung von Multicast- oder Unicast-Videostreams in einer VDI-Umgebung sollte der Medienstream unter Umgehung der virtuellen Desktops direkt von der Medienquelle an die Endpunkte gesendet werden. Die Flash-URL-Umleitung unterstützt diese Funktion, indem die ShockWave-Datei (SWF) abgefangen und vom virtuellen Desktop an den Clientendpunkt umgeleitet wird.

Die Flash-URL-Umleitung verwendet ein JavaScript, das durch den Webseitenadministrator in eine HTML-Webseite eingebettet wird. Immer dann, wenn ein Benutzer eines virtuellen Desktops aus einer Webseite auf den festgelegten URL-Link klickt, fängt das JavaScript die SWF-Datei von der virtuellen Desktop-Sitzung ab und leitet sie an den Clientendpunkt um. Der Endpunkt kann anschließend außerhalb der virtuellen Desktop-Sitzung einen lokalen Flash Projector öffnen und den Medienstream lokal abspielen.

Zum Konfigurieren der Flash-URL-Umleitung müssen Sie Ihre HTML-Webseite und Ihre Clientgeräte einrichten.

Vorgehensweise

1 Sicherstellen, dass die Flash-URL-Umleitung installiert ist auf Seite 33

Bevor Sie diese Funktion verwenden, müssen Sie sicherstellen, dass der Remote Experience Agent mit der Flash-URL-Umleitung auf Ihren virtuellen Desktops installiert wurde und ausgeführt wird.

2 Einrichten der Webseiten zur Bereitstellung von Multicast- oder Unicast-Streams auf Seite 33

Zur Unterstützung der Flash-URL-Umleitung müssen Sie einen JavaScript-Befehl in die MIME HTML-Webseiten (MHTML) einbetten, der Links zu den Multicast- oder Unicast-Streams bereitstellt. Benutzer zeigen diese Webseiten in den Browsern auf ihren virtuellen Desktops an, um auf die Video-Streams zuzugreifen.

3 Einrichten von Clientgeräten für die Flash-URL-Umleitung auf Seite 34

Die Flash-URL-Umleitung leitet die SWF-Datei von virtuellen Desktops an Clientgeräte um. Um diesen Clientgeräten die Wiedergabe von Flash-Videos über einen Multicast- oder Unicast-Stream zu ermöglichen, müssen Sie sicherstellen, dass der geeignete Adobe Flash Player auf den Clientgeräten installiert ist. Die Clients müssen außerdem über IP-Konnektivität mit der Medienquelle verfügen.

4 Deaktivieren oder Aktivieren der Flash-URL-Umleitung auf Seite 34

Wenn Sie den Remote Experience Agent installieren und die Installationsoption für die Flash-URL-Umleitung auswählen, wird diese Funktion aktiviert. Sie können die Flash-URL-Umleitung für ausgewählte Desktops deaktivieren oder erneut aktivieren, indem Sie einen Windows-Registrierungsschlüssel auf diesen Desktops festlegen.

Sicherstellen, dass die Flash-URL-Umleitung installiert ist

Bevor Sie diese Funktion verwenden, müssen Sie sicherstellen, dass der Remote Experience Agent mit der Flash-URL-Umleitung auf Ihren virtuellen Desktops installiert wurde und ausgeführt wird.

Die Flash-URL-Umleitung muss auf jedem Desktop vorhanden sein, auf dem Sie die Multicast- oder Unicast-Umleitung unterstützen möchten. Anweisungen zur Installation des Remote Experience Agent finden Sie unter „Installation und Bereitstellung des Remote Experience Agent auf Horizon View-Desktops“, auf Seite 14.

Vorgehensweise

1 Starten Sie eine virtuelle Desktop-Sitzung, die PCoIP verwendet.

2 Öffnen Sie den Task-Manager.

3 Stellen Sie sicher, dass der Prozess `ViewMPServer.exe` auf dem Desktop ausgeführt wird.

Einrichten der Webseiten zur Bereitstellung von Multicast- oder Unicast-Streams

Zur Unterstützung der Flash-URL-Umleitung müssen Sie einen JavaScript-Befehl in die MIME HTML-Webseiten (MHTML) einbetten, der Links zu den Multicast- oder Unicast-Streams bereitstellt. Benutzer zeigen diese Webseiten in den Browsern auf ihren virtuellen Desktops an, um auf die Video-Streams zuzugreifen.

Darüber hinaus können Sie die englische Fehlermeldung anpassen, die dem Endbenutzer angezeigt wird, wenn ein Problem bei der Flash-URL-Umleitung auftritt. Führen Sie diesen optionalen Schritt aus, wenn Sie Ihren Endbenutzern eine lokalisierte Fehlermeldung anzeigen möchten. Sie müssen die Konfiguration „`var vmwareScriptErroMessage`“ zusammen mit dem lokalisierten Text in die MHTML-Webseite einbetten.

Voraussetzungen

Stellen Sie sicher, dass die Bibliothek `swfobject.js` in die MHTML-Webseite importiert wurde.

Vorgehensweise

1 Betten Sie den JavaScript-Befehl `viewmp.js` in die MHTML-Webseite ein.

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

2 (Optional) Passen Sie die Fehlermeldung zur Flash-URL-Umleitung an, die den Endbenutzern gesendet wird.

Beispiel: `"var vmwareScriptErroMessage=`*`lokalisierte Fehlermeldung`*`"`

3 Stellen Sie sicher, dass Sie den JavaScript-Befehl „`viewmp.js`“ einbetten und optional die Fehlermeldung zur Flash-URL-Umleitung anpassen, bevor Sie die ShockWave Flash-Datei (SWF) in die MHTML-Webseite importieren.

Wenn ein Benutzer die Webseite in einem virtuellen Desktop anzeigt, löst der JavaScript-Befehl `viewmp.js` den Flash-URL-Umleitungsmechanismus auf dem virtuellen Desktop aus, der die SWF-Datei vom Desktop an das hostende Clientgerät umleitet.

Einrichten von Clientgeräten für die Flash-URL-Umleitung

Die Flash-URL-Umleitung leitet die SWF-Datei von virtuellen Desktops an Clientgeräte um. Um diesen Clientgeräten die Wiedergabe von Flash-Videos über einen Multicast- oder Unicast-Stream zu ermöglichen, müssen Sie sicherstellen, dass der geeignete Adobe Flash Player auf den Clientgeräten installiert ist. Die Clients müssen außerdem über IP-Konnektivität mit der Medienquelle verfügen.

Hinweis Bei der Flash-URL-Umleitung wird der Multicast- oder Unicast-Stream an Clientgeräte umgeleitet, die sich möglicherweise außerhalb der Unternehmensfirewall befinden. Ihre Clients müssen auf den Adobe Webserver zugreifen können, auf dem die SWF-Datei zur Initiierung des Multicast- oder Unicast-Streaming gehostet wird. Falls erforderlich, müssen Sie in Ihrer Firewall die geeigneten Ports öffnen, um Clientgeräten den Zugriff auf diesen Server zu ermöglichen.

Vorgehensweise

- Installieren Sie Adobe Flash Player auf Ihren Clientgeräten.

Betriebssystem	Aktion
Windows	Installieren Sie Adobe Flash Player 10.1 oder höher für Internet Explorer.
Linux	a Installieren Sie die Datei „`libexpat.so.0`“ oder stellen Sie sicher, dass diese Datei bereits installiert ist. Stellen Sie sicher, dass die Datei im Verzeichnis „`/usr/lib`“ oder „`/usr/local/lib`“ installiert ist. b Installieren Sie die Datei `libflashplayer.so` oder stellen Sie sicher, dass diese Datei bereits installiert ist. Vergewissern Sie sich, dass die Datei im geeigneten Flash-Plug-In-Verzeichnis für Ihr Linux-Betriebssystem installiert ist. c Installieren Sie das Programm `wget` oder stellen Sie sicher, dass die Programmdatei bereits installiert ist.

Deaktivieren oder Aktivieren der Flash-URL-Umleitung

Wenn Sie den Remote Experience Agent installieren und die Installationsoption für die Flash-URL-Umleitung auswählen, wird diese Funktion aktiviert. Sie können die Flash-URL-Umleitung für ausgewählte Desktops deaktivieren oder erneut aktivieren, indem Sie einen Windows-Registrierungsschlüssel auf diesen Desktops festlegen.

Vorgehensweise

1 Starten Sie den Windows-Registrierungs-Editor auf dem virtuellen Desktop.

2 Navigieren Sie zum Windows-Registrierungsschlüssel, der die Flash-URL-Umleitung steuert.

Option	Beschreibung
Windows 7, 64 Bit	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware ViewMP\enabled = Wert`
Windows 7, 32 Bit	`HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware ViewMP\enabled = Wert`

3 Legen Sie den Wert so fest, dass Flash-URL-Umleitung deaktiviert oder aktiviert wird.

Option	Wert
Deaktiviert	`0`
Aktiviert	`1`

Per Voreinstellung ist der Wert auf `1` festgelegt.

Konfigurieren von Echtzeit-Audio/Video

Nachdem Sie Echtzeit-Audio/Video installiert haben, funktioniert diese Funktion auf Horizon View-Desktops ohne eine weitere Konfiguration. Die Standardwerte für Webcam-Bildrate und -Bildauflösung werden für die meisten Standardgeräte und -anwendungen empfohlen.

Sie können Gruppenrichtlinieneinstellungen konfigurieren, um diese Standardwerte an bestimmte Anwendungen, Webcams oder Umgebungen anzupassen. Siehe „Konfigurieren von Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video“, auf Seite 41.

Wenn Benutzer über mehrere integrierte oder an ihre Clientcomputer angeschlossene Webcams und Audioeingabegeräte verfügen, können Sie bevorzugte Webcams und Audioeingabegeräte konfigurieren, die an ihre Desktops umgeleitet werden. Siehe „Auswählen von bevorzugten Webcams und Mikrofonen“, auf Seite 36.

Hinweis Sie können ein bevorzugtes Audiogerät auswählen, es stehen jedoch keine weiteren Optionen für die Audiokonfiguration zur Verfügung.

Wenn Webcambilder und Audioeingangsdaten an einen Remote-Desktop umgeleitet werden, können Sie auf dem lokalen Computer nicht auf die Webcam oder die Audiogeräte zugreifen. Ebenso können diese Geräte nicht auf dem Remote-Desktop verwendet werden, wenn auf dem lokalen Computer darauf zugegriffen wird.

Echtzeit-Audio/Video wird für Desktops im lokalen Modus nicht unterstützt.

Weitere Informationen zu unterstützten Anwendungen finden Sie im VMware KB-Artikel *Richtlinien zur Arbeit mit Echzeit-Audio/Video mit Drittanbieteranwendungen auf Horizon View Desktops* unter http://kb.vmware.com/kb/2053754.

Sicherstellen, dass anstelle der USB-Umleitung Echtzeit-Audio/Video verwendet wird

Echtzeit-Audio/Video unterstützt die Umleitung von Webcams und Audioeingabegeräten für die Verwendung in Konferenzanwendungen. Die mit View Agent installierbare Funktion für die USB-Umleitung bietet keine Unterstützung für die Umleitung von Webcams. Wenn Sie für Audioeingabegeräte die USB-Umleitung nutzen, wird der Audiostream bei Echtzeit-Audio/Video-Sitzungen nicht ordnungsgemäß mit den Videodaten synchronisiert, und Sie können nicht von verringerten Anforderungen an die Netzwerkbandbreite profitieren. Durch die Ausführung bestimmter Schritte können Sie sicherstellen, dass Webcams und Audioeingabegeräte nicht die USB-Umleitung verwenden, sondern über Echtzeit-Audio/Video an Ihre Desktops umgeleitet werden.

Wenn Ihre Desktops zur Verwendung der USB-Umleitung konfiguriert sind, können Endbenutzer lokal angeschlossene USB-Geräte verbinden und anzeigen, indem sie die Option **USB-Gerät verbinden** in der Menüleiste von VMware Horizon View Client auswählen.

Wenn ein Endbenutzer ein USB-Gerät aus der Liste **USB-Gerät verbinden** auswählt, kann dieses Gerät nicht mehr für Video- oder Audiokonferenzen verwendet werden. Wenn ein Benutzer beispielsweise einen Skype-Anruf tätigt, wird das Videobild möglicherweise nicht angezeigt, oder die Qualität der Audiodaten ist herabgesetzt. Wenn ein Endbenutzer während einer Konferenzsitzung ein Gerät auswählt, kommt es zu einem Fehler bei der Webcam- oder Audioumleitung.

Zum Ausblenden dieser Geräte für die Endbenutzer und zur Vermeidung potenzieller Konflikte können Sie die Gruppenrichtlinieneinstellungen für die USB-Umleitung so konfigurieren, dass Webcams und Audioeingabegeräte in VMware Horizon View Client nicht angezeigt werden.

Insbesondere können Sie Filterregeln für die USB-Umleitung für den Horizon View Agent erstellen und die Anzeige der Gerätefamilien `audio-in` und `video` deaktivieren. Informationen zum Einrichten von Gruppenrichtlinien und die Festlegung von Filterregeln für die USB-Umleitung finden Sie unter „Verwenden von Richtlinien zur Steuerung der USB-Umleitung“ im Dokument *Verwaltung von VMware Horizon View-*.

Vorsicht Wenn Sie keine Filterregeln für die USB-Umleitung einrichten, um die Anzeige von USB-Gerätefamilien zu deaktivieren, informieren Sie Ihre Endbenutzer darüber, dass sie keine Webcams oder Audiogeräte aus der Liste **USB-Gerät verbinden** in der Menüleiste von VMware Horizon View Client auswählen können.

Auswählen von bevorzugten Webcams und Mikrofonen

Wenn ein Clientcomputer über mehrere Webcams und Mikrofone verfügt, können Sie eine bevorzugte Webcam und ein Standardmikrofon konfigurieren, die bzw. das über die Echtzeit-Audio/Video-Funktion an den Desktop umgeleitet wird. Diese Geräte können in den lokalen Clientcomputer integriert oder mit diesem verbunden sein.

Auf einem Windows-Clientcomputer wählen Sie eine bevorzugte Webcam aus, indem Sie einen Registrierungsschlüsselwert festlegen. Auf einem Linux-Clientcomputer können Sie eine bevorzugte Webcam oder ein Mikrofon angeben, indem Sie eine Konfigurationsdatei bearbeiten. Die Echtzeit-Audio/Video-Funktion leitet die bevorzugte Webcam um, sofern diese verfügbar ist. Falls nicht, verwendet die Echtzeit-Audio/Video-Funktion die erste Webcam, die bei der Systemauflistung bereitgestellt wird.

Zur Auswahl eines Standardmikrofons konfigurieren Sie die Option „Sound“ im Windows- oder Linux-Betriebssystem auf dem Clientcomputer.

Auswählen einer bevorzugten Webcam auf einem Windows-Clientsystem

Wenn Sie die Echtzeit-Audio/Video-Funktion einsetzen und auf Ihrem Clientsystem über mehrere Webcams verfügen, wird nur eine davon auf Ihrem View-Desktop verwendet. Zur Festlegung einer bevorzugten Webcam können Sie einen Registrierungsschlüsselwert festlegen.

Die bevorzugte Webcam wird auf dem View-Desktop verwendet, sofern Sie verfügbar ist. Andernfalls wird eine andere Webcam verwendet.

Voraussetzungen

- Stellen Sie sicher, dass auf Ihrem Clientsystem eine USB-Webcam installiert und betriebsbereit ist.
- Vergewissern Sie sich, dass Sie das PCoIP-Anzeigeprotokoll für Ihren View-Desktop verwenden.

Vorgehensweise

1 Schließen Sie die Webcam an, die Sie verwenden möchten.

2 Starten Sie einen Anruf, und stoppen Sie den Anruf.

  Auf diese Weise wird eine Protokolldatei erstellt.

3 Öffnen Sie die Debug-Protokolldatei mit einem Texteditor.

Betriebssystem	Protokolldatei, Speicherort
Windows XP	`C:\Dokumente und Einstellungen\Benutzername\Lokale Einstellungen\Anwendungsdaten\VMware\VDM\Logs\debug-20JJ-MM-TT-XXXXXX.txt`
Windows 7 oder Windows 8	`C:\Benutzer\%username%\AppData\Local\VMware\VDM\Logs\debug-20JJ-MM-TT-XXXXXX.txt`

Das Format der Protokolldatei lautet `debug-20JJ-MM-TT-XXXXXX.txt`, wobei 20*JJ* für das Jahr, *MM* für den Monat, *TT* für den Tag und *XXXXXX* für eine Nummer steht.

4 Durchsuchen Sie die Protokolldatei nach `[ViewMMDevRedir] VideoInputBase::LogDevEnum`, um die Protokolldateieinträge zu finden, in denen die angeschlossenen Webcams referenziert werden.

Nachfolgend sehen Sie einen Auszug aus der Protokolldatei zur Identifikation der Microsoft Lifecam HD-5000-Webcam:

```
[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 Kopieren Sie die Benutzer-ID der bevorzugten Webcam.

Beispiel: Kopieren Sie `vid_045e&pid_076d&mi_00#8&11811f49&0&0000`, um die Microsoft LifeCam HD-5000 als Standardwebcam festzulegen.

6 Starten Sie den Registrierungs-Editor (`regedit.exe`) und navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\RTAV`.

7 Fügen Sie den ID-Bestandteil der Zeichenfolgen in den REG_SZ-Wert **srcWCamId** ein.

Beispiel: Fügen Sie `vid_045e&pid_076d&mi_00#8&11811f49&0&0000` in **srcWCamId** ein.

8 Speichern Sie Ihre Änderungen und beenden Sie die Registrierung.

9 Starten Sie einen neuen Anruf.

Auswählen einer bevorzugten Webcam oder eines Mikrofons auf einem Linux-Clientsystem

Wenn Sie die Echtzeit-Audio/Video-Funktion einsetzen und auf Ihrem Clientsystem über mehrere Webcams und Mikrofone verfügen, kann nur eine Webcam oder ein Mikrofon auf Ihrem View-Desktop verwendet werden. Um die Webcam- und Mikrofonpräferenz anzugeben, können Sie eine Konfigurationsdatei bearbeiten.

Die bevorzugte Webcam oder das Mikrofon wird auf dem View-Desktop verwendet, sofern sie bzw. es verfügbar ist. Andernfalls wird eine andere Webcam oder ein anderes Mikrofon verwendet.

Mit der Echtzeit-Audio/Video-Funktion arbeiten Webcams, Audioeingabe- und Audioausgabegeräte ohne Verwendung der USB-Umleitung ordnungsgemäß und die erforderliche Netzwerkbandbreite wird erheblich verringert. Analoge Audioeingabegeräte werden ebenfalls unterstützt.

Um die Eigenschaften in der Datei „`/etc/vmware/config`“ sowie um ein bevorzugtes Gerät festzulegen, müssen Sie die Gerätekennung ermitteln.

- Für Webcams legen Sie die Eigenschaft „`rtav.srcWCamId`“ auf den Wert der in der Protokolldatei gefundenen Webcam-Beschreibung fest, wie im Folgenden beschrieben.

- Für Audiogeräte legen Sie die Eigenschaft „`rtav.srcAudioInId`“ auf den Wert des PULSE-Audio-Felds „`device.description`“ fest.

  Durchsuchen Sie die Protokolldatei wie nachfolgend beschrieben, um den Wert dieses Feldes zu ermitteln.

Voraussetzungen

Führen Sie die entsprechenden Vorabaufgaben durch, je nachdem, ob Sie eine Webcam, ein Mikrofon oder beides auswählen:

- Stellen Sie sicher, dass auf Ihrem Clientsystem eine USB-Webcam installiert und betriebsbereit ist.
- Stellen Sie sicher, dass ein USB-Mikrofon oder ein anderer Mikrofontyp auf Ihrem Clientsystem installiert und betriebsbereit ist.
- Vergewissern Sie sich, dass Sie das PCoIP-Anzeigeprotokoll für Ihren View-Desktop verwenden.

Vorgehensweise

1 Starten Sie den Client und eine Webcam- oder Mikrofonanwendung, um eine Auflistung der Kamerageräte oder Audiogeräte im Clientprotokoll auszulösen.

   a Schließen Sie die Webcam oder das Audiogerät an, die bzw. das Sie verwenden möchten.

   b Verwenden Sie den Befehl „`vmware-view`“, um View Client zu starten.

   c Starten Sie einen Anruf und beenden Sie ihn dann.

   Auf diese Weise wird eine Protokolldatei erstellt.

2 Suchen Sie nach Protokolleinträgen für die Webcam oder das Mikrofon.

a Öffnen Sie die Debug-Protokolldatei mit einem Texteditor.

Die Protokolldatei mit Echtzeit-Audio/Video-Protokollnachrichten befindet sich unter „/tmp/vmware-*<Benutzername>*/vmware-mks-*<pid>*.log“. Das Clientprotokoll befindet sich unter „/tmp/vmware-*<Benutzername>*/vmware-view-*<pid>*.log“.

b Durchsuchen Sie die Protokolldatei nach den Einträgen, die auf die angeschlossenen Webcams und Mikrofone verweisen.

Das folgende Beispiel zeigt einen Auszug der Webcam-Auswahl:

```
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
```

Das folgende Beispiel zeigt einen Auszug der Audiogeräteauswahl sowie den jeweiligen aktuellen Audiopegel:

```
vthread–18| I120: RTAV: bool AudioCaptureLin::TriggerEnumDevices() – Triggering enumera–
tion
vthread–18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) – PulseAudio Get Source (idx=1 'alsa_output.usb–Logi–
tech_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–Logi–
tech_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–Micro–
soft_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
```

Es werden Warnungen angezeigt, wenn einer der Quellaudiopegel für das ausgewählte Gerät nicht die PulseAudio-Kriterien erfüllt, wenn die Quelle nicht auf 100 % (0 dB) gesetzt ist oder wenn das ausgewählte Quellgerät stummgeschaltet wurde. Beispiel:

```
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 Kopieren Sie die Beschreibung des Geräts und verwenden Sie sie zum Festlegen der entsprechenden Eigenschaft in der Datei „`/etc/vmware/config`“.

Kopieren Sie beispielsweise bei einer Webcam „`Microsoft® LifeCam HD-6000 for Notebooks`“, um die Microsoft-Webcam als bevorzugte Webcam festzulegen sowie um die Eigenschaft folgendermaßen anzugeben:

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

In diesem Beispiel könnten Sie die Eigenschaft auch auf „`rtav.srcWCamId="Microsoft"`“ festlegen.

Kopieren Sie beispielsweise für ein Audiogerät „`Logitech USB Headset Analog Mono`“, um das Logitech-Headset als bevorzugtes Audiogerät festzulegen sowie um die Eigenschaft folgendermaßen anzugeben:

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

4 Speichern Sie Ihre Änderungen und schließen Sie die Konfigurationsdatei „`/etc/vmware/config`“.

5 Starten Sie einen neuen Anruf.

Auswählen eines Standardmikrofons auf einem Windows-Clientsystem

Wenn Sie auf Ihrem Clientsystem über mehrere Mikrofone verfügen, wird nur eines davon auf Ihrem View-Desktop verwendet. Zur Festlegung, welches Mikrofon standardmäßig verwendet werden soll, können Sie die Option „Sound“ auf Ihrem Clientsystem verwenden.

Mit der Echtzeit-Audio/Video-Funktion arbeiten Audioeingabe- und Audioausgabegeräte ohne Verwendung der USB-Umleitung ordnungsgemäß, und die erforderliche Netzwerkbandbreite wird erheblich verringert. Analoge Audioeingabegeräte werden ebenfalls unterstützt.

Wichtig Wenn Sie ein USB-Mikrofon verwenden, verbinden Sie dieses nicht über das Menü **USB-Gerät verbinden** in Horizon View Client. In diesem Fall würde das Gerät über die USB-Umleitung umgeleitet, sodass die Echtzeit-Audio/Video-Funktion nicht genutzt werden kann.

Voraussetzungen

- Stellen Sie sicher, dass ein USB-Mikrofon oder ein anderer Mikrofontyp auf Ihrem Clientsystem installiert und betriebsbereit ist.
- Vergewissern Sie sich, dass Sie das PCoIP-Anzeigeprotokoll für Ihren View-Desktop verwenden.

Vorgehensweise

1 Wenn Sie gerade einen Anruf tätigen, beenden Sie das Gespräch.

2 Klicken Sie mit der rechten Maustaste auf das Lautsprechersymbol in der Systemleiste und wählen Sie **Aufnahmegeräte**.

Alternativ können Sie die Option „Sound“ in der Systemsteuerung öffnen und auf die Registerkarte **Aufnahme** klicken.

3 Klicken Sie im Dialogfeld **Sound** auf der Registerkarte **Aufnahme** mit der rechten Maustaste auf das Mikrofon, das Sie verwenden möchten.

4 Wählen Sie **Als Standardgerät auswählen** und klicken Sie auf **OK**.

5 Starten Sie über View-Desktop einen neuen Anruf.

Auswählen eines Standardmikrofons auf einem Linux-Clientsystem

Wenn Sie auf Ihrem Clientsystem über mehrere Mikrofone verfügen, wird nur eines davon auf Ihrem View-Desktop verwendet. Zur Festlegung, welches Mikrofon standardmäßig verwendet werden soll, können Sie die Option „Sound“ auf Ihrem Clientsystem verwenden.

Mit der Echtzeit-Audio/Video-Funktion arbeiten Audioeingabe- und Audioausgabegeräte ohne Verwendung der USB-Umleitung ordnungsgemäß, und die erforderliche Netzwerkbandbreite wird erheblich verringert. Analoge Audioeingabegeräte werden ebenfalls unterstützt.

Dieses Verfahren beschreibt die Auswahl eines Standardmikrofons über die Benutzeroberfläche des Clientsystems. Administratoren können auch ein bevorzugtes Mikrofon konfigurieren, indem sie eine Konfigurationsdatei bearbeiten. Siehe „Auswählen einer bevorzugten Webcam oder eines Mikrofons auf einem Linux-Clientsystem“, auf Seite 37.

Voraussetzungen

- Stellen Sie sicher, dass ein USB-Mikrofon oder ein anderer Mikrofontyp auf Ihrem Clientsystem installiert und betriebsbereit ist.
- Vergewissern Sie sich, dass Sie das PCoIP-Anzeigeprotokoll für Ihren View-Desktop verwenden.

Vorgehensweise

1 Wählen Sie auf der Ubuntu-Benutzeroberfläche **System > Preferences > Sound**.

  Alternativ können Sie auf das **Sound**-Symbol am rechten Rand der Symbolleiste am oberen Bildschirmrand klicken.

2 Klicken Sie im Dialogfeld „Sound Preferences“ auf die Registerkarte **Input**.

3 Wählen Sie das bevorzugte Gerät aus und klicken Sie auf **Close**.

Konfigurieren von Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video

Sie können Gruppenrichtlinieneinstellungen konfigurieren, die das Verhalten der Echtzeit-Audio/Video-Funktion (Real-Time Audio-Video, RTAV) auf Ihren Horizon View-Desktops steuert. Mithilfe dieser Einstellungen wird die maximale Bildrate und -auflösung einer virtuellen Webcam festgelegt. Die Einstellungen ermöglichen es Ihnen, die maximale Bandbreite zu verwalten, die ein Benutzer belegen kann. Über eine zusätzliche Einstellung wird die RTAV-Funktion deaktiviert oder aktiviert.

Sie müssen diese Richtlinieneinstellungen nicht konfigurieren. Die Echtzeit-Audio/Video-Funktion verwendet die Bildrate und -auflösung, die für die Webcam auf den Clientsystemen festgelegt ist. Für die meisten Webcams und Audioanwendungen werden die Standardeinstellungen empfohlen.

Beispiele für die Bandbreitenbelegung durch die Echtzeit-Audio/Video-Funktion finden Sie unter „Bandbreite für Echtzeit-Audio/Video“, auf Seite 44.

Diese Richtlinieneinstellungen wirken sich auf Ihre Horizon View-Desktops aus, nicht auf die Clientsysteme, an die die physischen Geräte angeschlossen sind. Fügen Sie zum Konfigurieren dieser Einstellungen auf Ihren Desktops die administrative Vorlagendatei (ADM) für die RTAV-Gruppenrichtlinie in Active Directory hinzu.

Informationen zum Konfigurieren von Einstellungen auf Clientsystemen finden Sie im VMware KB-Artikel *Festlegen von Frame-Raten und Auflösung für Echtzeit-Audio/Video auf Horizon View Clients* unter http://kb.vmware.com/kb/2053644.

Hinzufügen der RTAV ADM-Vorlage in Active Directory und Konfigurieren der Einstellungen

Horizon View stellt auf der Seite für VMware-Produktdownloads eine RTAV ADM-Datei bereit, `vdm_agent_rtav.adm`. Sie können die Richtlinieneinstellungen in dieser ADM-Datei zu Gruppenrichtlinienobjekten (GPOs) in Active Directory hinzufügen und im Gruppenrichtlinienobjekt-Editor die zugehörigen Einstellungen konfigurieren.

Zur einfacheren Handhabung ist die RTAV ADM-Datei in einer ZIP-Datei mit allen weiteren Horizon View-ADM-Dateien gebündelt.

Die RTAV ADM-Datei ist in dieser Feature Pack-Version neu. Die weiteren ADM-Dateien entsprechen den Versionen, die mit Horizon View 5.3 auf dem View-Verbindungsserver im Pfad *`Installationsverzeichnis`*`\VMware\VMware View\Server\extras\GroupPolicyFiles` installiert werden. Es ist nicht erforderlich, die weiteren ADM-Dateien erneut zu installieren, wenn Sie diese bei der Installation von oder beim Upgrade auf Horizon View 5.3 bereits zu Active Directory hinzugefügt haben.

Voraussetzungen

- Stellen Sie sicher, dass der Remote Experience Agent mit der RTAV-Option auf Ihren Desktops installiert wurde. Die Einstellungen haben keine Auswirkungen, wenn RTAV nicht installiert ist. Siehe „Installation und Bereitstellung des Remote Experience Agent auf Horizon View-Desktops“, auf Seite 14.
- Stellen Sie sicher, dass Active Directory-GPOs für die RTAV-Gruppenrichtlinieneinstellungen erstellt wurden. Die GPOs müssen mit der OU verknüpft werden, die Ihre Desktops enthält. Allgemeine Informationen zum Einrichten von Horizon View-Gruppenrichtlinieneinstellungen in Active Directory finden Sie unter „Konfigurieren von Richtlinien“ im Dokument *Verwaltung von VMware Horizon View-*.
- Vergewissern Sie sich, dass Microsoft Management Console (MMC) und das Snap-In „Gruppenrichtlinienobjekt-Editor“ auf Ihrem Active Directory-Server installiert sind.
- Machen Sie sich mit den RTAV-Gruppenrichtlinieneinstellungen vertraut. Siehe „Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video“, auf Seite 43.

Vorgehensweise

1 Laden Sie die Horizon View-ADM-ZIP-Datei von der Webseite für VMware-Produktdownloads herunter.

   Die ZIP-Datei trägt den Namen `VMware-Horizon-View-GPO-Bundle-`*`y.y.y-xxxxxx`*`.zip`, wobei *y.y.y.* für die Version und *xxxxxx* für die Buildnummer steht.

2 Extrahieren Sie die Datei und kopieren Sie die RTAV ADM-Datei „`vdm_agent_rtav.adm`“ auf Ihren Active Directory-Server.

3 Bearbeiten Sie auf dem Active Directory-Server das GPO, indem Sie **Start > Verwaltung > Gruppenrichtlinienverwaltung** wählen, mit der rechten Maustaste auf das GPO klicken und **Bearbeiten** auswählen.

4 Klicken Sie im Gruppenrichtlinienobjekt-Editor mit der rechten Maustaste auf den Ordner **Computerkonfiguration > Administrative Vorlagen** und wählen Sie **Vorlagen hinzufügen/entfernen**.

5 Klicken Sie auf **Hinzufügen**, wechseln Sie zur Datei „`vdm_agent_rtav.adm`“ und klicken Sie auf **Öffnen**.

6 Klicken Sie auf **Schließen**, um die Richtlinieneinstellungen in der ADM-Datei auf das GPO anzuwenden.

   Die Einstellungen sind im Ordner **Computerkonfiguration > Administrative Vorlagen > Klassische administrative Vorlagen > VMware View Agent-Konfiguration > View RTAV-Konfiguration** enthalten.

7 Konfigurieren Sie die RTAV-Gruppenrichtlinieneinstellungen.

Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video

Die Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video (Real-Time Audio-Video, RTAV) steuern die maximale Bildrate und -auflösung für die virtuelle Webcam. Über eine zusätzliche Einstellung können Sie die RTAV-Funktion deaktivieren oder aktivieren. Diese Richtlinieneinstellungen wirken sich auf Horizon View-Desktops aus, nicht auf die Clientsysteme, an die die physischen Geräte angeschlossen sind.

Wenn Sie die RTAV-Gruppenrichtlinieneinstellungen nicht konfigurieren, verwendet RTAV die Werte, die auf den Clientsystemen festgelegt sind. Auf Clientsystemen beträgt die standardmäßige Bildrate für Webcams 15 Bilder pro Sekunde. Die standardmäßige Bildauflösung für Webcams beträgt 320 x 240 Pixel.

Die RTAV-Gruppenrichtlinieneinstellungen legen die Werte fest, die maximal verwendet werden können. Die auf den Clientsystemen festgelegte Bildrate und -auflösung sind absolute Werte. Wenn Sie beispielsweise die RTAV-Einstellungen auf eine maximale Bildauflösung von 640 x 480 Pixel festlegen, zeigt die Webcam eine beliebige auf dem Client festgelegt Auflösung bis 640 x 480 Pixel an. Wenn Sie die Bildauflösung auf dem Client auf einen höheren Wert als 640 x 480 Pixel festlegen, wird die Clientauflösung bei 640 x 480 Pixeln gedeckelt.

Nicht alle Konfigurationen können die maximale Gruppenrichtlinieneinstellung von 1920 x 1080 Pixeln bei 25 Bildern pro Sekunde erzielen. Die maximale Bildrate, die Ihre Konfiguration für eine vorgegebene Auflösung unterstützen kann, richtet sich nach der verwendeten Webcam, der Clientsystemhardware, der virtuellen View Agent-Hardware und der verfügbaren Bandbreite.

Gruppenrichtlinieneinstellung	Beschreibung
RTAV deaktivieren	Wenn Sie diese Einstellung aktivieren, wird die Echtzeit-Audio/Video-Funktion deaktiviert. Wenn diese Einstellung weder konfiguriert noch deaktiviert ist, wird die Echtzeit-Audio/Video-Funktion aktiviert. Diese Einstellung befindet sich im Ordner **View-RTAV-Konfiguration**.
Maximale Anzahl von Bildern pro Sekunde	Legt die maximale Rate pro Sekunde fest, mit der die Webcam Bilder erfassen kann. Sie können mit dieser Einstellung die Bildrate der Webcam in Netzwerkumgebungen mit niedriger Bandbreite einschränken. Der Mindestwert liegt bei einem Bild pro Sekunde. Der Maximalwert liegt bei 25 Bildern pro Sekunde. Wenn diese Einstellung weder konfiguriert noch deaktiviert ist, wird keine maximale Bildrate festgelegt. Für die Echtzeit-Audio/Video-Funktion wird die Bildrate verwendet, die auf dem Clientsystem für die Webcam ausgewählt wurde. Standardmäßig ist Clientwebcams eine Bildrate von 15 Bildern pro Sekunde zugewiesen. Wenn auf dem Clientsystem keine Einstellung konfiguriert ist und die Einstellung **Maximale Anzahl von Bildern pro Sekunde** weder konfiguriert noch deaktiviert ist, erfasst die Webcam 15 Bilder pro Sekunde. Diese Einstellung befindet sich im Ordner **View-RTAV-Konfiguration > View-RTAV-Webcameinstellungen**.

Gruppenrichtlinieneinstellung	Beschreibung
Auflösung – maximale Bildbreite in Pixeln	Legt die maximale Breite (in Pixeln) von Bildern fest, die von der Webcam erfasst werden. Durch Festlegung einer niedrigen maximalen Bildbreite können Sie die Auflösung erfasster Bilder senken, wodurch die Benutzererfahrung in Netzwerkumgebungen mit niedriger Bandbreite verbessert werden kann. Wenn diese Einstellung weder konfiguriert noch deaktiviert ist, wird keine maximale Bildbreite festgelegt. RTAV verwendet die Bildbreite, die auf dem Clientsystem festgelegt ist. Die Standardbreite eines Webcambildes auf einem Clientsystem liegt bei 320 Pixeln. Die Obergrenze für ein beliebiges Webcambild liegt bei 1920 x 1080 Pixeln. Wenn Sie diese Einstellung mit einem Wert konfigurieren, der über 1920 Pixeln liegt, beträgt die effektive maximale Bildbreite 1920 Pixel. Diese Einstellung befindet sich im Ordner **View-RTAV-Konfiguration > View-RTAV-Webcameinstellungen**.
Auflösung – maximale Bildhöhe in Pixeln	Legt die maximale Höhe (in Pixeln) von Bildern fest, die von der Webcam erfasst werden. Durch Festlegung einer niedrigen maximalen Bildhöhe können Sie die Auflösung erfasster Bilder senken, wodurch die Benutzererfahrung in Netzwerkumgebungen mit niedriger Bandbreite verbessert werden kann. Wenn diese Einstellung weder konfiguriert noch deaktiviert ist, wird keine maximale Bildhöhe festgelegt. RTAV verwendet die Bildhöhe, die auf dem Clientsystem festgelegt ist. Die Standardhöhe eines Webcambildes auf einem Clientsystem liegt bei 240 Pixeln. Die Obergrenze für ein beliebiges Webcambild liegt bei 1920 x 1080 Pixeln. Wenn Sie diese Einstellung mit einem Wert konfigurieren, der über 1080 Pixeln liegt, beträgt die effektive maximale Bildhöhe 1080 Pixel. Diese Einstellung befindet sich im Ordner **View-RTAV-Konfiguration > View-RTAV-Webcameinstellungen**.

Bandbreite für Echtzeit-Audio/Video

Die Bandbreite für Echtzeit-Audio/Video variiert in Abhängigkeit von der Bildauflösung und -rate der Webcam sowie den aufgezeichneten Bild- und Audiodaten.

Die Beispieltests unter Tabelle 7 messen die Bandbreite, die von der Echtzeit-Audio/Video-Funktion in einer Horizon View-Umgebung mit Standardwebcam und standardmäßigen Audioeingabegeräten belegt wird. Mit den Tests wird die Bandbreite gemessen, die zum Senden von Video- und Audiodaten von Horizon View Client an den Horizon View Agent erforderlich ist. Die insgesamt benötigte Bandbreite zur Durchführung einer Desktop-Sitzung über View Client kann höher liegen als hier angegeben. Bei diesen Tests erfasst die Webcam Bilder für jede Bildauflösung mit einer Rate von 15 Bildern pro Sekunde.

Tabelle 7. Beispielergebnisse für die erforderliche Bandbreite zum Senden von Echtzeit-Audio/Video-Daten von Horizon View Client an den Horizon View Agent

Bildauflösung (Breite x Höhe)	Belegte Bandbreite (Kbit/s)
160 x 120	225
320 x 240	320
640 x 480	600

Verwalten des Zugriffs auf die Multimedia-Umleitung von Windows 7

Sie können Maßnahmen ergreifen, um sicherzustellen, dass die Multimedia-Umleitung (MMR) von Windows 7 nur für View Client-Systeme zugänglich ist, die über entsprechende Ressourcen verfügen und in einem sicheren Netzwerk mit Horizon View verbunden sind.

MMR-Daten werden ohne anwendungsbasierte Verschlüsselung über das Netzwerk gesendet und können je nach umgeleitetem Inhalt vertrauliche Daten enthalten. Um sicherzustellen, dass diese Daten nicht im Netzwerk überwacht werden können, verwenden Sie MMR nur in einem sicheren Netzwerk.

Es bietet sich an, MMR zu deaktivieren, wenn die Clientsysteme über unzureichende Ressourcen verfügen, um die lokale Multimedia-Dekodierung zu verarbeiten, oder wenn Sie den Zugriff auf MMR nur für Clientsysteme in einem sicheren Netzwerk gewähren möchten. Sie können in View Administrator eine Richtlinie mit Namen **Multimedia-Umleitung (MMR)** konfigurieren, mit der Sie MMR für Clientsysteme aktivieren oder deaktivieren können. Sie können die Richtlinie global, für bestimmte Desktop-Pools oder für spezifische Benutzer festlegen. Die Richtlinie ist per Voreinstellung aktiviert. Die Richtlinie wirkt sich auf MMR für Windows 7-, Windows XP- und Windows Vista-Desktops aus. Nähere Informationen finden Sie unter „Konfigurieren von Richtlinien“ im Dokument *Verwaltung von VMware Horizon View-*.

Sicherstellen, dass Clients Windows 7 MMR initiieren können

Windows 7 MMR verwendet einen Handshake zwischen dem Horizon View Client-System und dem Desktop, um Anfragen für die Multimedia-Umleitung (MMR) zu überprüfen. Unter bestimmten Netzwerkbedingungen dauert dieser Handshake zu lange, sodass MMR nicht initiiert wird. Um sicherzustellen, dass Windows 7 MMR initiiert werden kann, können Sie auf dem Desktop einen Windows-Registrierungsschlüssel konfigurieren, um die Zeit zu verlängern, die für die Durchführung der Handshake-Überprüfung zulässig ist.

Der Windows-Registrierungsschlüssel steuert den TTL-Wert (Time to Live) des Handshakes und wird in Millisekunden angegeben. Der Schlüssel hat das REG_DWORD (hex)-Format. Der Standardwert liegt bei 5000 Millisekunden (5 Sekunden).

Bevor Sie Windows 7 MMR für Ihre Horizon View-Benutzer bereitstellen, sollten Sie ein paar Clientsysteme testen, um sicherzustellen, dass die zulässige Standardzeit für die Durchführung des Handshakes für Ihre Umgebung angemessen ist. Wenn für Ihre Netzwerkbedingungen ein längerer Handshake als fünf Sekunden erforderlich ist, erhöhen Sie den TTL-Wert.

Vorgehensweise

1 Starten Sie den Windows-Registrierungs-Editor auf dem virtuellen Desktop.

2 Navigieren Sie zum Windows-Registrierungsschlüssel, der den MMR-Überprüfungs-Handshake steuert.

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

3 Erhöhen Sie den `handshakeTTL`-Wert auf eine Zahl größer als 5000.

4 Starten Sie den Windows Media Player auf dem Desktop neu, um den aktualisierten Wert anzuwenden.

Index