Verwendung von VMware Horizon Client für Windows

Horizon Client 4.4

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-002434-00

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

Verwendung von VMware Horizon Client für Windows

Dieses Handbuch, *Verwendung von VMware Horizon Client für Windows*, bietet Informationen zur Installation und Verwendung der VMware Horizon® Client™-Software auf einem Microsoft Windows-Clientsystem zur Verbindungsherstellung mit einem Remote-Desktop oder einer Remoteanwendung im Datencenter.

Die Informationen in diesem Dokument umfassen Systemanforderungen und Anweisungen zur Installation und Verwendung von Horizon Client für Windows.

Diese Informationen sind für Administratoren bestimmt, die eine Bereitstellung von Horizon mit Microsoft Windows-Clientsystemen einrichten müssen, z. B. für Desktops und Laptops. Die Informationen wurden für erfahrene Systemadministratoren verfasst, die mit der Technologie virtueller Maschinen sowie mit Datencenter-Vorgängen vertraut sind.

Systemanforderungen und Setup von Windows-basierten Clients

1

Systeme, auf denen Horizon Client-Komponenten ausgeführt werden, müssen bestimmte Hardware- und Softwareanforderungen erfüllen.

Auf Windows-Systemen verwendet Horizon Client zum Herstellen einer Verbindung mit dem Verbindungsserver die Interneteinstellungen von Microsoft Internet Explorer (einschließlich Proxy-Einstellungen). Stellen Sie sicher, dass die richtigen Internet Explorer-Einstellungen festgelegt sind und dass Sie über Internet Explorer auf die Verbindungsserver-URL zugreifen können.

Dieses Kapitel behandelt die folgenden Themen:

Systemanforderungen für Windows-Clients

Sie können Horizon Client für Windows auf PCs oder Laptops installieren, auf denen ein unterstütztes Microsoft Windows-Betriebssystem ausgeführt wird.

Sowohl die PCs oder Laptops, auf denen Sie Horizon Client installieren, als auch die verwendeten Peripheriegeräte müssen bestimmte Systemanforderungen erfüllen.

Modell

Alle x86- oder x86-64-Windows-Geräte

Arbeitsspeicher

Mindestens 1GB RAM

Betriebssysteme

Es werden die folgenden Betriebssysteme unterstützt:

Betriebssystem	Version	Service Pack oder Wartungsoption	Unterstützte Editionen
Windows 10	32 oder 64 Bit	Current Branch (CB) Version 1607 Current Business Branch (CBB) Version 1607 Long-Term Servicing Branch (LTSB) Version 1607	Home, Pro, Enterprise und IoT Core
Windows 8 oder 8.1	32 oder 64 Bit	Keines oder Update 2	Pro , Enterprise und Embedded Industry
Windows 7	32 oder 64 Bit	SP1	Home, Enterprise, Professional und Ultimate
Windows Server 2008 R2	64 Bit	Letztes Update	Standard
Windows Server 2012 R2	64 Bit	Letztes Update	Standard

Windows Server 2008 R2 und Windows Server 2012 R2 werden für die Ausführung von Horizon Client im geschachtelten Modus unterstützt. Weitere Informationen finden Sie unter „Im geschachtelten Modus unterstützte Funktionen“, auf Seite 91.

Verbindungsserver, Sicherheitsserver und View Agent oder Horizon Agent

Aktuelle Wartungsversion von View 5.3.x und neuere Versionen

Wenn Clientsysteme von außerhalb der firmeneigenen Firewall eine Verbindung herstellen, empfiehlt VMware die Verwendung eines Sicherheitsservers oder der Access Point-Appliance, damit Clientsysteme keine VPN-Verbindung benötigen.

Veröffentlichte Remoteanwendungen sind nur auf Servern mit Horizon 6.0 oder höher verfügbar.

Hinweis Clients können sich auch mit der Access Point-Appliance verbinden, die in Horizon 6 Version 6.2 oder höher verfügbar ist.

Anzeigeprotokolle

VMware Blast, PCoIP und RDP

Hardwareanforderungen für PCoIP und VMware Blast

- x86-basierter Prozessor mit SSE2-Erweiterungen, mit einer Prozessorgeschwindigkeit von 800 MHz oder höher.

- Verfügbarer RAM über den Systemanforderungen zur Unterstützung verschiedener Monitorkonfigurationen. Im Allgemeinen gilt die folgende Formel:

  ```
  20MB + (24 * (# monitors) * (monitor width) * (monitor height))
  ```

  Als grobes Maß können Sie die folgenden Berechnungen verwenden:

  ```
  1 monitor: 1600 x 1200: 64MB
  2 monitors: 1600 x 1200: 128MB
  3 monitors: 1600 x 1200: 256MB
  ```

Hardwareanforderungen für RDP

- x86-basierter Prozessor mit SSE2-Erweiterungen, mit einer Prozessorgeschwindigkeit von 800 MHz oder höher.
- 128 MB RAM.

Softwareanforderungen für RDP

- In Verbindung mit Windows 7 sollten Sie RDP 7.1 oder 8.0 verwenden. Windows 7 schließt RDP 7 ein. Windows 7 SP1 schließt RDP 7.1 ein.
- In Verbindung mit Windows 8 sollten Sie RDP 8.0 und in Verbindung mit Windows 8.1 die Version RDP 8.1 verwenden.
- Für Windows 10 ist RDP 10.0 zu verwenden.
- (Nur mit View Agent 6.0.2 und niedriger unterstützt) Für virtuelle Windows XP-Maschinen müssen Sie die RDP-Patches installieren, die in den Knowledgebase-Artikeln 323497 und 884020 aufgeführt sind. Wenn Sie die RDP-Patches nicht installieren, wird möglicherweise ein `Windows Socket–Fehler` auf dem Client angezeigt.
- Das Agent-Installationsprogramm konfiguriert die lokale Firewall-Regel für eingehende RDP-Verbindungen entsprechend dem aktuellen RDP-Port des Hostbetriebssystems (üblicherweise 3389). Wenn Sie die RDP-Portnummer ändern, müssen Sie auch die dazugehörigen Firewall-Regeln ändern.

Die RDC-Versionen stehen im Microsoft Download Center zum Download zur Verfügung.

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-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen.

Remote-Desktops

Auf den Desktops muss View Agent 5.2 oder höher oder Horizon Agent 7.0 oder höher installiert sein. Für View Agent 5.2-Desktops muss auf den Desktops auch der entsprechende Remote Experience Agent installiert sein. Wenn beispielsweise View Agent 5.2 installiert ist, müssen Sie auch den Remote Experience Agent aus dem View 5.2 Feature Pack 2 installieren. Informationen dazu finden Sie im Dokument *Installation und Administration von*

View Feature Pack. Wenn Sie über View Agent 6.0 oder höher oder über Horizon Agent 7.0 oder höher verfügen, ist kein Feature Pack erforderlich. Um die Echtzeit-Audio-Video-Funktion mit veröffentlichten Desktops und Anwendungen zu verwenden, benötigen Sie Horizon Agent 7.0.2 oder höher.

Horizon Client-Computer oder Clientzugriffsgerät

- Echtzeit-Audio/Video wird auf allen Betriebssystemen unterstützt, auf denen Horizon Client für Windows ausgeführt wird. Weitere Informationen finden Sie unter „Systemanforderungen für Windows-Clients“, auf Seite 10.
- 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 der Agent installiert ist.

Anzeigeprotokolle

- PCoIP
- VMware Blast (erfordert Horizon Agent 7.0 oder höher)

Anforderungen für die Scannerumleitung

Sie können Informationen über Ihre Remote-Desktops und Remoteanwendungen unter Verwendung von Scannern einscannen, die mit Ihrem lokalen Clientsystem verbunden sind.

Damit Sie diese Funktion nutzen können, müssen Ihre Remote-Desktops, Remoteanwendungen und Clientcomputer bestimmte Systemanforderungen erfüllen.

Remote-Desktops

Auf den Remote-Desktops muss View Agent 6.0.2 oder höher oder Horizon Agent 7.0 höher mit aktivierter Setup-Option „Scannerumleitung“ auf übergeordneten virtuellen Maschinen oder VM-Vorlagen oder RDS-Hosts installiert sein. Auf Windows-Desktop- und Windows-Server-Gastbetriebssystemen ist die Horizon Agent-Setup-Option „Scannerumleitung“ standardmäßig deaktiviert.

Informationen zu den auf Einzelbenutzer-VMs und RDS-Hosts unterstützten Gastbetriebssystemen und zum Konfigurieren der Scannerumleitung auf Remote-Desktops und in Remoteanwendungen finden Sie unter „Konfigurieren der Scannerumleitung“ in *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Horizon Client-Computer oder Clientzugriffsgerät

- Die Scannerumleitung wird auf Windows 7, Windows 8/8.1 und Windows 10 unterstützt.
- Auf dem Clientcomputer müssen Treiber für das Scannergerät installiert sein, und der Scanner muss betriebsbereit sein. Es ist nicht erforderlich, die Scanner-Gerätetreiber auf dem Betriebssystem des Remote-Desktops zu installieren, auf dem der Agent installiert ist.

Scangerät-Standard

TWAIN oder WIA

Anzeigeprotokolle

- PCoIP
- VMware Blast (erfordert Horizon Agent 7.0 oder höher)

Scannerumleitung wird in RDP-Desktop-Sitzungen nicht unterstützt.

Anforderungen für die Umleitung serieller Ports

Mithilfe dieser Funktion können Benutzer lokal verbundene, serielle Ports (COM-Ports) wie integrierte RS232-Ports oder USB-Seriell-Adapter auf ihre Remote-Desktops umleiten. Zur Unterstützung der Umleitung für serielle Ports muss Ihre Horizon-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen.

Remote-Desktops

Auf den Remote-Desktops muss View Agent 6.1.1 oder höher oder Horizon Agent 7.0 oder höher mit aktivierter Setup-Option für die Umleitung serieller Ports auf übergeordneten virtuellen Maschinen oder VM-Vorlagen installiert sein. Diese Setup-Option ist standardmäßig nicht ausgewählt.

Die folgenden Gastbetriebssysteme werden auf virtuellen Einzelsitzungsmaschinen unterstützt.

- Windows 7, 32 oder 64 Bit
- Windows 8.x, 32 oder 64 Bit
- Windows 10, 32 oder 64 Bit
- Windows Server 2008 R2, als Desktop konfiguriert
- Windows Server 2012 R2, als Desktop konfiguriert
- Windows Server 2016, als Desktop konfiguriert

Diese Funktion wird aktuell nicht für Windows Server-RDS-Hosts unterstützt.

Es ist nicht erforderlich, die Gerätetreiber für serielle Ports auf dem Desktop-Betriebssystem zu installieren, auf dem der Agent installiert ist.

Hinweis Informationen zur Konfiguration der Umleitung für serielle Ports in Remote-Desktops finden Sie unter „Konfigurieren der Umleitung serieller Ports“ in *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Horizon Client-Computer oder Clientzugriffsgerät

- Die Umleitung für seriellen Port wird auf Windows 7, Windows 8.x-Clientsystemen und Windows 10 unterstützt.
- Auf dem Clientcomputer müssen die erforderlichen Gerätetreiber für serielle Ports installiert und der serielle Port muss betriebsbereit sein. Es ist nicht erforderlich, die Gerätetreiber auf dem Betriebssystem des Remote-Desktops zu installieren, auf dem der Agent installiert ist.

Anzeigeprotokolle

- PCoIP
- VMware Blast (erfordert Horizon Agent 7.0 oder höher)

Die Umleitung serieller Ports für VMware Horizon wird in RDP-Desktop-Sitzungen nicht unterstützt.

Voraussetzungen für die Multimedia-Umleitung (MMR)

Mit Multimedia-Umleitung (MMR) wird der Multimedia-Stream auf dem Clientsystem verarbeitet, d. h. entschlüsselt. Das Clientsystem gibt die Medieninhalte wieder und reduziert so die Auslastung des ESXi-Hosts.

Remote-Desktops

- Auf Einzelbenutzer-Desktops muss View Agent 6.0.2 oder höher oder Horizon Agent 7.0 oder höher installiert sein.
- Auf sitzungsbasierten Desktops muss View Agent 6.1.1 oder höher oder Horizon Agent 7.0 oder höher auf dem RDS-Host installiert sein.
- Informationen zu den Betriebssystem- und anderen Softwareanforderungen sowie zu Konfigurationseinstellungen für den Remote-Desktop bzw. für die Remoteanwendung finden Sie in den Themen über die Windows-Multimedia-Umleitung in *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Horizon Client-Computer oder Clientzugriffsgerät

Windows 7, Windows 8.x oder Windows 10 mit jeweils 32 oder 64 Bit.

Unterstützte Medienformate

In Windows Media Player unterstützte Medienformate werden unterstützt. Beispielsweise: M4V; MOV; MP4; WMP; MPEG-4 Part 2; WMV 7, 8 und 9; WMA; AVI; ACE; MP3; WAV.

Hinweis DRM-geschützter Inhalt wird nicht über Windows Media MMR umgeleitet.

Anforderungen für die Flash-URL-Umleitung

Mit der Flash-Umleitung wird bei Verwendung des Internet Explorers (Versionen 9, 10, 11) Flash-Inhalt an das Clientsystem gesendet. Das Clientsystem gibt die Medieninhalte wieder und verringert so die Last auf dem ESXi-Host.

Remote-Desktop

- Horizon Agent 7.0 oder höher muss in einem Remote-Desktop für Einzelbenutzer (VDI) mit der Option für die Flash-Umleitung installiert sein. Die Flash-Umleitung ist standardmäßig nicht ausgewählt.

  Informationen zur Installation von Horizon Agent finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.
- Es müssen auch die erforderlichen Gruppenrichtlinieneinstellungen konfiguriert werden. Zur Konfiguration der Flash-Umleitung finden Sie entsprechende Erläuterungen im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.
- Die Flash-URL-Umleitung wird auf Windows 7-, Windows 8-, Windows 8.1- und Windows 10-Einbenutzer-Remote-Desktops unterstützt.
- Internet Explorer 9, 10 oder 11 muss dazu mit dem entsprechenden Flash ActiveX-Plug-In installiert werden.

	■ Nach der Installation muss im Internet Explorer das VMware View FlashMMR Server-Add-On aktiviert werden.
Horizon Client-Computer oder Clientzugriffsgerät	■ Die Flash-URL-Umleitung wird auf Windows 7, Windows 8, Windows 8.1 und Windows 10 unterstützt. ■ Das Flash ActiveX-Plug-In muss installiert und aktiviert sein
Das Anzeigeprotokoll für die Remote-Sitzung ist	VMware Blast, PCoIP

Anforderungen zur Verwendung der Flash-URL-Umleitung

Durch das direkte Streaming von Flash-Inhalten von Adobe Media Server auf 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 Live-Video-Ereignissen an mehrere Clientendpunkte verringert.

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

Diese Funktion ist verfügbar, wenn sie zusammen mit der richtigen Version der Agent-Software verwendet wird. Für View 5.3 ist diese Funktion im Lieferumfang von Remote Experience Agent des View Feature Pack enthalten. Für View 6.0 und höhere Versionen ist diese Funktion in View Agent oder Horizon Agententhalten.

Um diese Funktion zu verwenden, müssen Sie Ihre Webseite und Ihre Clientgeräte einrichten. Die Clientsysteme müssen bestimmte Softwareanforderungen erfüllen:

- Clientsysteme müssen über IP-Konnektivität mit dem Adobe Webserver verfügen, auf dem die ShockWave-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.
- Clientsysteme müssen über Adobe Flash Player 10.1 oder höher für Internet Explorer verfügen (dieser verwendet ActiveX).

Eine Liste der Remote-Desktop-Anforderungen für die Flash-URL-Umleitung sowie Anweisungen zum Konfigurieren einer Webseite für die Bereitstellung eines Multicast- oder Unicast-Streams finden Sie in der Horizon-Dokumentation.

Anforderungen für die URL-Inhaltsumleitung

Mit der Funktion der URL-Inhaltsumleitung lässt sich ein URL-Inhalt von einem Client zu einem Remote-Desktop oder zu einer Remoteanwendung und umgekehrt umleiten. So kann beispielsweise nach dem Klicken auf einen Link in der nativen Anwendung „Microsoft Word“ auf dem Client dieser Link in der Remoteanwendung „Internet Explorer“ geöffnet werden. Umgekehrt lässt sich nach dem Klicken auf einen Link in der Remoteanwendung „Internet Explorer“ der Link in einem nativen Browser auf dem Client öffnen.

Sie können eine beliebige Anzahl von Protokollen inklusive HTTP, mailto und callto für die Umleitung konfigurieren. Diese Funktion unterstützt die Umleitung in beide Richtungen:

- Von einem Client zu einem Remote-Desktop oder zu einer Remoteanwendung (Client-zu-Agent)

Horizon Client startet entweder einen Remote-Desktop oder eine Remoteanwendung zur Verarbeitung der URL. Wird ein Desktop gestartet, wird die URL von der Standardanwendung für das URL-Protokoll verarbeitet.

- Von einem Remote-Desktop oder einer Remoteanwendung zu einem Client (Agent-zu-Client)

  Horizon Agent sendet die URL an Horizon Client, der die Standardanwendung für das in der URL angegebene Protokoll startet.

Für diese Funktion gelten die folgenden Anforderungen:

Remote-Desktop oder RDS-Host mit Remoteanwendungen	■ Horizon Agent 7.0 oder höher. Diese Funktion muss für die Konfiguration einer Agent-zu-Client-Umleitung installiert sein. ■ Ein Horizon-Administrator muss durch Konfiguration von Einstellungen festlegen, wie Horizon Agent URL-Inhalte von einem Remote-Desktop oder einer Remoteanwendung zum Clientsystem umleitet. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*. ■ Die Umleitung einer URL ist für Internet Explorer 9, 10 und 11 verfügbar.
Horizon Client-Computer oder Clientzugriffsgerät	■ Diese Funktion muss für die Konfiguration einer Client-zu-Agent-Umleitung installiert sein. ■ Ein Horizon-Administrator muss durch Konfiguration von Einstellungen festlegen, wie Horizon Client URL-Inhalte von einem Clientsystem zu einem Remote-Desktop oder einer Remoteanwendung umleitet. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*. ■ Die Umleitung einer URL ist für Internet Explorer 9, 10 und 11 verfügbar.
Das Anzeigeprotokoll für die Remote-Sitzung ist	■ VMware Blast ■ PCoIP

Voraussetzungen für die Verwendung von Microsoft Lync mit Horizon Client

Sie können einen Microsoft Lync 2013-Client auf Remote-Desktops einsetzen, um an Unified Communications (UC) VoIP (Voice over IP) und Video-Chats mit Lync-zertifizierten USB-Audio- und -Videogeräten teilzunehmen. Ein spezielles IP-Telefon ist nicht länger erforderlich.

Für diese Architektur ist die Installation eines Microsoft Lync 2013-Clients auf dem Remote-Desktop und von einem Microsoft Lync VDI-Plug-In auf dem Client-Endpoint erforderlich. Kunden können den Microsoft Lync 2013-Client für Präsenz, Instant Messaging, Webkonferenz und Microsoft Office-Funktionen verwenden.

Sobald ein Lync VoIP-Anruf oder Video-Chat eintrifft, nimmt das Lync-VDI-Plug-In die gesamte Medienverarbeitung vom Rechenzentrumsserver auf den Clientendpunkt und codiert alle Medien in Lync-optimierten Audio- und Videocodecs. Diese optimierte Architektur ist äußerst skalierbar, was zu einer geringeren Nutzung der Netzwerkbandbreite führt und Unterstützung für qualitativ hochwertige VoIP- und Video-Übertragung von Punkt zu Punkt in Echtzeit bietet. Weitere Informationen finden Sie im Whitepaper zu Horizon 6 und Microsoft Lync 2013 unter http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-microsoft-lync-install-configure.pdf.

Hinweis Die Aufnahme von Audio wird noch nicht unterstützt. Diese Integration wird nur mit dem PCoIP-Anzeigeprotokoll unterstützt.

Für diese Funktion gelten die folgenden Anforderungen.

Betriebssystem

- Client-Betriebssystem: Windows 7 SP1, Windows 8.x oder Windows 10.
- Das Betriebssystem der virtuellen Maschine (Agent) hängt von der Agent-Version ab.

Version	Gastbetriebssystem
View Agent 6.2 oder höher oder Horizon Agent 7.0 oder höher.	Windows 7 SP1 mit 32 oder 64 Bit, Windows 8.x, Windows 10 oder Windows Server 2008 R2 SP1 mit 64 Bit Für Microsoft RDS-Hosts: Windows Server 2008 R2, Windows Server 2012 oder Windows Server 2012 R2
View Agent 6.0 oder 6.1	Windows 7 SP1 mit 32 oder 64 Bit, Windows 8.x oder Windows Server 2008 R2 SP1 mit 64 Bit
View Agent 5.3	32- oder 64-Bit-Windows 7 SP1

Software des Clientsystems

- 32-Bit-Version des Microsoft Lync VDI-Plug-Ins

  Wichtig Die 64-Bit-Version von Microsoft Office muss nicht auf dem Clientcomputer installiert werden. Das erforderliche 32-Bit-Microsoft Lync VDI-Plug-In ist nicht mit der 64-Bit-Version von Microsoft Office 2013 kompatibel.

- Das Sicherheitszertifikat, das während der Bereitstellung von Microsoft Lync Server 2013 erzeugt wird, muss in das Verzeichnis der vertrauenswürdigen Stammzertifizierungsstellen importiert werden.

Software für den Remote-Desktop (Agent)

- View Agent 5.3 oder höher oder Horizon Agent 7.0 oder höher.
- Microsoft Lync 2013-Client

  Mit dem View 5.3-Agenten (oder höher) muss die Bit-Version des Lync 2013-Clients nicht mit der Bit-Version des Betriebssystems der virtuellen Maschine übereinstimmen.

- Das Sicherheitszertifikat, das während der Bereitstellung von Microsoft Lync Server 2013 erzeugt wird, muss in das Verzeichnis der vertrauenswürdigen Stammzertifizierungsstellen importiert werden

Erforderliche Server

- Ein Server, auf dem Verbindungsserver 5.3 oder später ausgeführt wird
- Ein Server, auf dem Microsoft Lync Server 2013 ausgeführt wird

- Eine vSphere-Infrastruktur zur Aufnahme der virtuellen Maschinen

  Auf dem vCenter Server und den ESXi-Hosts muss vSphere 5.0 oder höher ausgeführt werden.

Hardware

- Hardware, die alle der zuvor genannten erforderlichen Softwarekomponenten unterstützt
- Client-Endpoint: CPU mit 1,5 GHz oder schneller und mindestens 2 GB RAM für das Microsoft Lync 2013-Plug-In

Hinweis Informationen zur Fehlerbehebung finden Sie unter VMware KB 2063769 und VMware KB 2053732.

Anforderungen für die Smartcard-Authentifizierung

Clientsysteme, die eine Smartcard für die Benutzerauthentifizierung verwenden, müssen bestimmte Anforderungen erfüllen.

Für jedes Clientsystem, das zur Benutzerauthentifizierung eine Smartcard verwendet, gelten die folgenden Software- und Hardwareanforderungen:

- Horizon Client
- Ein kompatibler Smartcard-Leser
- Produktspezifische Anwendungstreiber

Sie müssen auf den Remote-Desktops oder dem Microsoft RDS-Host zusätzlich produktspezifische Anwendungstreiber installieren.

Horizon View unterstützt Smartcards und Smartcard-Leser, die einen PKCS#11- oder Microsoft CryptoAPI-Anbieter verwenden. Optional können Sie das ActivClient-Softwarepaket von ActivIdentity installieren, das Tools zur Interaktion mit Smartcards bereitstellt.

Benutzer, die sich mithilfe von Smartcards authentifizieren, müssen über ein Smartcard- oder USB-Smartcard-Token verfügen, und jede Smartcard muss ein Benutzerzertifikat enthalten.

Zum Installieren von Zertifikaten auf einer Smartcard müssen Sie einen Computer einrichten, der als Registrierungsstelle fungiert. Dieser Computer muss Smartcard-Zertifikate für Benutzer ausgeben können und Mitglied der Domäne sein, für die Sie Zertifikate ausgeben.

Wichtig Wenn Sie eine Smartcard anmelden, können Sie die Schlüsselgröße des resultierenden Zertifikats auswählen. Zur Verwendung von Smartcards auf lokalen Desktops müssen Sie bei der Smartcard-Registrierung eine Schlüsselgröße von 1024 Bit oder 2048 Bit auswählen. Zertifikate mit 512-Bit-Schlüsseln werden nicht unterstützt.

Die Microsoft TechNet-Website enthält ausführliche Informationen zu Planung und Implementierung der Smartcard-Authentifizierung für Windows-Systeme.

Neben der Einhaltung dieser Anforderungen für Horizon Client-Systeme müssen andere Horizon-Komponenten zur Unterstützung von Smartcards bestimmte Anforderungen an die Konfiguration erfüllen:

- Informationen zur Konfiguration des Verbindungsservers für die Unterstützung von Smartcards finden Sie im Dokument *Administration von View*.

  Sie müssen alle gültigen Zertifizierungsstellenzertifikate für alle vertrauenswürdigen Benutzerzertifikate einer Serververtrauensspeicher-Datei auf dem Verbindungsserver- oder Sicherheitsserver-Host hinzufügen. Diese Zertifikate beinhalten Stammzertifikate und müssen auch Zwischenzertifikate enthalten, wenn das Smartcard-Zertifikat des Benutzers von einer Zwischenzertifizierungsstelle herausgegeben wurde.

- Informationen zu den Aufgaben, die Sie eventuell in Active Directory zur Implementierung der Smartcard-Authentifizierung durchführen müssen, finden Sie im Dokument *Administration von View*.

Aktivieren des Feldes „Benutzernamenhinweis“ in Horizon Client

In einigen Umgebungen können Smartcard-Benutzer ein einziges Smartcard-Zertifikat zur Authentifizierung bei mehreren Benutzerkonten verwenden. Benutzer geben bei der Smartcard-Anmeldung ihren Benutzernamen in das Feld **Benutzernamenhinweis** ein.

Damit das Feld **Benutzernamenhinweis** im Anmeldungsdialogfeld von Horizon Client angezeigt wird, müssen Sie die Funktion für Smartcard-Benutzernamenhinweise für die Verbindungsserver-Instanz in Horizon Administrator aktivieren. Die Funktion für Smartcard-Benutzernamenhinweise wird nur mit Servern und Agenten von Horizon 7 Version 7.0.2 und höher unterstützt. Informationen zur Aktivierung von Smartcard-Benutzernamenhinweisen erhalten Sie im Dokument *Administration von View*.

Wenn Ihre Umgebung für den sicheren externen Zugriff statt eines Sicherheitsservers eine Access Point-Appliance verwendet, müssen Sie die Access Point-Appliance zur Unterstützung von Smartcard-Benutzernamenhinweisen konfigurieren. Die Funktion für Smartcard-Benutzernamenhinweise wird nur mit Access Point 2.7.2 und höher unterstützt. Informationen zur Aktivierung von Smartcard-Benutzernamenhinweisen in Access Point erhalten Sie im Dokument *Bereitstellen und Konfigurieren von Access Point*.

Hinweis Horizon Client unterstützt weiterhin Smartcard-Zertifikate für Einzelkonten, wenn die Funktion für Smartcard-Benutzernamenhinweise aktiviert ist.

Anforderungen für die Geräteauthentifizierung

Sie können die Zertifikatsauthentifizierung für Clientgeräte einrichten.

Für diese Funktion gelten die folgenden Anforderungen:

- Access Point 2.6 oder höher.
- Horizon 7 Version 7.0 oder höher.
- Ein auf dem Clientgerät installiertes Zertifikat, das von Access Point akzeptiert wird.

Unterstützte Desktop-Betriebssysteme

Administratoren erstellen virtuelle Maschinen mit einem Gastbetriebssystem und installieren die Agent-Software auf diesem Gastbetriebssystem. Die Endbenutzer können sich an diesen virtuellen Maschinen von einem Client-Gerät aus anmelden.

Eine Liste unterstützter Windows-Gastbetriebssysteme finden Sie im Dokument *View-Installation*.

Einige Linux-Gastbetriebssysteme werden auch unterstützt, wenn Sie über View Agent 6.1.1 und höher oder Horizon Agent 7.0 und höher verfügen. Informationen zu den Systemanforderungen, zur Konfiguration virtueller Linux-Maschinen für eine Verwendung in Horizon sowie eine Liste unterstützter Funktionen erhalten Sie in *Einrichten von Horizon 6 for Linux-Desktops* und in *Einrichten von Horizon 7 for Linux-Desktops* .

Vorbereiten des Verbindungsservers für Horizon Client

Administratoren müssen bestimmte Aufgaben durchführen, um Endbenutzern die Verbindung zu Remote-Desktops und -Anwendungen zu ermöglichen.

Bevor Endbenutzer eine Verbindung mit dem Verbindungsserver oder einem Sicherheitsserver herstellen und auf einen Remote-Desktop oder eine Remoteanwendung zugreifen können, müssen bestimmte Pool- und Sicherheitseinstellungen konfiguriert werden:

- Wenn Sie Access Point verwenden möchten, konfigurieren Sie den Verbindungsserver zur Zusammenarbeit mit Access Point. Siehe das Dokument *Bereitstellen und Konfigurieren von Access Point*. Access Point-Appliances erfüllen dieselbe Rolle, die früher nur Sicherheitsserver übernommen hatten.
- Wenn Sie einen Sicherheitsserver verwenden, stellen Sie sicher, dass Sie die aktuellen Wartungsversionen für einen Verbindungsserver der Version 5.3.x und für einen Sicherheitsserver der Version 5.3.x oder höher verwenden. Weitere Informationen finden Sie im Dokument *View-Installation*.
- Wenn Sie eine sichere Tunnelverbindung für Clientgeräte verwenden möchten und die sichere Verbindung mit einem DNS-Hostnamen für den Verbindungsserver oder einen Sicherheitsserver konfiguriert ist, muss sichergestellt werden, dass das Clientgerät diesen DNS-Namen auflösen kann.

  Wechseln Sie zur Aktivierung oder Deaktivierung der sicheren Tunnelverbindung in Horizon Administrator zum Dialogfeld Horizon-Verbindungsserver-Einstellungen bearbeiten und aktivieren Sie das Kontrollkästchen **Sichere Tunnelverbindung zum Desktop verwenden**.
- Vergewissern Sie sich, dass ein Desktop- oder Anwendungspool erstellt wurde und das Benutzerkonto, das Sie verwenden möchten, über die Rechte zum Zugriff auf diesen Pool verfügt. Informationen dazu finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

  Wichtig Wenn Endbenutzer mit einem hochauflösenden Anzeigegerät arbeiten und die Clienteinstellung „Hochauflösungsmodus“ verwenden, während ihre Remote-Desktops im Vollbildmodus angezeigt werden, müssen Sie jedem Remote-Desktop mit Windows 7 oder höher ausreichend VRAM zuteilen. Die Menge an vRAM ist von der Anzahl der für Endbenutzer konfigurierten Monitore und der Displayauflösung abhängig. Zur Bestimmung der erforderlichen Menge an vRAM finden Sie Informationen im Dokument *Planung der View-Architektur*.
- Für die Verwendung der zweistufigen Authentifizierung für Horizon Client, z. B. der RSA SecurID- oder RADIUS-Authentifizierung, müssen Sie diese Funktion auf dem Verbindungsserver aktivieren. Weitere Informationen finden Sie in den Themen zur zweistufigen Authentifizierung im Dokument *Administration von View*.
- Um Sicherheitsinformationen wie Server-URL-Informationen und das Dropdown-Menü **Domäne** in Horizon Client auszublenden, aktivieren Sie in Horizon Administrator die Einstellungen **Serverinformationen in der Kunden-Benutzeroberfläche ausblenden** und **Domänenliste in der Kunden-Benutzeroberfläche ausblenden**. Diese globalen Einstellungen sind in Horizon 7 Version 7.1 und höher verfügbar. Weitere Informationen zur Konfiguration globaler Einstellungen finden Sie im Dokument *Administration von View*.

Um eine Authentifizierung bei ausgeblendetem Dropdown-Menü **Domäne** durchführen zu können, müssen Benutzer die Domäneninformationen durch Eingabe ihres Benutzernamens im Format ***Domäne**Benutzername*** oder ***Benutzername@Domäne*** in das Textfeld **Benutzername** zur Verfügung stellen.

Wichtig Wenn Sie die Einstellungen **Serverinformationen in der Kunden-Benutzeroberfläche ausblenden** und **Domänenliste in der Kunden-Benutzeroberfläche ausblenden** aktivieren und die zweistufige Authentifizierung (RSA SecureID oder RADIUS) für die Verbindungsserver-Instanz auswählen, dürfen Sie nicht die Windows-Benutzernamenübereinstimmung erzwingen. Wenn die Windows-Benutzernamenübereinstimmung erzwungen wird, können Benutzer keine Domäneninformationen in das Textfeld „Benutzername“ eingeben und es ist keine Anmeldung mehr möglich. Weitere Informationen finden Sie in den Themen zur zweistufigen Authentifizierung im Dokument *Administration von View*.

- Um Benutzern einen nicht authentifizierten Zugriff auf veröffentlichte Anwendungen in Horizon Client zu ermöglichen, müssen Sie diese Funktion im Verbindungsserver aktivieren. Weitere Informationen finden Sie in den Themen zum nicht authentifizierten Zugriff im Dokument *Administration von View*.

Löschen des zuletzt für die Anmeldung bei einem Server verwendeten Benutzernamens

Wenn sich Benutzer bei einer Verbindungsserver-Instanz anmelden, für die die globale Einstellung **Domänenliste in der Kunden-Benutzeroberfläche ausblenden** aktiviert wurde, ist das Dropdown-Menü **Domäne** in Horizon Client ausgeblendet. Benutzer müssen dann die Domäneninformationen im Textfeld Horizon Client **Benutzername** bereitstellen. Der Benutzername muss dabei im Format ***Domäne**Benutzername*** oder ***Benutzername@Domäne*** eingegeben werden.

Auf einem Windows-Clientsystem wird durch einen Registrierungsschlüssel festgelegt, ob der letzte Benutzername gespeichert und im Textfeld **Benutzername** bei der nächsten Anmeldung des Benutzers beim Server angezeigt wird. Wenn der letzte Benutzername nicht im Feld **Benutzername** angezeigt werden soll und keine Domäneninformationen sichtbar sein sollen, müssen Sie den Wert des Registrierungsschlüssels `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\dontdisplaylastusername` auf dem Windows-Clientsystem in 1 ändern.

Informationen zum Ausblenden von Sicherheitsinformationen wie das Dropdown-Menü **Domäne** und Server-URL-Informationen in Horizon Client finden Sie in den Themen über globale Einstellungen im Dokument *Administration von View*.

Konfigurieren der VMware Blast-Optionen

Sie können die Optionen für die H.264-Decodierung und für die Netzwerkbedingung für Remote-Desktop- und -anwendungssitzungen konfigurieren, die das VMware Blast-Anzeigeprotokoll verwenden.

Die maximal unterstützte Auflösung hängt von der Kapazität des Grafikprozessors (GPU, Graphical Processing Unit) auf dem Client ab. Eine GPU, die die 4K-Auflösung für JPEG/PNG unterstützt, unterstützt nicht zwangsläufig auch die 4K-Auflösung für H.264. Wird die Auflösung für H.264 nicht unterstützt, verwendet Horizon Client stattdessen JPEG/PNG.

Die Option für die Netzwerkbedingung lässt sich nach der Anmeldung bei einem Server nicht mehr ändern. Die H.264-Decodierung können Sie vor und nach der Anmeldung bei einem Server konfigurieren.

Voraussetzungen

Diese Funktion erfordert Horizon Agent 7.0 oder höher.

Vorgehensweise

1 Klicken Sie auf die Schaltfläche **Optionen** in der Menüleiste und wählen Sie dann **VMware Blast konfigurieren** aus.

Wenn Sie bei einem Server angemeldet sind, können Sie auf das (Zahnrad-)Symbol **Einstellungen** klicken und **VMware Blast** auswählen. Die Option für die Netzwerkbedingung lässt sich nach der Anmeldung bei einem Server nicht mehr ändern.

2 Konfigurieren Sie die Optionen für das Decodieren und die Netzwerkbedingung.

Option	Aktion
H.264	Sie können diese Option vor oder nach der Herstellung einer Verbindung mit dem Verbindungsserver konfigurieren, um die H.264-Decodierung in Horizon Client aktivieren. Ist diese Option ausgewählt (Standardeinstellung), verwendet Horizon Client die H.264-Decodierung, wenn der Agent die H.264-Software- oder -Hardwarecodierung unterstützt. Unterstützt der Agent die H.264-Software- oder -Hardwarecodierung nicht, verwendet Horizon Client die JPG/PNG-Decodierung. Deaktivieren Sie diese Option, um die JPG/PNG-Decodierung zu verwenden.
Netzwerkstatus auswählen, um optimale Funktion zu gewährleisten	Sie können diese Option nur vor der Herstellung einer Verbindung mit dem Verbindungsserver konfigurieren. Wählen Sie eine der folgenden Optionen für die Netzwerkbedingung aus: ■ **Hervorragend** – Horizon Client verwendet nur das TCP-Netzwerk. Diese Option ist am besten für eine LAN-Umgebung geeignet. ■ **Normal (Standard)** – Horizon Client arbeitet im gemischten Modus. Im gemischten Modus verwendet Horizon Client das TCP-Netzwerk für die Herstellung einer Verbindung mit dem Server und das Protokoll Blast Extreme Adaptive Transport (BEAT), wenn der Agent und das Blast Security Gateway (bei Aktivierung) eine BEAT-Konnektivität unterstützen. Diese Option ist die Standardeinstellung. ■ **Schlecht** – Horizon Client verwendet nur das BEAT-Netzwerk, wenn BEAT Tunnel Server auf dem Server aktiviert ist. Ist dies nicht der Fall, wird in den gemischten Modus gewechselt. **Hinweis** In Horizon 7 Version 7.1 und früher wird BEAT Tunnel Server von den Instanzen des Verbindungsservers und des Sicherheitsservers nicht unterstützt. VMware Access Point 2.9 und höher unterstützt BEAT Tunnel Server. Blast Security Gateway für Verbindungsserver- und Sicherheitsserver-Instanzen unterstützt nicht das BEAT-Netzwerk.

3 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Änderungen für H.264 werden wirksam, wenn das nächste Mal ein Benutzer eine Verbindung mit einem Remote-Desktop oder einer Remoteanwendung herstellt und das VMware Blast-Anzeigeprotokoll auswählt. Ihre Änderungen haben keinen Einfluss auf vorhandene VMware Blast-Sitzungen.

Verwenden von Internet Explorer-Proxy-Einstellungen

Horizon Client verwendet automatisch die in Internet Explorer konfigurierten Proxy-Einstellungen.

Einstellungen für die Proxy-Umgehung

Horizon Client verwendet Internet Explorer-Einstellungen für die Proxy-Umgehung, um HTTPS-Verbindungen mit einem Verbindungsserver-Host, mit einem Sicherheitsserver oder mit einer Access Point-Appliance zu umgehen.

Wenn der sichere Tunnel auf dem Verbindungsserver-Host, dem Sicherheitsserver oder in der Access Point-Appliance aktiviert ist, müssen Sie mit der Gruppenrichtlinieneinstellung `Tunnel proxy bypass address list` in der ADM- oder ADMX-Vorlagendatei für die Horizon Client-Konfiguration eine Liste von Adressen angeben, um die Tunnelverbindung zu umgehen. Der Proxy-Server wird für diese Adressen nicht verwendet. Verwenden Sie ein Semikolon (;) zum Trennen mehrerer Einträge. Diese Gruppenrichtlinieneinstellung erstellt den folgenden Registrierungsschlüssel:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\VMware, Inc.\VMware VDM\Client\TunnelProxyBypass
```

Sie können diese Gruppenrichtlinieneinstellung nicht für direkte Verbindungen verwenden. Wenn die Anwendung der Gruppenrichtlinieneinstellung nicht wie vorgesehen funktioniert, versuchen Sie den Proxy für lokale Adressen zu umgehen. Weitere Informationen finden Sie unter https://blogs.msdn.microsoft.com/askie/2015/10/12/how-to-configure-proxy-settings-for-ie10-and-ie11-as-iem-is-not-available/.

Proxy-Failover

Horizon Client unterstützt ein Proxy-Failover mit der Einstellung **Skript für automatische Konfiguration verwenden** unter **Automatische Konfiguration** in **Internetoptionen > Verbindungen > LAN-Einstellungen** in Internet Explorer. Um diese Einstellung verwenden zu können, müssen Sie ein Skript zur automatischen Konfiguration erstellen, das mehrere Proxy-Server zurückgibt.

Durch VMware gesammelte Horizon Client -Daten

Wenn Ihr Unternehmen am Programm zur Verbesserung der Benutzerfreundlichkeit teilnimmt, erhebt VMware Daten aus bestimmten Horizon Client-Feldern. Felder mit vertraulichen Informationen werden anonymisiert.

VMware sammelt die Daten auf den Clients zur Priorisierung der Hardware- und Softwarekompatibilität. Wenn sich ein Administrator Ihres Unternehmens zur Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit entscheidet, sammelt VMware anonyme Daten über Ihre Bereitstellung, um die Reaktion von VMware auf die Kundenanforderungen verbessern zu können. Es werden jedoch keine Daten gesammelt, die Aufschluss über Ihr Unternehmen geben könnten. Die Horizon Client-Informationen werden erst an den Verbindungsserver und dann an VMware gesendet, zusammen mit den Daten der Verbindungsserver-Instanzen, Desktop-Pools und Remote-Desktops.

Auch wenn die Informationen bei der Übertragung an den Verbindungsserver verschlüsselt werden, werden die Informationen des Clientsystems unverschlüsselt in einem benutzerspezifischen Verzeichnis protokolliert. Die Protokolle enthalten jedoch keine personen- oder unternehmensbezogenen Informationen.

Der Administrator, der die Installation des Verbindungsservers durchführt, kann während der Ausführung des Installations-Assistenten für den Verbindungsserver entscheiden, ob am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit teilgenommen wird. Nach der Installation kann ein Administrator eine entsprechende Option in Horizon Administrator festlegen.

Tabelle 1-1. Von den Horizon Client-Instanzen gesammelte Daten für das Programm zur Verbesserung der Benutzerfreundlichkeit

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Unternehmen, das die Horizon Client-Anwendung hergestellt hat	Nein	VMware
Produktname	Nein	VMware Horizon Client
Client-Produktversion	Nein	(Das Format lautet *x.x.x-yyyyyy*, wobei *x.x.x* für die Client-Versionsnummer und *yyyyyy* für die Build-Nummer steht.)

Tabelle 1-1. Von den Horizon Client-Instanzen gesammelte Daten für das Programm zur Verbesserung der Benutzerfreundlichkeit (Fortsetzung)

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Client-Binärarchitektur	Nein	Beispiele hierfür sind: ■ i386 ■ x86_64 ■ arm
Client-Build-Name	Nein	Beispiele hierfür sind: ■ VMware-Horizon-Client-Win32-Windows ■ VMware-Horizon-Client-Linux ■ VMware-Horizon-Client-iOS ■ VMware-Horizon-Client-Mac ■ VMware-Horizon-Client-Android ■ VMware-Horizon-Client-WinStore
Host-Betriebssystem	Nein	Beispiele hierfür sind: ■ Windows 8.1 ■ Windows 7, Service Pack 1 für 64 Bit (Build 7601) ■ iPhone OS 5.1.1 (9B206) ■ Ubuntu 12.04.4 LTS ■ Mac OS X 10.8.5 (12F45)
Host-Betriebssystemkernel	Nein	Beispiele hierfür sind: ■ Windows 6.1.7601 SP1 ■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X ■ Darwin 11.4.2 ■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012 ■ unbekannt (für Windows Store)
Host-Betriebssystemarchitektur	Nein	Beispiele hierfür sind: ■ x86_64 ■ i386 ■ armv71 ■ ARM
Hostsystem-Modell	Nein	Beispiele hierfür sind: ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision WorkStation T3400 (A04 03/21/2008)
Hostsystem-CPU	Nein	Beispiele hierfür sind: ■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH ■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH ■ unbekannt (für iPad)
Anzahl der Cores bzw. Kerne im Prozessor des Hostsystems	Nein	Beispiel: 4
MB Arbeitsspeicher auf dem Hostsystem	Nein	Beispiele hierfür sind: ■ 4096 ■ unbekannt (für Windows Store)
Anzahl der angeschlossenen USB-Geräte	Nein	2 (Die Umleitung von USB-Geräten wird nur für Linux-, Windows- und Mac-Clients unterstützt.)

Tabelle 1-1. Von den Horizon Client-Instanzen gesammelte Daten für das Programm zur Verbesserung der Benutzerfreundlichkeit (Fortsetzung)

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Maximale Anzahl gleichzeitiger USB-Geräteverbindungen	Nein	2
Hersteller-ID des USB-Geräts	Nein	Beispiele hierfür sind: ■ Kingston ■ NEC ■ Nokia ■ Wacom
Produkt-ID des USB-Geräts	Nein	Beispiele hierfür sind: ■ DataTraveler ■ Gamepad ■ Speicherlaufwerk ■ Kabellose Maus
USB-Gerätefamilie	Nein	Beispiele hierfür sind: ■ Sicherheit ■ Eingabegeräte ■ Bildverarbeitung
Nutzungszähler für das USB-Gerät	Nein	(Gibt an, wie oft das Gerät gemeinsam genutzt wurde)

Installation von Horizon Client für Windows 2

Das Windows-basierte Horizon Client-Installationsprogramm können Sie entweder von der VMware-Website oder über eine Seite für den Webzugriff abrufen, die vom Verbindungsserver bereitgestellt wird. Nach der Installation von Horizon Client können Sie verschiedene Startoptionen für die Endbenutzer festlegen.

Dieses Kapitel behandelt die folgenden Themen:

Aktivieren des FIPS-Modus im Windows-Clientbetriebssystem

Wenn Sie eine Installation von Horizon Client mit Federal Information Processing Standard (FIPS-)konformer Kryptografie planen, müssen Sie den FIPS-Modus im Clientbetriebssystem aktivieren, bevor Sie das Horizon Client-Installationsprogramm ausführen.

Wenn der FIPS-Modus im Clientbetriebssystem aktiviert ist, verwenden Anwendungen nur kryptografische Algorithmen, die mit FIPS-140 und mit FIPS-genehmigten Betriebsarten konform sind. Sie können den FIPS-Modus aktivieren, indem Sie eine spezifische Sicherheitseinstellung aktivieren – entweder in der lokalen Sicherheitsrichtlinie, als Teil einer Gruppenrichtlinie oder durch Bearbeiten des Windows-Registrierungsschlüssels.

Wichtig Das Installieren von Horizon Client mit einer FIPS-konformen Kryptografie wird nur für Clientsysteme mit Windows 7 SP1-Betriebssystemen unterstützt.

Weitere Informationen zur FIPS-Unterstützung, die mit Horizon 6 Version 6.2 oder höher verfügbar ist, finden Sie im *View-Installation*-Dokument.

Festlegen der FIPS-Konfigurationseigenschaft

Um den FIPS-Modus im Clientbetriebssystem zu aktivieren, können Sie entweder eine Windows-Gruppenrichtlichtlinieneinstellung oder eine Windows-Registrierungseinstellung für den Clientcomputer verwenden.

- Zur Verwendung einer Gruppenrichtlichtlinie öffnen Sie den Gruppenrichtlinien-Editor, wechseln Sie zu `Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen` und aktivieren Sie die Einstellung **Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden**.
- Um die Windows-Registrierung zu verwenden, wechseln Sie zu `HKLM\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\Enabled` und legen Sie für **Aktiviert** 1 fest.

Weitere Informationen zum FIPS-Modus finden Sie unter https://support.microsoft.com/en-us/kb/811833.

Wichtig Damit die Installationsoption zur Verwendung der FIPS-konformen Kryptografie in einer benutzerdefinierten Installation angezeigt wird, muss der FIPS-Modus vor der Ausführung des Horizon Client-Installationsprogramms aktiviert werden. Die FIPS-konforme Kryptografie wird im Rahmen einer standardmäßigen Installation nicht aktiviert. Wenn Sie Horizon Client ohne die Option für eine FIPS-konforme Kryptografie installieren und sich später für die Verwendung dieser Option entscheiden, müssen Sie den Client deinstallieren, den FIPS-Modus im Clientbetriebssystem aktivieren und das Horizon Client-Installationsprogramm erneut ausführen.

Installation von Horizon Client für Windows

Endbenutzer öffnen Horizon Client, um von einem Clientsystem aus eine Verbindung mit ihren Remote-Desktops und Remoteanwendungen herzustellen. Sie können eine Windows-basierte Installationsdatei zum Installieren sämtlicher Komponenten von Horizon Client ausführen.

Das Installationsprogramm ermittelt, ob das Clientsystem über ein 64-Bit- oder ein 32-Bit-Betriebssystem verfügt, und installiert die entsprechende Version von Horizon Client für das Clientsystem. Das Installationsprogramm kann nicht auf Windows XP oder Windows Vista ausgeführt werden.

Dieser Vorgang beschreibt die Installation von Horizon Client über einen interaktiven Installationsassistenten. Um die Funktion der URL-Inhaltsumleitung zu installieren, müssen Sie das Installationsprogramm an der Befehlszeile ausführen und den Parameter `URL_FILTERING_ENABLED` festlegen, z. B. in der Form `VMware-Horizon-Client-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1`. Erläuterungen zur Durchführung der unbeaufsichtigten Befehlszeileninstallation von Microsoft Windows Installer (MSI) finden Sie unter „Unbeaufsichtigte Installation von Horizon Client“, auf Seite 30.

Hinweis Sie können Horizon Client auf einer virtuellen Maschine des Remote-Desktops installieren, wenn auf diesem Desktop View Agent 6.0 oder höher oder Horizon Agent 7.0 oder höher ausgeführt wird. Unternehmen verwenden eventuell diese Art der Installation, wenn ihre Endbenutzer auf Remoteanwendungen von Windows-Thin-Client-Diensten aus zugreifen.

Voraussetzungen

- Stellen Sie sicher, dass das Clientsystem ein unterstütztes Betriebssystem verwendet. Siehe „Systemanforderungen für Windows-Clients“, auf Seite 10.
- Stellen Sie sicher, dass Sie über die URL für eine Download-Seite verfügen, auf der sich das Horizon Client-Installationsprogramm befindet. Bei dieser URL kann es sich um die VMware Downloads-Seite unter http://www.vmware.com/go/viewclients oder um die URL für eine Verbindungsserver-Instanz handeln.
- Stellen Sie sicher, dass Sie sich als Administrator auf dem Clientsystem anmelden können.
- Stellen Sie sicher, dass auf den Domänencontrollern die neuesten Patches installiert sind, dass genügend freier Speicherplatz zur Verfügung steht und dass eine Kommunikation untereinander möglich ist. Andernfalls kann die Fertigstellung des Installationsprogramms, wenn es unter Windows 8.1 ausgeführt wird, ungewöhnlich lange dauern. Dieses Problem ist darauf zurückzuführen, dass der Domänencontroller der Maschine oder ein anderer Domänencontroller in dieser Hierarchie nicht reagiert oder nicht erreichbar ist.
- Wenn Sie eine Installation von Horizon Client mit FIPS-konformer Kryptografie planen, müssen Sie den FIPS-Modus im Clientbetriebssystem aktivieren, bevor Sie das Horizon Client-Installationsprogramm ausführen. Siehe „Aktivieren des FIPS-Modus im Windows-Clientbetriebssystem“, auf Seite 27.

- Wenn Sie die Komponente der **USB-Umleitung** installieren möchten, müssen Sie Folgendes durchführen:
  - Legen Sie fest, ob der Benutzer des Clientgeräts von einem Remote-Desktop auf lokal verbundene USB-Geräte zugreifen darf. Wenn der Zugriff nicht zulässig ist, installieren Sie entweder die Komponente der **USB-Umleitung** nicht oder Sie installieren die Komponente und deaktivieren diese mithilfe einer Gruppenrichtlinieneinstellung. Wenn Sie eine Gruppenrichtlinie zur Deaktivierung der USB-Umleitung verwenden, müssen Sie Horizon Client nicht erneut installieren, wenn Sie die USB-Umleitung später für einen Client aktivieren möchten. Weitere Informationen finden Sie unter „Einstellungen für die Skriptdefinition für Client-GPOs“, auf Seite 49.
  - Stellen Sie sicher, dass die Funktion für automatische Windows-Updates auf dem Clientcomputer nicht deaktiviert wurde.
- Legen Sie fest, ob diese Funktion verwendet werden soll, mit der Endbenutzer sich bei Horizon Client und ihrem Remote-Desktop als aktuell angemeldeter Benutzer anmelden können. Die Anmeldeinformationen des Benutzers, die dieser zur Anmeldung beim Clientsystem eingegeben hat, werden an die Verbindungsserver-Instanz und schließlich an den Remote-Desktop übergeben. Einige Clientbetriebssysteme bieten keine Unterstützung für diese Funktion.
- Wenn Sie nicht möchten, dass die Endbenutzer den vollqualifizierten Domänennamen (FQDN) der View-Verbindungsserverinstanz eingeben müssen, ermitteln Sie den FQDN, um ihn während der Installation angeben zu können.

Vorgehensweise

1 Melden Sie sich beim Clientsystem als Administrator an.

2 Wechseln Sie zur VMware-Produktseite unter http://www.vmware.com/go/viewclients.

3 Laden Sie die Installationsdatei herunter, z. B. `VMware-Horizon-Client-y.y.y-xxxxxx.exe`.

Dabei steht *xxxxxx* für die Build-Nummer und *y.y.y* für die Versionsnummer.

4 Doppelklicken Sie auf die Installationsdatei, um die Installation zu starten.

5 Wählen Sie den Installationstyp aus und folgen Sie den Aufforderungen.

Option	Beschreibung
Standard	Installiert das IPv4-Internetprotokoll und die USB-Umleitung sowie die Anmeldung als aktuelle Benutzerfunktionen. Wenn der FIPS-Modus im Clientbetriebssystem aktiviert ist, wird die FIPS-konforme Kryptografie deaktiviert.
Benutzerdefiniert	Ermöglicht Ihnen die Auswahl der zu installierenden Komponenten. Beachten Sie für die Auswahl der Komponenten die folgenden Richtlinien: ■ Wählen Sie das IPv6-Internetprotokoll nicht aus, es sei denn, alle Komponenten in Ihrer Horizon-Umgebung verwenden IPv6. Bei der Auswahl von IPv6 stehen mehrere Funktionen nicht zur Verfügung. Weitere Informationen finden Sie im Dokument *View-Installation*. ■ Sie können die FIPS-konforme Kryptografie nur aktivieren, wenn der FIPS-Modus im Clientbetriebssystem bereits aktiviert ist.

Das Installationsprogramm installiert bestimmte Windows-Dienste wie VMware Horizon Client (`horizon_client_service`) und VMware USB Arbitration Service (`VMUSBArbService`).

Weiter

Starten Sie Horizon Client und stellen Sie sicher, dass Sie sich am richtigen Remote-Desktop bzw. an der richtigen Anwendung anmelden können. Siehe „Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung“, auf Seite 75.

Unbeaufsichtigte Installation von Horizon Client

Sie können eine unbeaufsichtigte Installation von Horizon Client durchführen, indem Sie den Namen der Installationsdatei sowie die gewünschten Installationsoptionen an der Befehlszeile eingeben. Die unbeaufsichtigte Installation ermöglicht eine effiziente Bereitstellung von Horizon-Komponenten in einem großen Unternehmen.

Unbeaufsichtigte Installation von Horizon Client

Sie können die Microsoft Windows Installer-Funktion (MSI) für die unbeaufsichtigte Installation dazu verwenden, Horizon Client auf mehreren Windows-Computern zu installieren. Bei einer unbeaufsichtigten Installation verwenden Sie die Befehlszeile und müssen nicht auf Eingabeaufforderungen des Assistenten reagieren.

Das Installationsprogramm ermittelt, ob das Clientsystem über ein 64-Bit- oder ein 32-Bit-Betriebssystem verfügt, und installiert die entsprechende Version von Horizon Client für das Clientsystem.

Voraussetzungen

- Stellen Sie sicher, dass das Clientsystem ein unterstütztes Betriebssystem verwendet. Siehe „Systemanforderungen für Windows-Clients“, auf Seite 10.
- Stellen Sie sicher, dass Sie sich als Administrator auf dem Clientsystem anmelden können.
- Stellen Sie sicher, dass auf den Domänencontrollern die neuesten Patches installiert sind, dass genügend freier Speicherplatz zur Verfügung steht und dass eine Kommunikation untereinander möglich ist. Andernfalls kann die Fertigstellung des Installationsprogramms, wenn es unter Windows 8.1 ausgeführt wird, ungewöhnlich lange dauern. Dieses Problem ist darauf zurückzuführen, dass der Domänencontroller der Maschine oder ein anderer Domänencontroller in dieser Hierarchie nicht reagiert oder nicht erreichbar ist.
- Wenn Sie eine Installation von Horizon Client mit FIPS-konformer Kryptografie planen, müssen Sie den FIPS-Modus im Clientbetriebssystem aktivieren, bevor Sie das Horizon Client-Installationsprogramm ausführen. Siehe „Aktivieren des FIPS-Modus im Windows-Clientbetriebssystem“, auf Seite 27.
- Legen Sie fest, ob diese Funktion verwendet werden soll, mit der Endbenutzer sich bei Horizon Client und ihrem Remote-Desktop als aktuell angemeldeter Benutzer anmelden können. Die Anmeldeinformationen des Benutzers, die dieser zur Anmeldung beim Clientsystem eingegeben hat, werden an die Verbindungsserver-Instanz und schließlich an den Remote-Desktop übergeben. Einige Clientbetriebssysteme bieten keine Unterstützung für diese Funktion.
- Machen Sie sich mit den MSI-Befehlszeilenoptionen vertraut. Siehe „Befehlszeilenoptionen für Microsoft Windows Installer“, auf Seite 33.
- Machen Sie sich mit den verfügbaren MSI-Eigenschaften für die unbeaufsichtigte Installation von Horizon Client vertraut. Siehe „Eigenschaften für die unbeaufsichtigte Installation von Horizon Client“, auf Seite 31.
- Legen Sie fest, ob Sie Endbenutzern von ihren virtuellen Desktops aus den Zugriff auf lokal angeschlossene USB-Geräte gestatten möchten. Falls nicht, legen Sie über die MSI-Eigenschaft `ADDLOCAL` die Liste der relevanten Funktionen fest und lassen Sie die USB-Funktion aus. Weitere Informationen finden Sie unter „Eigenschaften für die unbeaufsichtigte Installation von Horizon Client“, auf Seite 31.
- Wenn Sie nicht möchten, dass die Endbenutzer den vollqualifizierten Domänennamen (FQDN) der View-Verbindungsserverinstanz eingeben müssen, ermitteln Sie den FQDN, um ihn während der Installation angeben zu können.

Vorgehensweise

1 Melden Sie sich beim Clientsystem als Administrator an.

2 Wechseln Sie zur VMware-Produktseite unter http://www.vmware.com/go/viewclients.

3 Laden Sie die Installationsdatei für Horizon Client herunter, z. B. `VMware-Horizon-Client-y.y.y-xxxxxx.exe`.

   Dabei steht *xxxxxx* für die Build-Nummer und *y.y.y* für die Versionsnummer.

4 Öffnen Sie auf dem Windows-Clientcomputer eine Eingabeaufforderung.

5 Geben Sie den Installationsbefehl in einer Zeile ein.

   In diesem Beispiel wird eine unbeaufsichtigte Installation von Horizon Client durchgeführt:

   ```
   VMware-Horizon-Client-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,USB,TSSO"
   ```

   Alternativ können Sie `ADDLOCAL=ALL` anstelle von `ADDLOCAL=Core,USB,TSSO` verwenden.

Hinweis Die Funktion `Core` ist verbindlich.

Das Installationsprogramm installiert bestimmte Windows-Dienste wie VMware Horizon Client (`horizon_client_service`) und VMware USB Arbitration Service (`VMUSBArbService`).

Weiter

(Optional) Wenn Sie Horizon Client mit der Funktion der URL-Inhaltsumleitung installiert haben, vergewissern Sie sich, dass deren Installation erfolgreich war. Dazu überprüfen Sie, ob die Dateien `vmware-url-protocol-launch-helper.exe` und `vmware-url-filtering-plugin.dll` im Verzeichnis `%PROGRAMFILES%\VMware\VMware Horizon View Client\` vorhanden sind. Außerdem müssen Sie sicherstellen, dass das Internet Explorer-Add-on VMware Horizon View URL Filtering Plugin installiert und aktiviert ist.

Starten Sie Horizon Client und stellen Sie sicher, dass Sie sich am richtigen Remote-Desktop bzw. an der richtigen Anwendung anmelden können. Siehe „Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung“, auf Seite 75.

Eigenschaften für die unbeaufsichtigte Installation von Horizon Client

Sie können spezifische Eigenschaften einschließen, wenn Sie eine unbeaufsichtigte Installation von Horizon Client über die Befehlszeile durchführen. Sie müssen das Format *`PROPERTY=value`* verwenden, damit Microsoft Windows Installer (MSI) die Eigenschaften und Werte interpretieren kann.

Im Abschnitt Tabelle 2-1 werden die Eigenschaften für die unbeaufsichtigte Installation von Horizon Client gezeigt, die Sie in der Befehlszeile verwenden können.

Tabelle 2-1. MSI-Eigenschaften für die unbeaufsichtigte Installation von Horizon Client

MSI-Eigenschaft	Beschreibung	Standardwert
INSTALLDIR	Pfad und Verzeichnis für die Installation der Horizon Client-Software. Beispiel: `INSTALLDIR=""D:\abc\mein Ordner""` Die Paare doppelter Anführungszeichen, die den Pfad umschließen, ermöglichen es dem MSI Installer, das Leerzeichen als gültigen Teil des Pfades zu interpretieren.	`%ProgramFiles%\VMware\VMware Horizon View Client`
VDM_IP_PROTOCOL_USAGE	Gibt die IP- (Netzwerkprotokoll-)Version an, die von Horizon-Komponenten für die Kommunikation verwendet wird. Mögliche Werte sind **`IPv4`** und **`IPv6`**.	IPv4

Tabelle 2-1. MSI-Eigenschaften für die unbeaufsichtigte Installation von Horizon Client (Fortsetzung)

MSI-Eigenschaft	Beschreibung	Standardwert
VDM_SERVER	Der vollqualifizierte Domänenname (FQDN) der Verbindungsserver-Instanz, mit der Horizon Client-Benutzer standardmäßig eine Verbindung herstellen. Wenn Sie diese Eigenschaft konfigurieren, müssen Horizon Client-Benutzer diesen FQDN nicht angeben. Beispiel: `VDM_SERVER=cs1.companydomain.com` Diese MSI-Eigenschaft ist optional.	Keine
DESKTOP_SHORTCUT	Konfiguriert ein Desktop-Verknüpfungssymbol für Horizon Client. Bei Verwendung des Werts 1 wird die Verknüpfung installiert. Bei Verwendung des Werts 0 wird die Verknüpfung nicht installiert.	1
STARTMENU_SHORTCUT	Konfiguriert eine Verknüpfung für Horizon Client im Startmenü. Bei Verwendung des Werts 1 wird die Verknüpfung installiert. Bei Verwendung des Werts 0 wird die Verknüpfung nicht installiert.	1
URL_FILTERING_ENABLED	Gibt an, ob die Funktion der URL-Inhaltsumleitung installiert werden soll. Bei Verwendung des Werts 1 wird die Funktion installiert. **Hinweis** Die Option `ADDLOCAL=ALL` legt diese Funktion nicht für die Installation fest.	0
VDM_FIPS_ENABLED	Gibt an, ob Horizon Client mit der FIPS-konformen Kryptografie installiert wird. Mit dem Wert 1 wird der Client mit FIPS-konformer Kryptografie installiert. Mit dem Wert 0 erfolgt die Installation ohne. **Hinweis** Bevor Sie diese Option auf 1 stellen, müssen Sie den FIPS-Modus im Windows-Clientbetriebssystem aktivieren. Siehe „Aktivieren des FIPS-Modus im Windows-Clientbetriebssystem“, auf Seite 27.	0

In einem Befehl für die unbeaufsichtigte Installation können Sie die MSI-Eigenschaft `ADDLOCAL=` zum Festlegen von Funktionen verwenden, die das Horizon Client-Installationsprogramm konfiguriert. Jede Funktion einer unbeaufsichtigten Installation entspricht einer Setupoption, die Sie während einer interaktiven Installation auswählen können.

Im Abschnitt Tabelle 2-2 werden die Horizon Client-Funktionen gezeigt, die Sie in der Befehlszeile eingeben können. Es werden außerdem die zugehörigen Optionen bei einer interaktiven Installation aufgeführt.

Tabelle 2-2. Horizon Client -Funktionen für die unbeaufsichtigte Installation und benutzerdefinierte Setup-Optionen für die interaktive Installation

Funktion für die unbeaufsichtigte Installation	Benutzerdefinierte Setup-Option in einer interaktiven Installation
Core Wenn Sie mit der MSI-Eigenschaft `ADDLOCAL=` einzelne Funktionen angeben, müssen Sie **`Core`** einschließen.	Keine. Während einer interaktiven Installation werden die Horizon Client-Core-Funktionen standardmäßig installiert.
TSSO	Melden Sie sich als derzeit angemeldeter Windows-Domänenbenutzer an.
USB	USB-Umleitung

Befehlszeilenoptionen für Microsoft Windows Installer

Zur unbeaufsichtigten Installation von Horizon Client müssen Sie die Befehlszeilenoptionen und Eigenschaften von Microsoft Windows Installer (MSI) verwenden. Die Installationsprogramme für Horizon Client sind MSI-Programme und verwenden standardmäßige MSI-Funktionen. Sie können auch MSI-Befehlszeilenoptionen zum unbeaufsichtigten Deinstallieren von Horizon Client verwenden.

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. Informationen zur Verwendung der MSI-Befehlszeile erhalten Sie, indem Sie auf dem Clientcomputer eine Eingabeaufforderung öffnen und `msiexec /?` eingeben.

Für die unbeaufsichtigte Installation von Horizon Client deaktivieren Sie zunächst das Bootstrap-Programm, mit dem das Installationsprogramm in ein temporäres Verzeichnis extrahiert und eine interaktive Installation gestartet wird.

In der folgenden Tabelle sind die Befehlszeilenoptionen aufgeführt, die das Bootstrap-Programm des Installationsprogramms steuern.

Tabelle 2-3. Befehlszeilenoptionen für das Bootstrap-Programm

Option	Beschreibung
`/s`	Deaktiviert den Bootstrap-Begrüßungsbildschirm und das Dialogfeld für die Extraktion, wodurch die Anzeige interaktiver Dialogfelder unterbunden wird. Beispiel: `VMware-Horizon-Client-`*`y.y.y-xxxxxx`*`.exe /s` Die Option `/s` ist erforderlich, um eine unbeaufsichtigte Installation durchzuführen. In den Beispielen steht *xxxxxx* für die Build-Nummer und *y.y.y* für die Versionsnummer.
`/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-Client-`*`y.y.y-xxxxxx`*`.exe /s /v"`*`command_line_options`*`"` Damit das MSI-Installationsprogramm eine Zeichenfolge mit Leerzeichen richtig auswertet, müssen Sie die Zeichenfolge in zwei Sätze doppelter Anführungszeichen einschließen. Angenommen, Sie möchten den Client in einem Pfad installieren, dessen Name Leerzeichen enthält. Beispiel: `VMware-Horizon-View-Client-`*`y.y.y-xxxxxx`*`.exe /s /v"`*`Befehlszeilenoptionen`*` INSTALLDIR=""d:\abc\my folder"""` In diesem Beispiel übergibt das MSI-Installationsprogramm den Verzeichnispfad für die Installation und versucht nicht, die Zeichenfolge als Befehlszeilenoptionen auszuwerten. Beachten Sie die zweifach gesetzten doppelten Anführungszeichen, die die gesamte Befehlszeile umschließen. 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. Das MSI-Installationsprogramm umfasst den Installationscode von Horizon Client. Das Installationsprogramm verwendet die in die Befehlszeile eingegebenen Werte und Optionen, um die Installationsauswahl und die für Horizon Client spezifischen Setup-Optionen auszuwerten.

In der folgenden Tabelle sind die Befehlszeilenoptionen und MSI-Eigenschaftenwerte aufgeführt, die an das MSI-Installationsprogramm übergeben werden.

Tabelle 2-4. MSI-Befehlszeilenoptionen und MSI-Eigenschaften

MSI-Option oder -Eigenschaft	Beschreibung
`/qn`	Weist den MSI Installer an, keine Seiten des Installationsassistenten anzuzeigen. Angenommen, Sie möchten den Agent unbeaufsichtigt installieren und nur standardmäßige Setup-Optionen und Funktionen verwenden: `VMware-Horizon-Client-y.y.y-xxxxxx.exe /s /v"/qn"` In den Beispielen steht *xxxxxx* für die Build-Nummer und *y.y.y* für die Versionsnummer. Alternativ haben Sie die Möglichkeit, mit der Option `/qr` oder `/qb` eine nicht interaktive, automatische Installation durchzuführen. Mit der Option `/qr` werden im Verlauf der Installation Assistentenseiten eingeblendet, in die Sie aber nichts eingeben können. Mit der Option `/qb` wird ein einfacher Fortschrittsbalken angezeigt. Die Option `/qn`, `/qb` oder `/qr` ist erforderlich, um eine nicht interaktive Installation durchzuführen.
`INSTALLDIR`	(Optional) Gibt einen alternativen Installationspfad für das Installationsverzeichnis an. Verwenden Sie das Format *`INSTALLDIR=Pfad`*, um den Installationspfad anzugeben. Sie können diese MSI-Eigenschaft ignorieren, wenn Sie den Client im Standardpfad installieren möchten.
`ADDLOCAL`	(Optional) Legt die komponentenspezifischen Funktionen fest, die installiert werden sollen. In einer interaktiven Installation zeigt das Installationsprogramm Auswahloptionen für das benutzerdefinierte Setup an. Mithilfe der MSI-Eigenschaft `ADDLOCAL` können Sie diese Setup-Optionen an der Befehlszeile angeben. Um alle verfügbaren Optionen für ein benutzerdefiniertes Setup zu installieren, geben Sie `ADDLOCAL=ALL` ein. Beispiel: `VMware-Horizon-Client-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=ALL"` Wenn Sie die MSI-Eigenschaft `ADDLOCAL` nicht verwenden, werden die standardmäßigen Setup-Optionen installiert. Zur Festlegung einzelner Setup-Optionen geben Sie eine Liste der Setup-Optionen ein. Trennen Sie hierbei die Namen der Optionen durch Kommata. Verwenden Sie zwischen den Namen keine Leerzeichen. Verwenden Sie das Format *`ADDLOCAL=Wert,Wert,Wert....`* Angenommen, Sie möchten den Client mit der Funktion zur USB-Umleitung, aber ohne die Funktion „Als aktueller Benutzer anmelden“ installieren: `VMware-Horizon-Client-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,USB"`
`LOGINASCURRENTUSER_DISPLAY`	(Optional) Legt fest, ob das Kontrollkästchen **Als aktueller Benutzer anmelden** im Dialogfeld für die Horizon Client-Verbindung angezeigt wird. Gültige Werte sind `1` (aktiviert) und `0` (deaktiviert). Der Standardwert ist `1`, womit das Kontrollkästchen sichtbar ist und die Benutzer dieses Kontrollkästchen aktivieren oder deaktivieren sowie den zugehörigen Standardwert außer Kraft setzen können. Wird das Kontrollkästchen ausgeblendet, können Benutzer den Standardwert im Dialogfeld für die Horizon Client-Verbindung nicht ändern.

Tabelle 2-4. MSI-Befehlszeilenoptionen und MSI-Eigenschaften (Fortsetzung)

MSI-Option oder -Eigenschaft	Beschreibung
LOGINASCURRENTUSER_DEFAULT	(Optional) Gibt den Standardwert des Kontrollkästchens **Als aktueller Benutzer anmelden** im Dialogfeld für die Horizon Client-Verbindung an. Gültige Werte sind 1 (aktiviert) und 0 (deaktiviert). Es ist kein Standardwert festgelegt. Dies bedeutet, dass das Kontrollkästchen deaktiviert ist und die Benutzer Identitäts- und Anmeldeinformationen mehrere Male eingeben müssen, bevor sie auf einen Remote-Desktop zugreifen können. Wenn das Kontrollkästchen **Als aktueller Benutzer anmelden** aktiviert ist, werden die Identität und die Anmeldedaten des Benutzers, die dieser zur Anmeldung am Clientsystem verwendet, an die Verbindungsserver-Instanz und schließlich an den Remote-Desktop übergeben. Verwenden Sie diese Option mit der Option LOGINASCURRENTUSER_DISPLAY . Beispiel: LOGINASCURRENTUSER_DISPLAY=1 LOGINASCURRENTUSER_DEFAULT=1 Wenn ein Benutzer Horizon Client über die Befehlszeile ausführt und die Option logInAsCurrentUser angibt, wird diese Einstellung durch den eingegebenen Wert überschrieben.
REBOOT	(Optional) Sie können die Option REBOOT=ReallySuppress verwenden, um alle Neustarts und Aufforderungen zum Neustart zu unterdrücken.
/l*v *Protokolldatei*	(Optional) Schreibt 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.

Beispiel: Installationsbeispiele

In den folgenden Beispielen steht *xxxxxx* für die Build-Nummer, *y.y.y* für die Versionsnummer, *install_folder* für den Pfad zum Installationsordner sowie view.mycompany.com für den Namen einer fiktiven Verbindungsserver-Instanz.

Standardinstallationsbeispiel:

```
VMware-Horizon-Client-y.y.y-xxxxxx.exe /s /v"/qn REBOOT=ReallySuppress INSTALLDIR=install_folder
ADDLOCAL=ALL DESKTOP_SHORTCUT=1 STARTMENU_SHORTCUT=1 VDM_SERVER=view.mycompany.com /l*v "%TEMP
%\log.txt""
```

Installations- und Konfigurationsbeispiel für die Funktion „Als aktueller Benutzer anmelden“:

```
VMware-Horizon-Client-y.y.y-xxxxxx.exe /s /v"/qn INSTALLDIR=install_folder ADDLOCAL=Core,TSSO LO-
GINASCURRENTUSER_DISPLAY=1 LOGINASCURRENTUSER_DEFAULT=1 DESKTOP_SHORTCUT=1 STARTMENU_SHORTCUT=1
VDM_SERVER=view.mycompany.com /l*v "%TEMP%\log.txt""
```

In diesem Beispiel wird REBOOT=ReallySuppress ausgelassen, da die TSSO-Option (Melden Sie sich als derzeit angemeldeter Windows-Domänenbenutzer an) einen Neustart erfordert.

Onlineaktualisierung von Horizon Client

Sie können Horizon Client online aktualisieren, sofern die Aktualisierungsfunktion aktiviert ist. Diese Funktion ist standardmäßig deaktiviert.

Sie können diese Funktion aktivieren, indem Sie die Gruppenrichtlinieneinstellungen Enable Horizon Client online update und URL for Horizon Client online update ändern. Weitere Informationen finden Sie unter „Allgemeine Einstellungen für Client-GPOs“, auf Seite 58.

Voraussetzungen

- Speichern Sie vor der Aktualisierung von Horizon Client Ihre Arbeit. Das Update startet eventuell das System neu.
- Stellen Sie sicher, dass Sie sich als Administrator auf dem Clientsystem anmelden können.

Vorgehensweise

1 Melden Sie sich als Administrator an.

2 Klicken Sie in Horizon Client auf **Software-Updates** von einem der zwei Bildschirme.

Horizon Client-Bildschirm	Aktion
Vor dem Herstellen einer Verbindung zu einem Verbindungsserver	Klicken Sie auf **Optionen > Software-Updates**.
Nach dem Herstellen einer Verbindung zu einem Verbindungsserver	Klicken Sie auf **Hilfe > Software-Updates**.

3 Klicken Sie auf **Auf Updates prüfen**.

4 Klicken Sie auf **Herunterladen und installieren**.

Konfigurieren von Horizon Client für Endbenutzer

3

Die Konfiguration von Horizon Client für Endbenutzer kann verschiedene Aufgaben umfassen wie die Konfiguration von URIs zum Start von Horizon Client, die Konfiguration des Zertifikatüberprüfungsmodus, die Festlegung erweiterter TLS/SSL-Optionen sowie die Konfiguration benutzerdefinierter Einstellungen mithilfe der ADM- und ADMX-Vorlagendateien für Gruppenrichtlinien.

Dieses Kapitel behandelt die folgenden Themen:

Allgemeine Konfigurationseinstellungen

Horizon Client bietet mehrere Konfigurationsmechanismen zur Vereinfachung der Anmeldung und Desktop-Auswahl und zur Verbesserung der Benutzererfahrung sowie zur Durchsetzung der Sicherheitsrichtlinien.

In der folgenden Tabelle werden nur einige Konfigurationseinstellungen beschrieben, die Sie auf verschiedene Weise festlegen können.

Tabelle 3-1. Allgemeine Konfigurationseinstellungen

Einstellung	Konfigurationsmechanismen
Adresse des Verbindungsservers	URI, Gruppenrichtlinie, Befehlszeile, Windows-Registrierung
Active Directory-Benutzername	URI, Gruppenrichtlinie, Befehlszeile, Windows-Registrierung
Domänenname	URI, Gruppenrichtlinie, Befehlszeile, Windows-Registrierung
Desktopanzeigename	URI, Gruppenrichtlinie, Befehlszeile
Fenstergröße	URI, Gruppenrichtlinie, Befehlszeile
Anzeigeprotokoll	URI, Befehlszeile

Tabelle 3-1. Allgemeine Konfigurationseinstellungen (Fortsetzung)

Einstellung	Konfigurationsmechanismen
Konfigurieren der Zertifikatsprüfung	Gruppenrichtlinie, Windows-Registrierung
Konfigurieren von SSL-Protokollen und kryptografischen Algorithmen	Gruppenrichtlinie, Windows-Registrierung

Verwenden von URIs zur Konfiguration von Horizon Client

Mithilfe so genannter Uniform Resource Identifiers (URIs) können Sie eine Webseite oder E-Mail mit verschiedenen Verknüpfungen erstellen, auf die die Endbenutzer zum Start von Horizon Client, zur Verbindung mit einem Server oder zum Öffnen eines bestimmten Desktops oder einer bestimmten Anwendung mit bestimmten Konfigurationsoptionen klicken.

Sie können die Verbindungsherstellung mit einem Remote-Desktop oder einer Anwendung durch Erstellen von Web- oder E-Mail-Verknüpfungen für die Endbenutzer deutlich vereinfachen. Diese Verknüpfungen werden durch die Generierung von URIs erstellt, die einige oder alle der folgenden Informationen bereitstellen, sodass die Endbenutzer diese nicht angeben müssen:

- Adresse des Verbindungsservers
- Portnummer für den Verbindungsserver
- Active Directory-Benutzername
- RADIUS- oder RSA SecurID-Benutzername, wenn dieser nicht mit dem Active Directory-Benutzernamen identisch ist
- Domänenname
- Desktop- oder Anwendungsanzeigename
- Fenstergröße
- Aktionen, darunter „Zurücksetzen“, „Abmelden“ und „Sitzung starten“
- Anzeigeprotokoll
- Optionen zur Umleitung von USB-Geräten

Verwenden Sie zur Generierung eines URI das URI-Schema `vmware-view` mit Horizon Client-spezifischen Pfad- und Abfragekomponenten.

Hinweis Sie können URIs zum Start von Horizon Client nur dann verwenden, wenn die Clientsoftware bereits auf den Clientcomputern installiert ist.

Syntax für die Erstellung von vmware-view-URIs

Die Syntax umfasst das URI-Schema `vmware-view`, einen Pfadauszug zur Angabe des Desktops oder der Anwendung sowie optional eine Abfrage zur Angabe der Desktop- bzw. Anwendungsaktionen oder Konfigurationsoptionen.

URI-Spezifikation

Verwenden Sie zum Generieren von URIs für den Start von Horizon Client die folgende Syntax:

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

Das einzig erforderliche Element ist das URI-Schema `vmware-view`. Für einige Versionen bestimmter Clientbetriebssysteme muss für den Namen des Schemas die Groß- und Kleinschreibung beachtet werden. Verwenden Sie daher `vmware-view`.

Wichtig In allen Abschnitten müssen Nicht-ASCII-Zeichen zunächst gemäß UTF-8 [STD63] codiert werden, anschließend muss für jedes Oktett der entsprechenden UTF-8-Sequenz eine Prozentcodierung durchgeführt werden, um diese als URI-Zeichen darzustellen.

Informationen zur Codierung von ASCII-Zeichen finden Sie in der URL-Codierungsreferenz unter http://www.utf8-chartable.de/.

authority-part

Gibt die Serveradresse und optional einen Benutzernamen, eine nicht standardmäßige Portnummer oder beides an. Unterstriche (_) werden in Servernamen nicht unterstützt. Die Servernamen müssen der DNS-Syntax entsprechen.

Verwenden Sie zur Angabe eines Benutzernamens die folgende Syntax:

`user1@server-address`

Sie können keine UPN-Adresse angeben, auch keine Domäne. Zur Angabe des Domänennamens können Sie den Abfrageteil `domainName` im URI verwenden.

Verwenden Sie zur Angabe einer Portnummer die folgende Syntax:

`server-address:port-number`

path-part

Gibt den Desktop oder die Anwendung an. Verwenden Sie den Anzeigenamen des Desktops oder der Anwendung. Dieser Name wurde in Horizon Administrator beim Erstellen des Desktop- oder Anwendungspools angegeben. Weist der Anzeigename ein Leerzeichen auf, müssen Sie den Codierungsmechanismus **`%20`** verwenden, um das Leerzeichen darzustellen.

query-part

Gibt die zu verwendenden Konfigurationsoptionen oder die durchzuführenden Desktop- oder Anwendungsaktionen an. Für die Abfragen muss die Groß- und Kleinschreibung nicht beachtet werden. Verwenden Sie für den Einsatz mehrerer Abfragen das kaufmännische Und-Zeichen (&) zwischen den Abfragen. Sollten die Abfragen miteinander in Konflikt stehen, wird die letzte Abfrage in der Liste verwendet. Verwenden Sie die folgende Syntax:

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

Unterstützte Abfragen

In diesem Abschnitt werden die Abfragen aufgeführt, die für diesen Horizon Client-Typ unterstützt werden. Wenn Sie URIs für mehrere Clienttypen generieren, so zum Beispiel für Desktop-Clients oder mobile Clients, finden Sie für jede Art von Clientsystem weitere Anweisungen im Handbuch *Verwendung von VMware Horizon Client*.

action

Tabelle 3-2. Werte, die mit der Abfrage „action“ verwendet werden können

Wert	Beschreibung
`browse`	Zeigt eine Liste der verfügbaren, auf dem angegebenen Server gehosteten Desktops und Anwendungen an. Bei Verwendung dieser Aktion müssen Sie keinen Desktop bzw. keine Anwendung angeben.
`start-session`	Öffnet den angegebenen Desktop oder die angegebene Anwendung. Wenn keine „action“-Abfrage bereitgestellt wird und der Desktop- oder Anwendungsname angegeben wird, ist `start-session` die Standardaktion.
`reset`	Fährt den angegebenen Desktop bzw. die angegebene Anwendung herunter und startet ihn bzw. sie neu. Nicht gespeicherte Daten gehen verloren. Das Zurücksetzen eines Remote-Desktops entspricht dem Betätigen der Reset-Taste auf einem physischen PC.
`restart`	Fährt den angegebenen Desktop herunter und startet ihn neu. Der Neustart eines Remote-Desktops entspricht dem Neustart des Windows-Betriebssystems. In der Regel wird der Benutzer dabei vom Betriebssystem aufgefordert, alle nicht gespeicherten Daten zu speichern, bevor der Neustart erfolgt.
`logoff`	Meldet den Benutzer vom Gastbetriebssystem auf dem Remote-Desktop ab. Wenn Sie eine Anwendung angeben, wird die Aktion ignoriert oder der Endbenutzer sieht die Warnmeldung „Ungültige URI-Aktion“.

args

Gibt Befehlszeilenargumente zum Hinzufügen beim Start einer Remoteanwendung an. Verwenden Sie die Syntax `args=`*Wert*, wobei *Wert* eine Zeichenfolge sein muss. Verwenden Sie für die folgenden Zeichen die Prozentkodierung:

- Für einen Doppelpunkt (:) verwenden Sie **`%3A`**.
- Für einen umgekehrten Schrägstrich (\) verwenden Sie **`%5C`**.
- Für ein Leerzeichen ( ) verwenden Sie **`%20`**.
- Für ein doppeltes Anführungszeichen (") verwenden Sie **`%22`**

Um beispielsweise den Dateinamen `"My new file.txt"` für die Notepad++-Anwendung anzugeben, verwenden Sie **`%22My%20new%20file.txt%22`**.

appProtocol

Gültige Werte für Remoteanwendungen sind **`PCOIP`** und **`BLAST`**. Zur Angabe von PCoIP verwenden Sie beispielsweise die Syntax **`appProtocol=PCOIP`**.

connectUSBOnInsert

Verbindet ein USB-Gerät beim Anschließen des Geräts mit dem im Vordergrund angezeigten Desktop. Diese Abfrage wird bedingungslos festgelegt, wenn Sie die Abfrage `unattended` angeben. Zur Verwendung dieser Abfrage müssen Sie die Abfrage `action` auf **`start-session`** setzen oder ohne die Abfrage `action` arbeiten. Gültige Werte sind **`yes`** und **`no`**. Ein Beispiel für die Syntax ist etwa **`connectUSBOnInsert=yes`**.

connectUSBOnStartup

Leitet alle aktuell mit dem Clientsystem verbundenen USB-Geräte an den Desktop um. Diese Abfrage wird bedingungslos festgelegt, wenn Sie die Abfrage `unattended` angeben. Zur Verwendung dieser Abfrage müssen Sie die Abfrage `action` auf **`start-session`** setzen oder ohne die Abfrage `action` arbeiten. Gültige Werte sind **`yes`** und **`no`**. Ein Beispiel für die Syntax ist etwa **`connectUSBOnStartup=yes`**.

desktopLayout

Legt die Größe des Fensters für die Anzeige eines Remote-Desktops fest. Zur Verwendung dieser Abfrage müssen Sie die Abfrage `action` auf **`start-session`** setzen oder ohne die Abfrage `action` arbeiten.

Tabelle 3-3. Gültige Werte für desktopLayout-Abfrage

Wert	Beschreibung
`fullscreen`	Vollbild auf einem Monitor. Dieser Wert ist der Standardwert.
`multimonitor`	Vollbild auf allen Monitoren.
`windowLarge`	Großes Fenster.
`windowSmall`	Kleines Fenster.
*W*x*H*	Benutzerdefinierte Auflösung, bei der Sie die Breite mal Höhe in Pixel angeben. Ein Beispiel für die Syntax ist etwa **`desktopLayout=1280x800`**.

desktopProtocol

Gültige Werte für Remote-Desktops sind **`RDP`**, **`PCOIP`** und **`BLAST`**. Zur Angabe von PCoIP verwenden Sie beispielsweise die Syntax **`desktopProtocol=PCOIP`**.

domainName

Der NETBIOS-Domänenname, der mit dem Benutzer verknüpft ist, der eine Verbindung zum Remote-Desktop oder zur Remoteanwendung herstellt. Beispielsweise ist es sinnvoller, `MeineFirma` als `MeineFirma.com` zu verwenden.

filePath

Gibt den Pfad zur Datei im lokalen System an, die Sie mit einer Remoteanwendung öffnen möchten. Sie müssen den vollständigen Pfad einschließlich des Laufwerksbuchstabens eingeben. Verwenden Sie für die folgenden Zeichen die Prozentkodierung:

- Für einen Doppelpunkt (:) verwenden Sie **`%3A`**.
- Für einen umgekehrten Schrägstrich (\) verwenden Sie **`%5C`**.
- Für ein Leerzeichen ( ) verwenden Sie **`%20`**.

Um beispielsweise den Dateipfad `C:\test file.txt` darzustellen, verwenden Sie **`C%3A%5Ctest%20file.txt`**.

tokenUserName

Gibt den RSA- oder RADIUS-Benutzernamen an. Verwenden Sie diese Abfrage nur, wenn der RSA- oder RADIUS-Benutzername nicht mit dem Active Directory-Benutzernamen identisch ist. Wenn Sie diese Abfrage nicht angeben und die RSA- oder RADIUS-Authentifizierung erforderlich ist, wird der Windows-Benutzername verwendet. Die Syntax lautet **`tokenUserName=`*`name`***.

unattended

Erstellt eine Serververbindung zu einem Remote-Desktop im Kioskmodus. Wenn Sie diese Abfrage verwenden, geben Sie keine Benutzerinformationen an, wenn Sie den Kontonamen aus der MAC-Adresse des Clientgeräts generiert haben. Wenn Sie jedoch benutzerdefinierte Kontonamen in ADAM generiert haben, z. B. Namen, die mit „custom-“ beginnen, müssen Sie die Kontoinformationen angeben.

useExisting	Wenn für diese Option **`True`** festgelegt ist, kann nur eine Horizon Client-Instanz ausgeführt werden. Wenn Benutzer eine Verbindung zu einem zweiten Server herstellen möchten, müssen sie sich vom ersten Server abmelden, damit die Desktop- und Anwendungssitzungen getrennt werden. Ist für diese Option **`False`** festgelegt, können mehrere Horizon Client-Instanzen ausgeführt werden und die Benutzer haben die Möglichkeit, mit mehreren Servern gleichzeitig eine Verbindung herzustellen. Die Standardeinstellung ist **`True`**. Ein Beispiel für die Syntax ist etwa **`useExisting=false`**.
unauthenticatedAccessEnabled	Wenn für diese Option **`True`** festgelegt ist, ist die Funktion für den nicht authentifizierten Zugriff standardmäßig aktiviert. Die Option **Anonym mit nicht authentifiziertem Zugriff anmelden** ist dann in der Benutzeroberfläche verfügbar und aktiviert. Wenn für diese Option **`False`** festgelegt ist, ist die Funktion für den nicht authentifizierten Zugriff deaktiviert. Die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** ist dann ausgeblendet und deaktiviert. Wenn für diese Option **""** festgelegt ist, ist die Funktion für den nicht authentifizierten Zugriff deaktiviert. Die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** ist dann nicht mehr in der Benutzeroberfläche verfügbar und deaktiviert. Ein Beispiel für die Syntax ist etwa **`unauthenticatedAccessEnabled=true`**.
unauthenticatedAccessAccount	Damit wird das Konto festgelegt, das verwendet werden soll, wenn die Funktion für den nicht authentifizierten Zugriff aktiviert ist. Wenn der nicht authentifizierte Zugriff deaktiviert ist, wird diese Abfrage ignoriert. Die entsprechende Syntax lautet beispielsweise bei Verwendung des Benutzerkontos **`anonymous1`** dann **`unauthenticatedAccessAccount=anonymous1`**.

Beispiele für vmware-view-URIs

Sie können Hypertext-Links oder Schaltflächen mit dem URI-Schema `vmware-view` erstellen und diese Links in E-Mails oder auf einer Webseite einbinden. Ihre Endbenutzer können dann auf diese Links klicken, um beispielsweise einen bestimmten Remote-Desktop mit den von Ihnen angegebenen Startoptionen zu öffnen.

URI-Syntaxbeispiele

Nach jedem URI-Beispiel finden Sie eine Beschreibung, was der Endbenutzer nach Anklicken des URI-Links sieht.

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

Horizon Client startet und stellt eine Verbindung zum `view.mycompany.com`-Server her. Das Anmeldefeld fordert den Benutzer zur Eingabe von Benutzernamen, Domänennamen und Kennwort auf. Nach einer erfolgreichen Anmeldung stellt der Client eine Verbindung zum Desktop her, dessen Anzeigename als **Primary Desktop** angezeigt wird. Der Benutzer ist dann beim Gast-Betriebssystem angemeldet.

Hinweis Die Standardvorgaben für das Anzeigeprotokoll und die Fenstergröße werden verwendet. Das Standardanzeigeprotokoll ist PCoIP. Die Standardfenstergröße ist Vollbild.

---

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

Dieser URI hat die gleiche Wirkung wie im vorherigen Beispiel, außer dass er den nicht standardmäßigen Port 7555 für den Verbindungsserver verwendet. (Der standardmäßige Port lautet 443.) Da ein Desktop-Bezeichner bereitgestellt wird, wird der Desktop geöffnet, obwohl die Aktion `start-session` nicht im URI enthalten ist.

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

Horizon Client startet und stellt eine Verbindung zum `view.mycompany.com`-Server her. Im Anmeldefeld wird das Textfeld **Benutzername** mit dem Namen **fred** gefüllt. Der Benutzer muss den Domänennamen und das Kennwort eingeben. Nach einer erfolgreichen Anmeldung stellt der Client eine Verbindung zum Desktop her, dessen Anzeigename als **Finance Desktop** angezeigt wird. Der Benutzer ist dann beim Gast-Betriebssystem angemeldet. Die Verbindung nutzt das PCoIP-Anzeigeprotokoll.

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

Horizon Client startet und stellt eine Verbindung zum `view.mycompany.com`-Server her. In das Anmeldefeld muss der Benutzer den Benutzernamen, den Domänennamen und das Kennwort eingeben. Nach einer erfolgreichen Anmeldung wird vom Client eine Verbindung mit der Anwendung hergestellt, deren Anzeigename als **Berechnung** dargestellt wird. Die Verbindung nutzt das VMware Blast-Anzeigeprotokoll.

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

Horizon Client startet und stellt eine Verbindung zum `view.mycompany.com`-Server her. Im Anmeldefeld wird das Textfeld **Benutzername** mit dem Namen **fred** und das Textfeld **Domäne** mit **mycompany** gefüllt. Der Benutzer muss das Kennwort eingeben. Nach einer erfolgreichen Anmeldung stellt der Client eine Verbindung zum Desktop her, dessen Anzeigename als **Finance Desktop** angezeigt wird. Der Benutzer ist dann beim Gast-Betriebssystem angemeldet.

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

Horizon Client startet und der Benutzer wird zur Anmeldeaufforderung für die Verbindung mit dem Server `view.mycompany.com` geleitet.

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

Horizon Client startet und stellt eine Verbindung zum `view.mycompany.com`-Server her. Das Anmeldefeld fordert den Benutzer zur Eingabe von Benutzernamen, Domänennamen und Kennwort auf. Nach einer erfolgreichen Anmeldung zeigt Horizon Client ein Dialogfeld an, in dem der Benutzer aufgefordert wird, das Zurücksetzen für „Primary Desktop“ zu bestätigen.

Hinweis Diese Aktion ist nur möglich, wenn ein Horizon-Administrator die Funktion zum Zurücksetzen eines Desktops für den Desktop aktiviert hat.

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

Horizon Client startet und stellt eine Verbindung zum `view.mycompany.com`-Server her. Das Anmeldefeld fordert den Benutzer zur Eingabe von Benutzernamen, Domänennamen und Kennwort auf. Nach einer erfolgreichen Anmeldung zeigt Horizon Client ein Dialogfeld an, in dem der Benutzer aufgefordert wird, den Neustart für „Primary Desktop“ zu bestätigen.

Hinweis Diese Aktion ist nur möglich, wenn ein Horizon-Administrator die Funktion zum Neustart eines Desktops für den Desktop aktiviert hat.

9 `vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session&connectUSBOnStartup=true`

Dieser URI hat die gleiche Wirkung wie das erste Beispiel, und alle an das Clientsystem angeschlossenen USB-Geräte werden an den Remote-Desktop umgeleitet.

10 `vmware-view://`

Dieser URI startet Horizon Client, wenn dieser nicht ausgeführt wird, oder setzt Horizon Client in den Vordergrund, wenn er ausgeführt wird.

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

Startet My Notepad++ auf dem Server 10.10.10.10 und übergibt das Argument `My new file.txt` an den Befehl zum Start der Anwendung. Für Leerzeichen und doppelte Anführungszeichen gilt die Prozentkodierung. Der Dateiname ist in doppelte Anführungszeichen gesetzt, da er Leerzeichen enthält.

Sie können diesen Befehl auch an der Windows-Befehlszeile mithilfe der folgenden Syntax eingeben:

```
vmware-view.exe --serverURL 10.10.10.10 --appName "My Notepad++" --args "\"my new.txt\""
```

In diesem Beispiel werden doppelte Anführungszeichen durch die Zeichen \" kodiert.

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

Startet Notepad++ 12 auf dem Server 10.10.10.10 und übergibt das Argument `a.text b.txt` an den Befehl zum Start der Anwendung. Da dieses Argument nicht in Anführungszeichen gesetzt ist, trennt ein Leerzeichen die Dateinamen und die beiden Dateien werden gesondert in Notepad++ geöffnet.

Hinweis Anwendungen können sich in der Umsetzung von Befehlszeilenargumenten unterscheiden. Wenn Sie beispielsweise das Argument `a.txt b.txt` an Wordpad übergeben, öffnet Wordpad nur eine Datei, `a.txt`.

---

13 `vmware-view://view.mycompany.com/Notepad?unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous1`

Horizon Client startet und stellt mithilfe des Benutzerkontos **`anonymous1`** eine Verbindung mit dem `view.mycompany.com`-Server her. Die Anwendung „Editor“ wird ohne Aufforderung des Benutzers zur Eingabe seiner Anmeldedaten gestartet.

Beispiel für HTML-Code

Sie können URIs verwenden, um Hypertext-Links und Schaltflächen zu erstellen, die in E-Mails oder auf Webseiten eingebunden werden können. Die folgenden Beispiele veranschaulichen, wie Sie den URI aus dem ersten Beispiel verwenden, um einen Hypertext-Link mit dem Text **Test Link** besagt und eine Schaltfläche mit dem Text **TestButton** zu codieren.

```
<html>
<body>

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

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

</body>
</html>
```

Konfigurieren der Zertifikatsprüfungen für Endbenutzer

Administratoren können den Zertifikatüberprüfungsmodus so konfigurieren, dass beispielsweise immer die vollständige Überprüfung durchgeführt wird.

Die Zertifikatsprüfung wird für SSL-Verbindungen zwischen dem Verbindungsserver und Horizon Client durchgeführt. Die Administratoren können den Überprüfungsmodus so konfigurieren, dass eine der folgenden Strategien verwendet wird:

- Die Endbenutzer wählen selbst den Überprüfungsmodus. In der restlichen Liste werden die drei Überprüfungsmodi beschrieben.
- (Keine Überprüfung) Es werden keine Zertifikatsprüfungen durchgeführt.
- (Warnen) Die Endbenutzer werden gewarnt, wenn der Server ein selbstsigniertes Zertifikat vorlegt. Die Benutzer können dann selbst entscheiden, ob sie diesen Verbindungstyp zulassen.
- (Volle Sicherheit) Es wird eine vollständige Überprüfung durchgeführt. Die Verbindungen, für die diese Prüfung nicht erfolgreich verläuft, werden abgelehnt.

Einzelheiten zu den verschiedenen Arten der durchgeführten Überprüfungen finden Sie unter „Festlegen des Zertifikatsprüfungsmodus für Horizon Client“, auf Seite 45.

Legen Sie mit der ADM- oder ADMX-Vorlagendatei (`vdm_client.adm` oder `vdm_client.admx`) für die Clientkonfiguration den Prüfungsmodus fest. Alle ADM- und ADMX-Dateien, die Gruppenrichtlinieneinstellungen bereitstellen, sind in einer `.zip`-Datei mit dem Namen `VMware-Horizon-View-Bundle-x.x.x-yyyyyyy.zip` verfügbar, wobei *x.x.x* für die Versionsnummer und *yyyyyyy* für die Build-Nummer steht. Sie können das GPO-Paket von der VMware Horizon-Download-Site unter http://www.vmware.com/go/downloadview herunterladen. Informationen zum Festlegen der GPO-Einstellungen mithilfe dieser Vorlage finden Sie unter „Konfigurieren von VMware Horizon Client für Windows mithilfe der Gruppenrichtlinienvorlage“, auf Seite 48.

Hinweis Mit der ADM- oder ADMX-Vorlagendatei für die Clientkonfiguration können Sie auch die Verwendung bestimmter kryptografischer Algorithmen und Protokolle einschränken, bevor Sie eine verschlüsselte SSL-Verbindung herstellen. Weitere Informationen zu dieser Einstellung finden Sie unter „Sicherheitseinstellungen für Client-GPOs“, auf Seite 51.

Wenn Sie die Einstellung für die Zertifikatüberprüfung nicht als Gruppenrichtlinie konfigurieren möchten, können Sie die Zertifikatüberprüfung auch durch Hinzufügen des Wertnamens `CertCheckMode` zu einem der folgenden Registrierungsschlüssel auf dem Clientcomputer aktivieren:

- Für 32-Bit-Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`
- Für 64-Bit-Windows: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`

Verwenden Sie die folgenden Werte im Registrierungsschlüssel:

- **`0`** implementiert `Do not verify server identity certificates.`
- **`1`** implementiert `Warn before connecting to untrusted servers.`
- **`2`** implementiert `Never connect to untrusted servers.`

Wenn Sie sowohl die Gruppenrichtlinieneinstellung als auch die Einstellung `CertCheckMode` im Registrierungsschlüssel konfigurieren, hat die Gruppenrichtlinieneinstellung Vorrang vor der Registrierungsschlüsseleinstellung.

Hinweis In einer künftigen Version wird die mithilfe der Windows-Registrierung vorgenommene Konfiguration dieser Einstellung möglicherweise nicht unterstützt. Es muss eine GPO-Einstellung verwendet werden.

Festlegen des Zertifikatsprüfungsmodus für Horizon Client

Administratoren und manchmal auch Endbenutzer können über eine Konfiguration festlegen, ob Client-Verbindungen abgelehnt werden sollen, wenn bei Zertifikatsüberprüfungen Fehler auftreten.

Die Zertifikatsprüfung wird für SSL-Verbindungen zwischen dem Verbindungsserver und Horizon Client durchgeführt. Die Zertifikatsüberprüfung umfasst die folgenden Checks:

- Wurde das Zertifikat widerrufen?
- Ist das Zertifikat für einen anderen Zweck bestimmt als für die Überprüfung der Identität des Absenders und die Verschlüsselung der Serverkommunikation? Mit anderen Worten: Handelt es sich um den korrekten Zertifikattyp?
- Ist das Zertifikat abgelaufen oder erst zukünftig gültig? Mit anderen Worten: Ist das Zertifikat laut Computeruhr gültig?

- Stimmt der allgemeine Name auf dem Zertifikat mit dem Hostnamen des Servers überein, der es sendet? Zu einer fehlenden Übereinstimmung kann es kommen, wenn ein Lastenausgleich Horizon Client an einen Server mit einem Zertifikat umleitet, das nicht mit dem in Horizon Client eingegebenen Hostnamen übereinstimmt. Ein weiterer möglicher Grund für eine fehlende Übereinstimmung ist die Eingabe einer IP-Adresse statt eines Hostnamens im Client.
- Ist das Zertifikat von einer unbekannten oder nicht als vertrauenswürdig eingestuften Zertifizierungsstelle (CA) signiert worden? Selbstsignierte Zertifikate sind ein Typ der nicht als vertrauenswürdig eingestuften CA.

  Um diese Prüfung zu bestehen, muss sich das Stammzertifikat für die Zertifikatvertrauenskette im lokalen Zertifikatspeicher des Geräts befinden.

Hinweis Informationen zur Verteilung eines selbstsignierten Stammzertifikats an alle Windows-Clientsysteme in einer Domäne finden Sie unter „Stammzertifikat zu den vertrauenswürdigen Zertifizierungsstellen hinzufügen“ im Dokument *Installation von View*.

Wenn Ihr Administrator Ihnen die Verwendung von Horizon Client bei der Anmeldung an einem Desktop ermöglicht hat, können Sie auf **SSL konfigurieren** klicken und den Zertifikatsprüfungsmodus einstellen. Sie haben drei Auswahlmöglichkeiten:

- **Nie mit nicht vertrauenswürdigen Servern verbinden**. Sollte eine beliebige der Zertifikatsprüfungen fehlschlagen, kann der Client keine Verbindung mit dem Server herstellen. Die nicht bestandenen Prüfungen werden in einer Fehlermeldung aufgelistet.
- **Warnung vor Verbindung mit nicht vertrauenswürdigen Servern ausgeben**. Wenn eine Zertifikatsprüfung fehlschlägt, weil der Server ein selbstsigniertes Zertifikat verwendet, können Sie auf **Weiter** klicken, um die Warnung zu ignorieren. Bei selbstsignierten Zertifikaten muss der Zertifikatsname nicht mit dem Servernamen übereinstimmen, den Sie in Horizon Client eingegeben haben.

  Möglicherweise erhalten Sie auch eine Warnung, wenn das Zertifikat abgelaufen ist.
- **Server-Identitätszertifikate nicht überprüfen**. Mit dieser Einstellung werden Zertifikate nicht überprüft.

Ist der Zertifikatsprüfungsmodus auf **Warnen** gesetzt, können Sie immer noch eine Verbindung mit einer Verbindungsserver-Instanz herstellen, die ein selbstsigniertes Zertifikat verwendet.

Installiert ein Administrator später ein Sicherheitszertifikat von einer vertrauenswürdigen Zertifikatsautorität, sodass alle Zertifikatsüberprüfungen bei der Verbindungsherstellung bestanden werden, wird diese vertrauenswürdige Verbindung für diesen speziellen Server vorgemerkt. Legt dieser Server in Zukunft wieder ein selbstsigniertes Zertifikat vor, schlägt die Verbindung fehl. Nachdem ein bestimmter Server ein vollständig überprüfbares Zertifikat vorgelegt hat, muss er dies auch in Zukunft immer so handhaben.

Wichtig In früheren Versionen wurden die Clientsysteme Ihres Unternehmens so konfiguriert, dass über ein GPO ein bestimmtes Verschlüsselungsverfahren verwendet wird, etwa durch Konfiguration von Gruppenrichtlinieneinstellungen für die Reihenfolge der SSL-Verschlüsselungssammlungen. Nun müssen Sie dafür eine Gruppenrichtlinien-Sicherheitseinstellung von Horizon Client verwenden. Diese ist in den ADM- und ADMX-Vorlagendateien enthalten. Siehe „Sicherheitseinstellungen für Client-GPOs“, auf Seite 51. Alternativ können Sie auch die Registrierungseinstellung `SSLCipherList` auf dem Client verwenden. Siehe „Konfigurieren des Horizon Client mithilfe der Windows-Registrierung“, auf Seite 72.

Konfigurieren erweiterter TLS-/SSL-Optionen

Sie können die Sicherheitsprotokolle und kryptografischen Algorithmen auswählen, die zum Verschlüsseln der Kommunikation zwischen Horizon Client und Horizon Servern oder zwischen Horizon Client und dem Agenten im Remote-Desktop verwendet werden.

Diese Sicherheitsoptionen werden auch zur Verschlüsselung des USB-Kanals verwendet.

In der Standardeinstellung verwenden Verschlüsselungssammlungen 128- oder 256-Bit-AES, entfernen anonyme DH-Algorithmen und sortieren anschließend die aktuelle Verschlüsselungsliste nach der Schlüssellänge des Verschlüsselungsalgorithmus.

TLS v1.0 , TLS v1.1 und TLS v1.2 sind standardmäßig aktiviert. SSL v2.0 und v3.0 werden nicht unterstützt.

Hinweis Wenn TLS v1.0 und RC4 deaktiviert sind, ist die USB-Umleitung nicht wirksam, wenn Benutzer mit Windows XP-Desktops verbunden sind. Bitte beachten Sie, dass bei Aktivierung dieser Funktion durch die Aktivierung von TLS v1.0 und RC4 Sicherheitsrisiken entstehen können.

Wenn Sie ein Sicherheitsprotokoll für Horizon Client konfigurieren, das auf dem Server, mit dem sich der Client verbindet, nicht aktiviert ist, tritt ein TLS-/SSL-Fehler auf und die Verbindung schlägt fehl.

Wichtig Mindestens eines der von Ihnen in Horizon Client aktivierten Protokolle muss auf dem Remote-Desktop aktiviert werden. Anderenfalls können USB-Geräte nicht auf den Remote-Desktop umgeleitet werden.

Sie können auf dem Clientsystem entweder eine Gruppenrichtlinien- oder eine Windows-Registrierungseinstellung verwenden, um die Standardverschlüsselungen und -protokolle zu ändern. Weitere Informationen zur Verwendung eines GPO finden Sie in der Einstellung „Configures SSL protocols and cryptographic algorithms“ unter „Sicherheitseinstellungen für Client-GPOs“, auf Seite 51. Weitere Informationen zur Verwendung der Einstellung „SSLCipherList“ in der Windows-Registrierung finden Sie unter „Konfigurieren des Horizon Client mithilfe der Windows-Registrierung“, auf Seite 72.

Konfigurieren des Wiederverbindungsverhaltens von Anwendungen

Wenn Sie die Verbindung mit einem Server trennen, bleiben die ausgeführten Anwendungen geöffnet. Durch eine entsprechende Konfiguration können Sie festlegen, wie sich ausgeführte Anwendungen verhalten, wenn Sie mit dem Server erneut eine Verbindung herstellen.

Ein Horizon-Administrator kann die Einstellungen für das Wiederverbindungsverhalten von Anwendungen in Horizon Client von der Befehlszeile aus oder durch Einrichtung einer entsprechenden Gruppenrichtlinieneinstellung deaktivieren. Die Gruppenrichtlinieneinstellung hat Vorrang gegenüber der Befehlszeileneinstellung. Weitere Informationen finden Sie unter der Option `–appSessionReconnectionBehavior` in „Verwenden von Horizon Client-Befehlen“, auf Seite 67 oder unter der Gruppenrichtlinieneinstellung **Disconnected application session resumption behavior** (Wiederaufnahmeverhalten von getrennten Anwendungssitzungen) in „Einstellungen für die Skriptdefinition für Client-GPOs“, auf Seite 49.

Vorgehensweise

1 Klicken Sie mit der rechten Maustaste im Fenster für die Desktop- und Anwendungsauswahl von Horizon Client auf eine Remoteanwendung und wählen Sie **Einstellungen** aus.

2 Wählen Sie im eingeblendeten Bereich für Remoteanwendungen eine Einstellung für das Wiederverbindungsverhalten von Anwendungen aus.

Option	Beschreibung
Vor Neuverbindung zum Öffnen von Anwendungen fragen	Wenn Sie erneut eine Verbindung mit dem Server herstellen, werden Sie von Horizon Client darüber informiert, dass eine oder mehrere Remoteanwendungen ausgeführt werden. Durch Klicken auf **Mit Anwendungen neu verbinden** können Sie die Anwendungsfenster erneut öffnen. Durch Klicken auf **Nicht jetzt** werden die Anwendungsfenster nicht erneut geöffnet.
Neuverbindung zum Öffnen von Anwendungen automatisch herstellen	Anwendungsfenster für ausgeführte Anwendungen werden automatisch wieder geöffnet, wenn Sie erneut eine Verbindung mit dem Server herstellen.
Vor Neuverbindung nicht fragen und nicht automatisch neu verbinden	Horizon Client fordert Sie nicht dazu auf, ausgeführte Anwendungen wieder zu öffnen und ausgeführte Anwendungsfenster werden nicht wieder geöffnet, wenn Sie erneut eine Verbindung mit dem Server herstellen.

3 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Die Einstellung wird wirksam, wenn Sie das nächste Mal eine Verbindung mit dem Server herstellen.

Konfigurieren von VMware Horizon Client für Windows mithilfe der Gruppenrichtlinienvorlage

VMware Horizon Client enthält die ADM- und ADMX-Vorlagendateien für Gruppenrichtlinien, mit denen Sie VMware Horizon Client konfigurieren können. Sie können Remote-Desktop-Verbindungen optimieren und schützen, indem Sie die Richtlinieneinstellungen in dieser ADM- oder ADMX-Vorlagendatei zu einem neuen oder vorhandenen Gruppenrichtlinienobjekt (Group Policy Object, GPO) in Active Directory hinzufügen.

Die Vorlagendateien enthalten sowohl Gruppenrichtlinien für die Computerkonfiguration als auch Gruppenrichtlinien für die Benutzerkonfiguration.

- Richtlinien für die Computerkonfiguration gelten für Horizon Client, unabhängig davon, wer den Client auf dem Host ausführt.
- Mit Richtlinien für die Benutzerkonfiguration werden Horizon Client-Richtlinien festgelegt, die für alle Benutzer gelten, die Horizon Client ausführen, sowie RDP-Verbindungseinstellungen. Richtlinien für die Benutzerkonfiguration setzen gleichwertige Richtlinien für die Computerkonfiguration außer Kraft.

Horizon wendet Richtlinien beim Start eines Desktops und bei der Benutzeranmeldung an.

Die ADM- und ADMX-Vorlagendateien für die Horizon Client-Konfiguration (`vdm_client.adm` und `vdm_client.admx`) sowie alle ADM- und ADMX-Dateien, die Gruppenrichtlinieneinstellungen bereitstellen, sind in einer `.zip`-Datei namens `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` verfügbar, wobei *x.x.x* die Versions- und *yyyyyyy* die Build-Nummer darstellt. Sie können die Datei von der VMware Horizon-Download-Site unter http://www.vmware.com/go/downloadview herunterladen. Sie müssen diese Dateien auf Ihren Active Directory-Server kopieren und diese Verwaltungsvorlagen mithilfe des Gruppenrichtlinienverwaltungseditors hinzufügen. Die Anweisungen dazu finden Sie im *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*-Dokument.

Einstellungen für die Skriptdefinition für Client-GPOs

Sie können Richtlinien für viele der Einstellungen festlegen, die beim Ausführen von VMware Horizon Client über die Befehlszeile verwendet werden, wie beispielsweise die Desktop-Größe, den Namen oder den Domänennamen.

In der folgenden Tabelle werden die in den ADM- und ADMX-Vorlagendateien für die VMware Horizon Client-Konfiguration enthaltenen Einstellungen für die Skriptdefinition beschrieben. Die Vorlagendateien stellen für jede Skriptdefinition eine Version für die Computerkonfiguration und eine Version für die Benutzerkonfiguration bereit. Die Einstellung für die Benutzerkonfiguration setzt hierbei die äquivalente Einstellung für die Computerkonfiguration außer Kraft.

Tabelle 3-4. Konfigurationsvorlage für VMware Horizon Client : Skriptdefinitionen

Einstellung	Beschreibung
`Automatically connect if only one launch item is entitled`	Wird automatisch mit dem Desktop verbunden, wenn der Benutzer nur für diesen eine Berechtigung besitzt. Dem Benutzer wird dadurch die Auswahl des Desktops aus einer Liste mit nur einem Desktop erspart.
`Connect all USB devices to the desktop on launch`	Legt fest, ob alle der verfügbaren USB-Geräte auf dem Clientsystem mit dem Desktop verbunden werden, wenn dieser gestartet wird.
`Connect all USB devices to the desktop when they are plugged in`	Legt fest, ob USB-Geräte mit dem Desktop verbunden werden, wenn die Geräte an das Clientsystem angeschlossen werden.
`DesktopLayout`	Legt das Layout des VMware Horizon Client-Fensters fest, das einem Benutzer bei der Anmeldung an einem Remote-Desktop angezeigt wird. Es stehen folgende Optionen zur Auswahl: ■ `Full Screen` ■ `Multimonitor` ■ `Window – Large` ■ `Window – Small` Diese Einstellung ist nur verfügbar, wenn die Einstellung `DesktopName to select setting` ebenfalls gesetzt ist.
`DesktopName to select`	Legt den von VMware Horizon Client während der Anmeldung verwendeten Standard-Desktop fest.
`Disable 3rd-party Terminal Services plugins`	Legt fest, ob Terminaldienste-Plug-Ins von Drittanbietern, die als normale RDP-Plug-Ins installiert sind, von VMware Horizon Client überprüft werden. Wenn Sie diese Einstellung nicht konfigurieren, überprüft VMware Horizon Client standardmäßig Plug-Ins von Drittanbietern. Diese Einstellung hat keine Auswirkung auf Horizon-spezifische Plug-Ins, wie beispielsweise die USB-Umleitung.

Tabelle 3-4. Konfigurationsvorlage für VMware Horizon Client : Skriptdefinitionen (Fortsetzung)

Einstellung	Beschreibung
`Locked Guest Size`	Gibt die Bildschirmauflösung des Remote-Desktops an, wenn die Anzeige auf einem Bildschirm verwendet wird. Dies bedeutet, dass diese Einstellung nicht funktioniert, wenn Sie die Remote-Desktop-Anzeige auf „Alle Monitore“ festlegen. Nachdem Sie die Einstellung aktiviert haben, wird die Remote-Desktop-Funktion der automatischen Anpassung deaktiviert. Die Mindest-Bildschirmgröße ist 640 x 480. Die maximale Bildschirmgröße ist 4096 x 4096. Diese Einstellung gilt nur für PCoIP-Verbindungen und nicht für RDP-Verbindungen. **Wichtig** Legen Sie als Best Practice die Auflösung nicht höher als die in Horizon Administrator festgelegte Maximalauflösung fest, die für den Remote-Desktop unterstützt wird: ■ Wenn 3D aktiviert ist, werden bis zu zwei Monitore mit einer Auflösung von bis zu 1920 x 1200 unterstützt. ■ Wenn 3D nicht aktiviert ist, werden bis zu 4 Monitore mit einer Auflösung von bis zu 2560 x 1600 unterstützt. In der Praxis wird diese clientseitige Einstellung ignoriert, wenn sie auf eine höhere Auflösung festgelegt wird, als dies durch die vorhandene Betriebssystemversion, die Menge an vRAM und die Farbtiefe des Remote-Desktops möglich ist. Wenn beispielsweise in Horizon Administrator die Auflösung für den Desktop auf 1920 x 1200 festgelegt ist, ist die im Client verfügbare Auflösung je nach den Möglichkeiten des Remote-Desktops möglicherweise nicht höher als 1920 x 1200.
`Logon DomainName`	Legt die von Horizon Client während der Anmeldung verwendete NetBIOS-Domäne fest.
`Logon Password`	Legt das von Horizon Client während der Anmeldung verwendete Kennwort fest. Das Kennwort wird von Active Directory im Textformat gespeichert. Aus Sicherheitsgründen wird empfohlen, diese Einstellung nicht festzulegen. Benutzer können das Kennwort interaktiv eingeben.
`Logon UserName`	Legt das von Horizon Client während der Anmeldung verwendete Kennwort fest. Das Kennwort wird von Active Directory im Textformat gespeichert.
`Server URL`	Legt die von Horizon Client während der Anmeldung verwendete URL fest, z. B. `https://view1.beispiel.com`.
`Suppress error messages (when fully scripted only)`	Legt fest, ob Horizon Client Fehlermeldungen während der Anmeldung unterdrückt. Diese Einstellung ist nur anwendbar, wenn der Anmeldevorgang vollständig per Skript ausgeführt wird, z.B. wenn alle erforderlichen Anmeldeinformationen über eine Richtlinie vorausgefüllt werden. Wenn die Anmeldung aufgrund von falschen Anmeldeinformationen fehlschlägt, wird der Benutzer hierüber nicht benachrichtigt, und der Horizon Client-Prozess wird beendet.
`Disconnected application session resumption behavior`	Legt fest, wie ausgeführte Anwendungen sich verhalten, wenn Benutzer erneut eine Verbindung mit einem Server herstellen. Es stehen folgende Optionen zur Auswahl: ■ Vor Neuverbindung zum Öffnen von Anwendungen fragen ■ Neuverbindung zum Öffnen von Anwendungen automatisch herstellen ■ Nicht fragen und nicht automatisch erneut verbinden Wenn diese Einstellung aktiviert ist, können Endbenutzer das Wiederverbindungsverhalten von Anwendungen auf der Seite „Einstellungen“ in Horizon Client nicht konfigurieren. Wenn diese Einstellung deaktiviert ist, haben Endbenutzer die Möglichkeit, das Wiederverbindungsverhalten von Anwendungen in Horizon Client zu konfigurieren. Diese Einstellung ist standardmäßig deaktiviert.

Tabelle 3-4. Konfigurationsvorlage für VMware Horizon Client : Skriptdefinitionen (Fortsetzung)

Einstellung	Beschreibung
`Enable Unauthenticated Access to the server`	Legt fest, ob Benutzer Anmeldedaten für den Zugriff auf ihre Anwendungen eingeben müssen, wenn sie Horizon Client verwenden. Wenn diese Einstellung aktiviert ist, wird die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** in Horizon Client angezeigt, deaktiviert und ausgewählt. Wenn der nicht authentifizierte Zugriff nicht verfügbar ist, verwendet der Client eventuell eine andere Authentifizierungsmethode. Wenn diese Einstellung deaktiviert ist, müssen Benutzer immer ihre Anmeldedaten für die Anmeldung bei ihren Anwendungen und für den Zugriff darauf eingeben. Die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** in Horizon Client ist ausgeblendet und nicht ausgewählt. Wenn diese Einstellung nicht konfiguriert ist (Standardeinstellung), haben Benutzer die Möglichkeit, den nicht authentifizierten Zugriff in Horizon Client zu aktivieren. Die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** wird angezeigt, aktiviert und nicht ausgewählt.
`Account to use for Unauthenticated Access`	Legt das Benutzerkonto für einen nicht authentifizierten Zugriff fest, das Horizon Client für die anonyme Anmeldung beim Server verwendet, wenn die `Enable Unauthenticated Access to the server`-Gruppenrichtlinieneinstellung aktiviert ist oder wenn ein Benutzer den nicht authentifizierten Zugriff durch Auswahl von **Anonym mit nicht authentifiziertem Zugriff anmelden** in Horizon Client aktiviert. Wenn der nicht authentifizierte Zugriff nicht für eine bestimmte Verbindung mit einem Server verwendet wird, wird diese Einstellung ignoriert. Wenn diese Einstellung nicht konfiguriert ist, können Benutzer das Konto selbst auswählen. Diese Einstellung ist standardmäßig nicht konfiguriert.

Sicherheitseinstellungen für Client-GPOs

Zu den Sicherheitseinstellungen zählen Optionen für das Sicherheitszertifikat, für Anmeldeinformationen und für die Single Sign-On-Funktion (SSO).

In der folgenden Tabelle werden die in den ADM- und ADMX-Vorlagendateien für die Horizon Client-Konfiguration enthaltenen Sicherheitseinstellungen beschrieben. Diese Tabelle zeigt, ob die Konfiguration die Einstellungen „Computer Configuration (Computerkonfiguration)“ und „User Configuration (Benutzerkonfiguration)“ enthält oder nur die Einstellung „Computer Configuration (Computerkonfiguration)“. Bei den Sicherheitseinstellungen, die beide Typen einschließen, setzt die Einstellung für die Benutzerkonfiguration hierbei die äquivalente Einstellung für die Computerkonfiguration außer Kraft.

Tabelle 3-5. Horizon Client -Konfigurationsvorlage: Sicherheitseinstellungen

Einstellung	Beschreibung
`Allow command line credentials` (Einstellung für die Computerkonfiguration)	Legt fest, ob Benutzeranmeldedaten mit Horizon Client-Befehlszeilenoptionen bereitgestellt werden können. Wenn diese Einstellung deaktiviert ist, stehen die Optionen `smartCardPIN` und `password` nicht zur Verfügung, wenn Benutzer Horizon Client über die Befehlszeile ausführen. Diese Einstellung ist standardmäßig aktiviert. Der entsprechende Wert in der Windows-Registrierung lautet `AllowCmdLineCredentials`.
`Servers Trusted For Delegation` (Einstellung für die Computerkonfiguration)	Gibt die Verbindungsserver-Instanzen an, die die Benutzeridentitäts- und Anmeldedaten akzeptieren, die bei Aktivierung des Kontrollkästchens **Als aktueller Benutzer anmelden** übergeben werden. Wenn Sie keine Verbindungsserver-Instanzen angeben, akzeptieren alle Verbindungsserver-Instanzen diese Informationen. Verwenden Sie zum Hinzufügen einer Verbindungsserver-Instanz eines der folgenden Formate: ■ **`domain\system$`** ■ **`system$@domain.com`** ■ Service Principal Name (SPN) des Verbindungsserver-Dienstes Der entsprechende Wert in der Windows-Registrierung lautet `BrokersTrustedForDelegation`.

Tabelle 3-5. Horizon Client -Konfigurationsvorlage: Sicherheitseinstellungen (Fortsetzung)

Einstellung	Beschreibung
`Certificate verification mode` (Einstellung für die Computerkonfiguration)	Konfiguriert die Ebene der Zertifikatsprüfung, die durch Horizon Client durchgeführt wird. Es stehen folgende Modi zur Auswahl: ■ `No Security`. Horizon führt keine Zertifikatsprüfung durch. ■ `Warn But Allow`. Von Horizon wird ein selbstsigniertes Zertifikat bereitgestellt. In diesem Fall ist es akzeptabel, wenn der Zertifikatname nicht mit dem Namen des Verbindungsservers übereinstimmt, der in Horizon Client vom Benutzer angegeben wurde. Wenn andere Zertifikatfehlerbedingungen vorliegen, zeigt Horizon ein Fehlerdialogfeld an und verhindert, dass der Benutzer eine Verbindung mit dem Verbindungsserver herstellt. `Warn But Allow` ist der Standardwert. ■ `Full Security`. Wenn ein beliebiger Zertifikatfehler auftritt, kann der Benutzer keine Verbindung mit dem Verbindungsserver herstellen. Horizon zeigt dem Benutzer die Zertifikatfehler an. Wenn diese Gruppenrichtlinieneinstellung konfiguriert ist, können die Benutzer den ausgewählten Modus für die Zertifikatsprüfung in Horizon Client sehen, ihn aber nicht konfigurieren. Das Dialogfeld für die SSL-Konfiguration informiert die Benutzer darüber, dass der Administrator die Einstellung gesperrt hat. Wenn diese Einstellung nicht konfiguriert oder deaktiviert wurde, können Horizon Client-Benutzer einen Zertifikatsprüfungsmodus auswählen. Damit ein Server die von Horizon Client bereitgestellten Zertifikate prüfen kann, muss der Client HTTPS-Verbindungen zum Verbindungsserver- oder Sicherheitsserver-Host herstellen. Die Zertifikatsprüfung wird nicht unterstützt, wenn Sie SSL auf ein Zwischengerät verlagern, das HTTP-Verbindungen zum Verbindungsserver- oder Sicherheitsserver-Host herstellt. Wenn Sie diese Einstellung nicht als Gruppenrichtlinie konfigurieren möchten, können Sie die Zertifikatsprüfung auch durch Hinzufügen des Wertnamens `CertCheckMode` zu einem der folgenden Registrierungsschlüssel auf dem Clientcomputer aktivieren: ■ Für 32-Bit-Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security` ■ Für 64-Bit-Windows: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security` Verwenden Sie die folgenden Werte im Registrierungsschlüssel: ■ **`0`** implementiert `No Security`. ■ **`1`** implementiert `Warn But Allow`. ■ **`2`** implementiert `Full Security`. Wenn Sie sowohl die Gruppenrichtlinieneinstellung als auch die Einstellung `CertCheckMode` im Windows-Registrierungsschlüssel konfigurieren, hat die Gruppenrichtlinieneinstellung Vorrang vor dem Registrierungsschlüsselwert. **Hinweis** In einer künftigen Version wird die mithilfe der Windows-Registrierung vorgenommene Konfiguration dieser Einstellung möglicherweise nicht unterstützt. Es muss eine GPO-Einstellung verwendet werden.

Tabelle 3-5. Horizon Client -Konfigurationsvorlage: Sicherheitseinstellungen (Fortsetzung)

Einstellung	Beschreibung
`Default value of the 'Log in as current user' checkbox` (Einstellung für die Computer- und Benutzerkonfiguration)	Gibt den Standardwert des Kontrollkästchens **Als aktueller Benutzer anmelden** im Dialogfeld für die Horizon Client-Verbindung an. Diese Einstellung setzt den Standardwert außer Kraft, der während der Horizon Client-Installation angegeben wurde. Wenn ein Benutzer Horizon Client über die Befehlszeile ausführt und die Option `logInAsCurrentUser` angibt, wird diese Einstellung durch den eingegebenen Wert überschrieben. Wenn das Kontrollkästchen **Als aktueller Benutzer anmelden** aktiviert ist, werden die Identität und die Anmeldedaten des Benutzers, die dieser zur Anmeldung am Clientsystem verwendet, an die Verbindungsserver-Instanz und schließlich an den Remote-Desktop übergeben. Ist das Kontrollkästchen deaktiviert, müssen Benutzer Identitäts- und Anmeldeinformationen mehrere Male eingeben, bevor sie auf einen Remote-Desktop zugreifen können. Diese Einstellung ist standardmäßig deaktiviert. Der entsprechende Wert in der Windows-Registrierung lautet `LogInAsCurrentUser`.
`Display option to Log in as current user` (Einstellung für die Computer- und Benutzerkonfiguration)	Legt fest, ob das Kontrollkästchen **Als aktueller Benutzer anmelden** im Dialogfeld für die Horizon Client-Verbindung angezeigt wird. Bei Anzeige des Kontrollkästchens können Benutzer die Option aktivieren oder deaktivieren oder den zugehörigen Standardwert außer Kraft setzen. Wird das Kontrollkästchen ausgeblendet, können Benutzer den Standardwert im Dialogfeld für die Horizon Client-Verbindung nicht ändern. Sie können den Standardwert für **Als aktueller Benutzer anmelden** über die Richtlinieneinstellung `Default value of the 'Log in as current user' checkbox` festlegen. Diese Einstellung ist standardmäßig aktiviert. Der entsprechende Wert in der Windows-Registrierung lautet `LogInAsCurrentUser_Display`.
`Enable jump list integration` (Einstellung für die Computerkonfiguration)	Legt fest, ob eine Sprungliste im Horizon Client icon on the taskbar of Windows 7 and later systems. Über die Sprungliste können Benutzer eine Verbindung zu zuletzt verwendeten Verbindungsserver-Instanzen und Remote-Desktops herstellen. Wenn Horizon Client gemeinsam verwendet wird, sollen Benutzer möglicherweise nicht die Namen der zuletzt verwendeten Desktops sehen. Die Sprungliste können Sie deaktivieren, indem Sie diese Einstellung deaktivieren. Diese Einstellung ist standardmäßig aktiviert. Der entsprechende Wert in der Windows-Registrierung lautet `EnableJumplist`.
`Enable SSL encrypted framework channel` (Einstellung für die Computer- und Benutzerkonfiguration)	Legt fest, ob SSL für View 5.0 und ältere Desktops aktiviert wird. Vor View 5.0 wurden die über den Port TCP 32111 an den Desktop gesendeten Daten nicht verschlüsselt. ■ **Aktivieren**: Aktiviert SSL, aber ermöglicht das Zurücksetzen auf die vorherige unverschlüsselte Verbindung, falls der Remote-Desktop SSL nicht unterstützt. Beispielsweise wird SSL von View 5.0 und älteren Desktops nicht unterstützt. **Enable** ist die Standardeinstellung. ■ **Deaktivieren**: Deaktiviert SSL. Diese Einstellung wird nicht empfohlen. Sie kann aber hilfreich sein für das Debugging oder wenn der Kanal nicht getunnelt wird und deshalb möglicherweise durch ein Produkt zur WAN-Beschleunigung optimiert werden könnte. ■ **Erzwingen**: Aktiviert SSL und verweigert das Herstellen einer Verbindung zu Desktops ohne SSL-Unterstützung. Der entsprechende Wert in der Windows-Registrierung lautet `EnableTicketSSLAuth`.

Tabelle 3-5. Horizon Client -Konfigurationsvorlage: Sicherheitseinstellungen (Fortsetzung)

Einstellung	Beschreibung
`Configures SSL protocols and cryptographic algorithms` (Einstellung für die Computer- und Benutzerkonfiguration)	Konfiguriert die Verschlüsselungsliste, um die Verwendung bestimmter kryptografischer Algorithmen und Protokolle zu beschränken, bevor Sie eine verschlüsselte SSL-Verbindung herstellen. Die Verschlüsselungsliste besteht aus einer oder mehreren Verschlüsselungszeichenfolgen, die durch Doppelpunkte voneinander getrennt werden. **Hinweis** Bei der Schlüsselzeichenfolge wird die Groß-/Kleinschreibung beachtet. Der Standardwert ist **TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES**. Demnach werden TLS v1, TLS v1.1 und TLS v1.2 aktiviert. (SSL v2.0 und v3.0 wurden entfernt.) Verschlüsselungssammlungen verwenden 128- oder 256-Bit-AES, entfernen anonyme DH-Algorithmen und sortieren anschließend die aktuelle Verschlüsselungsliste nach der Schlüssellänge des Verschlüsselungsalgorithmus. Referenz-Link für die Konfiguration: http://www.openssl.org/docs/apps/ciphers.html Der entsprechende Wert in der Windows-Registrierung lautet `SSLCipherList`.
`Enable Single Sign-On for smart card authentication` (Einstellung für die Computerkonfiguration)	Legt fest, ob für die Smartcard-Authentifizierung das Single Sign-On (SSO) aktiviert ist. Ist ein Single Sign-On aktiviert, speichert Horizon Client die verschlüsselte Smartcard-PIN im temporären Arbeitsspeicher, bevor sie an den Verbindungsserver gesendet wird. Ist SSO deaktiviert, zeigt Horizon Client kein benutzerdefiniertes PIN-Dialogfeld an. Der entsprechende Wert in der Windows-Registrierung lautet `EnableSmartCardSSO`.
`Ignore bad SSL certificate date received from the server` (Einstellung für die Computerkonfiguration)	(Nur View 4.6 und frühere Versionen) Legt fest, ob Fehler in Zusammenhang mit ungültigen Datumswerten für das Serverzertifikat ignoriert werden. Diese Fehler treten auf, wenn ein Server ein abgelaufenes Zertifikat sendet. Der entsprechende Wert in der Windows-Registrierung lautet `IgnoreCertDateInvalid`.
`Ignore certificate revocation problems` (Einstellung für die Computerkonfiguration)	(Nur View 4.6 und frühere Versionen) Legt fest, ob Fehler in Zusammenhang mit einem gesperrten Serverzertifikat ignoriert werden. Diese Fehler treten auf, wenn der Server ein Zertifikat sendet, das gesperrt wurde, und der Client den Sperrstatus eines Zertifikats nicht überprüfen kann. Diese Einstellung ist standardmäßig deaktiviert. Der entsprechende Wert in der Windows-Registrierung lautet `IgnoreRevocation`.
`Ignore incorrect SSL certificate common name (host name field)` (Einstellung für die Computerkonfiguration)	(Nur View 4.6 und frühere Versionen) Legt fest, ob Fehler in Zusammenhang mit falschen allgemeinen Namen im Serverzertifikat ignoriert werden. Diese Fehler treten auf, wenn der allgemeine Name des Zertifikats nicht mit dem Hostnamen des Servers übereinstimmt, der das Zertifikat sendet. Der entsprechende Wert in der Windows-Registrierung lautet `IgnoreCertCnInvalid`.

Tabelle 3-5. Horizon Client -Konfigurationsvorlage: Sicherheitseinstellungen (Fortsetzung)

Einstellung	Beschreibung
`Ignore incorrect usage problems` (Einstellung für die Computerkonfiguration)	(Nur View 4.6 und frühere Versionen) Legt fest, ob Fehler in Zusammenhang mit einer falschen Verwendung des Serverzertifikats ignoriert werden. Diese Fehler treten auf, wenn das vom Server gesendete Zertifikat für einen anderen Zweck als die Überprüfung der Absenderidentität und zum Verschlüsseln der Serverkommunikation gedacht ist. Der entsprechende Wert in der Windows-Registrierung lautet `IgnoreWrongUsage`.
`Ignore unknown certificate authority problems` (Einstellung für die Computerkonfiguration)	(Nur View 4.6 und frühere Versionen) Legt fest, ob bestimmte Fehler in Zusammenhang mit einer unbekannten Zertifizierungsstelle im Serverzertifikat ignoriert werden. Diese Fehler treten auf, wenn das vom Server gesendete Zertifikat durch eine nicht vertrauenswürdige Drittanbieter-Zertifizierungsstelle signiert wurde. Der entsprechende Wert in der Windows-Registrierung lautet `IgnoreUnknownCa`.

RDP-Einstellungen für Client-GPOs

Sie können Gruppenrichtlinien für Optionen wie die Umleitung von Audio, Druckern, Ports und anderen Geräten festlegen, wenn Sie das Microsoft RDP-Anzeigeprotokoll verwenden.

In der folgenden Tabelle werden die in den ADM- und ADMX-Vorlagendateien für die Horizon Client-Konfiguration enthaltenen RDP-Einstellungen (Remote Desktop Protocol) beschrieben. Alle RDP-Einstellungen sind Einstellungen für die Benutzerkonfiguration.

Tabelle 3-6. ADM-Vorlage für Horizon Client -Konfiguration: RDP-Einstellungen

Einstellung	Beschreibung
`Audio redirection`	Legt fest, ob auf dem Remote-Desktop wiedergegebene Audioinformationen umgeleitet werden. Es stehen folgende Einstellungen zur Auswahl: ■ **Audio deaktivieren**: Audio ist deaktiviert. ■ **In VM wiedergeben (erforderlich für VoIP USB-Unterstützung)**: Audiodaten werden im Remote-Desktop wiedergegeben. Diese Einstellung erfordert ein gemeinsam genutztes USB-Audiogerät zur Wiedergabe von Sound auf dem Client. ■ **An Client umleiten**: Audiodaten werden an den Client umgeleitet. Dies ist der Standardmodus. Diese Eigenschaft gilt nur für RDP-Audio. Über MMR umgeleitete Audiodaten werden im Client wiedergegeben.
`Enable audio capture redirection`	Legt fest, ob das standardmäßige Audioeingabegerät vom Client an die Remote-Sitzung umgeleitet wird. Wenn diese Einstellung aktiviert ist, wird das Audioaufzeichnungsgerät des Clients im Remote-Desktop angezeigt und kann zur Aufzeichnung von Audioeingabedaten verwendet werden. Diese Einstellung ist standardmäßig deaktiviert.
`Bitmap cache file size in` *unit* `for` *number* `bpp bitmaps`	Gibt die Größe des Bitmapcaches (in KB oder MB) für die Zwischenspeicherung von Bitmaps mit einer bestimmten Farbeinstellung (Bits pro Pixel, bpp) an. Für die verschiedenen Kombinationen aus Einheit und Bits pro Pixel stehen unterschiedliche Versionen zur Verfügung: ■ KB/8bpp ■ MB/8bpp ■ MB/16bpp ■ MB/24bpp ■ MB/32bpp
`Bitmap caching/cache persistence active`	Legt fest, ob für Bitmaps eine dauerhafte Zwischenspeicherung durchgeführt wird (aktiv ist). Eine dauerhafte Zwischenspeicherung für Bitmaps kann die Leistung verbessern, erfordert jedoch zusätzlichen Speicherplatz.

Tabelle 3-6. ADM-Vorlage für Horizon Client -Konfiguration: RDP-Einstellungen (Fortsetzung)

Einstellung	Beschreibung
`Color depth`	Legt die Farbtiefe für den Remote-Desktop fest. Es stehen folgende Einstellungen zur Auswahl: ■ 8 Bit ■ 15 Bit ■ 16 Bit ■ 24 Bit ■ 32 Bit Für Windows XP-Systeme mit 24 Bit müssen Sie die Richtlinie „Maximale Farbtiefe einschränken“ unter **Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Terminaldienste** aktivieren und sie auf 24 Bit einstellen.
`Cursor shadow`	Legt fest, ob auf dem Remote-Desktop unter dem Cursor ein Schatten angezeigt wird.
`Desktop background`	Legt fest, ob der Desktop-Hintergrund angezeigt wird, wenn Clients eine Verbindung zu einem Remote-Desktop herstellen.
`Desktop composition`	(Windows Vista oder höher) Legt fest, ob die Desktop-Gestaltung auf dem Remote-Desktop aktiviert ist. Wenn die Desktop-Gestaltung aktiviert ist, werden einzelne Fenster nicht länger direkt auf dem Bildschirm oder dem primären Anzeigegerät dargestellt, wie dies in früheren Versionen von Microsoft Windows der Fall war. Stattdessen werden die Bilddaten zunächst in den nicht sichtbaren Offscreen-Bereich des Videospeichers umgeleitet und anschließend zur Darstellung auf dem Anzeigegerät in ein Desktop-Bild gerendert.
`Enable compression`	Legt fest, ob RDP-Daten komprimiert werden. Diese Einstellung ist standardmäßig aktiviert.
`Enable RDP Auto-Reconnect`	Legt fest, ob die RDP-Clientkomponente versucht, erneut eine Verbindung mit einem Remote-Desktop herzustellen, nachdem ein RDP-Verbindungsfehler aufgetreten ist. Diese Einstellung hat keine Auswirkung, wenn die Option **Sichere Tunnelverbindung zum Desktop verwenden** in Horizon Administrator aktiviert wurde. Diese Einstellung ist standardmäßig deaktiviert.
`Font smoothing`	(Windows Vista oder höher) Legt fest, ob Anti-Aliasing auf die Schriftarten auf dem Remote-Desktop angewendet wird.
`Menu and window animation`	Legt fest, ob die Animation für Menüs und Fenster aktiviert ist, wenn Clients eine Verbindung zu einem Remote-Desktop herstellen.
`Redirect clipboard`	Legt fest, ob die Informationen in der lokalen Zwischenablage umgeleitet werden, wenn Clients eine Verbindung zum Remote-Desktop herstellen.
`Redirect drives`	Legt fest, ob lokale Festplattenlaufwerke umgeleitet werden, wenn Clients eine Verbindung zum Remote-Desktop herstellen. Lokale Laufwerke werden standardmäßig umgeleitet. Durch Aktivieren oder Nichtkonfigurieren dieser Einstellung können Daten auf dem umgeleiteten Laufwerk des Remote-Desktops auf das Laufwerk des Clientcomputers kopiert werden. Deaktivieren Sie diese Einstellung, wenn das Übertragen von Daten vom Remote-Desktop zu den Clientcomputern des Benutzers ein mögliches Sicherheitsrisiko für Ihre Bereitstellung darstellt. Alternativ können Sie auch die Ordnerumleitung in der virtuellen Maschine des Remote-Desktops deaktivieren, indem Sie die Microsoft Windows-Gruppenrichtlinieneinstellung `Do not allow drive redirection` aktivieren. Die Einstellung `Redirect drives` wirkt sich nur auf RDP aus.
`Redirect printers`	Legt fest, ob lokale Drucker umgeleitet werden, wenn Clients eine Verbindung zum Remote-Desktop herstellen.
`Redirect serial ports`	Legt fest, ob lokale COM-Ports umgeleitet werden, wenn Clients eine Verbindung zum Remote-Desktop herstellen.

Tabelle 3-6. ADM-Vorlage für Horizon Client -Konfiguration: RDP-Einstellungen (Fortsetzung)

Einstellung	Beschreibung
`Redirect smart cards`	Legt fest, ob lokale Smartcards umgeleitet werden, wenn Clients eine Verbindung zum Remote-Desktop herstellen. **Hinweis** Diese Einstellung gilt sowohl für RDP- als auch für PCoIP-Verbindungen.
`Redirect supported plug-and-play devices`	Legt fest, ob lokale Plug & Play- sowie POS-Geräte (Point of Sale) umgeleitet werden, wenn Clients eine Verbindung zum Remote-Desktop herstellen. Dieses Verhalten unterscheidet sich dahingehend von der Umleitung, dass es durch die Agent-Komponente für die USB-Umleitung verwaltet wird.
`Shadow bitmaps`	Legt fest, ob Schattenbitmaps verwendet werden. Diese Einstellung hat im Vollbildmodus keine Auswirkung.
`Show contents of window while dragging`	Legt fest, ob Ordnerinhalte angezeigt werden, wenn der Benutzer einen Ordner an einen neuen Speicherort zieht.
`Themes`	Legt fest, ob Designs angezeigt werden, wenn Clients eine Verbindung zu einem Remote-Desktop herstellen.
`Windows key combination redirection`	Legt fest, wo Windows-Tastenkombinationen angewendet werden. Mit dieser Einstellung können Sie Tastenkombinationen an die virtuelle Remote-Maschine senden oder lokal Tastenkombinationen anwenden. Wenn diese Einstellung nicht konfiguriert ist, werden Tastenkombinationen lokal angewandt.

Allgemeine Einstellungen für Client-GPOs

Zu den Einstellungen zählen Proxy-Optionen, Zeitzonenweiterleitung, Multimediabeschleunigung und sonstige Anzeigeeinstellungen.

Allgemeine Einstellungen

In der folgenden Tabelle werden die in den ADM- und ADMX-Vorlagendateien für die Horizon Client-Konfiguration enthaltenen allgemeinen Einstellungen beschrieben. Zu den allgemeinen Einstellungen gehören sowohl Einstellungen für die Computerkonfiguration als auch Einstellungen für die Benutzerkonfiguration. Die Einstellung für die Benutzerkonfiguration setzt hierbei die äquivalente Einstellung für die Computerkonfiguration außer Kraft.

Tabelle 3-7. Horizon Client -Konfigurationsvorlage: Allgemeine Einstellungen

Einstellung	Beschreibung
`Always on top` (Einstellung für die Benutzerkonfiguration)	Legt fest, ob das Horizon Client-Fenster immer im Vordergrund angezeigt wird. Durch Aktivierung dieser Einstellung wird verhindert, dass die Windows-Taskleiste ein Horizon Client-Fenster im Vollbildmodus überlappt. Diese Einstellung ist standardmäßig deaktiviert.
`Default value of the "Hide the selector after launching an item" check box` (Einstellung für die Computer- und Benutzerkonfiguration)	Legt fest, ob das Kontrollkästchen **Selektor nach Start eines Elements ausblenden** standardmäßig ausgewählt ist. Diese Einstellung ist standardmäßig deaktiviert.

Tabelle 3-7. Horizon Client -Konfigurationsvorlage: Allgemeine Einstellungen (Fortsetzung)

Einstellung	Beschreibung
`Determines if the VMware View Client should use proxy.pac file` (Einstellung für die Computerkonfiguration)	(Nur View 4.6 und frühere Versionen) Legt fest, ob Horizon Client eine PAC-Datei (Proxy Automatic Configuration) verwendet. Wenn diese Einstellung aktiviert ist, verwendet Horizon Client eine PAC-Datei. Eine PAC-Datei (häufig als `proxy.pac` bezeichnet) hilft Webbrowsern und anderen Agenten, den geeigneten Proxy-Server für eine bestimmte URL oder Website-Anforderung zu finden. Wenn Sie diese Einstellung auf einer Maschine mit mehreren Kernen aktivieren, stürzt möglicherweise die WinINet-Anwendung ab, die Horizon Client für die Suche nach Proxy-Server-Informationen verwendet. Deaktivieren Sie diese Einstellung, wenn dieses Problem auf Ihrer Maschine auftritt. Diese Einstellung ist standardmäßig deaktiviert. **Hinweis** Diese Einstellung gilt nur für direkte Verbindungen. Auf Tunnelverbindungen hat die Einstellung keine Auswirkung.
`Disable time zone forwarding` (Einstellung für die Computerkonfiguration)	Legt fest, ob die Zeitzonensynchronisierung des Remote-Desktops mit der des verbundenen Clients deaktiviert ist.
`Disable toast notifications` (Einstellung für die Computer- und Benutzerkonfiguration)	Hierdurch wird festgelegt, ob Toastnachrichten von Horizon Client deaktiviert werden sollen. Aktivieren Sie diese Einstellung, wenn Sie nicht möchten, dass dem Benutzer Toastnachrichten in der Ecke des Bildschirms angezeigt werden. **Hinweis** Wenn Sie diese Einstellung aktivieren, wird dem Benutzer bei Aktivierung der Funktion „Sitzungszeitüberschreitung“ keine 5-Minuten-Warnung eingeblendet.
`Disallow passing through client information in a nested session` (Einstellung für die Computerkonfiguration)	Gibt an, ob verhindert werden sollte, dass Horizon Client durch Clientinformationen in einer verschachtelten Sitzung weitergegeben wird. Wenn aktiviert, sofern Horizon Client in einer Horizon-Sitzung ausgeführt wird, werden die tatsächlichen Informationen zum physischen Client anstelle der VM-Geräteinformationen gesendet. Diese Einstellung gilt für die folgenden Clientinformationen: Gerätename und Domäne, Clienttyp, IP-Adresse und MAC-Adresse. Diese Einstellung ist standardmäßig deaktiviert. Demnach ist das Weitergeben von Clientinformationen in einer verschachtelten Sitzung zulässig.
`Don't check monitor alignment on spanning` (Einstellung für die Benutzerkonfiguration)	Standardmäßig wird der Client-Desktop nicht in den Mehrfachmonitor-Modus geschaltet, wenn die Bildschirme in Kombination kein exaktes Rechteck bilden (d.h. identische Höhe bei horizontaler Anordnung oder identische Breite bei vertikaler Anordnung). Aktivieren Sie diese Einstellung, um den Standardwert außer Kraft zu setzen. Diese Einstellung ist standardmäßig deaktiviert.
`Enable multi-media acceleration` (Einstellung für die Benutzerkonfiguration)	Legt fest, ob die Multimedia-Umleitung (Multimedia Redirection, MMR) auf dem Client aktiviert ist. MMR funktioniert nicht ordnungsgemäß, wenn die Horizon Client-Hardware zur Videoanzeige keine Overlay-Unterstützung bietet.
`Enable relative mouse` (Einstellung für die Computer- und Benutzerkonfiguration)	(Nur View 5.2 und höhere Versionen) Aktiviert die relative Maus bei Verwendung des PCoIP-Anzeigeprotokolls. Der Modus für relative Maus optimiert das Mausverhalten für bestimmte Grafikanwendungen und Spiele. Falls der Modus für relative Maus nicht vom Remote-Desktop unterstützt wird, wird diese Einstellung nicht verwendet. Diese Einstellung ist standardmäßig deaktiviert.
`Enable the shade` (Einstellung für die Benutzerkonfiguration)	Legt fest, ob die Schatten-Menüleiste im oberen Bereich des Horizon Client-Fensters sichtbar ist. Diese Einstellung ist standardmäßig aktiviert. **Hinweis** Die Schatten-Menüleiste im oberen Bereich ist für den Kiosk-Modus standardmäßig deaktiviert.
`Enable Horizon Client online update` (Einstellung für die Computerkonfiguration)	Aktiviert die Onlineaktualisierungsfunktion. Diese Einstellung ist standardmäßig deaktiviert.

Tabelle 3-7. Horizon Client -Konfigurationsvorlage: Allgemeine Einstellungen (Fortsetzung)

Einstellung	Beschreibung
`Tunnel proxy bypass address list` (Einstellung für die Computerkonfiguration)	Gibt eine Liste von Tunneladressen an. Der Proxy-Server wird für diese Adressen nicht verwendet. Verwenden Sie ein Semikolon (;) zum Trennen mehrerer Einträge.
`URL for View Client online help` (Einstellung für die Computerkonfiguration)	Gibt eine alternative URL an, von der Horizon Client Hilfeseiten abrufen kann. Diese Einstellung ist zur Verwendung in Umgebungen gedacht, die das remote verwaltete Hilfesystem nicht abrufen können, da kein Internetzugriff verfügbar ist.
`URL for Horizon Client online update` (Einstellung für die Computerkonfiguration)	Gibt eine alternative URL an, von der Horizon Client Aktualisierungen abrufen kann. Diese Einstellung soll in einer Umgebung verwendet werden, die ihr eigenes privates/persönliches Aktualisierungszentrum aufweist. Wenn sie nicht aktiviert ist, wird der offizielle VMware-Aktualisierungsserver verwendet.
`Pin the shade` (Einstellung für die Benutzerkonfiguration)	Legt fest, ob die Fixierung der Menüleiste im oberen Bereich des Horizon Client-Fensters aktiviert ist, sodass die Menüleiste nicht automatisch ausgeblendet wird. Diese Einstellung hat keine Auswirkung, wenn die Menüleiste deaktiviert wurde. Diese Einstellung ist standardmäßig aktiviert.
`Disable desktop disconnect messages` (Einstellung für die Computer- und Benutzerkonfiguration)	Legt fest, ob Meldungen, die normalerweise beim Trennen von Desktops angezeigt werden, deaktiviert werden sollen. Diese Meldungen werden standardmäßig angezeigt.
`Disable sharing files and folders` (Einstellung für die Benutzerkonfiguration)	Legt fest, ob die Funktionalität der Clientlaufwerksumleitung in Horizon Client verfügbar ist. Wenn für diese Einstellung „Aktiviert“ ausgewählt ist, wird die gesamte Funktionalität der Clientlaufwerksumleitung in Horizon Client deaktiviert, inklusive der Möglichkeit, lokale Dateien mit Remotenanwendungen zu öffnen. Darüber hinaus werden die folgenden Elemente in der Benutzeroberfläche von Horizon Client ausgeblendet: ■ Freigabebereich im Dialogfeld „Einstellungen“ ■ Option **Ordner freigeben** im Menü **Option** eines Remote-Desktops ■ Option **Freigabe** für Horizon Client in der Taskleiste ■ Das Dialogfeld „Freigabe“, das angezeigt wird, wenn Sie das erste Mal eine Verbindung mit einem Remote-Desktop oder einer Remoteanwendung herstellen, nachdem Sie sich mit einem Server verbunden haben Wenn für diese Einstellung „Deaktiviert“ festgelegt ist, ist die Funktion der Clientlaufwerksumleitung komplett verwendbar. Wenn Sie diese Einstellung nicht konfigurieren, ist als Standardeinstellung „Deaktiviert“ ausgewählt. Diese Einstellung ist standardmäßig nicht konfiguriert.
`Always hide the remote floating language (IME) bar for Hosted Apps` (Einstellung für die Computer- und Benutzerkonfiguration)	Schaltet die flexibel platzierbare Sprachleiste für Anwendungssitzungen aus. Wenn diese Einstellung aktiviert ist, wird die flexibel platzierbare Sprachleiste in Sitzungen von Remoteanwendungen nicht angezeigt, unabhängig von der Aktivierung der lokalen IME-Funktion. Wenn diese Einstellung deaktiviert ist, wird die flexibel platzierbare Sprachleiste nur angezeigt, wenn die lokale IME-Funktion deaktiviert ist. Diese Einstellung ist standardmäßig deaktiviert.

Tabelle 3-7. Horizon Client -Konfigurationsvorlage: Allgemeine Einstellungen (Fortsetzung)

Einstellung	Beschreibung
`Put icon cache in user's Local profile folder` (Einstellung für die Computerkonfiguration)	Legt fest, ob Horizon Client seine Symbol-Cache-Dateien im Ordner `Local` des Benutzers statt im zuvor verwendeten Ordner `Roaming` ablegt. Wenn diese Einstellung aktiviert ist, platziert Horizon Client seine Symbol-Cache-Dateien im Ordner `Local` des Benutzers. Beim ersten Start von Horizon Client werden dann alle vorhandenen Cache-Dateien aus dem Ordner `Roaming` in den Ordner `Local` übertragen und neue Cache-Dateien im Ordner `Local` abgelegt. Durch Aktivierung dieser Richtlinie lässt sich die Antwortzeit von Remoteanwendungen verkürzen, wenn Roaming-Profile durch Vermeidung der Synchronisierung von Cache-Dateien verwendet werden. Wenn Sie diese Einstellung nicht konfigurieren, ist als Standardeinstellung „Deaktiviert“ ausgewählt. Diese Einstellung ist standardmäßig nicht konfiguriert.
`Allow opening local files in hosted applications` (Einstellung für die Benutzerkonfiguration)	Legt fest, ob Horizon Client lokale Handler für Dateierweiterungen registriert, die von gehosteten Anwendungen unterstützt werden. Wenn diese Einstellung deaktiviert ist, registriert Horizon Client keine Handler für Dateierweiterungen. Benutzer können diese Einstellung dann nicht überschreiben. Ist diese Einstellung aktiviert, werden Handler für Dateierweiterungen immer von Horizon Client registriert. Handler für Dateierweiterungen werden standardmäßig registriert. Benutzer haben aber die Möglichkeit, die Funktion in der Benutzeroberfläche von Horizon Client mit der Einstellung **Turn on the ability to open a local file with a remote application from the local file system** (Aktivieren der Möglichkeit, eine lokale Datei mit einer Remoteanwendung aus dem lokalen Dateisystem zu öffnen) im Bereich „Freigabe“ des Dialogfeldes „Einstellungen“ zu deaktivieren. Weitere Informationen finden Sie unter „Freigegebener Zugriff auf lokale Ordner und Laufwerke“, auf Seite 81. Wenn Sie diese Einstellung nicht konfigurieren, ist als Standardeinstellung „Aktiviert“ ausgewählt. Diese Einstellung ist standardmäßig nicht konfiguriert.

USB-Einstellungen für Client-GPOs

Sie können USB-Richtlinieneinstellungen sowohl für den Agent als auch für Horizon Client für Windows definieren. Nach dem Herstellen der Verbindung lädt Horizon Client die USB-Richtlinieneinstellungen des Agent herunter und verwendet diese zusammen mit den Horizon Client-USB-Richtlinieneinstellungen, um zu entscheiden, welche Geräte vom Hostcomputer umgeleitet werden dürfen.

In der folgenden Tabelle werden die Richtlinieneinstellungen zum Splitten von USB-Verbundgeräten in den ADM- und ADMX-Vorlagendateien für die Horizon Client-Konfiguration beschrieben. Die Einstellungen gelten auf Computerebene. Horizon Client liest die Einstellungen vorzugsweise aus dem GPO auf der Computerebene, andernfalls aus der Registrierung unter `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB`. Eine Beschreibung, wie Horizon die Richtlinien zum Splitten von USB-Verbundgeräten anwendet, finden Sie in den Themen zur Verwendung von Richtlinien für die Steuerung der USB-Umleitung im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Tabelle 3-8. Konfigurationsvorlage für Horizon Client : Einstellungen für die USB-Aufteilung

Einstellung	Eigenschaften
`Allow Auto Device Splitting`	Lässt das automatische Splitten von Composite USB-Geräten zu. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
`Exclude Vid/Pid Device From Split`	Schließt ein Composite USB-Gerät vom Splitten aus, das durch Anbieter- und Produkt-IDs angegeben ist. Das Format der Einstellung lautet `vid-`*xxx1*`_pid-`*yyy2*`[;vid-`*xxx2*`_pid-`*yyy2*`]...` Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (**`*`**) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: **`vid-0781_pid-55**`** Der Standardwert ist nicht definiert.
`Split Vid/Pid Device`	Behandelt die Komponenten eines Composite USB-Gerätes, die durch Anbieter- und Produkt-IDs angegeben sind, als separate Geräte. Das Format der Einstellung ist `vid-`*xxxx*`_pid-`*yyyy*`(exintf:`*zz*`[;exintf:`*ww*` ])` Sie können das Stichwort `exintf` verwenden, um Komponenten durch Angabe ihrer Schnittstellennummer von der Umleitung auszuschließen. Sie müssen hexadezimale ID-Nummern und dezimale Schnittstellennummern einschließlich der 0 am Anfang angeben. Sie können das Platzhalterzeichen (**`*`**) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: **`vid-0781_pid-554c(exintf:01;exintf:02)`** **Hinweis** Horizon schließt nicht automatisch die Komponenten ein, die Sie nicht explizit ausgeschlossen haben. Sie müssen eine Filterrichtlinie wie z. B. `Include Vid/Pid Device` angeben, um diese Komponenten einzuschließen. Der Standardwert ist nicht definiert.

In der folgenden Tabelle werden die Richtlinieneinstellungen zum Filtern von USB-Verbundgeräten in den ADM- und ADMX-Vorlagendateien für die Horizon Client-Konfiguration beschrieben. Die Einstellungen gelten auf Computerebene. Horizon Client liest die Einstellungen vorzugsweise aus dem GPO auf der Computerebene, andernfalls aus der Registrierung unter `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB`. Eine Beschreibung, wie Horizon die Richtlinien zum Filtern von USB-Geräten anwendet, finden Sie in den Themen zur Konfiguration von Filterrichtlinieneinstellungen für die USB-Umleitung im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Tabelle 3-9. Konfigurationsvorlage für Horizon Client : Einstellungen für USB-Filter

Einstellung	Eigenschaften
`Allow Audio Input Devices`	Lässt zu, dass Audioeingabegeräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`true`** ist.
`Allow Audio Output Devices`	Lässt zu, dass Audioausgabegeräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
`Allow HIDBootable`	Ermöglicht die Umleitung anderer Eingabegeräte neben Tastaturen und Mäusen, die zur Startzeit verfügbar sind (auch bezeichnet als „startfähige Eingabegeräte“). Der Standardwert ist nicht definiert, was gleichbedeutend mit **`true`** ist.
`Allow Device Descriptor Failsafe Behavior`	Ermöglicht die Umleitung der Geräte, auch wenn Horizon Client die Konfigurations-/Gerätebeschreibungen nicht abrufen kann. Um ein Gerät trotz Fehler in der Konfiguration/Beschreibung zuzulassen, muss dieses in den Filter „Include“ eingeschlossen werden, zum Beispiel in `IncludeVidPid` oder `IncludePath`. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
`Allow Other Input Devices`	Lässt zu, dass Eingabegeräte außer HID-startfähigen Geräten oder Tastaturen mit integrierten Zeigegeräten umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`true`** ist.
`Allow Keyboard and Mouse Devices`	Lässt zu, dass Tastaturen mit eingebauten Zeigegeräten (Maus, Trackball oder Touchpad) umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.

Tabelle 3-9. Konfigurationsvorlage für Horizon Client : Einstellungen für USB-Filter (Fortsetzung)

Einstellung	Eigenschaften
`Allow Smart Cards`	Lässt zu, dass Smartcard-Geräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
`Allow Video Devices`	Lässt zu, dass Videogeräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`true`** ist.
`Disable Remote Configuration`	Deaktiviert die Verwendung der Agent-Einstellungen beim Durchführen der USB-Gerätefilterung. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
`Exclude All Devices`	Schließt alle USB-Geräte von der Umleitung aus. Wenn für diese Einstellung **`true`** festgelegt ist, können Sie andere Richtlinieneinstellungen verwenden, um zuzulassen, dass bestimmte Geräte oder Gerätefamilien umgeleitet werden. Wenn für diese Einstellung **`false`** festgelegt ist, können Sie andere Richtlinieneinstellungen verwenden, um zu verhindern, dass bestimmte Geräte oder Gerätefamilien umgeleitet werden. Wenn Sie den Wert von `Exclude All Devices` im Agent auf **`true`** setzen und diese Einstellung an Horizon Client weitergegeben wird, überschreibt die Agent-Einstellung die Horizon Client-Einstellung. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
`Exclude Device Family`	Schließt Gerätefamilien von der Umleitung aus. Das Format der Einstellung lautet *Familienname_1*[`;`*Familienname_2*]... Beispiel: **`bluetooth;smart-card`** Wenn Sie das automatische Gerätesplitten aktiviert haben, prüft Horizon die Gerätefamilie jeder Schnittstelle eines Composite USB-Gerätes, um zu entscheiden, welche Schnittstelle ausgeschlossen werden sollte. Wenn Sie das automatische Gerätesplitten deaktiviert haben, prüft Horizon die Gerätefamilie des gesamten Composite USB-Gerätes. Der Standardwert ist nicht definiert.
`Exclude Vid/Pid Device`	Schließt Geräte mit einer angegebenen Anbieter- oder Produkt-ID von der Umleitung aus. Das Format der Einstellung lautet `vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]... Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (**`*`**) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: **`vid-0781_pid-****;vid-0561_pid-554c`** Der Standardwert ist nicht definiert.
`Exclude Path`	Schließt Geräte an angegebenen Hub- oder Portpfaden von der Umleitung aus. Das Format der Einstellung lautet `bus-`*x1*[`/`*y1*]`.../port-`*z1*[`;bus-`*x2*[`/`*y2*]`.../port-`*z2*]... Bus- und Portnummern müssen im hexadezimalen Format angegeben werden. Sie können das Platzhalterzeichen nicht in Pfaden verwenden. Beispiel: **`bus-1/2/3_port-02;bus-1/1/1/4_port-ff`** Der Standardwert ist nicht definiert.
`Include Device Family`	Bestimmt Gerätefamilien, die umgeleitet werden können. Das Format der Einstellung lautet *Familienname_1*[`;`*Familienname_2*]... Beispiel: **`storage`** Der Standardwert ist nicht definiert.

Tabelle 3-9. Konfigurationsvorlage für Horizon Client : Einstellungen für USB-Filter (Fortsetzung)

Einstellung	Eigenschaften
`Include Path`	Schließt Geräte an angegebenen Hub- oder Portpfaden in die Umleitung ein. Das Format der Einstellung lautet `bus-`*x1*`[/`*y1*`].../port-`*z1*`[;bus-`*x2*`[/`*y2*`]...port-`*z2*`]...` Bus- und Portnummern müssen im hexadezimalen Format angegeben werden. Sie können das Platzhalterzeichen nicht in Pfaden verwenden. Beispiel: **`bus-1/2_port-02;bus-1/7/1/4_port-0f`** Der Standardwert ist nicht definiert.
`Include Vid/Pid Device`	Bestimmt Geräte mit einer angegebenen Anbieter- und Produkt-ID, die umgeleitet werden können. Das Format der Einstellung lautet `vid-`*xxx1*`_pid-`*yyy2*`[;vid-`*xxx2*`_pid-`*yyy2*`]...` Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (**`*`**) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: **`vid-0561_pid-554c`** Der Standardwert ist nicht definiert.

ADM-Vorlageneinstellungen für PCoIP-Client-Sitzungsvariablen

Die ADM- und ADMX-Vorlagendateien für PCoIP-Client-Sitzungsvariablen (`pcoip.client.adm` und `pcoip.cient.admx`) enthalten Richtlinieneinstellungen für das PCoIP-Anzeigeprotokoll. Sie können die Einstellungen entweder mit den Standardwerten konfigurieren, die durch einen Administrator außer Kraft gesetzt werden können, oder die Einstellungen mit nicht überschreibbaren Werten konfigurieren.

Die ADMX- und ADM-Dateien stehen in einer mitgelieferten `.zip`-Datei namens `VMware-Horizon-Extras-Bundle-`*x.x.x-yyyyyyy*`.zip` zur Verfügung, die Sie von der VMware-Download-Site unter https://my.vmware.com/web/vmware/downloads herunterladen können. Unter „Desktop- und Endbenutzer-Computing“ wählen Sie den VMware Horizon-7-Download, der die mitgelieferte `.zip`-Datei enthält.

Tabelle 3-10. PCoIP-Client-Sitzungsvariablen

Einstellung	Beschreibung
`Configure PCoIP client image cache size policy`	Reguliert die Größe des PCoIP-Client-Bildcaches. Der Client verwendet die Bild-Zwischenspeicherung, um Teile der vorab übertragenen Anzeige zu speichern. Durch die Bild-Zwischenspeicherung wird die Menge der erneut übermittelten Daten minimiert. Ist diese Einstellung nicht konfiguriert oder ist sie deaktiviert, verwendet PCoIP für das Clientbild eine Standard-Cachegröße von 250 MB. Bei Aktivierung dieser Einstellung können Sie die Client-Bildcachegröße von mindestens 50 MB auf 300 MB konfigurieren. Der Standardwert ist 250 MB.
`Configure PCoIP event log verbosity`	Legt die Ausführlichkeit der PCoIP-Ereignisprotokolle fest. Sie können einen Wert zwischen 0 (geringste Ausführlichkeit) und 3 (höchste Ausführlichkeit) festlegen. Bei Aktivierung dieser Einstellung können Sie einen Ausführlichkeitsgrad zwischen 0 und 3 festlegen. Wenn die Einstellung nicht konfiguriert oder deaktiviert ist, wird der standardmäßige Ausführlichkeitsgrad 2 verwendet. Wird diese Einstellung während einer aktiven PCoIP-Sitzung geändert, ist die neue Einstellung umgehend wirksam.

Tabelle 3-10. PCoIP-Client-Sitzungsvariablen (Fortsetzung)

Einstellung	Beschreibung
`Configure PCoIP session encryption algorithms`	Steuert die Verschlüsselungsalgorithmen, die vom PCoIP-Endpunkt während der Sitzungsaushandlung angeboten werden. Durch Aktivierung eines Kontrollkästchens wird der entsprechende Verschlüsselungsalgorithmus deaktiviert. Sie müssen mindestens einen Algorithmus aktivieren. Diese Einstellung gilt sowohl für den Agenten als auch für den Client. Die Endpunkte handeln den tatsächlich verwendeten Algorithmus für die Sitzungsverschlüsselung aus. Wenn der FIPS140-2-validierte Modus aktiviert ist, wird der Wert für **Disable AES-128-GCM encryption (AES-128-GCM-Verschlüsselung deaktivieren)** immer außer Kraft gesetzt, wenn sowohl die AES-128-GCM- als auch die AES-256-GCM-Verschlüsselung deaktiviert ist. Wenn die `Configure SSL Connections`-Einstellung deaktiviert wurde oder nicht konfiguriert ist, stehen die Algorithmen Salsa20-256round12 und AES-128-GCM zur Aushandlung durch diesen Endpunkt zur Verfügung. Unterstützte Verschlüsselungsalgorithmen sind in der bevorzugten Reihenfolge SALSA20/12-256, AES-GCM-128 und AES-GCM-256. Standardmäßig sind alle unterstützten Verschlüsselungsalgorithmen zur Aushandlung durch diesen Endpunkt verfügbar.
`Configure PCoIP virtual channels`	Gibt die virtuellen Kanäle an, die bei PCoIP-Sitzungen verwendet bzw. nicht verwendet werden können. Diese Einstellung legt auch fest, ob die Zwischenablageverarbeitung auf dem PCoIP-Host deaktiviert wird. Virtuelle Kanäle, die in PCoIP-Sitzungen verwendet werden, müssen in der Tabelle der autorisierten virtuellen Kanäle aufgeführt sein. Virtuelle Kanäle, die in der Ausschlussliste für virtuelle Kanäle erscheinen, können in PCoIP-Sitzungen nicht verwendet werden. Sie können maximal 15 virtuelle Kanäle zur Verwendung in PCoIP-Sitzungen angeben. Trennen Sie mehrere Kanäle durch einen senkrechten Strich (|) voneinander. Die Zeichenfolge zum Zulassen der virtuellen Kanäle „mksvchan“ und „vdp_rdpvcbridge“ lautet z.B. **`mksvchan|vdp_rdpvcbridge`**. Wenn ein Kanalname einen senkrechten Strich oder einen umgekehrten Schrägstrich (\) enthält, fügen Sie vor dem Kanalnamen einen umgekehrten Schrägstrich ein. Der Kanalname „awk|ward\channel“ wird beispielsweise folgendermaßen eingegeben: **`awk\\|ward\\channel`**. Ist die Tabelle der autorisierten virtuellen Kanäle leer, ist die Verwendung von virtuellen Kanälen nicht zulässig. Ist die Ausschlusstabelle für virtuelle Kanäle leer, sind alle virtuellen Kanäle zugelassen. Die Einstellung der virtuellen Kanäle gilt sowohl für den Agenten als auch für den Client. Zum Verwenden virtueller Kanäle müssen diese sowohl auf dem Agenten als auch auf dem Client aktiviert werden. Bei Festlegung der virtuellen Kanäle wird ein separates Kontrollkästchen angezeigt, mit dem Sie die Remote-Zwischenablageverarbeitung auf dem PCoIP-Host deaktivieren können. Dieser Wert gilt nur für den Agent. Standardmäßig sind alle virtuellen Kanäle aktiviert, einschließlich der Zwischenablageverarbeitung.
`Configure the Client PCoIP UDP port`	Gibt den UDP-Port an, der von Software-PCoIP-Clients verwendet wird. Der Wert des UDP-Ports gibt den zu verwendenden Basisport vor. Der Wert für den UDP-Portbereich legt fest, wie viele zusätzliche Ports ausprobiert werden, falls der Basisport nicht verfügbar ist. Der Bereich erstreckt sich vom Basisport bis zur Summe aus Basisport und Portbereich. Wenn der Basisport beispielsweise 50002 lautet und der Portbereich auf 64 festgelegt ist, umfasst der Bereich die Ports 50002 bis 50066. Diese Einstellung gilt nur für den Client. Standardmäßig lautet der Basisport 50002 und der Portbereich ist auf 64 festgelegt.

Tabelle 3-10. PCoIP-Client-Sitzungsvariablen (Fortsetzung)

Einstellung	Beschreibung
`Configure the maximum PCoIP session bandwidth`	Legt die maximale Bandbreite für eine PCoIP-Sitzung in Kilobits pro Sekunde fest. Die Bandbreite umfasst den gesamten Sitzungsdatenverkehr, Bilddarstellung, Audio, virtuelle Kanäle, USB und PCoIP-Steuerung eingeschlossen. Legen Sie diesen Wert auf die Gesamtkapazität der Verbindung fest, über die Ihr Endpunkt verbunden ist, und berücksichtigen Sie dabei die Anzahl der erwarteten gleichzeitigen PCoIP-Sitzungen. Beispiel: Legen Sie diesen Wert bei einer Einzelbenutzer-VDI-Konfiguration (eine einzelne PCoIP-Sitzung), die über eine Internetverbindung mit 4 MBit/s verbunden ist, auf 4 MBit oder auf 90 % dieses Werts fest, um etwas Spielraum für anderen Netzwerkdatenverkehr zu lassen. Wenn Sie erwarten, dass sich mehrere gleichzeitige PCoIP-Sitzungen, die entweder mehrere VDI-Benutzer oder eine RDS-Konfiguration umfassen, einen Link teilen, können Sie die Einstellung entsprechend anpassen. Durch eine Senkung dieses Werts wird jedoch die maximale Bandbreite für jede aktive Sitzung beschränkt. Durch eine Festlegung dieses Werts verhindern Sie, dass der Agent eine die Verbindungskapazität übersteigende Übertragungsrate wählt – was zu einem übermäßigen Paketverlust und einem schlechteren Benutzererlebnis führen würde. Dieser Wert ist symmetrisch. Client und Agent werden gezwungen, den niedrigeren der beiden Werte zu verwenden, die auf Client- und Agentseite festgelegt sind. Beispielsweise wird der Agent bei Festlegung einer maximalen Bandbreite von 4 MBit/s gezwungen, eine niedrigere Übertragungsrate zu verwenden – auch wenn die Einstellung auf dem Client konfiguriert ist. Wenn diese Einstellung deaktiviert wurde oder auf einem Endpunkt nicht konfiguriert ist, legt der Endpunkt keine Bandbreiteneinschränkungen fest. Wenn diese Einstellung konfiguriert ist, wird sie als maximale Bandbreiteneinschränkung des Endpunkts in KBit/s verwendet. Der Standardwert für die nicht konfigurierte Einstellung liegt bei 900000 KBit/s. Diese Einstellung gilt sowohl für den Agenten als auch für den Client. Haben die beiden Endpunkte unterschiedliche Einstellungen, wird der niedrigere Wert verwendet.
`Configure the PCoIP transport header`	Konfiguriert den PCoIP-Übertragungsheader und legt die Priorität der Transportsitzung fest. Der PCoIP-Übertragungsheader ist ein 32-Bit-Header, der zu allen PCoIP-UDP-Paketen hinzugefügt wird (sofern der Übertragungsheader auf beiden Seiten aktiviert ist und unterstützt wird). Anhand des PCoIP-Übertragungsheaders können Netzwerkgeräte bei Netzwerkkonflikten eine bessere Priorisierung vornehmen bzw. bessere QoS-Entscheidungen treffen. Der Übertragungsheader ist standardmäßig aktiviert. Die Priorität einer Transportsitzung bestimmt die PCoIP-Sitzungspriorität, die im PCoIP-Übertragungsheader angegeben wird. Netzwerkgeräte können basierend auf der angegebenen Priorität einer Transportsitzung eine bessere Priorisierung vornehmen und bessere QoS-Entscheidungen treffen. Bei Aktivierung der Einstellung `Configure the PCoIP transport header` sind die folgenden Prioritäten für eine Transportsitzung verfügbar: ■ **Hoch** ■ **Mittel** (Standardwert) ■ **Niedrig** ■ **Nicht definiert** Der Prioritätswert für die Transportsitzung wird vom PCoIP-Agent und -Client ausgehandelt. Wenn der PCoIP-Agent einen Prioritätswert für die Transportsitzung angibt, wird die vom Agent angegebene Sitzungspriorität für die Sitzung verwendet. Wenn nur auf dem Client eine Priorität für die Transportsitzung angegeben ist, wird die vom Client angegebene Priorität für die Sitzung verwendet. Wenn weder der Agent noch der Client eine Priorität für die Transportsitzung angibt oder der Wert **Nicht definiert** festgelegt wurde, wird der Standardwert (**Mittel**) für die Sitzung verwendet.
`Enable/disable audio in the PCoIP session`	Legt fest, ob die Audiofunktion während PCoIP-Sitzungen aktiviert ist. Die Audiofunktion muss für beide Endpunkte aktiviert sein. Ist diese Einstellung aktiviert, ist die Verwendung von PCoIP-Audio zulässig. Wurde diese Einstellung deaktiviert, kann die PCoIP-Audiofunktion nicht verwendet werden. Wurde diese Einstellung nicht konfiguriert, ist die Audiofunktion standardmäßig aktiviert.

Tabelle 3-10. PCoIP-Client-Sitzungsvariablen (Fortsetzung)

Einstellung	Beschreibung
`Configure the PCoIP session bandwidth floor`	Legt die Mindestbandbreite in Kilobits pro Sekunde fest, die von der PCoIP-Sitzung reserviert wird. Mit dieser Einstellung wird die minimale erwartete Bandbreitenübertragungsrate für den Endpunkt konfiguriert. Wenn Sie diese Einstellung zum Reservieren der Bandbreite für einen Endpunkt verwenden, muss der Benutzer nicht warten, bis Bandbreite verfügbar ist, was die Reaktionszeit während der Sitzung verbessert. Achten Sie jedoch darauf, dass Sie allen Endpunkten gemeinsam nicht mehr Bandbreite zuweisen, als insgesamt zur Verfügung steht. Die Summe der Mindestbandbreitenwerte für alle Verbindungen in Ihrer Konfiguration darf die Netzwerkkapazität nicht überschreiten. Der Standardwert lautet 0, d.h. es wird keine Mindestbandbreite reserviert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, wird keine Mindestbandbreite reserviert. Diese Einstellung gilt sowohl für den Agenten als auch für den Client, wirkt sich allerdings nur auf den Endpunkt aus, für den sie konfiguriert wurde. Wird diese Einstellung während einer aktiven PCoIP-Sitzung geändert, wird die Änderung umgehend wirksam.
`Configure the PCoIP session MTU`	Legt die Größe der maximalen Übertragungseinheit (Maximum Transmission Unit, MTU) für UDP-Pakete bei einer PCoIP-Sitzung fest. Die MTU-Größe umfasst den IP- und UDP-Paketvorspann. TCP verwendet den standardmäßigen MTU-Ermittlungsmechanismus zum Festlegen der maximalen Übertragungseinheit und wird von dieser Einstellung nicht beeinflusst. Die maximale MTU-Größe beträgt 1.500 Byte. Die minimale MTU-Größe beträgt 500 Byte. Der Standardwert lautet 1.300 Byte. Normalerweise muss die MTU-Größe nicht geändert werden. Ändern Sie diesen Wert, wenn Sie in einer nicht standardmäßig eingerichteten Netzwerkumgebung arbeiten, die zu einer PCoIP-Paketfragmentierung führt. Diese Einstellung gilt sowohl für den Agenten als auch für den Client. Unterscheiden sich die MTU-Größeneinstellungen der beiden Endpunkte, wird der niedrigere Wert verwendet. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, verwendet der Client bei der Aushandlung mit dem Agenten den Standardwert.

Ausführen von Horizon Client über die Befehlszeile

Sie können Horizon Client für Windows von der Befehlszeile aus oder über Skripts ausführen. Dies kann erwünscht sein, wenn Sie eine kioskbasierte Anwendung implementieren, die Endbenutzern Zugriff auf Desktop-Anwendungen gewährt.

Sie verwenden den Befehl `vmware-view.exe`, um Horizon Client für Windows über die Befehlszeile auszuführen. Der Befehl umfasst Optionen, die Sie angeben können, um das Verhalten von Horizon Client zu ändern.

Verwenden von Horizon Client -Befehlen

Die Syntax des Befehls `vmware-view` legt fest, wie Horizon Client ausgeführt wird.

Verwenden Sie den Befehl `vmware-view` an einer Windows-Eingabeaufforderung mit dem folgenden Format.

`vmware-view [`*`Befehlszeilenoption`* `[`*`Argument`*`]] ...`

Der Standardpfad zur ausführbaren Datei des Befehls `vmware-view` ist vom System abhängig.

- Auf 32-Bit-Systemen lautet der Pfad `C:\Programme\VMware\VMware Horizon View Client\`.
- Auf 64-Bit-Systemen lautet der Pfad `C:\Programme (x86)\VMware\VMware Horizon View Client\`.

Zur Vereinfachung fügen Sie diesen Pfad zu Ihrer Umgebungsvariable *PATH* hinzu.

In der folgenden Tabelle sind die Befehlszeilenoptionen aufgeführt, die mit dem Befehl `vmware-view` verwendet werden können.

Tabelle 3-11. Horizon Client -Befehlszeilenoptionen

Option	Beschreibung
`/?`	Zeigt die Liste der Befehlsoptionen an.
`-appName` *Anwendungsname*	Gibt den Namen der Anwendung an, der im Dialogfeld zur Desktop- und Anwendungsauswahl angezeigt wird. Hierbei handelt es sich um den Anzeigenamen, der für den Anwendungspool im Assistenten zur Poolerstellung angegeben wurde.
`-appSessionReconnectionBehavior` *argument*	Legt die Einstellung für das Wiederverbindungsverhalten von Anwendungen fest. ■ `always` implementiert **Neuverbindung zum Öffnen von Anwendungen automatisch herstellen** ■ `never` implementiert **Vor Neuverbindung nicht fragen und nicht automatisch neu verbinden** ■ `ask` implementiert **Vor Neuverbindung zum Öffnen von Anwendungen fragen** Durch Verwendung dieser Option werden die Einstellungen für die Wiederverbindung von Anwendungen auf der Seite „Einstellungen“ in Horizon Client deaktiviert.
`-args` *argument*	Gibt Befehlszeilenargumente zum Hinzufügen beim Start einer Remoteanwendung an. Beispiel: `vmware-view.exe --serverURL 10.10.10.10 --appName "My Notepad++" --args "\"my new.txt\""`
`-connectUSBOnStartup`	Wenn hier `true` angegeben ist, werden alle gegenwärtig mit dem Host verbundenen USB-Geräte an den Desktop umgeleitet. Diese Option wird bei Angabe der Option `-unattended` implizit festgelegt. Die Standardeinstellung ist `false`.
`-connectUSBOnInsert`	Wenn hier `true` angegeben ist, wird ein USB-Gerät mit dem Desktop im Vordergrund verbunden, wenn Sie das Gerät anschließen. Diese Option wird bei Angabe der Option `-unattended` implizit festgelegt. Die Standardeinstellung ist `false`.
`-desktopLayout` *Fenstergröße*	Gibt an, wie das Desktop-Fenster angezeigt wird: **`fullscreen`** Vollbildanzeige. **`multimonitor`** Mehrfachmonitoranzeige. **`windowLarge`** Großes Fenster. **`windowSmall`** Kleines Fenster. **`length X width`** Benutzerdefinierte Größe. Zum Beispiel: 800 X 600
`-desktopName` *Desktop-Name*	Gibt den Namen des Desktops an, der im Dialogfeld zur Desktop- und Anwendungsauswahl angezeigt wird. Hierbei handelt es sich um den Anzeigenamen, der für den Pool im Assistenten zur Poolerstellung angegeben wurde. **Wichtig** Geben Sie diese Option für Clients im Kiosk-Modus nicht an. Diese Option bleibt wirkungslos, wenn der Desktop im Kiosk-Modus ausgeführt wird. Im Kiosk-Modus wird die Verbindung zum ersten Desktop in der Liste der berechtigten Desktops hergestellt.
`-desktopProtocol` *Protokoll*	Gibt den Namen des zu verwendenden Anzeigeprotokolls an, der im Dialogfeld zur Desktop- und Anwendungsauswahl angezeigt wird. Beim Anzeigeprotokoll kann es sich um Blast, PCoIP oder RDP handeln.
`-domainName` *Domänenname*	Gibt die NETBIOS-Domäne an, die der Endbenutzer zur Anmeldung bei Horizon Client verwendet. Beispielsweise ist es sinnvoller, `MeineFirma` als `MeineFirma.com` zu verwenden.

Tabelle 3-11. Horizon Client -Befehlszeilenoptionen (Fortsetzung)

Option	Beschreibung
`–file` *Dateipfad*	Gibt den Pfad einer Konfigurationsdatei mit zusätzlichen Befehlsoptionen und -argumenten an. Siehe „Horizon Client-Konfigurationsdatei“, auf Seite 71.
`–h`	Zeigt Hilfeoptionen an.
`–hideClientAfterLaunchSession`	Wenn auf `true` festgelegt, werden das Remote-Desktop- und Anwendungsauswahlfenster sowie das Menü **VMware Horizon Client anzeigen** nach dem Starten einer Remote-Sitzung ausgeblendet. Wenn auf `false` festgelegt, werden das Remote-Desktop- und Anwendungsauswahlfenster sowie das Menü **VMware Horizon Client anzeigen** nach dem Starten einer Remote-Sitzung angezeigt. Die Standardeinstellung ist `true`.
`–languageId` *Gebietsschema-ID*	Bietet Lokalisierungsunterstützung für verschiedene Sprachen in Horizon Client. Wenn eine Ressourcenbibliothek verfügbar ist, geben Sie die zu verwendende Gebietsschema-ID (Locale ID, LCID) an. Für Englisch (USA) geben Sie 0x409 ein.

`–listMonitors`	Führt die Indexwerte auf und zeigt die Layoutinformationen für die verbundenen Monitore an. Beispiel:
	`1: (0, 0, 1920, 1200)`
	`2: (1920, 0, 3840, 1200)`
	`3: (–900, –410, 0, 1190)`
	Sie können die Indexwerte mit der Option `–monitors` verwenden.

`–logInAsCurrentUser`	Wenn hier `true` angegeben ist, werden die Anmeldedaten des Endbenutzers, die dieser zur Anmeldung beim Clientsystem eingegeben hat, zur Anmeldung bei der Verbindungsserver-Instanz und schließlich beim Remote-Desktop verwendet. Die Standardeinstellung ist `false`.
`–monitors "`*n*`[,`*n*`,`*n*`,`*n*`]"`	Gibt die Monitore an, die in einer Mehrfachmonitorumgebung verwendet werden sollen, wobei *n* der Indexwert eines Monitors ist. Sie können mit der Option `–listMonitors` die Indexwerte der verbundenen Monitore bestimmen. Es lassen sich bis zu vier Indexwerte, durch Kommas getrennt, angeben. Beispiel: **`–monitors "1,2"`** Diese Option ist nur wirksam, wenn für `–desktopLayout` die Einstellung `multimonitor` festgelegt ist.
`–nonInteractive`	Unterdrückt Fehlermeldungen beim Starten von Horizon Client über ein Skript. Diese Option wird bei Angabe der Option `–unattended` implizit festgelegt.
`–noVMwareAddins`	Verhindert das Laden von VMware-spezifischen virtuellen Kanälen, wie z. B. für den virtuellen Druck.
`–password` *Kennwort*	Gibt das Kennwort an, das der Endbenutzer zur Anmeldung an Horizon Client verwendet. Das Kennwort wird von der Befehlskonsole und von jedem Skripttool im Textformat weiterverarbeitet. Diese Option muss für Clients im Kiosk-Modus nicht angegeben werden, wenn das Kennwort automatisch generiert wird. Aus Sicherheitsgründen wird empfohlen, diese Option nicht anzugeben. Benutzer können das Kennwort interaktiv eingeben.
`–printEnvironmentInfo`	Zeigt die IP-Adresse, die MAC-Adresse und den Maschinennamen des Clientgeräts an.
`–serverURL` *Verbindungsserver*	Gibt die URL, die IP-Adresse oder den FQDN der Verbindungsserver-Instanz an.
`–shutdown`	Fährt alle Desktops und Anwendungen sowie die relevanten Benutzeroberflächenkomponenten herunter.
`–singleAutoConnect`	Wenn ein Benutzer nur Anspruch auf einen Remote-Desktop oder eine Remoteanwendung hat, wird mit dieser Einstellung nach der Authentifizierung des Benutzers beim Server automatisch eine Verbindung mit dem Desktop oder der Anwendung hergestellt und der Benutzer wird angemeldet. Dem Benutzer wird dadurch die Auswahl des Desktops oder der Anwendung aus einer Liste mit nur einem Element erspart.

Tabelle 3-11. Horizon Client -Befehlszeilenoptionen (Fortsetzung)

Option	Beschreibung
`–smartCardPIN` *PIN*	Gibt die PIN an, wenn ein Endbenutzer eine Smartcard zur Anmeldung einführt.
`–usernameHint` *Benutzername*	Gibt den Kontonamen an, der als Benutzernamenhinweis verwendet werden soll.
`–standalone`	Unterstützt zur Bereitstellung von Abwärtskompatibilität. Dies ist das Standardverhalten für diesen Client. Die Angabe von `–standalone` ist nicht erforderlich. Startet eine zweite Instanz von Horizon Client, die eine Verbindung mit derselben oder einer anderen Verbindungsserver-Instanz herstellen kann. Für mehrere Desktopverbindungen zum selben oder einem anderen Server wird keine sichere Tunnelverbindung unterstützt. **Hinweis** Die zweite Desktopverbindung hat möglicherweise keinen Zugriff auf die lokale Hardware, wie USB-Geräte, Smartcards, Drucker und mehrere Monitore.
`–supportText` *file_name*	Gibt den vollständigen Pfad einer Textdatei an. Der Inhalt der Datei wird im Dialogfeld „Support-Informationen“ angezeigt.
`–unattended`	Führt Horizon Client im nicht interaktiven Modus aus, der sich für Clients im Kiosk-Modus eignet. Zusätzlich müssen folgende Informationen angegeben werden: ■ Der Kontoname des Clients, wenn dieser nicht über die MAC-Adresse des Clientgeräts generiert wurde. Der Name muss mit der Zeichenfolge „custom-“ oder einem alternativen Präfix beginnen, das Sie in ADAM konfiguriert haben. ■ Das Kennwort des Clients, wenn dieses nicht automatisch beim Einrichten des Clientkontos generiert wurde. Über die Option `–unattended` werden die Optionen `–nonInteractive`, `–connectUSBOnStartup`, `–connectUSBOnInsert` und `–desktopLayout multimonitor` implizit festgelegt.
`–unauthenticatedAccessAccount`	Legt ein Benutzerkonto für einen nicht authentifizierten Zugriff zur anonymen Anmeldung beim Server fest, wenn der nicht authentifizierte Zugriff aktiviert ist. Wenn der nicht authentifizierte Zugriff nicht aktiviert ist, wird diese Option ignoriert. Beispiel: `vmware–view.exe –serverURL ag–broker.agwork.com –unauthenticatedAccessEnabled true –unauthenticatedAccessAccount anonymous1`
`–unauthenticatedAccessEnabled`	Legt das Verhalten für den nicht authentifizierten Zugriff fest: ■ `true` aktiviert den nicht authentifizierten Zugriff. Wenn der nicht authentifizierte Zugriff nicht verfügbar ist, verwendet der Client eventuell eine andere Authentifizierungsmethode. Die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** wird in Horizon Client angezeigt, deaktiviert und ausgewählt. ■ Bei `false` ist die Eingabe Ihrer Anmeldedaten für die Anmeldung bei Ihren Anwendungen und den Zugriff darauf erforderlich. Die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** wird in Horizon Client ausgeblendet und nicht ausgewählt. Wenn Sie diese Option nicht festlegen, haben Sie die Möglichkeit, den nicht authentifizierten Zugriff in Horizon Client zu aktivieren. Die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** wird angezeigt, aktiviert und nicht ausgewählt.

Tabelle 3-11. Horizon Client -Befehlszeilenoptionen (Fortsetzung)

Option	Beschreibung

`–useExisting`	Ermöglicht den Start mehrerer Remote-Desktops und -anwendungen aus einer einzelnen Horizon Client-Sitzung.
	Wenn Sie diese Option festlegen, ermittelt Horizon Client, ob eine Sitzung mit dem gleichen Benutzernamen, der gleichen Domäne und der gleichen URL bereits vorhanden ist. Ist dies der Fall, wird diese Sitzung wiederverwendet, anstatt eine neue zu erstellen.
	Im nachfolgend aufgeführten Befehl startet user-1 beispielsweise die Anwendung Rechner und eine neue Sitzung wird erstellt.
	`vmware–view.exe –userName user–1 –password secret –domainName domain –appName Calculator –serverURL view.mycompany.com –useExisting`
	Im nächsten Befehl startet user-1 die Anwendung Paint mit dem gleichen Benutzernamen, der gleichen Domäne und der gleichen URL. Dieselbe Sitzung wird verwendet.
	`vmware–view.exe –userName user–1 –password secret –domainName domain –appName Paint –serverURL view.mycompany.com –useExisting`

`–userName` *Benutzername*	Gibt den Kontonamen an, den der Endbenutzer zur Anmeldung an Horizon Client verwendet. Diese Option muss für Clients im Kiosk-Modus nicht angegeben werden, wenn der Kontoname über die MAC-Adresse des Clientgeräts generiert wird.

Mit Ausnahme von `–file`, `–languageId`, `–printEnvironmentInfo`, `–smartCardPIN` und `–unattended` können alle Optionen über Active Directory-Gruppenrichtlinien angegeben werden.

Hinweis Gruppenrichtlinieneinstellungen haben Vorrang vor Einstellungen, die Sie in der Befehlszeile angeben.

Horizon Client -Konfigurationsdatei

Sie können Befehlszeileninformationen für Horizon Client aus einer Konfigurationsdatei auslesen.

Sie können den Pfad der Konfigurationsdatei als Argument der Option `–file`*Dateipfad* des Befehls `vmware–view` angeben. Bei der Datei muss es sich um eine Unicode- (UTF-16) oder um eine ASCII-Textdatei handeln.

Beispiel: Beispiel einer Konfigurationsdatei für eine nicht interaktive Anwendung

Das folgende Beispiel zeigt die Inhalte einer Konfigurationsdatei für eine nicht interaktive Anwendung.

```
–serverURL https://view.yourcompany.com
–userName autouser
–password auto123
–domainName companydomain
–desktopName autodesktop
–nonInteractive
```

Beispiel: Beispiel einer Konfigurationsdatei für einen Client im Kioskmodus

Das folgende Beispiel zeigt einen Client im Kioskmodus, dessen Kontoname auf seiner MAC-Adresse basiert. Der Client verwendet ein automatisch generiertes Kennwort.

```
–serverURL 145.124.24.100
–unattended
```

Konfigurieren des Horizon Client mithilfe der Windows-Registrierung

Sie können Standardeinstellungen für den Horizon Client in der Windows-Registrierung definieren, anstatt diese Einstellungen über die Befehlszeile anzugeben. Gruppenrichtlinieneinstellungen haben Vorrang vor Windows-Registrierungseinstellungen. Windows-Registrierungseinstellungen haben wiederum Vorrang vor der Befehlszeile.

Hinweis In einer künftigen Version werden die in diesem Abschnitt beschriebenen Windows-Registrierungseinstellungen möglicherweise nicht unterstützt. Es müssen GPO-Einstellungen verwendet werden.

Tabelle 3-12 zeigt die Registrierungseinstellungen für die Anmeldung bei Horizon Client. Diese Einstellungen befinden sich in der Registrierung unter „`HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDM\Client\`“. Dieser Speicherort ist spezifisch für einen bestimmten Benutzer, wohingegen die Einstellungen „`HKEY_LOCAL_MACHINE`“, die in der nächsten Tabelle beschrieben werden, computerweite Einstellungen sind, die für alle lokalen Benutzer und alle Domänenbenutzer in einer Windows-Domänenumgebung gelten, die über die Berechtigung verfügen, sich am Computer anzumelden.

Tabelle 3-12. Horizon Client Registrierungseinstellungen für Anmeldedaten

Registrierungs-einstellung	Beschreibung
`Password`	Bestimmt das Standardkennwort.
`UserName`	Bestimmt den standardmäßigen Benutzernamen.

Tabelle 3-13 zeigt die Registrierungseinstellungen für Horizon Client, die nicht die Anmeldedaten beinhalten. Der Speicherort dieser Einstellungen hängt vom Systemtyp ab:

- Für 32-Bit-Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\`
- Für 64-Bit-Windows: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\`

Tabelle 3-13. Horizon Client -Registrierungseinstellungen

Registrierungsein-stellung	Beschreibung
`DomainName`	Bestimmt den standardmäßigen NETBIOS-Domänennamen. Beispielsweise ist es sinnvoller, `MeineFirma` als `MeineFirma.com` zu verwenden.
`EnableShade`	Bestimmt, ob die Menüleiste (Shade) am oberen Rand des Horizon Client-Fensters aktiviert ist. Die Menüleiste ist standardmäßig aktiviert, mit Ausnahme bei Clients im Kioskmodus. Mit dem Wert **`false`** wird die Menüleiste deaktiviert. **Hinweis** Diese Einstellung ist nur verfügbar, wenn das Anzeigelayout auf **Alle Monitore** oder **Vollbild** festgelegt ist.
`ServerURL`	Bestimmt die standardmäßige Verbindungsserver-Instanz anhand der URL, IP-Adresse oder des FQDN.
`EnableSoftKeypad`	Wenn dies auf **`true`** eingestellt ist und ein Horizon Client-Fenster den Fokus aufweist, werden Ereignisse auf der physischen Tastatur, auf der Bildschirmtastatur, mit der Maus und im Schreibbereich an den Remote-Desktop oder an die Remoteanwendung gesendet, selbst wenn sich die Maus oder die Bildschirmtastatur außerhalb des Horizon Client-Fensters befindet. Die Standardeinstellung ist **`false`**.

In der folgenden Tabelle werden Sicherheitseinstellungen beschrieben, die Sie hinzufügen können. Der Speicherort dieser Einstellungen hängt vom Systemtyp ab:

- Für 32-Bit-Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`
- Für 64-Bit-Windows: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`

Tabelle 3-14. Sicherheitseinstellungen

Registrierungseinstellung	Beschreibung und gültige Werte
`CertCheckMode`	Legt den Zertifikatsprüfungsmodus fest. ■ **`0`** implementiert `Do not verify server identity certificates`. ■ **`1`** implementiert `Warn before connecting to untrusted servers`. ■ **`2`** implementiert `Never connect to untrusted servers`.
`SSLCipherList`	Konfiguriert die Verschlüsselungsliste, um die Verwendung bestimmter kryptografischer Algorithmen und Protokolle zu beschränken, bevor Sie eine verschlüsselte SSL-Verbindung herstellen. Die Verschlüsselungsliste besteht aus einer oder mehreren Verschlüsselungszeichenfolgen, die durch Doppelpunkte voneinander getrennt werden. **Hinweis** Für alle Verschlüsselungszeichenfolgen wird die Groß-/Kleinschreibung berücksichtigt. Der Standardwert ist **TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES**. Das heißt, dass TLSv.1, TLSv1.1 und TLSv1.2 aktiviert sind. (SSL v2.0 und v3.0 wurden entfernt.) Verschlüsselungssammlungen verwenden 128- oder 256-Bit-AES, entfernen anonyme DH-Algorithmen und sortieren anschließend die aktuelle Verschlüsselungsliste nach der Schlüssellänge des Verschlüsselungsalgorithmus. Referenz-Link für die Konfiguration: http://www.openssl.org/docs/apps/ciphers.html

Verwalten der Remote-Desktop- und Anwendungsverbindungen

4

Mit Horizon Client können Sie eine Verbindung zu einem Verbindungsserver oder Sicherheitsserver herstellen, sich bei einem Remote-Desktop an- oder abmelden sowie Remoteanwendungen verwenden. Zur Fehlerbehebung können Sie auch Remote-Desktops und -Anwendungen zurücksetzen.

Je nachdem, wie der Administrator die Richtlinien für Remote-Desktops festlegt, können die Endbenutzer viele verschiedene Vorgänge auf ihren Desktops durchführen.

Dieses Kapitel behandelt die folgenden Themen:

Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung

Nach der Anmeldung bei einem Server können Sie sich mit den Remote-Desktops und -anwendungen verbinden, für deren Verwendung Sie autorisiert sind.

Bevor Endbenutzer auf ihre Remote-Desktops und -Anwendungen zugreifen, sollten Sie testen, ob Sie über ein Clientgerät eine Verbindung mit einem Remote-Desktop oder einer Remoteanwendung herstellen können. Sie müssen eventuell einen Server angeben und die Anmeldedaten für Ihr Benutzerkonto eingeben.

Für die Verwendung von Remoteanwendungen müssen Sie eine Verbindung mit dem Verbindungsserver der Version 6.0 oder höher herstellen.

Die Funktion **Als aktueller Benutzer anmelden** steht selbst dann zur Verfügung, wenn Horizon Client auf einem Remote-Desktop installiert ist.

Voraussetzungen

- Besorgen Sie sich die Informationen zur Anmeldung, so etwa einen Benutzernamen und das zugehörige Kennwort, den RSA SecurID-Benutzernamen und -Passcode, den RADIUS-Authentifizierungsbenutzernamen und -Passcode oder die Smartcard-PIN.
- Besorgen Sie sich den NETBIOS-Domänennamen für die Anmeldung. Beispielsweise ist es sinnvoller, `MeineFirma` als `MeineFirma.com` zu verwenden.
- Führen Sie die unter „Vorbereiten des Verbindungsservers für Horizon Client“, auf Seite 20 beschriebenen administrativen Aufgaben aus.
- Wenn Sie sich außerhalb des Firmennetzwerks befinden und für den Zugriff auf den Remote-Desktop keinen Sicherheitsserver verwenden, stellen Sie sicher, dass Ihr Clientgerät für die Verwendung einer VPN-Verbindung konfiguriert ist, und aktivieren Sie diese Verbindung.

  Wichtig VMware empfiehlt die Verwendung eines Sicherheitsservers anstelle eines VPNs.

- Stellen Sie sicher, dass Sie über den vollqualifizierten Domänennamen (FQDN) des Servers verfügen, der Zugriff auf den Remote-Desktop oder die Remoteanwendung gewährt. Unterstriche (_) werden in Servernamen nicht unterstützt. Sie benötigen zudem auch die Portnummer, wenn es sich beim Port nicht um 443 handelt.
- Wenn Sie beabsichtigen, das RDP-Anzeigeprotokoll zur Verbindungsherstellung mit einem Remote-Desktop zu verwenden, müssen Sie sicherstellen, dass die Gruppenrichtlinieneinstellung AllowDirectRDP des Agenten aktiviert ist.
- Wenn Ihr Administrator dies zulässt, konfigurieren Sie den Zertifikatsprüfungsmodus für das vom Verbindungsserver vorgelegte SSL-Zertifikat. Informationen zur Bestimmung des zu verwendenden Modus finden Sie unter „Festlegen des Zertifikatsprüfungsmodus für Horizon Client“, auf Seite 45.

Vorgehensweise

1. Doppelklicken Sie auf die Desktop-Verknüpfung **VMware Horizon Client** oder klicken Sie auf **Start > Programme > VMware Horizon Client**.
2. (Optional) Zur Festlegung des Zertifikatsprüfungsmodus klicken Sie auf die Schaltfläche **Optionen** in der Menüleiste und wählen Sie **SSL konfigurieren** aus.

   Sie können diese Option nur konfigurieren, wenn Ihr Administrator dies zugelassen hat.
3. (Optional) Um sich als derzeit angemeldeter Windows-Domänenbenutzer anzumelden, klicken Sie in der Menüleiste auf die Schaltfläche **Optionen** und wählen Sie **Als aktueller Benutzer anmelden** aus.

   Diese Option steht zur Verfügung, wenn das Modul **Anmelden als aktueller Benutzer** auf Ihrem Clientsystem installiert ist und wenn der Administrator die globale Einstellung für diese Funktion aktiviert hat. Einige Unternehmen entschließen sich, die Funktion nicht zu aktivieren.

4 Doppelklicken Sie in der Menüleiste auf **+ Server hinzufügen**, sofern noch keine Server hinzugefügt wurden, oder auf **+ Neuer Server**, geben Sie den Namen des Verbindungsservers oder eines Sicherheitsservers ein und klicken Sie auf **Verbinden**.

Verbindungen zwischen Horizon Client und dem Verbindungsserver verwenden immer SSL. Der Standardport für SSL-Verbindungen ist 443. Wenn der Verbindungsserver nicht zur Verwendung des Standardports konfiguriert ist, muss das in folgendem Beispiel gezeigte Format verwendet werden: **`view.firma.com:1443`**.

Es wird eventuell eine Meldung eingeblendet, die Sie bestätigen müssen, bevor das Anmeldedialogfenster erscheint.

Hinweis Nach dem erfolgreichen Herstellen einer Verbindung wird auf der Startseite von Horizon Client ein Symbol für diesen Server gespeichert. Wenn Sie das nächste Mal Horizon Client öffnen, um eine Verbindung mit diesem Server herzustellen, können Sie auf das Symbol doppelklicken. Wenn Sie nur diesen einen Server verwenden, können Sie stattdessen mit der rechten Maustaste auf das Symbol für den Server klicken und im Kontextmenü **Verbindung mit diesem Server automatisch herstellen** auswählen.

---

5 Wenn Sie zur Eingabe von RSA SecurID- oder RADIUS-Authentifizierungs-Anmeldedaten aufgefordert werden, geben Sie den Benutzernamen und den Passcode ein und klicken Sie auf **Weiter**.

6 Geben Sie die Anmeldedaten eines Benutzers ein, der für die Verwendung von mindestens einem Desktop- oder Anwendungspool berechtigt ist, wählen Sie die Domäne aus und klicken Sie auf **Anmelden**.

Wenn Sie den Benutzernamen im Format **`Benutzername@Domäne`** eingeben, wird er aufgrund des At-Zeichens (@) als Benutzerprinzipalname (User Principal Name, UPN) behandelt, und das Dropdown-Menü **Domäne** wird deaktiviert.

Wenn das Dropdown-Menü **Domäne** ausgeblendet ist, müssen Sie den Benutzernamen in der Form ***`Benutzername@Domäne`*** oder ***`Domäne\Benutzername`*** eingeben.

7 (Optional) Zum Konfigurieren von Anzeigeeinstellungen für Remote-Desktops klicken Sie entweder mit der rechten Maustaste auf ein Desktop-Symbol oder wählen Sie ein Desktop-Symbol aus und klicken Sie im oberen Bereich des Bildschirms auf das Symbol **Einstellungen** (Zahnradsymbol) neben dem Servernamen.

Option	Beschreibung
Anzeigeprotokoll	Wenn Ihr Administrator dies gestattet, können Sie anhand der Liste **Verbinden über** das Anzeigeprotokoll auswählen. VMware Blast erfordert Horizon Agent 7.0 oder höher.
Anzeigelayout	Verwenden Sie die Liste **Anzeige**, um eine Fenstergröße auszuwählen oder mehrere Monitore zu verwenden.

8 (Optional) Wenn Sie den Remote-Desktop oder die Remoteanwendung als Favorit markieren möchten, klicken Sie mit der rechten Maustaste auf das Desktop- oder Anwendungssymbol und wählen Sie im angezeigten Kontextmenü **Als Favorit markieren** aus.

In der oberen rechten Ecke des Desktop- oder Anwendungsnamens wird ein Sternchensymbol angezeigt. Wenn Sie sich das nächste Mal anmelden, können Sie auf die Schaltfläche **Favoriten anzeigen** klicken, um die Favoritenanwendung oder den Favoriten-Desktop schnell zu finden.

9 Wenn Sie eine Verbindung mit einem Remote-Desktop oder einer Remoteanwendung herstellen möchten, doppelklicken Sie auf das entsprechende Symbol oder klicken Sie mit der rechten Maustaste auf das Symbol und wählen Sie im Kontextmenü **Starten** aus.

Wenn Sie eine Verbindung mit einem veröffentlichten Desktop auf einem Microsoft RDS-Host herstellen und für den Desktop bereits ein anderes Anzeigeprotokoll festgelegt ist, kann die Verbindung nicht sofort hergestellt werden. Sie werden aufgefordert, entweder das derzeit festgelegte Protokoll zu verwenden oder sich vom Remote-Betriebssystem abzumelden, damit eine Verbindung unter Verwendung des von Ihnen ausgewählten Protokolls hergestellt werden kann.

Nachdem die Verbindung hergestellt wurde, wird das Remote-Desktop-Fenster oder Remoteanwendungsfenster angezeigt. Wenn Sie zur Verwendung mehrerer Desktops oder Anwendungen berechtigt sind, bleibt das Fenster zur Desktop- und Anwendungsauswahl geöffnet, sodass Sie sich mit mehreren Elementen gleichzeitig verbinden können.

In diesem Dialogfeld können Sie den Zugriff auf Dateien Ihres lokalen Systems freigeben oder unterbinden. Weitere Informationen finden Sie unter „Freigegebener Zugriff auf lokale Ordner und Laufwerke“, auf Seite 81.

Wenn keine Authentifizierung beim Server möglich ist oder wenn der Client keine Verbindung mit dem Remote-Desktop oder der Remoteanwendung herstellen kann, führen Sie die folgenden Aufgaben aus:

- Legen Sie fest, ob der Verbindungsserver dahingehend konfiguriert werden soll, SSL nicht zu verwenden. Die Clientsoftware erfordert SSL-Verbindungen. Prüfen Sie, ob die globale Einstellung in Horizon Administrator für das Kontrollkästchen **SSL für Client-Verbindungen verwenden** deaktiviert ist. Ist dies der Fall, müssen Sie entweder das Kontrollkästchen markieren, sodass SSL verwendet wird, oder Ihre Umgebung so einrichten, dass die Clients eine Verbindung zu einem HTTPS-fähigen Lastenausgleich oder einem anderen Zwischengerät herstellen können, das zur Herstellung einer HTTP-Verbindung zum Verbindungsserver konfiguriert ist.
- Stellen Sie eine ordnungsgemäße Funktionsweise des Sicherheitszertifikats für den Verbindungsserver sicher. Ist dies nicht der Fall, wird in Horizon Administrator möglicherweise angezeigt, dass der Agent auf Desktops nicht erreichbar ist. Dies sind Hinweise auf zusätzliche Verbindungsprobleme, die durch Zertifikatprobleme verursacht werden.
- Stellen Sie sicher, dass die für die Verbindungsserver-Instanz festgelegten Kennzeichen Verbindungen von diesem Benutzer erlauben. Siehe das Dokument *Administration von View*.
- Stellen Sie sicher, dass der Benutzer zum Zugriff auf diesen Desktop oder diese Anwendung berechtigt ist. Weitere Erläuterungen finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.
- Wenn Sie das RDP-Anzeigeprotokoll zur Verbindungsherstellung mit einem Remote-Desktop verwenden, müssen Sie bestätigen, dass das Remote-Betriebssystem Remote-Desktop-Verbindungen zulässt.

Weiter

Konfigurieren Sie Startoptionen. Wenn Sie nicht möchten, dass Endbenutzer den Hostnamen der Verbindungsserver-Instanz eingeben müssen, oder wenn Sie andere Startoptionen konfigurieren möchten, verwenden Sie eine Befehlszeilenoption zum Erstellen einer Desktop-Verknüpfung. Siehe „Ausführen von Horizon Client über die Befehlszeile“, auf Seite 67.

Verwenden des nicht authentifizierten Zugriffs zur Verbindung mit Remoteanwendungen

Ein Horizon-Administrator kann mit der Funktion des nicht authentifizierten Zugriffs Benutzer für einen nicht authentifizierten Zugriff erstellen und diesen Benutzern Berechtigungen für Remoteanwendungen auf einer Verbindungsserver-Instanz erteilen. Benutzer für einen nicht authentifizierten Zugriff können sich anonym beim Server anmelden, um eine Verbindung zu ihren Remoteanwendungen herzustellen.

Standardmäßig wählen Benutzer die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** aus dem Menü **Optionen** und ein Benutzerkonto für eine anonyme Anmeldung aus. Ein Horizon-Administrator kann Gruppenrichtlinieneinstellungen für ein anderes Verhalten des nicht authentifiziertem Zugriff konfigurieren, sodass die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** bereits ausgewählt ist und Benutzer automatisch mit einem bestimmten Benutzerkonto für einen nicht authentifizierten Zugriff angemeldet werden.

Voraussetzungen

- Führen Sie die unter „Vorbereiten des Verbindungsservers für Horizon Client“, auf Seite 20 beschriebenen administrativen Aufgaben aus.
- Richten Sie Benutzer für einen nicht authentifizierten Zugriff auf der Verbindungsserver-Instanz ein. Informationen dazu finden Sie unter „Bereitstellen eines nicht authentifizierten Zugriffs für veröffentlichte Anwendungen“ im Dokument *Administration von View*.
- (Optional) Konfigurieren Sie die Gruppenrichtlinieneinstellungen **Konto für einen nicht authentifizierten Zugriff** und **Anonym mit nicht authentifiziertem Zugriff anmelden**, um das Standardverhalten für einen nicht authentifizierten Zugriff zu ändern. Weitere Informationen hierzu finden Sie unter „Einstellungen für die Skriptdefinition für Client-GPOs“, auf Seite 49.

Vorgehensweise

1 Doppelklicken Sie auf die Desktop-Verknüpfung **VMware Horizon Client** oder klicken Sie auf **Start > Programme > VMware Horizon Client**.

2 Wenn Sie von Ihrem Horizon-Administrator dazu angewiesen werden, klicken Sie in der Menüleiste auf die Schaltfläche **Optionen** und wählen Sie **Anonym mit nicht authentifiziertem Zugriff anmelden** aus.

Je nach Konfiguration Ihres Clientsystems ist diese Einstellung eventuell bereits ausgewählt.

3 (Optional) Zur Festlegung des Zertifikatsprüfungsmodus klicken Sie auf die Schaltfläche **Optionen** in der Menüleiste und wählen Sie **SSL konfigurieren** aus.

Sie können diese Option nur konfigurieren, wenn Ihr Administrator dies zugelassen hat.

4 Stellen Sie eine Verbindung mit dem Server her, auf dem Sie über einen nicht authentifizierten Zugriff auf Remoteanwendungen verfügen.

Option	Aktion
Verbindung mit einem neuen Server herstellen	Doppelklicken Sie auf die Schaltfläche **+ Server hinzufügen** oder klicken Sie auf die Schaltfläche **+ Neuer Server** in der Menüleiste, geben Sie den Namen des Servers ein und klicken Sie auf **Verbinden**.
Verbindung mit einem vorhandenen Server herstellen	Doppelklicken Sie auf das Serversymbol auf der Startseite von Horizon Client.

Verbindungen zwischen Horizon Client und dem Verbindungsserver verwenden immer SSL. Der Standardport für SSL-Verbindungen ist 443. Wenn der Verbindungsserver nicht zur Verwendung des Standardports konfiguriert ist, muss das in folgendem Beispiel gezeigte Format verwendet werden: `view.firma.com:1443`.

Es wird eventuell eine Meldung eingeblendet, die Sie bestätigen müssen, bevor das Anmeldedialogfenster angezeigt wird.

5 Wenn das Anmeldedialogfeld angezeigt wird, wählen Sie ein Benutzerkonto aus dem Dropdown-Menü **Benutzerkonto** aus, falls erforderlich.

Wenn nur ein Benutzerkonto verfügbar ist, ist das Dropdown-Menü deaktiviert und das Benutzerkonto wird automatisch ausgewählt.

6 (Optional) Wenn das Kontrollkästchen **Immer dieses Konto verwenden** verfügbar ist, aktivieren Sie dieses zur Umgehung des Anmeldedialogfeldes bei der nächsten Herstellung einer Verbindung mit dem Server.

Sie können diese Option deaktivieren, bevor Sie das nächste Mal eine Verbindung mit dem Server herstellen, indem Sie mit der rechten Maustaste auf das Serversymbol auf der Horizon Client-Startseite klicken und **Gespeichertes Konto mit nicht authentifiziertem Zugriff löschen** auswählen.

7 Klicken Sie auf **Anmelden**, um sich beim Server anzumelden.

Das Auswahlfenster für Anwendungen wird angezeigt.

8 Doppelklicken Sie auf das jeweilige Anwendungssymbol, um die Anwendung zu starten.

Tipps zur Verwendung der Desktop- und Anwendungsauswahl

Zur einfacheren Handhabung können Sie die Anzahl der Symbole im Bildschirm für die Desktop- und Anwendungsauswahl von Horizon Client neu anordnen oder reduzieren.

Nachdem Sie sich authentifiziert und mit einem bestimmten Server verbunden haben, wird ein Fenster mit Symbolen für alle Remote-Desktops und Remoteanwendungen angezeigt, die Sie verwenden dürfen. Anhand der folgenden Vorschläge können Sie die am häufigsten verwendeten Remote-Desktops und Remoteanwendungen schnell starten:

- Geben Sie die ersten Buchstaben des Namens ein. Wenn z. B. Symbole für Paint, PowerPoint und Publisher vorhanden sind, können Sie **pa** eingeben, um Paint auszuwählen.

  Sofern mehrere Elemente mit den eingegebenen Buchstaben anfangen, können Sie durch Drücken von F4 zum nächsten übereinstimmenden Element übergehen. Wird das letzte Element erreicht, kehren Sie durch Drücken von F4 wieder zum ersten übereinstimmenden Element zurück.

- Markieren Sie ein Symbol als Favorit, indem Sie mit der rechten Maustaste auf das Symbol klicken und im Kontextmenü **Als Favorit markieren** auswählen. Klicken Sie nach der Auswahl von Favoriten auf die Schaltfläche **Favoritenansicht anzeigen** (Sternsymbol), um alle Symbole zu entfernen, bei denen es sich nicht um Favoriten handelt.

- Wählen Sie in der Favoritenansicht ein Symbol aus und ziehen Sie es an eine neue Position, um die Reihenfolge der Symbole zu ändern. Wenn Sie sich nicht in der Favoritenansicht befinden, werden standardmäßig zuerst Desktop-Symbole in alphabetischer Reihenfolge gefolgt von Anwendungssymbolen in alphabetischer Reihenfolge aufgeführt. Sie können Symbole in der Favoritenansicht durch Ziehen und Ablegen neu anordnen.

  Die Reihenfolge der Symbole wird entweder zum Zeitpunkt der Trennung der Verbindung zum Server oder beim Starten einer Anwendung oder eines Desktops auf dem verwendeten Server gespeichert. Wenn Sie die Verbindung zum Server nicht manuell trennen oder kein Element starten, werden Ihre Änderungen nicht gespeichert.

- Erstellen Sie eine Verknüpfung, sodass Sie vom eigenen lokalen Desktop aus auf den Remote-Desktop oder die Anwendung zugreifen können, ohne das Auswahlfenster zu öffnen. Klicken Sie mit der rechten Maustaste auf das Symbol und wählen Sie im Kontextmenü **Verknüpfung erstellen** aus.

- Klicken Sie mit der rechten Maustaste auf das Symbol für den Remote-Desktop bzw. die Remoteanwendung und wählen Sie im Kontextmenü **Zum Startmenü hinzufügen** aus, sodass Sie von Ihrem eigenen lokalen Startmenü aus auf den Remote-Desktop oder die Remoteanwendung zugreifen können und das Auswahlfenster nicht benötigt wird.

Hinweis Bei Verwendung von Windows 7 oder eines neueren Clientsystems können Sie nach der Herstellung der Verbindung mit einem Server, einem Desktop oder einer Anwendung Horizon Client öffnen und mit der rechten Maustaste auf das Symbol von Horizon Client in der Windows-Taskleiste klicken, um den zuletzt verwendeten Server oder Desktop bzw. die zuletzt verwendete Anwendung auszuwählen. Es werden bis zu 10 Elemente in der Liste aufgeführt. Um ein Element zu entfernen, klicken Sie mit der rechten Maustaste darauf und wählen **Aus dieser Liste entfernen** aus.

Wenn Sie mit der rechten Maustaste auf das Horizon Client-Symbol in der Taskleiste klicken und keine Sprungliste angezeigt wird, klicken Sie mit der rechten Maustaste auf die Taskleiste, wählen Sie **Eigenschaften** und klicken Sie auf die Registerkarte **Startmenü**. Aktivieren Sie im Abschnitt „Datenschutz“ das Kontrollkästchen **Zuletzt geöffnete Elemente im Startmenü und in der Taskleiste speichern und anzeigen** und klicken Sie auf **OK**.

Freigegebener Zugriff auf lokale Ordner und Laufwerke

Sie können Horizon Client zur Freigabe von Ordnern und Laufwerken auf Ihren lokalen Systemen für Remote-Desktops und Remoteanwendungen konfigurieren. Zu Laufwerken können auch zugeordnete Laufwerke und USB-Speichergeräte gehören. Diese Funktion wird als Clientlaufwerksumleitung bezeichnet.

In einem Windows-Remote-Desktop werden freigegebene Ordner und Laufwerke im Abschnitt **Geräte und Laufwerke** im Ordner **Dieser PC** oder im Abschnitt **Andere** im Ordner **Computer** je nach verwendetem Windows-Betriebssystem angezeigt. In einer Remoteanwendung (z. B. Editor) können Sie zu einer Datei in einem freigegeben Ordner oder auf einem freigegebenem Laufwerk wechseln und diese öffnen. Die für die Freigabe ausgewählten Ordner und Laufwerke erscheinen im Dateisystem als Netzwerklaufwerke mit dem Namensformat ***Name*** **unter** ***COMPUTERNAME***.

Um die Einstellungen für die Clientlaufwerksumleitung zu konfigurieren, müssen Sie nicht mit einem Remote-Desktop oder mit einer Remoteanwendung verbunden sein. Diese Einstellungen gelten für Ihre gesamten Remote-Desktops und Remoteanwendungen. Das bedeutet, dass lokale Clientordner nicht nur für einen Remote-Desktop oder eine Remoteanwendung freigegeben werden können. Die konfigurierte Freigabe gilt immer für alle Remote-Desktops oder Remoteanwendungen.

Sie können auch die Funktion zum Öffnen von lokalen Dateien mit Remoteanwendungen direkt aus dem lokalen Dateisystem aktivieren. Wenn Sie mit der rechten Maustaste auf eine lokale Datei klicken, führt das Menü **Öffnen mit** auch die verfügbaren Remoteanwendungen auf. Sie können Dateien auch so einstellen, dass sie automatisch mit Remoteanwendungen geöffnet werden, wenn Sie darauf doppelklicken. Wenn Sie diese Funktion aktivieren, werden alle Dateien in Ihrem lokalen Dateisystem mit einer bestimmten Dateierweiterung bei dem Server registriert, auf dem Sie angemeldet sind. Wenn beispielsweise Microsoft Word eine der verfügbaren Remoteanwendungen des Servers ist, können Sie mit der rechten Maustaste auf eine `.docx`-Datei in Ihrem lokalen Dateisystem klicken und sie mit der MS Word-Remoteanwendung öffnen. Diese Funktion erfordert Horizon 6.2-Server und -Agents.

Ein Administrator kann die Funktion der Clientlaufwerksumleitung in Horizon Client durch Aktivierung einer Gruppenrichtlinieneinstellung ausblenden. Weitere Informationen finden Sie unter **Deaktivieren der Freigabe von Dateien und Ordnern** in Tabelle 3-7.

Die Konfiguration des Browsers auf dem Clientsystem für die Verwendung eines Proxy-Servers kann die Leistung der Clientlaufwerksumleitung reduzieren, wenn für die Verbindungsserver-Instanz der sichere Tunnel aktiviert ist. Für eine optimale Leistung der Clientlaufwerksumleitung konfigurieren Sie den Browser so, dass kein Proxy-Server verwendet wird oder dass die LAN-Einstellungen automatisch ermittelt werden.

Voraussetzungen

Um Ordner und Laufwerke für einen Remote-Desktop oder eine Remoteanwendung freizugeben, müssen Sie die Funktion der Clientlaufwerksumleitung aktivieren. Diese Aufgabe beinhaltet die Installation von View Agent 6.1.1 oder höher oder von Horizon Agent 7.0 oder höher und die Aktivierung der Agentenoption **Clientlaufwerksumleitung**. Außerdem besteht die Möglichkeit, Richtlinien zur Steuerung des Verhaltens der Laufwerksumleitung festzulegen. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Vorgehensweise

1 Öffnen Sie das Dialogfeld „Einstellungen“ mit dem Bereich „Freigabe“.

Option	Beschreibung
Im Fenster für die Desktop- und Anwendungsauswahl	Klicken Sie mit der rechten Maustaste auf ein Desktop- oder Anwendungssymbol, wählen Sie **Einstellungen** aus und dann **Freigabe** im linken Bereich des eingeblendeten Fensters.
Im bei der Verbindung mit einem Desktop oder mit einer Anwendung eingeblendeten Dialogfeld „Freigabe“	Klicken Sie im Dialogfeld auf den Link **Einstellungen > Freigabe**.
Aus einem Desktop-Betriebssystem heraus	Wählen Sie in der Menüleiste **Optionen > Ordner freigeben** aus.

2 Konfigurieren Sie die Einstellungen für die Clientlaufwerksumleitung.

Option	Aktion
Freigeben eines bestimmten Ordners oder Laufwerks für Remote-Desktops und Remoteanwendungen	Klicken Sie auf die Schaltfläche **Hinzufügen**, wechseln Sie zum Ordner oder Laufwerk, der/das freigegeben werden soll und klicken Sie auf **OK**. **Hinweis** Sie können keinen Ordner auf einem USB-Gerät freigeben, das bereits mit einem Remote-Desktop oder mit einer Remoteanwendung über die USB-Umleitungsfunktion verbunden ist. Darüber hinaus sollten Sie nicht die Funktion zur USB-Umleitung aktivieren, die USB-Geräte automatisch beim Start oder beim Anschließen des Geräts verbindet. In diesem Fall wird beim nächsten Start von Horizon Client oder beim Anschließen des USB-Geräts dieses mithilfe der Funktion zur USB-Umleitung verbunden und nicht mithilfe der Funktion zur Clientlaufwerksumleitung.
Freigabe für einen bestimmten Ordner oder ein bestimmtes Laufwerk aufheben	Wählen Sie den Ordner oder das Laufwerk in der Ordnerliste aus und klicken Sie auf die Schaltfläche **Entfernen**.
Erlauben Sie Remote-Desktops und Remoteanwendungen den Zugriff auf Dateien in Ihrem lokalen Benutzerordner	Aktivieren Sie das Kontrollkästchen **Ihre lokalen Dateien freigeben *Benutzername***.
Geben Sie die USB-Speichergeräte für Remote-Desktops und -anwendungen frei.	Aktivieren Sie das Kontrollkästchen **Zugriff auf Wechselmedien erlauben**. Die Funktion der Clientlaufwerksumleitung gibt alle USB-Speichergeräte in Ihrem Clientsystem und alle über FireWire und Thunderbolt verbundenen externe Laufwerke frei. Sie müssen kein bestimmtes Laufwerk für die Freigabe auswählen. **Hinweis** USB-Speichergeräte, die bereits über die Funktion zur USB-Umleitung mit einem Remote-Desktop oder mit einer Remoteanwendung verbunden sind, werden nicht freigegeben. Wenn dieses Kontrollkästchen deaktiviert ist, können Sie mit der Funktion zur USB-Umleitung USB-Speichergeräte mit Remote-Desktops und Remoteanwendungen verbinden.

Option	Aktion
Aktivieren Sie die Möglichkeit, eine lokale Datei mit einer Remoteanwendung aus dem lokalen Dateisystem zu öffnen.	Aktivieren Sie das Kontrollkästchen **Lokale Dateien in gehosteten Anwendungen öffnen**. Mit dieser Option können Sie mit der rechten Maustaste auf eine Datei in Ihrem lokalen Dateisystem klicken und diese wahlweise mit einer Remoteanwendung öffnen. Sie können zudem die Eigenschaften der Datei ändern, sodass alle Dateien mit dieser Dateierweiterung standardmäßig mit der Remoteanwendung geöffnet werden, etwa wenn Sie auf die Datei doppelklicken. Sie können beispielsweise mit der rechten Maustaste auf die Datei klicken, die Option **Eigenschaften** auswählen und auf **Ändern** klicken, um die Remoteanwendung zum Öffnen dieses Dateityps auszuwählen. Ihr Administrator hat die Möglichkeit, diese Funktion zu deaktivieren.
Dialogfeld „Freigabe“ beim Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung nicht anzeigen	Aktivieren Sie das KontrollkästchenDialogfeld bei der Verbindung mit einem Desktop oder einer Anwendung nicht anzeigen. Wenn dieses Kontrollkästchen deaktiviert ist, erscheint das Dialogfeld „Freigabe“, wenn Sie nach der Verbindung mit einem Server zum ersten Mal eine Verbindung mit einem Desktop oder einer Anwendung herstellen. Melden Sie sich beispielsweise bei einem Server an und stellen Sie eine Verbindung zu einem Desktop her, wird das Dialogfeld „Freigabe“ eingeblendet. Wenn Sie dann eine Verbindung zu einem anderen Desktop oder zu einer anderen Anwendung herstellen, wird das Dialogfeld nicht mehr angezeigt. Um das Dialogfeld wieder einzublenden, müssen Sie die Verbindung zum Server trennen und sich erneut anmelden.

Weiter

Stellen Sie sicher, dass die freigegebenen Ordner im Remote-Desktop oder in der Remoteanwendung erscheinen.

- Öffnen Sie in einem Windows-Remote-Desktop den Datei-Explorer und wechseln Sie dann zum Abschnitt **Geräte und Laufwerke** im Ordner **Dieser PC** oder öffnen Sie Windows Explorer und wechseln Sie dann zum Abschnitt **Andere** im Ordner **Computer**.
- Wählen Sie gegebenenfalls in einer Remoteanwendung **Datei > Öffnen** oder **Datei > Speichern unter** aus und wechseln Sie zum Ordner oder Laufwerk, das im Dateisystem als das Netzwerklaufwerk mit dem Namensformat ***Ordnername* auf *COMPUTERNAME*** erscheint.

Ausblenden des VMware Horizon Client -Fensters

Sie können das VMware Horizon Client-Fenster nach dem Öffnen eines Remote-Desktops oder einer Remoteanwendung ausblenden.

Außerdem können Sie mit einer speziellen Voreinstellung festlegen, dass das VMware Horizon Client-Fenster nach dem Öffnen eines Remote-Desktops oder einer Remoteanwendung immer ausgeblendet wird.

Hinweis Administratoren können anhand einer Gruppenrichtlinieneinstellung konfigurieren, ob nach dem Öffnen von Remote-Desktops oder Remoteanwendungen das Fenster immer ausgeblendet wird.

Weitere Informationen finden Sie unter „Allgemeine Einstellungen für Client-GPOs“, auf Seite 58.

Vorgehensweise

- Zum Ausblenden des VMware Horizon Client-Fensters nach dem Öffnen eines Remote-Desktops oder einer Remoteanwendung klicken Sie in der Ecke des VMware Horizon Client-Fensters auf die Schaltfläche **Schließen**.
- Um einzustellen, dass das VMware Horizon Client-Fenster nach dem Öffnen eines Remote-Desktops oder einer Remoteanwendung immer ausgeblendet wird, bevor Sie eine Verbindung zu einem Server herstellen, klicken Sie in der Menüleiste auf **Optionen** und wählen Sie **Selektor nach Start eines Elements ausblenden** aus.

- Um das VMware Horizon Client-Fenster anzuzeigen, nachdem es ausgeblendet wurde, klicken Sie mit der rechten Maustaste auf das VMware Horizon Client-Symbol im Infobereich und wählen Sie **VMware Horizon Client anzeigen** oder klicken Sie, wenn Sie bei einem Remote-Desktop angemeldet sind, in der Menüleiste auf die Schaltfläche **Optionen** und wählen Sie **Zu einem anderen Desktop wechseln**.

Erneute Verbindungsherstellung mit einem Desktop oder einer Anwendung

Aus Sicherheitsgründen legen Administratoren Zeitüberschreitungen fest, mit denen nach Ablauf einer bestimmten Anzahl von Stunden eine Abmeldung von einem Server erfolgt und eine Remoteanwendung nach einer bestimmten Anzahl von Minuten der Inaktivität gesperrt wird.

Wenn eine Remoteanwendung eine bestimmte Zeit lang nicht verwendet wird, wird mit der View 6.0-Remoteanwendungsfunktion 30 Sekunden vor der automatischen Sperrung der Anwendung eine Warnung ausgegeben. Erfolgt keine Reaktion auf diese Warnung, wird die Anwendung gesperrt. Standardmäßig wird die Zeitsperre nach 15 Minuten der Inaktivität aktiviert, doch kann ein Administrator dies ändern.

Wenn z. B. eine oder mehrere Anwendungen geöffnet sind und Sie den Computer verlassen, sind die Anwendungsfenster möglicherweise nicht mehr geöffnet, wenn Sie eine Stunde später zurückzukehren. Stattdessen kann ein Dialogfeld angezeigt werden, in dem Sie zum Klicken auf die Schaltfläche **OK** aufgefordert werden, damit die Anwendungsfenster erneut geöffnet werden.

Der Zeitraum der Zeitüberschreitung des Servers wird normalerweise auf eine bestimmte Anzahl von Stunden der Inaktivität eingestellt. Standardmäßig müssen Sie sich erneut anmelden, wenn Horizon Client mehr als 10 Stunden lang geöffnet und mit einem Server verbunden ist. Diese Zeitüberschreitung gilt unabhängig davon, ob Sie mit einer Remoteanwendung oder einem Remote-Desktop verbunden sind.

Um diese Zeitüberschreitungseinstellungen zu konfigurieren, wechseln Sie in Horizon Administrator zu **Globale Einstellungen** und bearbeiten Sie die allgemeinen Einstellungen.

Erstellen einer Desktop- oder Anwendungsverknüpfung auf Ihrem Client-Desktop oder im Startmenü

Sie können eine Verknüpfung für einen Remote-Desktop oder eine Remoteanwendung erstellen. Verknüpfungen werden auf Ihrem Client-Desktop genau wie Verknüpfungen für lokal installierte Anwendungen angezeigt. Sie können zudem ein Startmenüelement erstellen, das unter „Programme“ angezeigt wird.

Vorgehensweise

1 Starten Sie Horizon Client und melden Sie sich beim Server an.

2 Klicken Sie im Menü zur Desktop- und Anwendungsauswahl mit der rechten Maustaste auf eine Anwendung oder einen Desktop und wählen Sie **Verknüpfung erstellen** oder **Zum Startmenü hinzufügen** im daraufhin geöffneten Kontextmenü aus.

Je nach ausgewähltem Befehl wird eine Verknüpfung auf Ihrem Client-Desktop oder im Startmenü Ihres Clientsystems erstellt.

Weiter

Sie können diese Verknüpfung umbenennen, löschen oder andere Aktionen für sie ausführen, die sich auf lokal installierte Anwendungen anwenden lassen. Sofern Sie noch nicht beim Server angemeldet sind, werden Sie beim Verwenden der Verknüpfung zur Anmeldung aufgefordert, bevor das Fenster für den Remote-Desktop bzw. die Remoteanwendung geöffnet wird.

Wechseln zwischen Desktops oder Anwendungen

Wenn Sie mit einem Remote-Desktop verbunden sind, können Sie zu einem anderen Desktop wechseln. Sie können auch eine Verbindung mit Remoteanwendungen herstellen, während Sie mit einem Remote-Desktop verbunden sind.

Vorgehensweise

- Wählen Sie einen Remote-Desktop oder eine Remoteanwendung auf demselben oder einem anderen Server aus.

Option	Aktion
Einen anderen Desktop oder eine andere Anwendung auf demselben Server auswählen	Führen Sie einen der folgenden Schritte aus: ■ Wenn Sie zurzeit bei einem Remote-Desktop angemeldet sind, wählen Sie **Optionen > Zu einem anderen Desktop wechseln** in der Horizon Client-Menüleiste aus und wählen Sie dann einen Desktop oder eine Anwendung zum Starten. ■ Wenn Sie zurzeit bei einer Remoteanwendung angemeldet sind, klicken Sie mit der rechten Maustaste auf das **VMware Horizon Client**-Symbol im Infobereich und wählen Sie **VMware Horizon Client anzeigen**, um das Fenster für die Desktop- und Anwendungsauswahl anzuzeigen, und doppelklicken Sie auf das Symbol für den anderen Desktop bzw. die andere Anwendung. ■ Doppelklicken Sie im Fenster für die Desktop- und Anwendungsauswahl auf das Symbol für den anderen Desktop bzw. die andere Anwendung. Der Desktop oder die Anwendung wird in einem neuen Fenster geöffnet, sodass mehrere Fenster geöffnet sind und Sie zwischen diesen wechseln können.
Einen anderen Desktop oder eine andere Anwendung auf einem anderen Server auswählen	Führen Sie einen der folgenden Schritte aus: ■ Wenn der aktuelle Desktop bzw. die aktuelle Anwendung geöffnet bleiben soll und Sie außerdem eine Verbindung mit einem Remote-Desktop bzw. einer Anwendung auf einem anderen Server herstellen möchten, starten Sie eine neue Instanz von Horizon Client und stellen Sie eine Verbindung mit dem anderen Desktop bzw. der anderen Anwendung her. ■ Wenn Sie den aktuellen Desktop schließen und eine Verbindung mit einem Desktop auf einem anderen Server herstellen möchten, wechseln Sie zum Fenster für die Desktop-Auswahl, klicken Sie in der oberen linke Ecke des Fensters auf das Symbol **Trennen** und bestätigen Sie, dass Sie sich vom Server abmelden möchten. Sie werden vom aktuellen Server und allen offenen Desktop-Sitzungen abgemeldet. Sie können anschließend eine Verbindung mit einem anderen Server herstellen.

Abmelden oder trennen

Wenn Sie die Verbindung mit einem Remote-Desktop trennen, ohne sich abzumelden, bleiben bei einigen Konfigurationen die Anwendungen im Desktop geöffnet. Sie können auch die Verbindung mit einem Server trennen und Remoteanwendungen geöffnet lassen.

Selbst wenn Sie keinen Remote-Desktop geöffnet haben, können Sie sich vom Remote-Desktop-Betriebssystem abmelden. Die Verwendung dieser Option hat dieselbe Funktion, wie wenn Sie die Tastenkombination Strg+Alt+Delete drücken und anschließend auf **Abmelden** klicken.

Hinweis Die Eingabe der Windows-Tastenkombination Strg+Alt+Entf wird für Remote-Desktops nicht unterstützt. Klicken Sie, um dieselben Resultate wie bei einer Betätigung von Strg+Alt+Entf zu erzielen, in der Menüleiste auf die Schaltfläche **Strg+Alt+Entf senden**. Alternativ können Sie in den meisten Fällen auch die Tastenkombination Strg+Alt+Einfg betätigen.

Vorgehensweise

- Trennen Sie die Verbindung mit einem Remote-Desktop, ohne sich abzumelden.

Option	Aktion
Vom Remote-Desktop-Fenster aus	Führen Sie einen der folgenden Schritte aus: ■ Klicken Sie auf die Schaltfläche **Schließen** in der Ecke des Desktop-Fensters. ■ Wählen Sie in der Menüleiste des Desktop-Fensters **Optionen > Verbindung trennen** aus.
Im Fenster für die Desktop- und Anwendungsauswahl	Das Fenster für die Desktop- und Anwendungsauswahl ist geöffnet, wenn Sie über Berechtigungen für mehrere Desktops oder Anwendungen auf dem Server verfügen. Klicken Sie in der oberen linken Ecke des Fensters für die Desktop-Auswahl auf das Symbol **Verbindung zu diesem Server trennen** und anschließend im Warnungsfeld auf **Ja**.

Hinweis Der Administrator kann Ihren Desktop so konfigurieren, dass Sie beim Trennen der Verbindung automatisch abgemeldet werden. In diesem Fall werden alle geöffneten Programme auf Ihrem Desktop angehalten.

- Melden Sie sich ab und trennen Sie die Verbindung mit einem Remote-Desktop.

Option	Aktion
Aus dem Desktop-Betriebssystem heraus	Melden Sie sich über das Windows-**Start**-Menü ab.
Über die Menüleiste	Wählen Sie **Optionen > Verbindung trennen und abmelden** aus. Bei Verwendung dieser Option werden alle Dateien, die auf dem Remote-Desktop geöffnet sind, ohne vorheriges Speichern geschlossen.

- Trennen Sie die Verbindung mit einer Remoteanwendung.

Option	Aktion
Die Verbindung zur Anwendung, aber nicht die Verbindung zum Server trennen	Beenden Sie die Anwendung auf die übliche Weise. Klicken Sie beispielsweise in der Ecke des Anwendungsfensters auf die Schaltfläche **Schließen**.
Die Verbindung zur Anwendung und zum Server trennen	Führen Sie einen der folgenden Schritte aus: ■ Klicken Sie in der oberen linken Ecke des Fensters für die Anwendungsauswahl auf das Symbol **Verbindung zu diesem Server trennen** und anschließend im Warnungsfeld auf **Ja**. ■ Klicken Sie mit der rechten Maustaste auf das Horizon Client-Symbol im Infobereich und wählen Sie **Beenden**.
Schließen Sie das Fenster für die Anwendungsauswahl, beenden Sie die Anwendung jedoch nicht.	Durch Klicken auf die Schaltfläche **Schließen** wird nur das Anwendungsauswahlfenster geschlossen.

- Melden Sie sich ab, wenn kein Remote-Desktop geöffnet ist.

  Bei Verwendung dieser Option werden alle Dateien, die auf dem Remote-Desktop geöffnet sind, ohne vorheriges Speichern geschlossen.

  a Starten Sie Horizon Client, stellen Sie eine Verbindung mit dem Server her, der einen Zugriff auf den Remote-Desktop bietet, und geben Sie Ihre Anmeldeinformationen für die Authentifizierung an.

  b Klicken Sie mit der rechten Maustaste auf das Desktop-Symbol und wählen Sie **Abmelden**.

Arbeiten mit einem Remote-Desktop oder einer Remoteanwendung 5

Horizon bietet die vertraute, individuell angepasste Desktop- und Anwendungsumgebung, die Benutzer erwarten. Benutzer können auf an ihren lokalen Computer angeschlossene USB- und andere Geräte zugreifen, Dokumente an beliebige Drucker senden, die von ihrem lokalen Computer erkannt werden, eine Authentifizierung mithilfe von Smartcards durchführen und mehrere Anzeigemonitore verwenden.

Dieses Kapitel behandelt die folgenden Themen:

Funktionsunterstützungs-Matrix für Windows-Clients

Einige Funktionen werden auf manchen Horizon Client-Typen unterstützt, auf anderen nicht.

Halten Sie sich bei der Planung der Anzeigeprotokolle und Funktionen, die Sie Ihren Benutzern zur Verfügung stellen möchten, an die folgenden Informationen, um zu bestimmen, welche Clientbetriebssysteme die jeweilige Funktion unterstützen.

Tabelle 5-1. Auf Windows-basierten Horizon Client -Systemen unterstützte Remote-Desktop-Funktionen

Funktion	Windows XP Desktop (View Agent 6.0.2 und niedriger)	Windows Vista Desktop (View Agent 6.0.2 und niedriger)	Windows 7-Desktop	Windows 8.x-Desktop	Windows 10-Desktop	Windows Server 2008/2012 R2 Desktop oder Windows Server 2016 Desktop
USB-Umleitung	Begrenzt	Begrenzt	X	X	X	X
Clientlaufwerksumleitung			X	X	X	X
Echtzeit-Audio/Video (RTAV)	Begrenzt	Begrenzt	X	X	X	X
Scannerumleitung		Begrenzt	X	X	X	X
Umleitung serieller Ports			X	X	X	X
VMware Blast-Anzeigeprotokoll			X	X	X	X
RDP-Anzeigeprotokoll	Begrenzt	Begrenzt	X	X	X	X
PCoIP-Anzeigeprotokoll	Begrenzt	Begrenzt	X	X	X	X
Persona-Verwaltung	Begrenzt	Begrenzt	X	X		
Wyse MMR	Begrenzt	Begrenzt				
Windows Media MMR			X	X	X	
Standortbasierter Druck	Begrenzt	Begrenzt	X	X	X	X
Virtuelles Drucken	Begrenzt	Begrenzt	X	X	X	X
Smartcards	Begrenzt	Begrenzt	X	X	X	X
RSA SecurID oder RADIUS	Begrenzt	Begrenzt	X	X	X	X
Einmaliges Anmelden	Begrenzt	Begrenzt	X	X	X	X
Mehrere Monitore	Begrenzt	Begrenzt	X	X	X	X

Windows 10-Desktops erfordern View Agent 6.2 oder höher oder Horizon Agent 7.0 oder höher. Windows Server 2012 R2-Desktops erfordern View Agent 6.1 oder höher oder Horizon Agent 7.0 oder höher.

Wichtig Windows XP- und Windows Vista-Desktops werden von View Agent 6.1 und neueren Versionen nicht unterstützt. View Agent 6.0.2 ist die letzte Version von View, die diese Gastbetriebssysteme unterstützt. Kunden, die über einen Vertrag mit Microsoft über erweiterten Support für Windows XP und Windows Vista sowie über einen Vertrag mit VMware über erweiterten Support für diese Gastbetriebssysteme verfügen, können View Agent 6.0.2 ihrer Windows XP- und Windows Vista-Desktops mit View-Verbindungsserver 6.1 bereitstellen.

Informationen darüber, welche Editionen bzw. Service Packs der einzelnen Clientbetriebssysteme unterstützt werden, finden Sie unter „Systemanforderungen für Windows-Clients“, auf Seite 10.

Funktionsunterstützung für veröffentlichte Desktops auf RDS-Hosts

RDS-Hosts sind Server-Computer, auf denen Windows-Remotedesktopdienste und View Agent oder Horizon Agent installiert sind. Mehrere Benutzer können gleichzeitig über Desktop-Sitzungen auf einem RDS-Host verfügen. Ein RDS-Host kann ein physischer Computer oder eine virtuelle Maschine sein.

Hinweis Die folgende Tabelle enthält nur Zeilen für die unterstützten Funktionen. Wenn im Text Mindestversionen von View Agent festgelegt sind, gilt die Angabe „und höher“ auch für Horizon Agent 7.0.x und höher.

Tabelle 5-2. Unterstützte Funktionen für RDS-Hosts mit installiertem View Agent 6.0.x oder höher oder mit Horizon Agent 7.0.x oder höher

Funktion	Windows Server 2008 R2 RDS-Host	Windows Server 2012 RDS-Host	Windows Server 2016 RDS-Host
RSA SecurID oder RADIUS	X	X	Horizon Agent 7.0.2 und höher
Smartcard	View Agent 6.1 und höher	View Agent 6.1 und höher	Horizon Agent 7.0.2 und höher
Einmaliges Anmelden	X	X	Horizon Agent 7.0.2 und höher
RDP-Anzeigeprotokoll (für Desktop-Clients)	X	X	Horizon Agent 7.0.2 und höher
PCoIP-Anzeigeprotokoll	X	X	Horizon Agent 7.0.2 und höher
VMware Blast-Anzeigeprotokoll	Horizon Agent 7.0 und höher	Horizon Agent 7.0 und höher	Horizon Agent 7.0.2 und höher
HTML Access	View Agent 6.0.2 und höher (nur virtuelle Maschine)	View Agent 6.0.2 und höher (nur virtuelle Maschine)	Horizon Agent 7.0.2 und höher
Windows Media MMR	View Agent 6.1.1 und höher	View Agent 6.1.1 und höher	Horizon Agent 7.0.2 und höher
USB-Umleitung (nur USB-Speichergeräte)		View Agent 6.1 und höher	Horizon Agent 7.0.2 und höher
Clientlaufwerksumleitung	View Agent 6.1.1 und höher	View Agent 6.1.1 und höher	Horizon Agent 7.0.2 und höher
Virtuelles Drucken (für Desktop-Clients)	View Agent 6.0.1 und höher (nur virtuelle Maschine)	View Agent 6.0.1 und höher (nur virtuelle Maschine)	Horizon Agent 7.0.2 und höher (nur virtuelle Maschine)
Scannerumleitung	View Agent 6.0.2 und höher	View Agent 6.0.2 und höher	Horizon Agent 7.0.2 und höher
Standortbasierter Druck	View Agent 6.0.1 und höher (nur virtuelle Maschine)	View Agent 6.0.1 und höher (nur virtuelle Maschine)	Horizon Agent 7.0.2 und höher (nur virtuelle Maschine)
Mehrere Monitore (für Desktop-Clients)	X	X	Horizon Agent 7.0.2 und höher
Unity Touch (für mobile und Chrome OS-Clients)	X	X	Horizon Agent 7.0.2 und höher
Echtzeit-Audio/Video (RTAV)	Horizon Agent 7.0.2 und höher	Horizon Agent 7.0.2 und höher	Horizon Agent 7.0.3 und höher

Informationen darüber, welche Editionen bzw. Service Packs der einzelnen Gastbetriebssysteme unterstützt werden, finden Sie im Dokument *View-Installation*.

Einschränkungen für Sonderfunktionen

Für Funktionen, die auf Windows-basierten Clients unterstützt werden, gelten die folgenden Einschränkungen.

Tabelle 5-3. Anforderungen für Sonderfunktionen

Funktion	Anforderungen
Windows Media MMR	Erfordert View View Agent 6.0.2 oder höher. Für die Verwendung der Windows-Multimedia-Umleitung (MMR) mit RDS-Desktops müssen Sie über View Agent 6.1.1 oder höher oder über Horizon Agent 7.0 oder höher verfügen. Wenn Sie das VMware Blast-Anzeigeprotokoll verwenden, müssen Sie über Horizon Agent 7.0 oder höher verfügen.
Umleitung serieller Ports	Erfordert View View Agent 6.1.1 oder höher. Windows 10 erfordert View Agent 6.2 oder höher oder Horizon Agent 7.0 oder höher. Wenn Sie das VMware Blast-Anzeigeprotokoll verwenden, müssen Sie über Horizon Agent 7.0 oder höher verfügen.
Virtuelles und standortbasiertes Drucken für Windows Server 2008 R2 Desktops, RDS-Desktops (auf RDS-Hosts auf virtueller Maschine) und Remoteanwendungen	Erfordert Horizon 6.0.1 mit View oder höher. Wenn Sie das VMware Blast-Anzeigeprotokoll für diese Funktion verwenden, müssen Sie über Horizon Agent 7.0 oder höher verfügen.
Scannerumleitung	Erfordert View View Agent 6.0.2 oder höher. Benötigt das PCoIP-Anzeigeprotokoll. Windows 10 erfordert View Agent 6.2 oder höher oder Horizon Agent 7.0 oder höher. Wenn Sie das VMware Blast-Anzeigeprotokoll verwenden, müssen Sie über Horizon Agent 7.0 oder höher verfügen.
Clientlaufwerksumleitung	Einzelplatz-Desktops mit einer virtuellen Maschine und veröffentlichte Desktops auf RDS-Hosts erfordern View Agent 6.1.1 oder höher oder Horizon Agent 7.0 oder höher. Wenn Sie das VMware Blast-Anzeigeprotokoll verwenden, müssen Sie über Horizon Agent 7.0 oder höher verfügen.

Hinweis Mit Horizon Client haben Sie nicht nur auf Remote-Desktops, sondern auch auf Windows-basierte Remoteanwendungen sicheren Zugriff. Durch die Auswahl einer Anwendung in Horizon Client wird ein Fenster für diese Anwendung auf dem lokalen Clientgerät geöffnet, und das Erscheinungsbild und das Verhalten der Anwendung entspricht einer lokal installierten Anwendung.

Remoteanwendungen können Sie nur verwenden, wenn Sie mit Verbindungsserver 6.0 oder höher verbunden sind. Einzelheiten zu den unterstützten Betriebssystemen für den RDS-Host, der veröffentlichte Anwendungen und veröffentlichte Desktops bereitstellt, finden Sie im Dokument *View-Installation*.

Weitere Erläuterungen für diese Funktionen und deren Einschränkungen finden Sie im Dokument *Planung der View-Architektur*.

Funktionsunterstützung für Linux-Desktops

Einige Linux-Gastbetriebssysteme werden unterstützt, wenn Sie über View Agent 6.1.1 und höher oder Horizon Agent 7.0 und höher verfügen. Im Dokument *Einrichten von Horizon 6 for Linux-Desktops* und im Dokument *Einrichten von virtuellen Desktops in Horizon 7* finden Sie eine Liste unterstützter Linux-Betriebssysteme sowie Informationen zu den unterstützten Funktionen.

Im geschachtelten Modus unterstützte Funktionen

Der geschachtelte Modus wird manchmal für Zero Clients oder Thin Clients verwendet, bei denen Horizon Client automatisch gestartet und der Benutzer bei einem Remote-Desktop angemeldet wird, wenn sich der Endbenutzer beim Zero Client anmeldet. Von diesem Remote-Desktop aus startet der Benutzer dann gehostete Anwendungen.

In diesem Setup handelt es sich beim Remote-Desktop entweder um einen Einzelplatz-Desktop einer virtuellen Maschine oder um einen von einem RDS-Host bereitgestellten Desktop. In jedem Fall muss zur Bereitstellung gehosteter Anwendungen die Horizon Client-Software auf dem Remote-Desktop installiert sein. Dieses Setup wird als „geschachtelter Modus“ bezeichnet, da der Client eine Verbindung mit einem Desktop herstellt, der ebenfalls über den installierten Client verfügt.

Die im Folgenden aufgeführten Betriebssysteme werden bei der Ausführung von Horizon Client im geschachtelten Modus unterstützt.

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows 7 Enterprise SP1
- Windows 10 Enterprise, Version 1607

Die nachfolgend aufgeführten Funktionen werden unterstützt, wenn ein Benutzer Horizon Client im geschachtelten Modus verwendet.

- VMware Blast-, PCoIP- und RDP-Anzeigeprotokolle
- Standortbasiertes Drucken
- Virtuelles Drucken
- Single Sign-On (ohne Smartcard)
- Zwischenablagenumleitung
- URL-Inhaltsumleitung

Internationalisierung

Die Benutzeroberfläche und die Dokumentation sind in den Sprachen Englisch, Japanisch, Französisch, Deutsch, vereinfachtes Chinesisch, traditionelles Chinesisch, Koreanisch und Spanisch verfügbar.

Verwenden eines lokalen IMEs mit Remoteanwendungen

Wenn Sie nicht englische Tastaturen und Gebietsschemata verwenden, können Sie einen auf Ihrem lokalen System installierten IME (Eingabemethoden-Editor) dazu nutzen, nicht englische Zeichen an eine gehostete Remoteanwendung zu senden.

Darüber hinaus können Sie mit Abkürzungstasten und Symbolen im Infobereich (Taskleiste) Ihres lokalen Systems zu einem anderen IME wechseln. Es besteht keine Notwendigkeit, einen IME auf dem Remote-RDS-Host zu installieren.

Bei Deaktivierung dieser Funktion wird der lokale IME verwendet. Sofern auf dem RDS-Host, auf dem die Remoteanwendung installiert ist, ein IME installiert und konfiguriert ist, wird dieser Remote-IME ignoriert.

Die Funktion ist standardmäßig deaktiviert. Wann immer Sie die Einstellung ändern, um die Funktion zu aktivieren oder zu deaktivieren, müssen Sie die Verbindung zum Server trennen und sich erneut anmelden, bevor die Änderung wirksam werden kann.

Voraussetzungen

- Stellen Sie sicher, dass einer oder mehrere IMEs auf dem Clientsystem installiert sind.
- Stellen Sie sicher, dass die Eingabesprache auf Ihrem lokalen Clientsystem der in Ihrem IME verwendeten Sprache entspricht.

  Die Eingabesprache auf dem RDS-Host ist nicht maßgeblich.
- Stellen Sie sicher, dass auf dem Remote-Desktop View Agent 6.0.2 oder Horizon Agent 7.0 oder höher installiert ist.

Vorgehensweise

1 Klicken Sie mit der rechten Maustaste im Fenster für die Desktop- und Anwendungsauswahl von Horizon Client auf eine Remoteanwendung und wählen Sie **Einstellungen** aus.

2 Aktivieren Sie im anschließend angezeigten Bereich „Remoteanwendungen“ das Kontrollkästchen **Den lokalen IME auf gehostete Anwendungen erweitern** und klicken Sie auf **OK**.

3 Starten Sie die Sitzung erneut unter Verwendung einer der folgenden Optionen:

Option	Beschreibung
Vom Server abmelden	Trennen Sie die Verbindung zum Server, führen Sie erneut eine Anmeldung beim Server durch und stellen Sie erneut eine Verbindung zur Anwendung her. Sie können die Arbeit mit Ihren Anwendungen fortsetzen, da diese zwar getrennt, jedoch nicht geschlossen wurden, wie es bei Remote-Desktops der Fall wäre.
Anwendungen zurücksetzen	Klicken Sie mit der rechten Maustaste auf das Symbol einer Remoteanwendung, wählen Sie **Einstellungen** aus und klicken Sie auf **Zurücksetzen**. Bei Verwendung dieser Option werden geöffnete Remote-Desktops nicht getrennt. Allerdings werden alle Remoteanwendungen geschlossen, und Sie müssen sie neu starten.

   Die Einstellung wird erst nach dem Neustart der Sitzung wirksam. Sie gilt für alle gehosteten Remoteanwendungen auf dem Server.

4 Verwenden Sie den lokalen IME so, wie Sie jede andere lokal installierte Anwendung verwenden würden.

Die Sprachbezeichnung und ein Symbol für den IME werden im Infobereich (bzw. in der Taskleiste) des lokalen Clientsystems angezeigt. Sie können Abkürzungstasten verwenden, um zu einer anderen Sprache oder einem anderen IME zu wechseln. Tastenkombinationen zur Durchführung bestimmter Aktionen, wie z. B. Strg+X für das Ausschneiden von Text sowie Alt+Pfeil rechts für das Verschieben zu einer anderen Registerkarte, funktionieren weiterhin ordnungsgemäß.

Hinweis Auf Windows 7- und Windows 8.x-Systemen können Sie Abkürzungstasten für IMEs im Dialogfeld Textdienste und Eingabesprachen festlegen. (Das Dialogfeld ist über **Systemsteuerung > Region und Sprache > Registerkarte 'Tastaturen und Sprachen' > Schaltfläche 'Tastaturen ändern' > Textdienste und Eingabesprachen > Registerkarte 'Erweiterte Tastatureinstellungen'** erreichbar.)

Aktivieren der Unterstützung für Bildschirmtastaturen

Sie können Ihr Clientsystem so konfigurieren, dass bei einem Horizon Client-Fenster mit Fokus Ereignisse auf der physischen Tastatur, auf der Bildschirmtastatur, mit der Maus und im Schreibbereich an den Remote-Desktop oder an die Remoteanwendung gesendet werden, selbst wenn sich die Maus oder die Bildschirmtastatur außerhalb des Horizon Client-Fensters befindet.

Diese Funktion ist besonders nützlich, wenn Sie ein x86-basiertes Windows-Tablet (z. B. Windows Surface Pro) verwenden. Um diese Funktion nutzen zu können, müssen Sie den Windows-Registrierungsschlüssel `EnableSoftKeypad` auf `true` setzen. Der Speicherort dieses Schlüssels hängt vom Systemtyp ab:

- Für 32-Bit-Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\`
- Für 64-Bit-Windows: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\`

Anpassen der Größe des Remote-Desktop-Fensters

Wenn Sie eine Ecke des Remote-Desktop-Fensters ziehen, um dessen Größe zu ändern, wird eine QuickInfo eingeblendet, die die Bildschirmauflösung rechts unten im Fenster anzeigt.

Wenn Sie das VMware Blast- oder PCoIP-Anzeigeprotokoll verwenden, zeigt die QuickInfo unterschiedliche Bildschirmauflösungen an, wenn Sie die Größe des Desktop-Fensters ändern. Diese Informationen sind hilfreich, wenn Sie die Größe des Remote-Desktops auf eine bestimmte Auflösung ändern möchten.

Wenn ein Administrator die Guest-Size-Einstellung gesperrt hat oder wenn Sie das RDP-Anzeigeprotokoll verwenden, lässt sich die Auflösung des Remote-Desktop-Fensters nicht ändern. In diesem Fall zeigt die Auflösungsquickinfo die ursprüngliche Auflösung an.

Monitore und Bildschirmauflösung

Sie können einen Remote-Desktop auf mehrere Monitore erweitern. Wenn Sie einen hochauflösenden Monitor besitzen, können Sie den Remote-Desktop oder die Remoteanwendung in voller Auflösung sehen.

Der Anzeigemodus „Alle Monitore“ zeigt einen Remote-Desktop auf mehreren Monitoren an. Das Remote-Desktop-Fenster wird standardmäßig auf allen Monitoren dargestellt. Sie können mit der Funktion zur selektiven Festlegung mehrerer Monitore einen Remote-Desktop auf einer Teilmenge Ihrer Monitore anzeigen.

Wenn Sie im Modus „Alle Monitore“ das Fenster minimiert haben, wechselt es nach der Maximierung zurück in den Modus „Alle Monitore“. Dies gilt ebenso für ein minimiertes Vollbildfenster: Nach der Maximierung wird wieder der Vollbildmodus auf einem Monitor angezeigt.

Wenn Horizon Client alle Monitore verwendet und Sie ein Anwendungsfenster maximieren, wird das Fenster nur in dem Monitor auf die Vollbildansicht erweitert, der das Fenster enthält.

Unterstützte Konfigurationen für mehrere Monitore

Horizon Client unterstützt die folgenden Mehrfachmonitorkonfigurationen:

- Wenn Sie zwei Monitore verwenden, müssen sich die Monitore nicht im gleichen Modus befinden. Wenn Sie zum Beispiel einen Laptop verwenden, der mit einem externen Monitor verbunden ist, kann sich der externe Monitor sowohl im Quer- als auch im Hochformat befinden.
- Monitore können nur dann nebeneinander, in Zweiergruppen oder vertikal übereinander platziert werden, wenn Sie zwei Monitore verwenden und die maximale Gesamtlänge weniger als 4096 Pixel beträgt.
- Um die Funktion zur selektiven Festlegung mehrerer Monitore nutzen zu können, muss das VMware Blast-Anzeigeprotokoll oder das PCoIP-Anzeigeprotokoll verwendet werden. Weitere Informationen finden Sie unter „Auswählen bestimmter Monitore in einer Mehrfachmonitorumgebung“, auf Seite 94.

- Um die 3D-Rendering-Funktion nutzen zu können, muss das VMware Blast-Anzeigeprotokoll oder das PCoIP-Anzeigeprotokoll verwendet werden. Sie können bis zu zwei Monitore mit einer Auflösung von bis zu 1920x1200 verwenden. Für eine Auflösung von 4K (3840 X 2160) wird nur ein Monitor unterstützt.
- Wenn Sie Instant-Clone-Desktops benutzen, können Sie maximal zwei Monitore verwenden, um einen Remote-Desktop mit einer Auflösung von bis zu 2560x1600 anzuzeigen.
- Mit dem VMware Blast- oder dem PCoIP-Anzeigeprotokoll wird eine Bildschirmauflösung von 4K (3840 x 2160) für den Remote-Desktop unterstützt. Die Anzahl der unterstützten 4K-Bildschirme hängt von der Hardwareversion der virtuellen Maschine des Desktops und der Windows-Version ab.

Hardwareversion	Windows-Version	Anzahl der unterstützten 4K-Bildschirme
10 (ESXi 5.5.x-kompatibel)	7, 8, 8.x, 10	1
11 (ESXi 6.0-kompatibel)	7 (3D-Rendern-Funktion deaktiviert und Windows Aero deaktiviert)	3
11	7 (3D-Rendern-Funktion aktiviert)	1
11	8, 8.x, 10	1

  Auf dem Remote-Desktop muss View Agent 6.2 oder höher oder Horizon Agent 7.0 oder höher installiert sein. Für eine optimale Leistung muss die virtuelle Maschine mindestens über 2 GB RAM und 2 vCPUs verfügen. Diese Funktion kann gute Netzwerkbedingungen erfordern, wie eine Bandbreite von 1000 Mbit/s mit niedriger Netzwerklatenz und geringen Paketverlusten.

  Hinweis Wenn die Bildschirmauflösung des Remote-Desktop auf 3840 x 2160 (4K) eingestellt ist, können Elemente auf dem Bildschirm kleiner erscheinen. Möglicherweise können Sie auch das Dialogfeld zur Bildschirmauflösung im Remote-Desktop verwenden, um Text und andere Elemente zu vergrößern. In diesem Szenario können Sie für den DPI-Wert des Clientcomputers die passende Einstellung festlegen und die DPI-Synchronisierung aktivieren, damit die DPI-Einstellung des Clientcomputers an den Remote-Desktop umgeleitet wird.

- Wenn Sie Microsoft RDP 7 verwenden, können Sie maximal 16 Monitore verwenden, um einen Remote-Desktop anzuzeigen.
- Wenn Sie das Microsoft RDP-Anzeigeprotokoll verwenden, muss Microsoft Remotedesktopverbindung (RDV) 6.0 oder höher auf dem Remote-Desktop installiert sein.

Auswählen bestimmter Monitore in einer Mehrfachmonitorumgebung

Sie können mit der Funktion zur Auswahl mehrerer Monitore die Monitore auswählen, auf denen ein Remote-Desktop-Fenster angezeigt werden soll. Wenn Sie beispielsweise über drei Monitore verfügen, können Sie festlegen, dass das Fenster des Remote-Desktops nur auf zwei dieser drei Monitore angezeigt wird. Standardmäßig wird ein Remote-Desktop-Fenster auf allen Monitoren in einer Mehrfachmonitorumgebung angezeigt.

Es lassen sich bis zu vier benachbarte Monitore auswählen. Die Monitore können nebeneinander, jeweils zwei gestapelt oder vertikal gestapelt angeordnet sein. Es lassen sich maximal zwei Monitore vertikal stapeln.

Diese Funktion wird für Remoteanwendungen nicht unterstützt.

Vorgehensweise

1 Starten Sie Horizon Client und melden Sie sich bei einem Server an.

2 Klicken Sie im Desktop- und Anwendungsauswahlfenster mit der rechten Maustaste auf den Remote-Desktop und wählen Sie **Einstellungen** aus.

3 Wählen Sie **PCoIP** oder **VMware Blast** aus dem Dropdown-Menü **Verbinden über** aus.

4 Wählen Sie **Alle Monitore** aus dem Dropdown-Menü **Anzeige** aus.

   Unter den Anzeigeeinstellungen finden Sie Miniaturbilder der Monitore, die aktuell mit ihrem Clientsystem verbunden sind. Die Anzeigetopologie entspricht den Anzeigeeinstellungen auf Ihrem Clientsystem.

5 Klicken Sie auf ein Miniaturbild, um einen Monitor auszuwählen oder dessen Auswahl aufzuheben, in dem das Remote-Desktop-Fenster angezeigt wird.

   Nach der Auswahl eines Monitors erscheint dessen Miniaturbild in grün. Wenn Sie gegen eine Regel der Anzeigeauswahl verstoßen, wird eine Warnmeldung eingeblendet.

6 Klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.

7 Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

8 Stellen Sie eine Verbindung mit dem Remote-Desktop her.

   Ihre Änderungen werden sofort wirksam, wenn Sie eine Verbindung mit dem Remote-Desktop herstellen. Ihre Änderungen werden in der Horizon Client-Einstellungendatei für den Remote-Desktop nach dem Beenden von Horizon Client gespeichert.

Verwenden eines Monitors in einer Mehrfachmonitorumgebung

Wenn Sie über mehrere Monitore verfügen, das Fenster eines Remote-Desktops aber nur auf einem Monitor angezeigt werden soll, können Sie das Remote-Desktop-Fenster so konfigurieren, dass es nur auf einem Monitor geöffnet wird.

Diese Einstellung wird für Remoteanwendungen nicht unterstützt.

Vorgehensweise

1 Starten Sie Horizon Client und melden Sie sich bei einem Server an.

2 Klicken Sie im Desktop- und Anwendungsauswahlfenster mit der rechten Maustaste auf den Remote-Desktop und wählen Sie **Einstellungen** aus.

3 Wählen Sie **PCoIP** oder **VMware Blast** aus dem Dropdown-Menü **Verbinden über** aus.

4 Wählen Sie im Menü **Anzeige** die Option **Fenster - groß**, **Fenster - klein** oder **Benutzerdefiniert** aus.

   Bei Auswahl von **Benutzerdefiniert** können Sie eine bestimmte Fenstergröße festlegen.

5 Klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.

   Die Änderungen werden nach dem Anklicken von **Anwenden** wirksam.

6 Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

Standardmäßig wird das Remote-Desktop-Fenster auf dem primären Monitor geöffnet. Sie können das Remote-Desktop-Fenster auch zu einem nicht primären Monitor ziehen. Beim nächsten Öffnen des Remote-Desktops wird dann das Remote-Desktop-Fenster wieder auf diesem Monitor angezeigt. Das Fenster wird nach dem Öffnen in der Mitte des Monitors platziert. Es verwendet die für den Anzeigemodus ausgewählte Fenstergröße und nicht eine eventuell von Ihnen durch Ziehen angepasste Fenstergröße.

Verwenden der Anzeigeskalierung

Ein Benutzer, der einen hochauflösenden Bildschirm, z. B. einen 4K-Monitor, oder eine Sehschwäche hat, aktiviert meist die Anzeigeskalierung, indem er für den DPI-Wert (Dots Per Inch) auf dem Clientcomputer einen Wert über 100 Prozent einstellt. Mit der Funktion der Anzeigeskalierung unterstützt der Remote-Desktop oder die Remoteanwendung die Skalierungseinstellung des Clientcomputers. Der Remote-Desktop oder die Remoteanwendung wird dann nicht klein, sondern in normaler Größe dargestellt.

Horizon Client speichert die Einstellung für die Anzeigeskalierung für jeden Remote-Desktop separat. Für Remoteanwendungen ist die Einstellung für die Anzeigeskalierung für alle Remoteanwendungen gültig, die für den aktuell angemeldeten Benutzer verfügbar sind. Die Einstellung für die Anzeigeskalierung wird angezeigt, auch wenn die DPI-Einstellung auf dem Clientcomputer 100 Prozent beträgt.

Ein Administrator hat die Möglichkeit, die Einstellung für die Anzeigeskalierung durch Aktivierung der Gruppenrichtlinieneinstellung Horizon Client **Locked Guest Size** auszublenden. Durch die Aktivierung der Gruppenrichtlinieneinstellung **Locked Guest Size** wird die DPI-Synchronisierungsfunktion nicht deaktiviert. Um die DPI-Synchronisierungsfunktion zu deaktivieren, muss ein Administrator die Gruppenrichtlinieneinstellung für die **DPI-Synchronisierung** deaktivieren. Weitere Informationen finden Sie unter „Verwendung der DPI-Synchronisierung“, auf Seite 96.

In einer Mehrfachmonitorumgebung wirkt sich die Anzeigeskalierung nicht auf die von Horizon Client unterstützte Anzahl der Monitore und die maximale Auflösung aus. Wenn die Anzeigeskalierung zugelassen und aktiviert ist, basiert die Skalierung auf der DPI-Einstellung für den primären Monitor.

Dieser Vorgang beschreibt, wie Sie die Funktion der Anzeigeskalierung vor der Herstellung einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung aktivieren. Sie können nach dem Herstellen der Verbindung mit einem Remote-Desktop die Funktion für die Anzeigeskalierung aktivieren, indem Sie **Optionen > Anzeigeskalierung zulassen** auswählen.

Vorgehensweise

1 Starten Sie Horizon Client und stellen Sie eine Verbindung mit einem Server her.

2 Klicken Sie im Desktop- und Anwendungsauswahlfenster mit der rechten Maustaste auf den Remote-Desktop oder die Remtoeanwendung und wählen Sie **Einstellungen** aus.

3 Aktivieren Sie das Kontrollkästchen **Anzeigeskalierung zulassen**.

4 Klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.

5 Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

Verwendung der DPI-Synchronisierung

Mit der DPI-Synchronisierungsfunktion wird sichergestellt, dass für neue Remotesitzungen die DPI-Einstellung des Remote-Desktops mit der DPI-Einstellung des Clientcomputers übereinstimmt. Wenn Sie eine neue Sitzung starten, legt Horizon Agent den DPI-Wert für den Remote-Desktop auf den DPI-Wert des Clientcomputers fest.

Die DPI-Synchronisierungsfunktion kann die DPI-Einstellung für aktive Remotesitzungen nicht verändern. Wenn Sie die Verbindung zu einer bestehenden Remotesitzung erneut herstellen, führt die Anzeigeskalierungsfunktion (sofern aktiviert) eine entsprechende Skalierung für den Remote-Desktop oder die Remoteanwendung durch.

Die DPI-Synchronisierungsfunktion ist standardmäßig aktiviert. Ein Administrator kann die DPI-Synchronisierungsfunktion deaktivieren, indem er die Gruppenrichtlinieneinstellung von Horizon Agent für die **DPI-Synchronisierung** deaktiviert. Sie müssen sich abmelden und erneut anmelden, damit die Konfigurationsänderung wirksam wird. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Wenn sowohl die DPI-Synchronisierungsfunktion als auch die Anzeigeskalierungsfunktion aktiviert ist, ist jeweils nur eine Funktion verfügbar. Die Anzeigeskalierung findet nur statt, wenn noch keine DPI-Synchronisierung stattgefunden hat (dies ist der Fall, bevor die DPI-Einstellung auf dem Remote-Desktop mit der DPI-Einstellung auf dem Clientcomputer übereinstimmt). Die Anzeigeskalierung findet nicht mehr statt, sobald die DPI-Einstellungen übereinstimmen.

Für Desktops virtueller Einzelsitzungsmaschinen wird die DPI-Synchronisierungsfunktion auf folgenden Gastbetriebssystemen unterstützt:

- Windows 7, 32 oder 64 Bit
- Windows 8.x, 32 oder 64 Bit
- Windows 10, 32 oder 64 Bit
- Windows Server 2008 R2, als Desktop konfiguriert
- Windows Server 2012 R2, als Desktop konfiguriert
- Windows Server 2016, als Desktop konfiguriert

Für veröffentlichte Desktops und Anwendungen wird DPI-Synchronisierungsfunktion auf folgenden RDS-Hosts unterstützt:

- Windows Server 2012 R2
- Windows Server 2016

Die DPI-Synchronisierungsfunktion erfordert Horizon Agent 7.0.2 oder höher und Horizon Client 4.2 oder höher.

Hinweis Die DPI-Synchronisierungsfunktion ist nicht verfügbar, wenn Sie Horizon Client 4.2 mit Horizon Agent 7.0 oder 7.0.1 oder Horizon Client 4.0 oder 4.1 mit Horizon Agent 7.0.2 oder höher verwenden. In diesen Szenarios ist nur die Anzeigeskalierungsfunktion verfügbar.

Im Folgenden finden Sie Tipps zur Verwendung der DPI-Synchronisierungsfunktion:

- Wenn Sie die DPI-Einstellung auf dem Clientcomputer ändern, müssen Sie sich abmelden und erneut anmelden, damit Horizon Client die neue Einstellung auf dem Clientcomputer erkennt. Diese Anforderung gilt auch für Clientcomputer, auf denen Windows 10 ausgeführt wird.
- Wenn Sie eine Remotesitzung auf einem Clientcomputer starten, dessen DPI-Einstellung auf einen Wert über 100 Prozent festgelegt ist, und dann die gleiche Sitzung auf einem anderen Clientcomputer verwenden, dessen DPI-Einstellung auf einen anderen Wert über 100 Prozent festgelegt ist, müssen Sie sich auf dem zweiten Clientcomputer von der Sitzung abmelden und erneut anmelden, damit die DPI-Synchronisierung auf dem zweiten Clientcomputer funktioniert.
- Auch wenn Computer unter Windows 10 und Windows 8.x unterschiedliche DPI-Einstellungen für verschiedene Monitore unterstützen, verwendet die DPI-Synchronisierungsfunktion nur den für den primären Monitor des Clientcomputers festgelegten DPI-Wert. Auch alle Monitore des Remote-Desktops verwenden dieselbe DPI-Einstellung wie der primäre Monitor des Clientcomputers. Horizon Client unterstützt keine unterschiedlichen DPI-Einstellungen für verschiedene Monitore.
- Wenn ein Administrator den Gruppenrichtlinienwert für die **DPI-Synchronisierung** für Horizon Agent ändert, müssen Sie sich abmelden und erneut anmelden, damit die neue Einstellung wirksam wird.
- Wenn Sie einen Laptop, der verschiedene DPI-Einstellungen für unterschiedliche Monitore unterstützt, mit einem externen Monitor verbinden und den externen Monitor als primären Monitor festlegen, ändert Windows jedes Mal, wenn Sie den externen Monitor trennen oder erneut verbinden, automatisch den primären Monitor und die DPI-Einstellung des primären Monitors. In diesem Fall müssen Sie sich vom Clientsystem abmelden und erneut anmelden, damit Horizon Client die Änderung des primären Monitors erkennt, und sich vom Remote-Desktop oder der Remoteanwendung abmelden und erneut anmelden, damit die DPI-Einstellungen zwischen dem Clientsystem und dem Remote-Desktop oder der Remoteanwendung übereinstimmen.

- Klicken Sie auf Windows 10-Clientcomputern mit der rechten Maustaste auf Ihren Desktop, wählen Sie **Einstellungen anzeigen > Erweiterte Anzeigeeinstellungen > Erweiterte Größenänderung von Text und anderen Elementen** aus, klicken Sie auf den Link **Benutzerdefinierte Skalierungsebene festlegen** und melden Sie sich dann ab und erneut an, damit die neue DPI-Einstellung wirksam wird.

Ändern des Anzeigemodus bei geöffnetem Desktop-Fenster

Sie haben die Möglichkeit, Anzeigemodi zu ändern. Zum Beispiel können Sie vom Modus „Alle Monitore“ zum Vollbildmodus wechseln, ohne die Verbindung zum Remote-Desktop trennen zu müssen.

Diese Funktion wird für Remoteanwendungen nicht unterstützt.

Voraussetzungen

Stellen Sie sicher, dass das VMware Blast- oder das PCoIP-Anzeigeprotokoll verwendet wird.

Vorgehensweise

1 Im Infobereich (Taskleiste) des Clientsystems klicken Sie mit der rechten Maustaste auf das **Horizon Client**-Symbol und wählen die Option zum Öffnen des Einstellungenfensters.

Hinweis Dieses Fenster lässt sich auch aus dem Auswahlfenster für Anwendungen und Desktops öffnen.

2 Wählen Sie den betreffenden Remote-Desktop und eine Anzeigeoption aus.

Verbinden von USB-Geräten

Sie können lokal angeschlossene USB-Geräte, zum Beispiel Thumb-Flashlaufwerke, Kameras oder Drucker, von einem Remote-Desktop aus verwenden. Diese Funktion wird als USB-Umleitung bezeichnet.

Bei Aktivierung dieser Funktion stehen die meisten USB-Geräte, die an das lokale Clientsystem angeschlossen sind, in einem Menü in Horizon Client zur Verfügung. Über das Menü können Sie die Geräte verbinden oder deren Verbindung trennen.

Hinweis Mit View Agent 6.1 oder höher oder mit Horizon Agent 7.0 oder höher können Sie auch lokal angeschlossene USB-Thumb-Flashlaufwerke und Festplatten für die Verwendung in veröffentlichten Desktops und Anwendungen auf RDS-Hosts umleiten. Andere Arten von USB-Geräten, einschließlich anderer Arten von Speichergeräten (z. B. Sicherheitsspeicherlaufwerke und USB-CD-ROM-Laufwerke), werden in veröffentlichten Desktops und Anwendungen nicht unterstützt. Ab der Version Horizon Agent 7.0.2 unterstützen veröffentlichte Desktops und Anwendungen weitere generische USB-Geräte wie das TOPAZ-Signaturpad, den Olympus-Diktatfußschalter und das Wacom-Signaturpad. Andere Arten von USB-Geräten, einschließlich Sicherheitsspeicherlaufwerke und USB-CD-ROM-Laufwerke, werden in veröffentlichten Desktops und Anwendungen nicht unterstützt.

Bei der Verwendung von USB-Geräten mit Remote-Desktops gelten folgende Einschränkungen:

- Beim Zugriff auf ein USB-Gerät von einem Menü in Horizon Client und Verwendung des Geräts in einem Remote-Desktop können Sie nicht auf dem lokalen Computer auf das Gerät zugreifen.
- Zu den USB-Geräten, die nicht im Menü angezeigt werden, aber auf dem Remote-Desktop verfügbar sind, zählen Eingabegeräte (Human Interface Devices) wie zum Beispiel Tastaturen und Zeigegeräte. Der Remote-Desktop und der lokale Computer verwenden diese Geräte gleichzeitig. Die Interaktion mit diesen Geräten kann aufgrund der Netzwerklatenz manchmal recht langsam sein.
- Große USB-Festplattenlaufwerke können erst nach mehreren Minuten auf dem Desktop angezeigt werden.

- Manche USB-Geräte erfordern bestimmte Treiber. Wenn der erforderliche Treiber nicht bereits auf dem Remote-Desktop installiert ist, werden Sie möglicherweise bei Verbindung des USB-Geräts mit dem Remote-Desktop zu Installation dieses Treibers aufgefordert.
- Wenn Sie USB-Geräte verbinden möchten, die MTP-Treiber verwenden, so zum Beispiel Android-basierte Samsung-Smartphones und -Tablets, müssen Sie Horizon Client so konfigurieren, dass die USB-Geräte automatisch mit Ihrem Remote-Desktop verbunden werden. Anderenfalls wird das USB-Gerät beim Versuch der manuellen Umleitung über ein Menüelement erst umgeleitet, nachdem Sie das Gerät getrennt und neu verbunden haben.
- Stellen Sie keine Verbindung mit Scannern über das Menü **USB-Gerät verbinden** her. Um einen Scanner zu verwenden, nutzen Sie die Scannerumleitungsfunktion. Bei Verwendung mit View Agent 6.0.2 oder höher oder mit Horizon Agent 7.0 oder höher steht diese Funktion für Horizon Client zur Verfügung. Siehe „Verwenden von Scannern“, auf Seite 109.
- Webcams werden für die USB-Umleitung über das Menü **USB-Gerät verbinden** nicht unterstützt. Zur Verwendung einer Webcam oder eines Audioeingabegeräts müssen Sie die Echtzeit-Audio/Video-Funktion verwenden. Diese Funktion steht bei Verwendung von View 5.2 Feature Pack 2 oder höher zur Verfügung. Siehe „Verwenden der Echtzeit-Audio/Video-Funktion für Webcams und Mikrofone“, auf Seite 102.
- Die Umleitung von USB-Audiogeräten ist vom Netzwerkstatus abhängig und daher nicht zuverlässig. Manche Geräte erfordern auch im Ruhezustand einen hohen Datendurchsatz. Wenn Sie die in View 5.2 Feature Pack 2 oder höher enthaltene Echtzeit-Audio/Video-Funktion verwenden, arbeiten Audioeingabe- und Audioausgabegeräte ordnungsgemäß, und die Verwendung der USB-Umleitung ist für diese Geräte nicht erforderlich.

Sie können USB-Geräte sowohl manuell als auch automatisch mit einem Remote-Desktop verbinden.

Hinweis Leiten Sie keine USB-Geräte wie USB-Ethernet-Geräte und Touchscreen-Geräte an den Remote-Desktop um. Wenn Sie ein USB-Ethernet-Gerät umleiten, verliert Ihr lokales Clientsystem die Verbindung zum Netzwerk. Wenn Sie ein Touchscreen-Gerät umleiten, empfängt der Remote-Desktop Eingaben vom Touchscreen und nicht von der Tastatur. Wenn Sie Ihren virtuellen Desktop zur automatischen Verbindung von USB-Geräten konfiguriert haben, können Sie Richtlinien konfigurieren, um bestimmte Geräte auszuschließen.

Wichtig In diesem Verfahren wird die Verwendung des VMware Horizon Client-Menüelements zur Konfiguration der automatischen Verbindung von USB-Geräten mit dem Remote-Desktop erläutert. Sie können die automatische Verbindung auch konfigurieren, indem Sie die Horizon Client-Befehlszeilenschnittstelle verwenden oder eine Gruppenrichtlinie erstellen.

Weitere Informationen über die Befehlszeilenschnittstelle finden Sie unter „Ausführen von Horizon Client über die Befehlszeile“, auf Seite 67. Weitere Informationen zur Erstellung von Gruppenrichtlinien finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Voraussetzungen

- Um USB-Geräte mit einem Remote-Desktop verwenden zu können, muss ein Horizon-Administrator die USB-Funktion für den Remote-Desktop aktivieren.

  Diese Aufgabe schließt die Installation der Komponente **USB-Umleitung** des Agenten ein und kann auch die Erstellung von Einstellungsrichtlinien hinsichtlich der USB-Umleitung umfassen. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

- Bei der Installation von Horizon Client muss die Komponente **USB-Umleitung** mit installiert werden. Wenn Sie diese Komponente bei der Installation nicht berücksichtigt haben, deinstallieren Sie den Client und führen Sie das Installationsprogramm erneut aus, um die Komponente **USB-Umleitung** mit einzuschließen.

Vorgehensweise

- Verbinden Sie das USB-Gerät manuell mit einem Remote-Desktop.
  a Schließen Sie das USB-Gerät an Ihr lokales Clientsystem an.
  b Klicken Sie in der VMware Horizon Client-Menüleiste auf **USB-Gerät verbinden**.
  c Wählen Sie das USB-Gerät aus.

  Das Gerät wird manuell vom lokalen System an den Remote-Desktop umgeleitet.
- Schließen Sie das USB-Gerät an eine gehostete Remoteanwendung an.
  a Öffnen Sie im Desktop- und Anwendungsauswahlfenster die Remoteanwendung.

    Der Name der Anwendung entspricht dem Namen, den Ihr Administrator für die Anwendung konfiguriert hat.
  b Klicken Sie im Desktop- und Anwendungsauswahlfenster mit der rechten Maustaste auf das Anwendungssymbol und wählen Sie **Einstellungen** aus.
  c Wählen Sie im linken Bereich **USB-Geräte** aus.
  d Markieren Sie im rechten Bereich das USB-Gerät und klicken Sie auf **Verbinden**.
  e Wählen Sie die Anwendung aus und klicken Sie auf **OK**.

    Hinweis Der Name der Anwendung in der Liste stammt aus der Anwendung selbst und stimmt nicht unbedingt mit dem Anwendungsnamen überein, den Ihr Administrator für die Anzeige im Desktop- und Anwendungsauswahlfenster konfiguriert hat.

    Sie können das USB-Gerät nun mit der Remoteanwendung verwenden. Nach dem Schließen der Anwendung wird das USB-Gerät nicht umgehend freigegeben.
  f Wenn Sie die Anwendung nicht mehr verwenden und das USB-Gerät freigeben möchten, damit vom lokalen System aus darauf zugegriffen werden kann, öffnen Sie im Desktop- und Anwendungsauswahlfenster erneut das Fenster „Einstellungen“ und wählen Sie **USB-Geräte** und danach **Trennen** aus.
- Konfigurieren Sie Horizon Client dahingehend, dass USB-Geräte automatisch mit dem Remote-Desktop verbunden werden, wenn Sie diese an das lokale System anschließen.

  Mit der Funktion zur automatischen Verbindung haben Sie die Möglichkeit, Geräte mit MTP-Treibern zu verbinden, so zum Beispiel Android-basierte Samsung-Smartphones und -Tablets.
  a Bevor Sie das USB-Gerät anschließen, starten Sie Horizon Client und stellen Sie die Verbindung mit einem Remote-Desktop her.
  b Klicken Sie in der VMware Horizon Client-Menüleiste auf **USB-Gerät verbinden > USB-Geräte bei Einführen automatisch verbinden**.
  c Schließen Sie das USB-Gerät an.

  USB-Geräte, die Sie nach dem Start von Horizon Client an Ihr lokales System anschließen, werden an den Remote-Desktop umgeleitet.
- Konfigurieren Sie Horizon Client zur automatischen Verbindung von USB-Geräten mit dem Remote-Desktop, wenn Horizon Client gestartet wird.
  a Klicken Sie in der VMware Horizon Client-Menüleiste auf **USB-Gerät verbinden > USB-Geräte bei Start automatisch verbinden**.
  b Schließen Sie das USB-Gerät an und starten Sie Horizon Client neu.

  USB-Geräte, die Sie beim Start von Horizon Client an Ihr lokales System anschließen, werden an den Remote-Desktop umgeleitet.

Das USB-Gerät wird auf dem Desktop angezeigt. Es kann dabei bis zu 20 Sekunden dauern, bis das USB-Gerät auf dem Desktop eingeblendet wird. Bei erstmaliger Verbindung von Gerät und Desktop werden Sie eventuell dazu aufgefordert, bestimmte Treiber zu installieren.

Wird das USB-Gerät auch nach mehreren Minuten nicht auf dem Desktop angezeigt, sollten Sie die Verbindung trennen und das Gerät anschließend neu mit dem Clientcomputer verbinden.

Weiter

Bei Problemen mit der USB-Umleitung finden Sie weitere Informationen im Kapitel über die Behebung von Problemen bei der USB-Umleitung im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Konfigurieren von Clients zur erneuten Verbindung beim Neustart der USB-Geräte

Wenn Sie Horizon Client nicht zur automatischen Verbindung der USB-Geräte mit Ihrem Remote-Desktop konfigurieren, können Sie immer noch festlegen, dass Horizon Client mit bestimmten Geräten, die verschiedentlich neu starten, wieder eine Verbindung herstellt. Andernfalls stellt ein Gerät, wenn es während eines Upgrade-Vorgangs neu startet, eine Verbindung zum lokalen System anstatt zum Remote-Desktop her.

Wenn Sie als USB-Gerät zum Beispiel ein Smartphone oder ein Tablet verbinden möchten, das bei Betriebssystem-Upgrades automatisch neu gestartet wird, können Sie Horizon Client dazu anweisen, das jeweilige Gerät erneut mit dem Remote-Desktop zu verbinden. Zum Durchführen dieser Aufgabe muss die Konfigurationsdatei auf dem Client bearbeitet werden.

Wenn Sie die Option **Nach Einführung automatisch verbinden** in Horizon Client verwenden, werden alle Geräte, die Sie am Clientsystem anschließen, an den Remote-Desktop umgeleitet. Wenn Sie nicht möchten, dass alle Geräte verbunden werden, sollten Sie die folgende Vorgehensweise zur Konfiguration von Horizon Client anwenden, sodass nur bestimmte USB-Geräte automatisch neu verbunden werden.

Voraussetzungen

Ermitteln Sie das hexadezimale Format der Hersteller-ID (VID) und der Produkt-ID (PID) des Geräts. Anweisungen hierzu finden Sie im VMware KB-Artikel http://kb.vmware.com/kb/1011600.

Vorgehensweise

1 Öffnen Sie die Datei `config.ini` in einem Text-Editor auf dem Client.

Betriebssystemversion	Dateipfad
Windows 7, 8.x oder Windows 10	`C:\ProgramData\VMware\VMware USB Arbitration Service\config.ini`
Windows XP	`C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\VMware\VMware USB Arbitration Service\config.ini`

2 Legen Sie die Eigenschaft `slow-reconnect` für das bestimmte Gerät oder die Geräte fest.

```
usb.quirks.device0 = "vid:pid slow-reconnect"
```

Hier stehen *vid*:*pid* jeweils für die Hersteller- und die Produkt-ID (im hexadezimalen Format) des Geräts. Die folgenden Zeilen legen diese Eigenschaft beispielsweise für zwei USB-Geräte fest:

```
usb.quirks.device0 = "0x0529:0x0001 slow-reconnect"
usb.quirks.device1 = "0x0601:0x0009 slow-reconnect"
```

Geben Sie die Geräteeigenschaften `usb.quirks.deviceN` in der richtigen Reihenfolge, beginnend bei 0, an. Folgt auf die Zeile `usb.quirks.device0` zum Beispiel nicht eine Zeile mit `usb.quirks.device1`, sondern eine Zeile mit `usb.quirks.device2`, wird nur die erste Zeile gelesen.

Wenn nun für Geräte wie Smartphones oder Tablets ein Upgrade der Firmware oder des Betriebssystems durchgeführt wird, verläuft das Upgrade erfolgreich, da das Gerät neu startet und die Verbindung zu dem Remote-Desktop herstellt, der das Gerät verwaltet.

Verwenden der Echtzeit-Audio/Video-Funktion für Webcams und Mikrofone

Mit der Echtzeit-Audio/Video-Funktion können Sie die Webcam oder das Mikrofon Ihres lokalen Computers auf Ihrem Remote-Desktop verwenden. Echtzeit-Audio/Video ist mit Standard-Konferenzanwendungen und browserbasierten Videoanwendungen kompatibel und unterstützt standardmäßige Webcams, USB-Audiogeräte und analoge Audioeingänge.

Informationen zur Einrichtung der Echtzeit-Audio/Video-Funktion sowie zur Konfiguration der Frame-Rate und der Bildauflösung in einem Remote-Desktop finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*. Informationen zum Konfigurieren dieser 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.

Auf der Website http://labs.vmware.com/flings/real-time-audio-video-test-application können Sie eine Testanwendung herunterladen, mit der überprüft wird, ob die Echtzeit-Audio/Video-Funktion ordnungsgemäß installiert ist und fehlerfrei arbeitet. Diese Testanwendung ist als VMware-Fling verfügbar, weshalb kein technischer Support besteht.

In diesen Fällen können Sie Ihre Webcam verwenden

Wenn ein Horizon-Administrator die Echtzeit-Audio/Video-Funktion konfiguriert hat und Sie das PCoIP-Anzeigeprotokoll oder das VMware Blast-Anzeigeprotokoll verwenden, kann eine integrierte oder an Ihren lokalen Computer angeschlossene Webcam auf Ihrem Desktop verwendet werden. Sie können die Webcam in Konferenzanwendungen wie z. B. Skype, Webex oder Google Hangouts verwenden.

Bei der Einrichtung einer Anwendung wie Skype, Webex oder Google Hangouts auf Ihrem Remote-Desktop können Sie Ein- und Ausgabegeräte aus Menüs in der Anwendung auswählen. Für VM-Desktops können Sie das virtuelle VMware-Mikrofon und die virtuelle VMware-Webcam auswählen. Für veröffentlichte Desktops können Sie ein Remoteaudiogerät und die virtuelle VMware-Webcam auswählen.

Bei vielen Anwendungen kann diese Funktion ohne die Auswahl eines Eingabegeräts genutzt werden.

Wenn die Webcam zurzeit von Ihrem lokalen Computer genutzt wird, kann sie nicht gleichzeitig vom Remote-Desktop verwendet werden. Genauso kann die Webcam nicht vom lokalen Computer verwendet werden, wenn sie zurzeit vom Remote-Desktop genutzt wird.

Wichtig Wenn Sie eine USB-Webcam verwenden, verbinden Sie diese nicht über das Menü **USB-Gerät verbinden** in Horizon Client. Dies würde dazu führen, dass die USB-Umleitung für das Gerät aktiviert wird und die Leistung für einen Videochat nicht ausreicht.

Wenn mehr als eine Webcam an Ihren lokalen Computer angeschlossen ist, können Sie eine bevorzugte Webcam konfigurieren, die auf Ihrem Remote-Desktop verwendet wird.

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

Wenn Sie die Echtzeit-Audio/Video-Funktion einsetzen und auf Ihrem Clientsystem über mehrere Webcams oder Mikrofone verfügen, wird nur eine davon auf Ihrem Remotedesktop oder von Ihrer Remoteanwendung verwendet. Sie können Echtzeit-Audio/Video-Einstellungen in Horizon Client konfigurieren, um anzugeben, welche Webcam oder welches Mikrofon bevorzugt werden soll.

Die bevorzugte Webcam oder das Mikrofon wird auf dem Remotedesktop oder in der Remoteanwendung verwendet, sofern sie bzw. es verfügbar ist. Andernfalls wird eine andere Webcam oder ein anderes Mikrofon verwendet.

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

Hinweis Wenn Sie eine USB-Webcam oder ein USB-Mikrofon verwenden, verbinden Sie diese nicht über das Menü **USB-Gerät verbinden** in Horizon 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 eine USB-Webcam, ein USB-Mikrofon oder ein anderer Mikrofontyp auf Ihrem Clientsystem installiert und betriebsbereit ist.
- Stellen Sie sicher, dass das VMware Blast-Anzeigeprotokoll oder das PCoIP-Anzeigeprotokoll für Ihre Remotedesktops oder Remoteanwendungen verwendet wird.
- Stellen Sie eine Verbindung mit einem Server her.

Vorgehensweise

1 Öffnen Sie das Dialogfeld „Einstellungen“ und wählen Sie im linken Bereich **Echtzeit-Audio/Video** aus.

   Sie können dieses Dialogfeld öffnen, indem Sie rechts oben auf dem Desktop- und Anwendungsbildschirm auf das Symbol **Einstellungen** (Zahnrad) klicken. Sie können auch mit der rechten Maustaste auf ein Desktop- oder Anwendungssymbol klicken und **Einstellungen** auswählen.

2 Wählen Sie im Dropdown-Menü **Bevorzugte Webcam** die bevorzugte Webcam und im Dropdown-Menü **Bevorzugtes Mikrofon** das bevorzugte Mikrofon aus.

   In diesen Dropdown-Menüs werden die auf dem Clientsystem verfügbaren Webcams und Mikrofone angezeigt.

3 Klicken Sie auf **OK** oder auf **Übernehmen**, um Ihre Änderungen zu speichern.

Wenn Sie das nächste Mal einen Remotedesktop oder eine Remoteanwendung starten, werden die ausgewählte bevorzugte Webcam und das ausgewählte bevorzugte Mikrofon zum Remotedesktop oder der Remoteanwendung umgeleitet.

Kopieren und Einfügen von Text und Bildern

Sie können standardmäßig Text von Ihrem Clientsystem auf einen Remote-Desktop oder in eine Remoteanwendung kopieren und einfügen. Wenn ein Horizon-Administrator die Funktion aktiviert, können Sie auch Text zwischen einem Remote-Desktop oder einer Remoteanwendung und Ihrem Clientsystem oder zwischen zwei Remote-Desktops oder -anwendungen kopieren und einfügen. Zu den unterstützten Dateiformaten gehören Text, Bilder und RTF (Rich Text Format). Hierfür gelten allerdings einige Einschränkungen.

Wenn Sie das VMware Blast-Anzeigeprotokoll oder das PCoIP-Anzeigeprotokoll verwenden, kann ein Horizon-Administrator diese Funktion so einstellen, dass Kopier- und Einfügevorgänge nur von Ihrem Clientsystem zu einem Remote-Desktop oder zu einer Remoteanwendung oder nur von einem Remote-Desktop oder von einer Remoteanwendung zu Ihrem Clientsystem zugelassen werden oder beide bzw. keiner der beiden Vorgänge möglich sind.

Horizon-Administratoren haben die Möglichkeit, das Kopieren/Einfügen durch entsprechende Konfiguration der Gruppenrichtlinieneinstellungen zu aktivieren, die Horizon Agent zugeordnet sind. Je nach installierter Version von Horizon Server und Agent können Administratoren auch mit Gruppenrichtlinien Zwischenablageformate für das Kopieren/Einfügen beschränken oder das Kopieren/Einfügen auf Remote-Desktops mithilfe von intelligenten Richtlinien steuern. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

In Horizon 7 Version 7.0 und früher sowie in Horizon Client 4.0 und früher kann die Zwischenablage 1 MB Daten für das Kopieren/Einfügen aufnehmen. In Horizon 7 Version 7.0.1 und höher sowie in Horizon Client 4.1 und höher lässt sich die Größe des Zwischenablagespeichers sowohl für den Server wie für den Client konfigurieren. Wenn eine PCoIP- oder VMware Blast-Sitzung eingerichtet wurde, sendet der Server die Größe seines Zwischenablagespeichers an den Client. Die effektive Größe des Zwischenablagespeichers entspricht dem kleineren Wert des Zwischenablagespeichers von Server und Client.

Wenn Sie formatierten Text kopieren, handelt es sich bei den Daten teilweise um Text und teilweise um Formatierungsinformationen. Wenn Sie daher eine große Menge an formatiertem Text oder Text und ein Bild kopieren, kann es beim Einfügen dazu kommen, dass Sie den Text ganz oder teilweise sehen, nicht aber die Formatierung oder das Bild. Dies liegt daran, dass die drei Arten von Daten separat gespeichert werden können. Je nach Art des Dokuments, von dem aus Sie kopieren, können Bilder möglicherweise als Bilder oder als RTF-Daten gespeichert werden.

Beträgt die Gesamtmenge von Text und RTF weniger als die maximale Größe der Zwischenablage, wird der formatierte Text eingefügt. Es ist häufig der Fall, dass die RTF-Daten nicht gekürzt werden können, sodass die RTF-Daten verworfen und nur der reine Text eingefügt wird, sollten Text und Formatierung zusammen mehr als die maximale Größe der Zwischenablage umfassen.

Sollten Sie nicht in der Lage sein, den gesamten formatierten Text und die von Ihnen ausgewählten Bilder einzufügen, versuchen Sie geringere Teilmengen zu speichern und einzufügen.

Sie können keine Dateien zwischen einem Remote-Desktop und dem Dateisystem auf Ihrem Clientcomputer kopieren und einfügen.

Konfigurieren der Größe des Zwischenablagespeichers für den Client

In Horizon 7 Version 7.0.1 und höher sowie in Horizon Client 4.1 und höher lässt sich die Größe des Zwischenablagespeichers sowohl für den Server wie für den Client konfigurieren.

Wenn eine PCoIP- oder VMware Blast-Sitzung eingerichtet wurde, sendet der Server die Größe seines Zwischenablagespeichers an den Client. Die effektive Größe des Zwischenablagespeichers entspricht dem kleineren Wert des Zwischenablagespeichers von Server und Client.

Ändern Sie zum Festlegen der Größe des Zwischenablagespeichers den Windows-Registrierungswert `HKLM\Software\VMware, Inc.\VMware VDPService\Plugins\MKSVchan\ClientClipboardSize`. Der Werttyp lautet REG_DWORD. Der Wert wird in KB angegeben. Wenn Sie 0 oder keinen Wert eingeben, gilt für den Client die Standardgröße des Zwischenablagespeichers von 8.192 KB (8 MB).

Ein hoher Wert für die Größe des Zwischenablagespeichers kann sich, je nach verwendetem Netzwerk, negativ auf die Leistung auswirken. VMware empfiehlt für die maximale Größe des Zwischenablagespeichers einen Wert von 16 MB.

Verwenden von Remoteanwendungen

Remoteanwendungen ähneln Anwendungen, die auf Ihrem Client-PC oder Laptop installiert sind.

- Sie können eine Remoteanwendung über die Anwendung minimieren und maximieren. Wenn eine Remoteanwendung minimiert wird, wird sie in der Taskleiste Ihres Clientsystems angezeigt. Sie können die Remoteanwendung auch minimieren und maximieren, indem Sie auf ihr Symbol in der Taskleiste klicken.
- Sie können eine Remoteanwendung über die Anwendung oder dadurch beenden, dass Sie mit der rechten Maustaste auf ihr Symbol in der Taskleiste klicken.
- Sie können Alt+Tabulator drücken, um zwischen geöffneten Remoteanwendungen zu wechseln.
- Wenn eine Remoteanwendung ein Element im Windows-Infobereich erstellt, erscheint dieses Element auch im Infobereich Ihres Windows-Client-Computers. Standardmäßig werden die Infobereichsymbole nur angezeigt, um Benachrichtigungen anzuzeigen. Dieses Verhalten können Sie jedoch so anpassen, wie Sie es mit nativ installierten Anwendungen auch tun.

Hinweis Wenn Sie die Systemsteuerung öffnen, um die Symbole im Infobereich anzupassen, werden die Namen der Symbole für Remoteanwendungen als VMware Horizon Client - *Name der Anwendung* aufgeführt.

Speichern von Dokumenten in einer Remoteanwendung

Sie können mit bestimmten Remoteanwendungen, z. B. Microsoft Word oder WordPad, Dokumente erstellen und speichern. Der Speicherort für diese Dokumente hängt von der Netzwerkumgebung Ihres Unternehmens ab. Beispielsweise können die Dokumente in einer Basisfreigabe gespeichert werden, die auf Ihrem lokalen Computer gemountet wird.

Administratoren können anhand einer ADMX-Vorlagendatei eine Gruppenrichtlinie zur Angabe des Speicherorts für Dokumente einrichten. Hierbei handelt es sich um die Richtlinie **Basisverzeichnis für Remote-Desktop-Dienste-Benutzer festlegen**. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Drucken über einen Remote-Desktop oder über eine Remoteanwendung

Sie können von einem Remote-Desktop aus Dokumente auf einem virtuellen Drucker oder einem USB-Drucker ausdrucken, der mit Ihrem Clientcomputer verbunden ist. Die virtuelle Druckfunktion und das Drucken mit USB-Umleitung können ohne Konflikte gemeinsam eingesetzt werden.

Sie können die virtuelle Druckfunktion mit den folgenden Typen von Remote-Desktops und -anwendungen verwenden:

- Remote-Desktops, auf denen Windows Server-Betriebssysteme ausgeführt werden
- Sitzungsbasierte Desktops (auf RDS-Hosts von virtuellen Maschinen)
- Gehostete Remoteanwendungen

Festlegen von Voreinstellungen für die virtuelle Druckfunktion auf einem Remote-Desktop

Die virtuelle Druckfunktion ermöglicht Endbenutzern das Verwenden von lokalen oder Netzwerkdruckern auf einem Remote-Desktop, ohne dass im Remote-Desktop zusätzliche Druckertreiber installiert werden müssen. Für jeden Drucker, der über diese Funktion zur Verfügung steht, können Sie Voreinstellungen für Datenkomprimierung, Druckqualität, doppelseitigen Druck, Farbe usw. festlegen.

Nachdem dem lokalen Computer ein Drucker hinzugefügt wurde, fügt Horizon Client diesen Drucker der Liste der verfügbaren Drucker auf dem Remote-Desktop hinzu. Keine weitere Konfiguration ist erforderlich. Benutzer mit Administratorrechten können weiterhin Druckertreiber auf dem Remote-Desktop installieren, ohne einen Konflikt mit der virtuellen Druckfunktion zu verursachen.

Wichtig Diese Funktion steht für die folgenden Druckertypen nicht zur Verfügung:

- USB-Drucker, die die USB-Umleitungsfunktion zur Verbindung mit einem virtuellen USB-Port im Remote-Desktop verwenden

  Sie müssen den USB-Drucker im Remote-Desktop trennen, um die virtuelle Druckfunktion verwenden zu können.

- Die Windows-Funktion für die Ausgabe in einer Datei

  Das Kontrollkästchen **Ausgabe in Datei** im Dialogfeld „Drucken“ kann nicht ausgewählt werden. Ein Druckertreiber, über den eine Datei erstellt wird, kann verwendet werden. Beispielsweise können Sie einen PDF-Writer zum Drucken einer PDF-Datei verwenden.

Dieses Verfahren beschreibt die Schritte auf einem Remote-Desktop mit einem Windows 7- oder Windows 8.x-Betriebssystem (Desktop). Die Vorgehensweise ähnelt derjenigen für Windows Server 2008 und Windows Server 2012, ist aber nicht identisch.

Voraussetzungen

Stellen Sie sicher, dass die virtuelle Druckfunktion des Agenten auf dem Remote-Desktop installiert ist. Stellen Sie sicher, dass im Dateisystem des Remote-Desktops der folgende Ordner vorhanden ist: `C:\Program–me\Common Files\ThinPrint`.

Zur Anwendung der virtuellen Druckfunktion muss diese in Horizon Administrator für den Remote-Desktop aktiviert werden. Diese Aufgabe beinhaltet die Aktivierung der Option **Virtueller Druck** im Agenteninstallationsprogramm. Außerdem können Richtlinien für das Verhalten der virtuellen Druckfunktion eingerichtet werden. Weitere Informationen finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

Vorgehensweise

1. Klicken Sie auf einem Remote-Desktop unter Windows 7 oder Windows 8.x auf **Start > Geräte und Drucker**.
2. Klicken Sie im Fenster „Geräte und Drucker“ mit der rechten Maustaste auf den Standarddrucker und wählen Sie aus dem Kontextmenü **Druckereigenschaften** und dann den Drucker aus.

   Virtuelle Drucker werden auf Einzelplatz-Desktops mit einer virtuellen Maschine in der Form *<Druckername>* und auf veröffentlichten Desktops von RDS-Hosts in der Form *<Druckername>(<Sitzungs_ID>)* angezeigt, wenn View Agent 6.2 oder höher oder Horizon Agent 7.0 oder höher installiert ist. Wenn View Agent 6.1 oder früher im Remote-Desktop installiert ist, werden virtuelle Drucker als *<printer_name>#:<number>* angezeigt.
3. Klicken Sie im Fenster mit den Druckereigenschaften auf die Registerkarte **Geräteeinstellungen** und geben Sie die zu verwendenden Einstellungen an.

4 Klicken Sie auf der Registerkarte **Allgemein** auf **Einstellungen** und geben Sie die zu verwendenden Einstellungen an.

5 Klicken Sie im Dialogfeld mit den Druckeinstellungen auf die verschiedenen Registerkarten und geben Sie an, welche Einstellungen verwendet werden sollen.

   Für die erweiterte Einstellung **Seitenanpassung** empfiehlt VMware, die Standardeinstellungen beizubehalten.

6 Klicken Sie auf **OK**.

7 Zum Verwenden benutzerdefinierter Papierformulare definieren Sie die Formulare auf dem Client.

   a Navigieren Sie zu **Systemsteuerung > Hardware und Sound > Geräte und Drucker**.

   b Wählen Sie den Drucker aus und klicken Sie oben im Fenster auf **Eigenschaften des Druckservers**.

   c Legen Sie auf der Registerkarte **Formulare** die Einstellungen fest und klicken Sie auf **Formular speichern**.

   Dieses Formular ist nun auf dem Remote-Desktop verfügbar.

Verwenden von USB-Druckern

In einer Horizon-Umgebung können virtuelle Drucker und umgeleitete USB-Drucker konfliktfrei zusammen eingesetzt werden.

Ein USB-Drucker ist ein Drucker, der an einen USB-Port auf dem lokalen Clientsystem angeschlossen ist. Zum Senden von Druckaufträgen an einen USB-Drucker können Sie entweder die USB-Umleitungsfunktion oder die virtuelle Druckfunktion verwenden. Der USB-Druck ist gelegentlich schneller als der virtuelle Druck, abhängig von den Netzwerkbedingungen.

- Sie können die USB-Umleitungsfunktion zum Anschließen eines USB-Druckers an einen virtuellen USB-Port auf dem Remote-Desktop verwenden, sofern die erforderlichen Treiber auf dem Remote-Desktop installiert sind.

  Wenn Sie diese Umleitungsfunktion verwenden, ist der Drucker nicht länger logisch an den physischen USB-Port auf dem Client angeschlossen. Aus diesem Grund wird der USB-Drucker nicht mehr in der Liste der lokalen Drucker angezeigt. Dies bedeutet auch, dass Sie über den USB-Drucker auf dem Remote-Desktop drucken können, nicht jedoch über die lokale Clientmaschine.

  Auf dem Remote-Desktop werden umgeleitete USB-Drucker als <*Druckername*> angezeigt.

  Informationen zur Verbindungsherstellung mit einem USB-Drucker finden Sie unter „Verbinden von USB-Geräten“, auf Seite 98.

- Auf einigen Clients können Sie alternativ die virtuelle Druckfunktion nutzen, um Druckaufträge an einen USB-Drucker zu senden. Wenn Sie die virtuelle Druckfunktion verwenden, können Sie sowohl über den Remote-Desktop als auch über den lokalen Client auf dem USB-Drucker drucken, und es ist nicht erforderlich, Druckertreiber auf dem Remote-Desktop zu installieren.

Steuern der Anzeige von Adobe Flash

Der Horizon-Administrator kann die Wiedergabe von Adobe Flash-Inhalten in Ihrem Remote-Desktop so festlegen, dass Rechenressourcen eingespart werden. In einigen Fällen können diese Einstellungen zu einer verringerten Wiedergabequalität führen. Wenn Sie den Mauszeiger in die Adobe Flash-Inhalte setzen, haben Sie die Möglichkeit, die von Ihrem Horizon Administrator festgelegten Adobe Flash-Einstellungen zu überschreiben.

Die Steuerung der Adobe Flash-Anzeige ist ausschließlich für Internet Explorer-Sitzungen unter Windows sowie für Adobe Flash 9 und 10 verfügbar. Zur Steuerung der Adobe Flash-Anzeigequalität darf Adobe Flash nicht im Vollbildmodus ausgeführt werden.

Vorgehensweise

1 Navigieren Sie im Internet Explorer-Browser des Remote-Desktops zu den gewünschten Adobe Flash-Inhalten und starten Sie diese, falls erforderlich.

   Je nach Konfiguration der Adobe Flash-Einstellungen durch Ihren Horizon-Administrator ist die Wiedergabequalität möglicherweise gemindert.

2 Setzen Sie den Mauszeiger während der Wiedergabe in die Adobe Flash-Inhalte.

   Die Anzeigequalität wird verbessert, solange sich der Cursor innerhalb der Adobe Flash-Inhalte befindet.

3 Doppelklicken Sie in die Adobe Flash-Inhalte, um die verbesserte Wiedergabequalität beizubehalten.

Anklicken von URL-Links zum Öffnen außerhalb von Horizon Client

Ein Administrator kann URL-Links so konfigurieren, dass diese durch Klicken in einem Remote-Desktop oder in einer Remoteanwendung im Standardbrowser auf Ihrem Clientsystem geöffnet werden. Ein Link kann zu einer Webseite, einer Telefonnummer, einer E-Mail oder zu einer anderen Art von Links führen. Diese Funktion wird als URL-Inhaltsumleitung bezeichnet.

Ein Administrator kann außerdem URL-Links konfigurieren, die, wenn Sie auf Ihrem Clientsystem in einem Browser oder einer Anwendung darauf klicken, in einem Remotedesktop oder einer Remoteanwendung geöffnet werden. Falls Horizon Client in diesem Szenario noch nicht geöffnet ist, erfolgt der Start und Sie werden zur Anmeldung aufgefordert.

Ein Administrator kann die URL-Inhaltsumleitung aus Sicherheitsgründen einrichten. Wenn Sie sich z. B. in Ihrem Unternehmensnetzwerk befinden und auf einen Link klicken, der auf eine URL verweist, die sich außerhalb des Netzwerks befindet, ist es sicherer, wenn der Link in einer Remoteanwendung geöffnet wird. Ein Administrator kann konfigurieren, welche Anwendung den Link öffnet.

Beim ersten Start von Horizon Client und beim ersten Herstellen einer Verbindung mit einem Server, auf dem die Funktion der URL-Inhaltsumleitung konfiguriert ist, werden Sie, wenn Sie auf einen Link für die Umleitung klicken, von Horizon Client aufgefordert, die Anwendung VMware Horizon URL Filter zu öffnen. Klicken Sie auf **Öffnen**, um die URL-Inhaltsumleitung zu aktivieren.

Je nachdem, wie die Funktion der URL-Inhaltsumleitung konfiguriert ist, wird von Horizon Client eventuell eine Warnmeldung eingeblendet, die Sie zur Änderung Ihres Standardwebbrowsers in „VMware Horizon URL Filter“ auffordert. Klicken Sie in diesem Fall auf die Schaltfläche **„VMware Horizon URL Filter“ verwenden**, um „VMware Horizon URL Filter“ als Standardbrowser zu verwenden. Diese Eingabeaufforderung wird dann nicht mehr angezeigt, bis Sie Ihren Standardbrowser nach dem Anklicken von **„VMware Horizon URL Filter“ verwenden** wieder ändern.

Horizon Client blendet eventuell auch eine Warnmeldung ein, die Sie zur Auswahl einer Anwendung auffordert, wenn Sie auf eine URL klicken. In diesem Fall klicken Sie auf **Anwendung auswählen**, um nach einer Anwendung auf Ihrem Clientsystem zu suchen, oder auf **Im App Store suchen**, um eine neue Anwendung zu suchen und gegebenenfalls zu installieren. Wenn Sie auf **Abbrechen** klicken, wird die URL nicht geöffnet.

Jedes Unternehmen konfiguriert seine eigenen URL-Umleitungsrichtlinien. Bei Fragen, wie die Funktion der URL-Inhaltsumleitung in Ihrer Firma gehandhabt wird, wenden Sie sich an Ihren Systemadministrator.

Verwenden der Funktion der relativen Mausbewegung für CAD- und 3D-Anwendungen

Wenn Sie das Blast Extreme-Anzeigeprotokoll oder das PCoIP-Anzeigeprotokoll bei CAD- oder 3D-Anwendungen in einem View 5.2-Desktop oder höher verwenden, können Sie die Mausleistung durch Aktivierung der Funktion für die relative Mausbewegung verbessern.

In den meisten Fällen überträgt Horizon Client bei Verwendung von Anwendungen, die kein 3D-Rendering erfordern, Informationen über Mauszeigerbewegungen mithilfe von absoluten Koordinaten. Bei der Verwendung von absoluten Koordinaten rendert der Client die Mausbewegungen lokal, wodurch die Leistung insbesondere dann verbessert wird, wenn Sie sich außerhalb des Firmennetzwerks befinden.

Bei der Arbeit mit grafikintensiven Anwendungen wie AutoCAD oder bei 3D-Videospielen können Sie die Mausleistung verbessern, indem Sie die Funktion für die relative Mausbewegung aktivieren. Diese Funktion verwendet relative statt absoluter Koordinaten. Um diese Funktion zu verwenden, wählen Sie **Optionen > Relative Maus aktivieren** in der Horizon Client-Menüleiste aus.

Hinweis Wenn Sie Horizon Client im Fenstermodus und nicht im Vollbildmodus verwenden und die Funktion der relativen Mausbewegung aktiviert ist, können Sie möglicherweise den Mauszeiger nicht auf die Horizon Client-Menüoptionen oder aus dem Horizon Client-Fenster hinaus bewegen. Um diese Situation zu beheben, drücken Sie Strg+Alt.

Wenn die Funktion der relativen Mausbewegung aktiviert ist, kann die Performance langsam sein, wenn Sie sich außerhalb des Firmennetzwerks in einem WAN befinden.

Wichtig Für diese Funktion wird ein View 5.2-Desktop oder höher benötigt, und Sie müssen das 3D-Rendering für den Desktop-Pool einschalten. Weitere Informationen zu Pooleinstellungen und zu den Optionen für ein 3D-Rendering finden Sie in den Dokumenten *Einrichten von virtuellen Desktops in Horizon 7* und *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

Verwenden von Scannern

Sie können Informationen über Ihre Remote-Desktops und Remoteanwendungen unter Verwendung von Scannern einscannen, die mit Ihrem lokalen Clientsystem verbunden sind. Diese Funktion leitet Scandaten mit deutlich weniger Bandbreite um, als mit der USB-Umleitung erreicht werden kann.

Scannerumleitung unterstützt Standard-Scangeräte, die zu den TWAIN- und WIA (Windows Image Acquisition)-Formaten kompatibel sind. Obwohl die Gerätetreiber für den Scanner auf dem Clientsystem installiert sein müssen, ist es nicht nötig, sie auf dem Betriebssystem des Remote-Desktops, auf dem der Agent installiert ist, zu installieren.

Sofern ein Horizon-Administrator die Scannerumleitungsfunktion konfiguriert hat und Sie das PCoIP-Anzeigeprotokoll oder das Blast Extreme-Anzeigeprotokoll verwenden, kann ein mit Ihrem lokalen System verbundener Scanner auf einem Remote-Desktop oder in einer Remoteanwendung genutzt werden.

Wichtig Wenn Sie einen Scanner verwenden, verbinden Sie ihn nicht über das Menü **USB-Gerät verbinden** in Horizon Client. Dies würde dazu führen, dass das Gerät über die USB-Umleitung umgeleitet wird und die Leistung nicht ausreicht.

Wenn Scandaten zu einem Remote-Desktop oder einer Remoteanwendung umgeleitet werden, können Sie auf dem lokalen Computer nicht auf den Scanner zugreifen. Umgekehrt können Sie über den Remote-Desktop oder die Remoteanwendung nicht auf den Scanner zugreifen, wenn dieser gleichzeitig vom lokalen Computer genutzt wird.

Tipps zur Verwendung der Scannerumleitungsfunktion

- Um einen anderen als den Standardscanner auszuwählen oder um die Konfigurationseinstellungen zu ändern, klicken Sie auf das Scannersymbol des Remote-Desktops () in der Taskleiste oder im Infobereich. In RDS-Anwendungen wird das Taskleistensymbol zum lokalen Clientcomputer umgeleitet.

  Es besteht keine Notwendigkeit, das Menü zu verwenden, das angezeigt wird, wenn Sie auf dieses Symbol klicken. Die Scannerumleitung funktioniert ohne weitere Konfiguration. Das Symbolmenü ermöglicht es Ihnen, Optionen zu konfigurieren und beispielsweise die Festlegung, welche Geräte zu verwenden sind, wenn mehrere Geräte mit dem Clientcomputer verbunden sind, zu ändern.

  Hinweis Wenn das angezeigte Menü keine Scanner auflistet, bedeutet dies, dass ein inkompatibler Scanner mit dem Clientcomputer verbunden ist. Wenn das Scanner-Symbol nicht angezeigt wird, bedeutet dies, dass die Scannerumleitungsfunktion auf dem Remote-Desktop deaktiviert oder dort nicht installiert ist. Dieses Symbol wird auch auf Mac- und Linux-Clientsystemen nicht angezeigt, da die Funktion auf diesen Systemen nicht unterstützt wird.

- Klicken Sie im Menü auf die Option **Einstellungen**, um Optionen zur Steuerung der Bildkomprimierung, zum Ausblenden von Webcams aus dem Scannerumleitungsmenü und zur Festlegung der Vorgehensweise bei der Auswahl des Standardscanners auszuwählen.

  Sie können die Option zum Ausblenden vom Webcams auswählen, wenn Sie die Echtzeit-Audio/Video-Funktion zur Umleitung von Webcams verwenden möchten, was von VMware empfohlen wird. Verwenden Sie die Scannerumleitung in Verbindung mit Webcams, um ein Foto von sich selbst aufzunehmen und zu scannen.

  Hinweis Wenn Sie die Scannerumleitung für die Verwendung eines bestimmten Scanners konfigurieren und dieser Scanner nicht verfügbar ist, funktioniert die Scannerumleitung nicht.

- Auch wenn die meisten TWAIN-Scanner standardmäßig ein Dialogfeld mit Scannereinstellungen anzeigen, gilt dies nicht für alle von ihnen. Für jene, die keine Scannereinstellungen anzeigen, können Sie die Option **Einstellungen** im Menü des Scanner-Symbols verwenden und die Option **Dialogfeld 'Scannereinstellungen' immer einblenden** auswählen.
- Wenn ein zu scannendes Bild zu groß ist oder mit zu hoher Auflösung gescannt wird, funktioniert das Scannen möglicherweise nicht. In diesem Fall kann es vorkommen, dass die Fortschrittsanzeige für den Scanvorgang einzufrieren scheint oder die Scanneranwendung unerwartet schließt. Wenn Sie den Remote-Desktop minimieren, wird möglicherweise eine Fehlermeldung auf Ihrem Clientsystem angezeigt, die darauf hinweist, dass die Auflösung zu hoch eingestellt ist. Zur Behebung dieses Problems verringern Sie die Auflösung oder beschränken den zu scannenden Bereich auf einen Bildausschnitt und wiederholen den Scanvorgang.

Verwenden der Umleitung serieller Ports

Mit dieser Funktion haben Benutzer die Möglichkeit, lokal verbundene serielle Ports (COM-Ports) wie z. B. integrierte RS232-Ports oder USB-Seriell-Adapter umzuleiten. Geräte wie Drucker, Barcodeleser und andere serielle Geräte können mit diesen Ports verbunden und in Remote-Desktops verwendet werden.

Wenn ein Horizon-Administrator die Funktion zur Umleitung für serielle Ports konfiguriert hat, kann bei der Verwendung des VMware Blast Extreme- oder des PCoIP-Anzeigeprotokolls die Umleitung für serielle Ports ohne weitere Konfiguration auf Ihrem Remote-Desktop angewendet werden. Beispielsweise lässt sich ein COM1-Port auf dem lokalen Clientsystem als COM1-Port auf einen Remote-Desktop umleiten. Der COM2-Port wird als COM2-Port umgeleitet, solange der COM-Port nicht verwendet wird. Ist dies doch der Fall, wird der COM-Port zur Vermeidung von Konflikten neu zugeordnet. Wenn beispielsweise der COM1- und der COM2-Port bereits auf dem Remote-Desktop vorhanden sind, wird der COM1-Port standardmäßig dem COM3-Port zugeordnet.

Es müssen alle erforderlichen Gerätetreiber auf dem Clientsystem installiert sein, jedoch ist es nicht notwendig, diese auch auf dem Betriebssystem des Remote-Desktops, auf dem der Agent installiert ist, zu installieren. Wenn Sie beispielsweise einen USB-Seriell-Adapter verwenden, der für Ihr lokales Clientsystem bestimmte Gerätetreiber benötigt, müssen Sie diese Gerätetreiber nur auf dem Clientsystem installieren.

Wichtig Wenn Sie ein Gerät in einem USB-Seriell-Adapter verwenden, verbinden Sie dieses nicht über das Menü **USB-Gerät verbinden** in Horizon Client. Dies würde dazu führen, dass das Gerät über die USB-Umleitung umgeleitet und die Umleitung serieller Ports umgangen wird.

Tipps zur Verwendung der Umleitung serieller Ports

- Um die zugeordneten COM-Ports zu verbinden, deren Verbindung zu trennen oder anzupassen, klicken Sie auf das Symbol des seriellen Ports des Remote-Desktops () in der Taskleiste oder im Infobereich des Remote-Desktops.

  Wenn Sie auf das Symbol des seriellen Ports klicken, erscheint das Kontextmenü **Umleitung serieller COM-Ports für VMware Horizon**.

  Hinweis Sind die Optionen im Kontextmenü abgeblendet dargestellt, wurde die Konfiguration vom Administrator gesperrt. Beachten Sie auch, dass dieses Symbol nur angezeigt wird, wenn Sie die erforderlichen Versionen des Agenten und Horizon Client für Windows verwenden und eine Verbindung über Blast Extreme oder PCoIP hergestellt haben. Es erscheint nicht, wenn Sie sich mit einem Remote-Desktop von einem Mac-, Linux- oder einem mobilen Client aus verbinden.

- Im Kontextmenü werden die einzelnen Ports in einer bestimmten Form dargestellt, z. B. **COM1 zugeordnet zu COM3**. Der erste Port (in diesem Beispiel COM1) ist der physische Port oder der USB-Seriell-Adapter auf dem lokalen Clientsystem. Der zweite Port (in diesem Beispiel COM3) ist der Port, der auf dem virtuellen Desktop verwendet wird.
- Klicken Sie mit der rechten Maustaste auf einen COM-Port und wählen Sie im eingeblendeten Kontextmenü die Option **Porteigenschaften**.

  Im Dialogfeld „Porteigenschaften“ können Sie einen Port für die automatische Herstellung einer Verbindung beim Beginn einer Remote-Desktop-Sitzung konfigurieren. Außerdem haben Sie die Möglichkeit, festzulegen, dass das DSR-Signal (Data Set Ready) ignoriert wird, das für einige Modems oder andere Geräte erforderlich ist.

  Sie können auch die im Remote-Desktop verwendete Portnummer ändern. Wenn z. B. der Port COM1 auf dem Clientsystem dem Port COM3 auf dem Remote-Desktop zugeordnet ist und die verwendete Anwendung aber COM1 benötigt, können Sie die Portnummer in COM1 ändern. Wenn COM1 auf dem Remote-Desktop bereits vorhanden ist, erscheint eventuell die Anzeige **COM1 (Überlappend)**. Dieser überlappende Port lässt sich weiterhin verwenden. Der Remote-Desktop kann serielle Daten vom ESXi-Host oder vom Clientsystem über den Port empfangen.
- Stellen Sie sicher, dass die Verbindung mit einem zugeordneten COM-Port vor dem Start einer Anwendung hergestellt wird, die auf diesen Port zugreifen soll. Klicken Sie z. B. mit der rechten Maustaste auf einen COM-Port und wählen Sie im eingeblendeten Kontextmenü die Option **Verbinden**, um den Port auf dem Remote-Desktop zu verwenden. Beim Start der Anwendung wird dann der serielle Port geöffnet.

  Wenn ein umgeleiteter COM-Port auf einem Remote-Desktop geöffnet und verwendet wird, können Sie auf diesen Port auf dem lokalen Computer nicht zugreifen. Umgekehrt können Sie auf den COM-Port auf dem Remote-Desktop nicht zugreifen, wenn dieser Port auf dem lokalen Computer verwendet wird.

- Auf dem Remote-Desktop haben Sie die Möglichkeit, mithilfe der Registerkarte **Porteinstellungen** im Windows-Geräte-Manager die Standard-Baudrate für einen bestimmten COM-Port festzulegen. Stellen Sie sicher, dass diese Einstellungen mit jenen im Windows-Geräte-Manager auf Ihrem lokalen Clientsystem übereinstimmen. Beachten Sie, dass die Einstellungen auf dieser Registerkarte nur verwendet werden, wenn in der Anwendung keine Porteinstellungen festgelegt wurden.
- Bevor Sie die Verbindung mit dem COM-Port aufheben können, muss der Port in der Anwendung oder die Anwendung selbst geschlossen werden. Sie können dann mit der Option **Verbindung trennen** die Verbindung trennen und den physischen COM-Port für die Verwendung auf dem Clientcomputer zur Verfügung stellen.
- Wenn Sie einen seriellen Port für eine automatische Verbindung konfigurieren, eine Anwendung starten, die den seriellen Port öffnet, und dann die Desktop-Sitzung trennen sowie erneut verbinden, ist die Funktion zur automatischen Verbindung nicht wirksam. Sie können dann auch mit dem Taskleistensymbol des seriellen Ports keine Verbindung herstellen. In den meisten Fällen kann die Anwendung den seriellen Port nicht mehr verwenden. Dies ist das erwartete Verhalten. Sie müssen die Anwendung beenden, die Desktop-Sitzung trennen und dann erneut verbinden, um das Problem zu beheben.

Tastenkombinationen

Sie können Tastenkombinationen für Menübefehle und häufig auszuführende Aktionen verwenden.

Tastenkombinationen, die in Horizon Client genau wie in allen Anwendungen funktionieren

Tabelle 5-4. Häufig verwendete Tastenkombinationen

Aktion	Taste oder Tastenkombination
Klicken auf die markierte Schaltfläche im Dialogfeld.	Drücken Enter.
Aufrufen des Kontextmenüs.	Drücken Sie Umschalt+F10.
Klicken auf **Abbrechen** in einem Dialogfeld.	Drücken Sie die Esc-Taste.
Navigieren zwischen Elementen im Serverabschnittsfenster oder im Fenster für die Desktop- und Anwendungsauswahl.	Verwenden Sie eine Pfeiltaste für die Bewegung in Richtung des Pfeils. Drücken Sie die Tabulatortaste für die Bewegung nach rechts. Drücken Sie Umschalttaste+Tabulatortaste für die Bewegung nach links.
Löschen eines Elements im Serverabschnittsfenster oder im Fenster für die Desktop- und Anwendungsauswahl.	Drücken Sie die „Entf“-Taste.
Navigieren zwischen dem Start- und dem Desktop-Bildschirm in Windows 8.x	Drücken Sie die Windows-Taste.

Horizon Client -Tastenkombinationen im Fenster (Serverauswahlliste)

Tabelle 5-5. Tastenkombinationen speziell für das Fenster, in dem Sie angeben, mit welchem Server eine Verbindung hergestellt werden soll

Menübefehl oder Aktion	Tastenkombination
Öffnen des Hilfesystems in einem Browserfenster	Alt+O+H, Strg+H
Befehl **Neuer Server**	Alt+N
Anzeigen des Fensters mit Support-Informationen	Alt+O+S
Anzeigen des Infofensters von Horizon Client	Alt+O+V
Befehl **SSL konfigurieren**	Alt+O+O
Befehl **Selektor nach Start eines Elements ausblenden**	Alt+O+A

Tastenkombinationen für die Remote-Desktop- und -Anwendungsauswahl

Tabelle 5-6. Tasten und Tastenkombinationen im Fenster für die Desktop- und Anwendungsauswahl

Menübefehl oder Aktion	Tastenkombination
Öffnen des Hilfesystems in einem Browserfenster	Alt+O+H, Strg+H
Anzeigen des Menüs **Optionen**	Alt+O
Anzeigen des Fensters mit Support-Informationen	Alt+O+S
Anzeigen des Infofensters von Horizon Client	Alt+O+V
Abmelden vom Remote-Desktop	Shift+F10+B
Trennen der Verbindung zum Server und Abmelden vom Server	Alt+D
Wechseln zwischen **Favoriten anzeigen** und **Alle anzeigen**	Alt+F
Beim Anzeigen von Favoriten: Wechseln zum nächsten Element im Suchergebnis, nachdem die ersten Zeichen des Anwendungs- bzw. Desktop-Namens eingegeben wurden	F4
Beim Anzeigen von Favoriten: Wechseln zum vorherigen Element im Suchergebnis	Shift+F4
Markieren als Favorit oder Entfernen der Kennzeichnung als Favorit	Shift+F10+F
Anzeigen des Menüs **Einstellungen**	Alt+S oder Shift+F10+E
Starten des ausgewählten Elements	Enter oder Shift+F10+S
Anheften einer Verknüpfung für den Remote-Desktop oder die Remoteanwendung zum Startmenü des Clientsystems (für Windows 7 und früher) oder zum Startbildschirm (für Windows 8.x)	Shift+F10+Z
Anzeigen des Kontextmenüs für Anzeigeeinstellungen für den ausgewählten Remote-Desktop	Shift+F10+A
Verwenden des PCoIP-Anzeigeprotokolls zum Herstellen einer Verbindung mit dem ausgewählten Remote-Desktop	Shift+F10+P
Verwenden des RDP-Anzeigeprotokolls zum Herstellen einer Verbindung mit dem ausgewählten Remote-Desktop	Shift+F10+M
Erstellen einer Desktop-Verknüpfung für das ausgewählte Element	Shift+F10+V
Hinzufügen des ausgewählten Elements zu Ihrem Startmenü oder zu Ihrem Startbildschirm	Shift+F10+Z
Zurücksetzen des ausgewählten Desktops (falls Ihr Administrator Ihnen das Zurücksetzen erlaubt)	Shift+F10+D
Aktualisieren der Desktop- und Anwendungsliste	F5

Tastenkombinationen des Desktop-Fensters (mit einer PCoIP- oder VMware Blast Extreme-Sitzung)

Diese Tastenkombinationen funktionieren, wenn Sie zuerst Strg+Alt drücken oder auf die Horizon Client-Menüleiste klicken, anstatt innerhalb des Remote-Desktop-Betriebssystems, bevor Sie die Tasten verwenden.

Tabelle 5-7. Tastenkombinationen für PCoIP- und VMware Blast-Sitzungen

Menübefehl oder Aktion	Tastenkombination
Freigeben des Mauszeigers, sodass er sich nicht mehr im Remote-Desktop-Betriebssystem befindet	Strg+Alt
Menü „Optionen“ anzeigen	Alt+O
Anzeigen des Fensters mit Support-Informationen	Alt+O+S
Anzeigen des Infofensters von Horizon Client	Alt+O+V
Aufrufen des Dialogfeldes für die Einstellungen der Ordnerfreigabe	Alt+O+F
Umschalten von **Anzeigeskalierung aktivieren**	Alt+O+N
Befehl **Zu einem anderen Desktop wechseln**	Alt+O+S
Befehl **Verbindung mit diesem Desktop automatisch herstellen**	Alt+O+B
Befehl **Relative Maus aktivieren**	Alt+O+R
Befehl **Strg+Alt+Entf senden**	Alt+O+C
Befehl **Trennen**	Alt+O+E
Befehl **Trennen und abmelden**	Alt+O+A
Befehl **USB-Gerät verbinden**	Alt+V

Fehlerbehebung für Horizon Client 6

Sie können die meisten Probleme mit Horizon Client lösen, indem Sie den Desktop neu starten oder zurücksetzen oder die VMware Horizon Client-Anwendung neu installieren.

Dieses Kapitel behandelt die folgenden Themen:

Probleme bei der Tastatureingabe

Wenn bei einer Tastatureingabe in einem Remote-Desktop oder einer Remoteanwendung die Tasten nicht funktionieren, kann dies mit der Sicherheitssoftware auf Ihrem lokalen Client zusammenhängen.

Problem

Bei einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung werden während der Eingabe keine Zeichen auf dem Bildschirm dargestellt. Ein anderes mögliches Phänomen ist die mehrmalige Wiederholung einer Taste.

Ursache

Einige Sicherheitsprogramme wie z. B. Norton 360 Total Security verfügen über eine Funktion zur Ermittlung von Keylogger-Programmen, die die Tastatureingabe sperrt. Mit dieser Sicherheitsfunktion soll das System gegen unerwünschte Spyware geschützt werden, mit der z. B. Kennwörter oder Kreditkartennummern entwendet werden. Allerdings kann es vorkommen, dass diese Sicherheitssoftware Horizon Client an der Übergabe von Tastatureingaben an den Remote-Desktop oder an die Remoteanwendung hindert.

Lösung

- Deaktivieren Sie auf dem Clientsystem die Funktion zur Ermittlung von Keyloggern Ihrer Antivirus- oder Sicherheitsoftware.

Was tun, wenn Horizon Client unerwartet beendet wird

Horizon Client wird möglicherweise beendet, selbst wenn Sie die Anwendung nicht schließen.

Problem

Horizon Client wird möglicherweise unerwartet beendet. Abhängig von Ihrer Verbindungsserver-Konfiguration kann eine Meldung wie die folgende angezeigt werden: `Es besteht keine sichere Verbindung mit View-Verbindungsserver`. In manchen Fällen wird jedoch keine Meldung angezeigt.

Ursache

Dieses Problem tritt auf, wenn die Verbindung zum Verbindungsserver getrennt wird.

Lösung

- Starten Sie Horizon Client neu. Sobald der Verbindungsserver wieder ausgeführt wird, können Sie wieder erfolgreich eine Verbindung herstellen. Sollten weiterhin Probleme mit der Verbindung bestehen, wenden Sie sich an Ihren Horizon-Administrator.

Neustarten eines Remote-Desktops

Eventuell muss ein Remote-Desktop neu gestartet werden, wenn das Desktop-Betriebssystem nicht mehr reagiert. Der Neustart eines Remote-Desktops entspricht dem Neustart des Windows-Betriebssystems. In der Regel werden Sie dabei vom Desktop-Betriebssystem aufgefordert, alle nicht gespeicherten Daten zu speichern, bevor der Neustart erfolgt.

Sie können einen Remote-Desktop nur dann neu starten, wenn ein Horizon-Administrator die Funktion zum Neustart eines Desktops für den Desktop aktiviert hat.

Informationen zur Aktivierung der Funktion zum Neustart eines Desktops finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

Vorgehensweise

- Verwenden Sie die Option **Desktop neu starten**.

Option	Aktion
Aus dem Desktop-Betriebssystem heraus	Wählen Sie **Optionen > Desktop neu starten** aus der Menüleiste aus.
Im Desktop-Auswahlfenster	Klicken Sie mit der rechten Maustaste auf das Desktop-Symbol und wählen Sie **Desktop neu starten** aus.

  Horizon Client fordert Sie zur Bestätigung des Neustarts auf.

Das Betriebssystem im Remote-Desktop wird neu gestartet und Horizon Client wird getrennt bzw. vom Desktop abgemeldet.

Weiter

Warten Sie eine Weile, bis das System gestartet wurde, und versuchen Sie anschließend, erneut eine Verbindung zum Remote-Desktop herzustellen.

Wenn das Problem durch den Neustart des Remote-Desktops nicht behoben werden kann, müssen Sie den Remote-Desktop eventuell zurücksetzen. Siehe „Zurücksetzen eines Remote-Desktops oder von Remoteanwendungen“, auf Seite 117.

Zurücksetzen eines Remote-Desktops oder von Remoteanwendungen

Sie müssen einen Remote-Desktop eventuell zurücksetzen, wenn das Betriebssystem nicht mehr reagiert und der Neustart des Remote-Desktops das Problem nicht löst. Durch das Zurücksetzen von Remoteanwendungen werden alle geöffneten Anwendungen beendet.

Das Zurücksetzen eines Remote-Desktops entspricht dem Betätigen der Reset-Taste auf einem physischen Computer, mit der der Neustart des Computers erzwungen wird. Alle Dateien, die auf dem Remote-Desktop geöffnet sind, werden geschlossen und nicht gespeichert.

Das Zurücksetzen von Remoteanwendungen entspricht dem Beenden der Anwendungen, ohne nicht gespeicherte Daten zu speichern. Alle geöffneten Anwendungen werden geschlossen, auch die Anwendungen, die zu verschiedenen RDS-Server-Farmen gehören.

Sie können einen Remote-Desktop nur zurücksetzen, wenn ein Horizon-Administrator die Funktion zum Zurücksetzen eines Desktops für den Desktop aktiviert hat.

Informationen zur Aktivierung der Funktion zum Zurücksetzen eines Desktops finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

Vorgehensweise

1 Verwenden Sie zum Zurücksetzen eines Remote-Desktops den Befehl **Desktop zurücksetzen**.

Option	Aktion
Aus dem Desktop-Betriebssystem heraus	Wählen Sie **Optionen > Desktop zurücksetzen** aus der Menüleiste aus.
Im Fenster für die Desktop- und Anwendungsauswahl	Klicken Sie mit der rechten Maustaste auf das Desktop-Symbol und wählen Sie **Desktop zurücksetzen** aus.

2 Verwenden Sie zum Zurücksetzen von Remoteanwendungen die Schaltfläche **Zurücksetzen** im Fenster für die Desktop- und Anwendungsauswahl.

   a Klicken Sie in der Menüleiste auf die Schaltfläche **Einstellungen** (Zahnradsymbol).

   b Wählen Sie im linken Fensterbereich **Anwendungen** aus, klicken Sie im rechten Fensterbereich auf die Schaltfläche **Zurücksetzen** und klicken Sie auf **OK**.

Wenn Sie einen Remote-Desktop zurücksetzen, wird das Betriebssystem im Remote-Desktop neu gestartet und Horizon Client getrennt bzw. vom Desktop abgemeldet. Wenn Sie Remoteanwendungen zurücksetzen, werden diese beendet.

Weiter

Warten Sie eine Weile, bis das System gestartet wurde, und versuchen Sie anschließend erneut, eine Verbindung mit dem Remote-Desktop oder der Remoteanwendung herzustellen.

Deinstallieren von Horizon Client

Manchmal können Sie Probleme mit Horizon Client einfach dadurch beheben, dass Sie die Horizon Client-Anwendung deinstallieren und anschließend neu installieren.

Die Vorgehensweise beim Deinstallieren von Horizon Client entspricht der Vorgehensweise bei der Deinstallation anderer Anwendungen.

Verwenden Sie beispielsweise das Applet **Software** Ihres Windows-Betriebssystems, um die VMware Horizon Client-Anwendung zu entfernen.

Nachdem Sie die Deinstallation durchgeführt haben, können Sie die Anwendung von neuem installieren.

Siehe Kapitel 2, „Installation von Horizon Client für Windows“, auf Seite 27.

Index

W

Z