Verwenden von VMware Horizon Client für Linux

VMware Horizon Client for Linux 4.4

vmware®

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

https://docs.vmware.com/de/

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

Verwenden von VMware Horizon Client für Linux

Das Handbuch *Verwenden von VMware Horizon Client für Linux* bietet Informationen zur Installation und Verwendung der VMware Horizon® Client™-Software auf einem Linux-Clientsystem zur Verbindungsherstellung mit einem View-Desktop im Datencenter.

Die Informationen in diesem Dokument enthalten Systemanforderungen und Anleitungen zur Installation und Verwendung von Horizon Client für Linux.

Diese Informationen sind für Administratoren vorgesehen, die eine Bereitstellung von View mit Linux-Clientsystemen einrichten müssen. Die Informationen wurden für erfahrene Systemadministratoren verfasst, die mit der Technologie virtueller Maschinen sowie mit Datencenter-Vorgängen vertraut sind.

Hinweis Dieses Dokument betrifft überwiegend Horizon Client für Linux, den VMware zur Verfügung stellt. Darüber hinaus bieten verschiedene VMware-Partner Thin Client- und Zero Client-Geräte für View-Bereitstellungen an. Die Funktionen, die für die einzelnen Thin Client- oder Zero Client-Geräte verfügbar sind, sowie die unterstützten Betriebssysteme hängen vom Hersteller, dem Modell und der Konfiguration ab, für die sich das jeweilige Unternehmen unterscheidet. Informationen zu Herstellern und Modellen für diese Client-Geräte finden Sie im VMware-Kompatibilitätsleitfaden, der auf der VMware-Website zur Verfügung steht.

Systemanforderungen und Installation

1

Clientsysteme müssen bestimmte Hardware- und Softwareanforderungen erfüllen. Die Installation von Horizon Client gestaltet sich ähnlich wie die Installation der meisten anderen Anwendungen.

Dieses Kapitel behandelt die folgenden Themen:

Systemanforderungen für Linux-Clientsysteme

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

Hinweis Diese Systemanforderungen betreffen den Horizon Client für Linux, den VMware zur Verfügung stellt. Darüber hinaus bieten verschiedene VMware-Partner Thin Client- und Zero Client-Geräte für View-Bereitstellungen an. Die Funktionen, die für die einzelnen Thin Client- oder Zero Client-Geräte verfügbar sind, sowie die unterstützten Betriebssysteme hängen vom Hersteller, dem Modell und der Konfiguration ab, für die sich das jeweilige Unternehmen unterscheidet. Informationen zu Herstellern und Modellen für diese Client-Geräte finden Sie im VMware-Kompatibilitätsleitfaden, der auf der VMware-Website zur Verfügung steht.

Hinweis

- Ab der Version 7.0 wird View Agent in Horizon Agent umbenannt.
- Das Anzeigeprotokoll VMware Blast, das ab Horizon Client 4.0 und Horizon Agent 7.0 verfügbar ist, wird auch als VMware Blast Extreme bezeichnet.

Architektur

i386, x86_64, ARM

Arbeitsspeicher

Mindestens 2GB Arbeitsspeicher (RAM)

Betriebssystem

Betriebssystem	Version
Ubuntu	12.04, 14.04
Ubuntu, 64-Bit	12.04, 14.04, 16.04
Red Hat Enterprise Linux (RHEL)	6.8
Red Hat Enterprise Linux (RHEL) 64 Bit	6.8, 7.2/7.3
SUSE Linux Enterprise Desktop (SLED)	11 SP4
CentOS	6.8

OpenSSL-Anforderung

Horizon Client erfordert eine bestimmte Version der OpenSSL-Bibliothek. Die richtige Version wird automatisch heruntergeladen und installiert.

View-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. Mit einem Sicherheitsserver erfordern die Clientsysteme keine VPN-Verbindung.

Gehostete Remoteanwendungen sind nur auf Servern mit Horizon 6.0 (mit View) oder höher verfügbar.

Anzeigeprotokoll

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

Bildschirmauflösung auf dem Clientsystem

Minimale Auflösung: 1024 x 768 Pixel

Hardwareanforderungen für VMware Blast und PCoIP

- x86- oder x64-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- oder x64-basierter Prozessor mit SSE2-Erweiterungen mit einer Prozessorgeschwindigkeit von 800 MHz oder höher.
- 128 MB RAM.

Softwareanforderungen für Microsoft RDP

Verwendet die neueste verfügbare `rdesktop`-Version.

Softwareanforderungen für FreeRDP

Wenn Sie vorhaben, eine RDP-Verbindung mit View-Desktops zu verwenden, und Sie lieber einen FreeRDP Client für die Verbindung verwenden möchten, müssen Sie die richtige Version von FreeRDP und alle verfügbaren Patches installieren. Siehe „Installation und Konfiguration von FreeRDP“, auf Seite 50.

Weitere Softwareanforderungen

Je nach verwendeter Linux-Distribution gelten für Horizon Client noch andere spezielle Softwareanforderungen. Stellen Sie sicher, dass der Installationsassistent von Horizon Client in der Lage ist, Ihr System auf Bibliothekskompatibilitäten und -abhängigkeiten zu überprüfen. Die folgende Liste von Anforderungen betrifft nur Ubuntu-Distributionen.

- `libudev0.so.0`

  Hinweis Wenn mit Horizon Client 4.2 begonnen wird, ist `libudev0` für den Start von Horizon Client erforderlich. Standardmäßig wird `libudev0` nicht in Ubuntu 14.04 installiert.

- Zur Unterstützung von Zeitüberschreitungen bei Sitzungen im Leerlauf: Bereitstellung von `libXsso.so.1`.
- Zur Unterstützung von Flash-URL-Umleitung: Bereitstellung von `libexpat.so.1`. (Die Datei `libexpat.so.0` ist nicht mehr erforderlich.)
- Bei Verwendung mehrerer Monitore Aktivierung von Xinerama zur Leistungsverbesserung.

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 x86- und x64-Geräten unterstützt. Auf ARM-Prozessoren wird diese Funktion nicht unterstützt. Das Clientsystem muss mindestens die folgenden Hardwareanforderungen erfüllen.

Auflösung	Frame-Rate	CPU	Erforderlicher Arbeitsspeicher
320 x 240	15 FPS	2 Kerne, 1800 MHz	105 MB
640 x 480	15 FPS	2 Kerne, 2700 MHz	150 MB
1280 x 720	15 FPS	4 Kerne, 3400 MHz	210 MB

- Horizon Client erfordert die folgenden Bibliotheken:
  - `Video4Linux2`
  - `libv4l`
  - `Pulse Audio`

  Die Plug-In-Datei „`/usr/lib/pcoip/vchan_plugins/libviewMMDevRedir.so`“ hat die folgenden Abhängigkeiten:

  ```
  libuuid.so.1
  libv4l2.so.0
  libspeex.so.1
  libudev0
  libtheoradec.so.1
  libtheoraenc.so.1
  libv4lconvert.so.0
  libjpeg.so.8
  ```

  Alle diese Dateien müssen auf dem Clientsystem vorhanden sein, da anderenfalls die Echtzeit-Audio/Video-Funktion nicht funktioniert. Beachten Sie, dass diese Abhängigkeiten neben den erforderlichen Abhängigkeiten für Horizon Client selbst benötigt werden.

- 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)

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

Da die MMR die Medienverarbeitung vom Server zum Client überträgt, muss der Client über die nachfolgend aufgeführten Mindesthardwareanforderungen verfügen.

Prozessor:	Intel Pentium 4 oder AMD Athlon Dual-Core
Prozessorgeschwindigkeit:	1,5 GHz allgemein oder 1,8 GHz für Full HD
Arbeitsspeicher:	2 GB RAM
Videoadapter:	Hardwarebeschleunigt

Sie müssen eine der im Folgenden genannten Bibliotheken installieren, um Videowiedergabeprobleme zu vermeiden:

- GStreamer Core Library und gstreamer-ffmpeg 0.10
- GStreamer Core Library und fluendo 0.10

Wenn Sie auf SLED 11 SP4 Videowiedergabeprobleme wie einen schwarzen Bildschirm feststellen, sollten Sie die Bibliothek „libvdpau“ entfernen.

Auf Thin Clients von HP müssen Sie die Datei `/usr/lib/gstreamer-0.10/libgstfluvadec.so` entfernen, um Videowiedergabeprobleme wie einen Horizon Client-Absturz oder einen schwarzen Bildschirm zu vermeiden.

Auf Thin Clients von Dell Wyse ist die Videowiedergabe möglicherweise nicht mit der vorinstallierten fluendo-Bibliothek kompatibel. Wenden Sie sich zum Beheben des Problems an den Dell-Support, um die neueste fluendo-Bibliothek abzurufen.

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.

MMR ist nicht standardmäßig aktiviert. Um sie zu aktivieren, müssen Sie die Konfigurationsoption `view.enableMMR` festlegen. Weitere Informationen finden Sie unter „Horizon Client-Konfigurationseinstellungen und -Befehlszeilenoptionen“, auf Seite 29.

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:

- Diese Funktion wird nur für PCoIP unterstützt. Auf ARM-Prozessoren wird diese Funktion nicht unterstützt.
- 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.
- Auf den Clientsystemen muss das geeignete Flash-Plug-In installiert sein.
  a Installieren Sie die Datei `libexpat.so.1` bzw. stellen Sie sicher, dass diese Datei bereits installiert ist.

    Stellen Sie sicher, dass die Datei im Verzeichnis „`/usr/lib`“ oder „`/usr/local/lib`“ installiert ist.

  b Installieren Sie die Datei `libflashplayer.so` oder stellen Sie sicher, dass diese Datei bereits installiert ist.

    Vergewissern Sie sich, dass die Datei im geeigneten Flash-Plug-In-Verzeichnis für Ihr Linux-Betriebssystem installiert ist.

  c Installieren Sie das Programm `wget` oder stellen Sie sicher, dass die Programmdatei bereits installiert ist.

- `libffi.so.5` ist bei Ubuntu 14.04- und Ubuntu 16.04-Distributionen für das Funktionieren der Flash-URL-Umleitung erforderlich. Standardmäßig verfügen Ubuntu 14.04- und Ubuntu 16.04-Distributionen aber nur über `libffi.so.6`. Sie können diese Beschränkung durch Herstellung einer symbolischen Verknüpfung zwischen `libffi.so.6` und `libffi.so.5` umgehen.

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 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.

Benutzer, die sich mithilfe von Smartcards authentifizieren, müssen über eine Smartcard verfügen, und jede Smartcard muss ein Benutzerzertifikat enthalten.

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.

Konfigurieren von Horizon Client für die Smartcard-Authentifizierung

Um eine Smartcard in Horizon Client verwenden zu können, müssen Sie bestimmte Konfigurationsschritte durchführen.

Voraussetzungen

- Installieren Sie Horizon Client.
- (Optional) Damit das Feld **Benutzernamenhinweis** im Anmeldungsdialogfeld von Horizon Client angezeigt wird, aktivieren Sie die Funktion für den Smartcard-Benutzernamenhinweis im Verbindungsserver. Weitere Informationen dazu finden Sie unter „Einrichten der Smartcard-Authentifizierung“ im Dokument *Administration von View*.

Vorgehensweise

1 Erstellen Sie den Ordner `/usr/lib/vmware/view/pkcs11`.

2 Erstellen Sie eine symbolische Verknüpfung zur pkcs11-Bibliothek, die für die Smartcard-Authentifizierung verwendet wird.

Führen Sie beispielsweise den folgenden Befehl aus:

```
sudo ln –s /usr/lib/pkcs11/libgtop11dotnet.so
                /usr/lib/vmware/view/pkcs11
```

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*.
- 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*.

Installationsoptionen

Während des Installationsvorgangs für Horizon Client werden Sie aufgefordert, zu bestätigen, dass verschiedene Komponenten installiert werden. Standardmäßig werden alle Komponenten installiert.

In der folgenden Tabelle finden Sie zu jeder optionalen Komponente eine kurze Übersicht.

Tabelle 1-1. Horizon Client für Linux-Installationsoptionen

Option	Beschreibung
USB-Umleitung	Gibt Benutzern Zugriff auf lokal verbundene USB-Geräte auf ihren Desktops. Die USB-Umleitung wird für Remote-Desktops unterstützt, die auf Maschinen für Einzelbenutzer bereitgestellt werden. Die Komponentendateien werden im Ordner `/usr/lib/vmware/view/usb/` installiert. Die Dienste `vmware-usbarbitrator` und `vmware-view-usbd` werden automatisch ausgeführt, wenn Sie dem Installationsprogramm ermöglichen, installierte Dienste nach der Installation zu registrieren und zu starten. Andernfalls können Sie die zwei Dienste manuell starten, indem Sie `vmware-usbarbitrator` und `vmware-view-usbd` unter `/usr/lib/vmware/view/usb/` ausführen. **Hinweis** Sie können mithilfe von Gruppenrichtlinieneinstellungen die USB-Umleitung für spezifische Benutzer deaktivieren.
Echtzeit-Audio/Video	Leitet Webcams und Audiogeräte um, die mit dem Clientsystem verbunden sind, sodass diese auf dem Remote-Desktop eingesetzt werden können. Die Komponentendatei wird im Ordner `/usr/lib/pcoip/vchan_plugins/` installiert.
Virtuelles Drucken	Benutzer können mit jedem beliebigen Drucker drucken, der auf ihren Clientcomputern zur Verfügung steht. Benutzer müssen keine zusätzlichen Treiber auf ihren Remote-Desktops installieren. Die Komponentendateien werden im Ordner `/usr/lib/vmware/view/virtualPrinting/` installiert. Nach dem Installieren des Clients müssen Sie diese Funktion nicht manuell konfigurieren, wenn Sie für das Installationsprogramm die Registrierung und den Start der installierten Dienste nach der Installation festlegen. Andernfalls können Sie diese Funktion konfigurieren und aktivieren, indem Sie die Anweisungen unter „Aktivieren der virtuellen Druckfunktion auf einem Linux-Client“, auf Seite 20 befolgen. In Horizon 6.0.2 und höher wird das virtuelle Drucken von den folgenden Remote-Desktops und -anwendungen unterstützt: ■ Auf Einzelbenutzer-Maschinen bereitgestellte Desktops. ■ Desktops, die auf RDS-Hosts bereitgestellt werden, wobei die RDS-Hosts virtuelle Maschinen sind. ■ Remoteanwendungen, die von RDS-Hosts bereitgestellt werden. ■ Remoteanwendungen, die von Horizon Client innerhalb von Remote-Desktops gestartet werden (geschachtelte Sitzungen).
Multimedia-Umleitung (MMR)	Leitet Multimedia-Streams vom Desktop zur Clientmaschine um, wo der Stream verarbeitet wird. Die Komponentendatei wird unter `/usr/lib/vmware/view/vdpService/` installiert.
Smartcard	Ermöglicht Benutzern die Authentifizierung per Smartcard, wenn sie das VMware Blast- oder PCoIP-Anzeigeprotokoll verwenden. Diese Option ist standardmäßig im Clientinstallationsprogramm ausgewählt. Dies gilt jedoch nicht für den Fall, dass Sie das View Agent-Installationsprogramm innerhalb des Remote-Desktops ausführen. Smartcard wird für Remote-Desktops unterstützt, die auf Maschinen für Einzelbenutzer und RDS-Hosts bereitgestellt werden. Für die Smartcard-Unterstützung auf RDS-Hosts müssen Sie über View Agent 6.1.1 oder höher verfügen. Die Komponentendateien werden im Ordner `/usr/lib/pcoip/vchan_plugins/` installiert.
Clientlaufwerksumleitung	Damit können Benutzer Ordner und Laufwerke auf dem Clientcomputer für Remote-Desktops und -anwendungen freigeben. Laufwerke können auch bereitgestellte Laufwerke und USB-Speichergeräte umfassen. Die Komponentendateien werden unter `/usr/lib/vmware/view/vdpService/` installiert.

Installieren oder Aktualisieren von Horizon Client für Linux über die VMware-Website für Produkt-Downloads

Sie können ein Horizon Client-Installationsprogrammpaket von der entsprechenden VMware-Downloadseite herunterladen und ausführen. Das Installationsprogramm umfasst Module für Funktionen wie zum Beispiel USB-Umleitung, virtuelles Drucken, Echtzeit-Audio/Video, Smartcard und Clientlaufwerksumleitung.

Hinweis Bei den meisten Linux-Distributionen wird vom Horizon Client-Installationsprogramm-Paket ein GUI-Assistent gestartet. Bei SUSE Linux-Distributionen wird vom Installationsprogramm-Paket ein Befehlszeilen-Assistent gestartet. Sie können das Installationsprogramm auch mit der Option `--console` ausführen, um den Befehlszeilen-Assistent zu starten.

Voraussetzungen

- Stellen Sie sicher, dass das Clientsystem ein unterstütztes Betriebssystem ausführt. Siehe „Systemanforderungen für Linux-Clientsysteme“, auf Seite 8.
- Machen Sie sich mit den Installationsoptionen vertraut. Siehe „Installationsoptionen“, auf Seite 15.
- Stellen Sie sicher, dass Sie auf dem Hostsystem über die Berechtigung zum Stammzugriff verfügen.
- Stellen Sie sicher, dass VMware Workstation nicht auf dem Clientsystem installiert ist.
- Wenn Sie beabsichtigen, das RDP-Anzeigeprotokoll zur Verbindungsherstellung mit einem View-Desktop zu verwenden, müssen Sie sicherstellen, dass Sie den entsprechenden RDP-Client installiert haben. Siehe „Systemanforderungen für Linux-Clientsysteme“, auf Seite 8.
- Deinstallieren Sie eine frühere Version der Horizon Client-Software. Siehe „Deinstallieren von Horizon Client für Linux“, auf Seite 85.
- Wenn Sie beabsichtigen, das Befehlszeilen-Installationsprogramm zu verwenden, machen Sie sich mit den Installationsoptionen der Linux-Befehlszeile vertraut. Siehe „Befehlszeilen-Installationsoptionen für den Linux Client“, auf Seite 18.
- Führen Sie auf SUSE Linux-Distributionen `sudo zypper install python-curses` zur Installation der `curses`-Bibliothek aus.
- Führen Sie in einer python2-Umgebung auf Ubuntu 16.04 x64-Distributionen `sudo apt-get install python-gtk2` zur Installation der `gtk2`-Bibliothek aus.

Das Installationsprogramm durchsucht standardmäßig während des Installationsvorgangs die Systembibliotheken, um festzustellen, ob das System zu Horizon Client kompatibel ist. Diesen Suchschritt können Sie jedoch durch entsprechende Auswahl überspringen.

Vorgehensweise

1 Laden Sie auf dem Linux-Clientsystem die Horizon Client-Installationsprogramm-Datei von der Produkt-Download-Seite für Horizon Client unter http://www.vmware.com/go/viewclients herunter.

  Der Name der Datei lautet `VMware-Horizon-Client-`*`x.x.x-yyyyyyy.arch`*`.bundle`, wobei *x.x.x* die Versionsnummer darstellt, *yyyyyyy* die Build-Nummer und *arch* entweder für `x86` oder für `x64` steht.

2 Öffnen Sie ein Terminalfenster, wechseln Sie zu dem Verzeichnis, in dem sich die Installationsprogramm-Datei befindet, und führen Sie das Installationsprogramm unter Verwendung des entsprechenden Befehls aus.

Option	Befehl
Für den GUI-Assistenten, wenn Sie über die Berechtigung zur Ausführung ausführbarer Dateien verfügen	`sudo ./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle`
Für den GUI-Assistenten, wenn Sie nicht über die Berechtigung zur Ausführung ausführbarer Dateien verfügen	`sudo sh ./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle`
Für das Befehlszeilen-Installationsprogramm	`sudo ./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle --console`

Der Assistent des Installationsprogramms wird geöffnet. Anschließend werden Sie aufgefordert, dem Endbenutzerlizenzvertrag zuzustimmen.

3 Folgen Sie den Anweisungen, um die Installation abzuschließen.

Wichtig Sie werden aufgefordert, dem Installationsprogramm zu ermöglichen, die installierten Dienste nach der Installation zu registrieren und zu starten. Wenn Sie für das Installationsprogramm die Durchführung dieser Aufgaben angeben, müssen Sie nicht nach jedem Neustart den USB-Umleitungsdienst manuell starten und auch die Funktion des virtuellen Druckens nicht manuell aktivieren.

4 Geben Sie nach dem Abschluss der Installation an, ob die Kompatibilitätsüberprüfung für Bibliotheken, von denen verschiedene Funktionskomponenten abhängig sind, durchgeführt werden soll.

Die Systemüberprüfung zeigt für jede Bibliothek ein Kompatibilitätsüberprüfungsergebnis an.

Ergebniswert	Beschreibung
Erfolgreich	Alle erforderlichen Bibliotheken wurden gefunden.
Fehlgeschlagen	Die angegebene Bibliothek wurde nicht gefunden.

Protokollinformationen zur Installation werden in der Datei `/tmp/vmware-root/vmware-installer-pid.log` aufgezeichnet.

Weiter

Starten Sie Horizon Client und stellen Sie sicher, dass Sie sich am richtigen virtuellen Desktop anmelden können. Siehe „Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung“, auf Seite 55.

Befehlszeilen-Installationsoptionen für den Linux Client

Sie können Horizon Client mithilfe der Befehlszeilen-Installationsoptionen auf einem Linux-System installieren.

Installieren Sie Horizon Client unbeaufsichtigt mithilfe der `--console`-Option und anderen Befehlszeilenoptionen und Einstellungen für Umgebungsvariablen. Die unbeaufsichtigte Installation ermöglicht eine effiziente Bereitstellung von View-Komponenten in einem großen Unternehmen.

Die folgende Tabelle führt die Optionen auf, die Sie für die Ausführung der Installationsdatei `VMware-Horizon-Client-x.x.x-yyyyyyyarch.bundle` verwenden können.

Tabelle 1-2. Linux Befehlszeilen-Installationsoptionen

Option	Beschreibung
`--help`	Zeigt Nutzungsdaten.
`--console`	Gibt Ihnen die Möglichkeit, das Befehlszeilen-Installationsprogramm in einem Terminal-Fenster zu verwenden.
`--custom`	Zeigt alle Installationsfragen, selbst wenn Standardantworten im Skript stehen, beispielsweise durch Verwenden der `--set-setting`-Optionen. Der Standard ist `--regular`, d. h. dass nur Fragen angezeigt werden, die keine Standardantwort haben.
`--eulas-agreed`	Stimmt dem Endbenutzerlizenzvertrag zu.
`--gtk`	Öffnet das GUI-basierte VMware-Installationsprogramm (Standard). Wenn die GUI aus welchem Grund auch immer nicht angezeigt oder geladen werden kann, wird der Konsolenmodus verwendet.
`--ignore-errors` oder `-I`	Lässt die Fortsetzung der Installation zu, selbst wenn eines der Installationsskripte einen Fehler aufweist. Da der fehlerhafte Bereich nicht vollständig ausgeführt wird, kann die Komponente möglicherweise nicht richtig konfiguriert werden.
`--regular`	Zeigt Installationsfragen, die zuvor nicht beantwortet wurden oder obligatorisch sind. Dies ist die Standardoption.
`--required`	Zeigt nur die Lizenzvereinbarung und fährt dann mit der Installation des Clients fort. Der Standard ist `--regular`, d. h. dass nur Fragen angezeigt werden, die keine Standardantwort haben.
`--set-setting vmware-horizon-smartcard smartcardEnable yes`	Installiert die Smartcard-Komponente.
`--set-setting vmware-horizon-rtav rtavEnable yes`	Installiert die Echtzeit-Audio/Video-Komponente.
`--set-setting vmware-horizon-usb usbEnable yes`	Installiert die USB-Umleitungsfunktion.
`--set-setting vmware-horizon-virtual-printing tpEnable yes`	Installiert die virtuelle Druckfunktion.
`--set-setting vmware-horizon-tsdr tsdrEnable yes`	Installiert die Funktion der Clientlaufwerksumleitung.
`--set-setting vmware-horizon-mmr mmrEnable yes`	Installiert die Funktion der Multimedia-Umleitung (MMR).
`--stop-services`	Installierte Dienste sollten weder registriert noch gestartet werden.

Neben den Optionen in der Tabelle können Sie folgende Umgebungsvariablen festlegen.

Tabelle 1-3. Installationseinstellungen für Variablen in Linux-Umgebung

Variablen	Beschreibung
`TERM=dumb`	Zeigt eine grundlegende Textoberfläche.
`VMWARE_EULAS_AGREED=yes`	Erlaubt eine automatische Annahme der Produkt-EULAs.
`VMIS_LOG_LEVEL=`*value*	Verwenden Sie einen der folgenden Werte für *Wert*: ■ `NOTSET` ■ `DEBUG` ■ `INFO` ■ `WARNING` ■ `ERROR` ■ `CRITICAL` Protokollinformationen werden in `/tmp/vmware-root/vmware-installer-`*pid*`.log` aufgezeichnet.

Beispiel: Befehle für die unbeaufsichtigte Installation

Nachfolgend sehen Sie ein Beispiel, wie Sie Horizon Client unbeaufsichtigt installieren können. Im Beispiel wird für jede Komponente festgelegt, ob sie installiert werden soll.

```
sudo env TERM=dumb VMWARE_EULAS_AGREED=yes \

./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle --console \

--set-setting vmware-horizon-usb usbEnable no \

--set-setting vmware-horizon-virtual-printing tpEnable yes \

--set-setting vmware-horizon-smartcard smartcardEnable no\

--set-setting vmware-horizon-rtav rtavEnable yes \

--set-setting vmware-horizon-tsdr tsdrEnable yes
```

Dieses nächste Beispiel zeigt, wie eine unbeaufsichtigte Installation von Horizon Client mithilfe der Standardeinstellungen ausgeführt wird.

```
sudo env TERM=dumb VMWARE_EULAS_AGREED=yes \
./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle --console --required
```

Aktivieren der virtuellen Druckfunktion auf einem Linux-Client

Das Installationspaket für Horizon Client 3.2 und höher enthält eine Komponente für das virtuelle Drucken. Wenn Sie Horizon Client 3.2 verwenden, müssen Sie zur Aktivierung dieser Funktion eine Konfigurationsdatei erstellen und einige Umgebungsvariablen festlegen.

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.

Wichtig Diese Prozedur ist mit Horizon Client 3.4 oder höher in der Regel nicht erforderlich, da sich damit im Zuge der Clientinstallation festlegen lässt, dass das Installationsprogramm installierte Dienste registriert und nach der Installation startet. Wenn der Benutzer den Client startet, wird automatisch eine Konfigurationsdatei erstellt und im `Benutzerordner` abgelegt.

Voraussetzungen

Sie müssen das Installationspaket von VMware zur Installation von Horizon Client 3.2 oder höher verwenden. Die virtuelle Druckkomponente wird dann standardmäßig installiert.

Vorgehensweise

1 Öffnen Sie ein Terminal-Fenster und geben Sie einen Befehl ein, um einen Ordner mit der Bezeichnung `.thnuclnt` im `home`-Verzeichnis zu erstellen.

```
$ mkdir ~/.thnuclnt/
```

Hinweis Da diese Datei im jeweiligen Benutzerordner erstellt wird, muss sie für jeden Benutzer separat angelegt werden, der das Linux-Clientsystem verwendet.

2 Erstellen Sie mithilfe eines Texteditors eine Konfigurationsdatei mit der Bezeichnung `thnuclnt.conf` im Ordner `~/.thnuclnt` und fügen Sie der Datei folgenden Text hinzu:

```
autoupdate = 15
automap = true
autoid = 0
updatecount = 1
editcount = 0

connector svc {
   protocol = listen
   interface = /home/user/.thnuclnt/svc
   setdefault = true
}
```

Ersetzen Sie in diesem Text den Benutzernamen für *Benutzer*.

3 Speichern und schließen Sie die Datei.

4 Geben Sie einen Befehl ein, um den `thnuclnt`-Prozess zu starten.

```
$ thnuclnt –fg
```

5 Geben Sie die Befehle ein, um die Umgebungsvariablen für die virtuellen Druckkomponenten festzulegen.

```
$ export TPCLIENTADDR=/home/user/.thnuclnt/svc
$ export THNURDPIMG=/usr/bin/thnurdp
```

6 Um Horizon Client zu öffnen, rufen Sie den `vmware–view`-Prozess auf.

Die Drucker, die normalerweise im Client erscheinen, werden ebenfalls umgeleitet, sodass sie in den Dialogfeldern „Drucken“ auf Ihrem Remote-Desktop erscheinen.

7 (Optional) Wenn Sie die virtuelle Druckfunktion deaktivieren möchten, gehen Sie wie folgt vor:

a Geben Sie einen Befehl ein, um den `thnuclnt`-Prozess zu beenden.

```
$ killall thnuclnt
```

b Trennen Sie den Remote-Desktop und stellen Sie erneut eine Verbindung zum Desktop her.

Die Drucker werden nicht mehr umgeleitet.

Installieren von Horizon Client für Linux über das Ubuntu Software Center

Wenn Sie ein Ubuntu-System verwenden, können Sie alternativ zur Installation der Version von der VMware Downloads-Website den Client auch aus dem Ubuntu Software Center installieren. Bei der Verwendung des Ubuntu Software Center installieren Sie den Client mithilfe des Synaptic Package Manager.

Dieses Thema enthält Anweisungen zum Abrufen der Clientsoftware vom Ubuntu Software Center. Sie können die Horizon Client-Software auch von der VMware-Website für Produkt-Downloads, wie unter „Installieren oder Aktualisieren von Horizon Client für Linux über die VMware-Website für Produkt-Downloads“, auf Seite 17 beschrieben, herunterladen.

Wichtig Kunden, die Linux-basierte Thin Clients verwenden, müssen sich wegen Updates für Horizon Client an ihren Thin Client-Hersteller wenden. Kunden, die erfolgreich ihre eigenen Linux-basierten Endpunkte eingerichtet haben und einen aktualisierten Client benötigen, müssen sich an den entsprechenden Vertriebsmitarbeiter von VMware wenden.

Voraussetzungen

- Stellen Sie sicher, dass das Clientsystem ein unterstütztes Betriebssystem verwendet. Siehe „Systemanforderungen für Linux-Clientsysteme“, auf Seite 8.
- Stellen Sie sicher, dass Sie über die erforderliche installierte Version der OpenSSL-Bibliothek verfügen. Siehe „Systemanforderungen für Linux-Clientsysteme“, auf Seite 8.
- Stellen Sie sicher, dass Sie sich als Administrator auf dem Clientsystem anmelden können.
- Wenn Sie beabsichtigen, das RDP-Anzeigeprotokoll zur Verbindungsherstellung mit einem View-Desktop zu verwenden, müssen Sie sicherstellen, dass Sie den entsprechenden RDP-Client installiert haben. Siehe „Systemanforderungen für Linux-Clientsysteme“, auf Seite 8.
- Deinstallieren Sie eine beliebige Version von View Client 1.x oder 2.x. Siehe „Deinstallieren von Horizon Client für Linux“, auf Seite 85.

Vorgehensweise

1 Aktivieren Sie auf Ihrem Linux-Laptop oder -PC Canonical Partners.

   a Wählen Sie in der Ubuntu-Menüleiste **System > Verwaltung > Update Manager** aus.

   b Klicken Sie auf die Schaltfläche **Einstellungen** und geben Sie das Kennwort für die Durchführung administrativer Aufgaben ein.

   c Im Dialogfeld „Software Sources“ klicken Sie auf die Registerkarte **Andere Software** und markieren Sie das Kontrollkästchen **Canonical Partners**, um das Archiv für die Software auszuwählen, das Canonical für seine Partner als Pakete zusammenstellt.

   d Klicken Sie auf **Schließen** und befolgen Sie die Anweisungen, um das Paket zu aktualisieren.

2 Falls Sie über Ubuntu 12.04 oder 14.04 verfügen, laden Sie das Paket vom Ubuntu Software Center wie folgt herunter und installieren Sie es.

   a Öffnen Sie ein Terminalfenster und geben Sie den Befehl zum Abrufen neuer Pakete ein:

   ```
   sudo apt-get update
   ```

   Die neuen Pakete werden heruntergeladen und im Terminalfenster wird eine Liste der Pakete angezeigt.

   b Öffnen Sie den Update Manager, prüfen Sie auf Updates und installieren Sie diese.

c Öffnen Sie die Ubuntu Software Center-App und suchen Sie nach **`vmware-view-client`**.

d Installieren Sie die `vmware-view-client`-App.

Wenn Sie Ubuntu 12.04 oder 14.04 als Betriebssystem verwenden, wird die neueste Version von Horizon Client installiert.

Im Startprogramm der Anwendung wird ein Anwendungssymbol für **VMware Horizon Client** angezeigt.

Weiter

Starten Sie Horizon Client und stellen Sie sicher, dass Sie sich am richtigen virtuellen Desktop anmelden können. Siehe „Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung“, auf Seite 55.

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 H.264-Decodierung wird für AMD, NVIDIA und Intel GPUs unterstützt. Für die H.264-Decodierung ist die Installation der Grafikbibliothek OpenGL 3.2 oder höher für AMD- und NVIDIA-GPUs erforderlich.

Wenn Sie die H.264-Decodierung mit einer NVIDIA-GPU verwenden möchten, installieren Sie VDPAU (Video Decode and Presentation API for Unix). VDPAU ist im aktuellsten NVIDIA-Treiber nicht mehr enthalten und muss separat installiert werden.

Um H.264 mit einer Intel GPU verwenden zu können, müssen der Intel VA-API-Treiber und die GLX VA-API-Bibliothek vorhanden sein. Mit dem Befehl `vainfo` können Sie die H.264-Profile darstellen. Liegt der VA-API-Treiber in der Version 1.2.x oder früher vor, müssen Sie `/etc/vmware/config`, `/usr/lib/vmware/config` oder `~/.vmware/config` den Eintrag `mks.enableGLBasicRenderer = TRUE` hinzufügen. Die Konfigurationsdateien werden in der folgenden Reihenfolge verarbeitet:

1 `/etc/vmware/config`

2 `/usr/lib/vmware/config`

3 `~/.vmware/config`

Mit Red Hat 7.2, Intel GPU, Intel-Treiber in der Version 1.2 oder früher, OpenGL 3.2 und aktivierter H.264-Decodierung müssen Sie einer der drei Konfigurationsdateien die nachfolgend aufgeführten Einträge hinzufügen, um Anzeigeprobleme wie z. B. einen schwarzen Bildschirm zu vermeiden.

```
mks.enableGLRenderer=FALSE
mks.enableGLBasicRenderer=TRUE
```

H.264 wird nicht für SLED 11 SP4 mit Intel GPU unterstützt, da die xorg-Version zu alt ist.

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 Wählen Sie **Datei > VMware Blast konfigurieren** in der Menüleiste aus.

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.

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 1-4. 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.)
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)

Tabelle 1-4. Von den Horizon Client-Instanzen gesammelte Daten für das Programm zur Verbesserung der Benutzerfreundlichkeit (Fortsetzung)

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
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.)
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)

Konfigurieren von Horizon Client für Endbenutzer 2

Die Konfiguration von Horizon Client für Endbenutzer kann verschiedene Aufgaben umfassen, wie die Generierung von URIs, die Festlegung des Zertifikatüberprüfungsmodus, die Änderung erweiterter TLS/SSL-Optionen, die Konfiguration bestimmter Schlüssel und Schlüsselkombinationen, die Festlegung des Anzeigeprotokolls und die Aktivierung des FIPS-Modus.

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 2-1. Allgemeine Konfigurationseinstellungen

Einstellung	Konfigurationsmechanismen
Adresse des Verbindungsservers	URI, Konfigurationsdatei-Eigenschaft, Befehlszeile
Active Directory-Benutzername	URI, Konfigurationsdatei-Eigenschaft, Befehlszeile
Domänenname	URI, Konfigurationsdatei-Eigenschaft, Befehlszeile
Desktopanzeigename	URI, Konfigurationsdatei-Eigenschaft, Befehlszeile
Fenstergröße	URI, Konfigurationsdatei-Eigenschaft, Befehlszeile
Anzeigeprotokoll	URI, Konfigurationsdatei-Eigenschaft, Befehlszeile

Tabelle 2-1. Allgemeine Konfigurationseinstellungen (Fortsetzung)

Einstellung	Konfigurationsmechanismen
Konfigurieren der Zertifikatsprüfung	Konfigurationsdatei-Eigenschaft
Konfigurieren von SSL-Protokollen und kryptografischen Algorithmen	Konfigurationsdatei-Eigenschaft, Befehlszeile

Verwenden der Horizon Client -Befehlszeilenschnittstelle und -Konfigurationsdateien

Sie können Horizon Client mithilfe von Befehlszeilenoptionen oder über die entsprechenden Eigenschaften in einer Konfigurationsdatei konfigurieren.

Sie können die Befehlszeilenschnittstelle `vmware-view` verwenden oder die Eigenschaften in den Konfigurationsdateien festlegen, um die Standardwerte zu definieren, die Ihren Benutzern in Horizon Client angezeigt werden, oder um das Einblenden einiger Dialogfelder zu verhindern, die den Benutzer zur Eingabe von Informationen auffordern. Sie können zudem auch Einstellungen angeben, von denen Sie nicht möchten, dass die Benutzer diese ändern.

Verarbeitungsreihenfolge für Konfigurationseinstellungen

Beim Start von Horizon Client werden die Konfigurationseinstellungen aus mehreren Speicherorten in der folgenden Reihenfolge verarbeitet:

1 `/etc/vmware/view-default-config`

2 `~/.vmware/view-preferences`

3 Befehlszeilenargumente

4 `/etc/vmware/view-mandatory-config`

Ist eine Einstellung in verschiedenen Speicherorten konfiguriert, entspricht der verwendete Wert dem Wert aus dem letzten Lesevorgang der Datei oder Befehlszeilenoption. Um beispielsweise Einstellungen anzugeben, die die Benutzereinstellungen außer Kraft setzen, müssen Sie die Eigenschaften in der Datei `/etc/vmware/view-mandatory-config` festlegen.

Um Standardwerte festzulegen, die von den Benutzern geändert werden können, müssen Sie die Datei `/etc/vmware/view-default-config` verwenden. Nach der Änderung einer Einstellung durch die Benutzer werden beim Beenden von Horizon Client alle geänderten Einstellungen in der Datei `~/.vmware/view-preferences` gespeichert.

Eigenschaften, die ein Ändern der Standardeinstellungen durch die Benutzer verhindern

Für viele Eigenschaften können Sie eine entsprechende `view.allow`-Eigenschaft festlegen, durch die gesteuert wird, ob eine Änderung der Einstellung durch die Benutzer zulässig ist. Wenn Sie beispielsweise die Eigenschaft `view.allowDefaultBroker` in der Datei `/etc/vmware/view-mandatory-config` auf „FALSE“ festlegen, sind Benutzer nicht in der Lage, den Namen des Servers zu ändern, wenn Sie mit Horizon Client eine Verbindung herstellen.

Syntax zur Verwendung der Befehlszeilenschnittstelle

Verwenden Sie die folgende Form des Befehls `vmware-view` aus einem Terminalfenster.

`vmware-view [`*`command-line-option`* `[`*`argument`*`]] ...`

Standardmäßig befindet sich der Befehl `vmware-view` im Verzeichnis `/usr/bin`.

Sie können entweder die Kurzform oder die Langform des Optionsnamens verwenden. Es verfügen jedoch nicht alle Optionen über eine Kurzform. Zur Angabe der Domäne können Sie beispielsweise entweder `-d` (Kurzform) oder `--domainName=` (Langform) verwenden. Um die visuelle Lesbarkeit eines Skripts zu verbessern, wird die Verwendung der Langform empfohlen.

Über die Option `--help` können Sie eine Liste von Befehlszeilenoptionen und Verwendungsinformationen abrufen.

Wichtig Ist die Verwendung eines Proxys erforderlich, verwenden Sie die folgende Syntax:

`http_proxy=`*`proxy_server_URL:port`* `https_proxy=`*`proxy_server_URL:port`* `vmware-view` *`options`*

Diese Umgebung ist nötig, da Sie die zuvor für den Proxy festgelegten Umgebungsvariablen löschen müssen. Wenn Sie diese Aktion nicht durchführen, ist die Proxy-Ausnahmeeinstellung in Horizon Client nicht wirksam. Sie können eine Proxyausnahme für die View-Verbindungsserver-Instanz konfigurieren.

Horizon Client -Konfigurationseinstellungen und -Befehlszeilenoptionen

Für Ihre Bequemlichkeit haben fast alle Konfigurationseinstellungen sowohl eine Eigenschaft *Schlüssel=Wert* und einen entsprechenden Befehlszeilenoptionsnamen. Für einige Einstellungen gibt es eine Befehlszeilenoption, aber keine entsprechende Eigenschaft, die Sie in einer Konfigurationsdatei einstellen können. Für einige andere Einstellungen müssen Sie eine Eigenschaft einstellen, weil keine Befehlszeilenoption verfügbar ist.

Wichtig Einige Befehlszeilenoptionen und Konfigurationsschlüssel werden nur in der Horizon Client-Version von Drittanbietern zur Verfügung gestellt. Weitere Informationen zu den Thin Client- und Zero Client-Partnern von VMware finden Sie im *VMware-Kompatibilitätshandbuch* unter http://www.vmware.com/resources/compatibility/search.php?deviceCategory=vdm.

Tabelle 2-2. Horizon Client -Befehlszeilenoptionen und -Schlüssel für Konfigurationsdateien

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung
`view.allMonitors`	`--allmonitors`	Blendet das Hostbetriebssystem aus und öffnet die Horizon Client-Benutzeroberfläche im Vollbildmodus auf allen Monitoren, die verbunden sind, sobald der Client gestartet wird. Wenn Sie den Konfigurationsschlüssel einstellen, geben Sie **„TRUE“** oder **„FALSE“** ein. Standardwert ist „FALSE“ (FALSCH).
`view.allowDefaultBroker`	`-l`, `--lockServer`	Mit dieser Befehlszeilenoption oder dem Einstellen der Eigenschaft auf „FALSE“ (FALSCH) wird das Feld **Server** deaktiviert, es sei denn, der Client hat sich noch nie mit einem Server verbunden, und in der Befehlszeile oder der Datei der Voreinstellungen wird keine Serveradresse angegeben. Beispiel zur Verwendung der Befehlszeilenoption: `--lockServer -s view.company.com`
`view.autoConnectBroker`	Keine	Verbindet automatisch zum letzten verwendeten View Server, außer wenn die Konfigurationseigenschaft `view.defaultBroker` eingestellt ist oder die Befehlszeilenoption `--serverURL=` verwendet wird. Geben Sie **„TRUE“** oder **„FALSE“** an. Standardwert ist „FALSE“ (FALSCH). Wenn Sie diese Eigenschaft und `view.autoConnectDesktop` auf „TRUE“ (WAHR) einstellen, ist es das Gleiche, als ob Sie die Eigenschaft `view.nonInteractive` auf „TRUE“ (WAHR) einstellen.

Tabelle 2-2. Horizon Client -Befehlszeilenoptionen und -Schlüssel für Konfigurationsdateien (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung
`view.autoConnectDesktop`	Keine	Stellt automatisch eine Verbindung zum letzten verwendeten View-Desktop her, außer wenn die Konfigurationseigenschaft `view.defaultDesktop` eingestellt ist oder die Befehlszeilenoption `--desktopName=` verwendet wird. Geben Sie **„TRUE“** oder **„FALSE“** an. Standardwert ist „FALSE“ (FALSCH). Wenn Sie diese Eigenschaft und `view.autoConnectBroker` auf „TRUE“ (WAHR) einstellen, ist es das Gleiche, als ob Sie die Eigenschaft `view.nonInteractive` auf „TRUE“ (WAHR) einstellen.
`view.autoDisconnectEmptyAppSession`	Keine	Leert sich die Anwendungssitzung, wenn der Benutzer alle Anwendungen schließt, erhält der Endbenutzer – falls **„TRUE“** (Standard) festgelegt wurde – eine Meldung. Diese Meldung fordert den Benutzer auf, zwischen dem Trennen oder der weiteren Ausführung der leeren Sitzung zu wählen. Bei der Einstellung **„FALSE“** wird die Sitzung entsprechend der Zeitüberschreitungseinstellung in View Administrator geschlossen. Standardmäßig erfolgt diese Trennung nach einer Minute.
`view.defaultAppHeight`	Keine	Gibt die Standardhöhe des Fensters für Remoteanwendungen in Pixel an. Verwenden Sie diese Eigenschaft in Verbindung mit `view.defaultAppWidth`, wenn Sie eine benutzerdefinierte Desktop-Größe (die Eigenschaft `view.defaultAppSize` ist auf „5“ festgelegt) angeben. Standard ist „480“.
`view.defaultAppSize`	`--appSize=`	Legt die Standardgröße des Fensters für die Anzeige der Remoteanwendungen fest: ■ Um alle Monitore zu verwenden, geben Sie **„1“** an. ■ Um den Vollbildmodus auf einem der Monitore zu verwenden, geben Sie **„2“** an. ■ Um ein großes Fenster zu verwenden, geben Sie **„3“** an. ■ Um ein kleines Fenster zu verwenden, geben Sie **„4“** an. ■ Um eine benutzerdefinierte Größe festzulegen, geben Sie **„5“** an und legen Sie zudem die Eigenschaften `view.defaultAppWidth` und `view.defaultAppHeight` fest. Standard ist „1“.
`view.defaultAppWidth`	Keine	Gibt die Standardbreite des Fensters für Remoteanwendungen in Pixel an. Verwenden Sie diese Eigenschaft in Verbindung mit `view.defaultAppHeight`, wenn Sie eine benutzerdefinierte Desktop-Größe (die Eigenschaft `view.defaultAppSize` ist auf „5“ festgelegt) angeben. Standard ist „640“.

Tabelle 2-2. Horizon Client -Befehlszeilenoptionen und -Schlüssel für Konfigurationsdateien (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung

`view.defaultBroker`	`-s`, `--serverURL=`	Fügt den Namen hinzu, den Sie im Feld **Server** in Horizon Client angeben. Geben Sie einen vollständig qualifizierten Domänennamen ein. Sie können auch eine Port-Nummer angeben, wenn Sie den Standard 443 nicht verwenden.
		Standard ist der zuletzt verwendete Wert.
		Beispiele zur Verwendung der Befehlszeilenoption:
		`--serverURL=https://view.company.com`
		`-s view.company.com`
		`--serverURL=view.company.com:1443`

`view.defaultDesktop`	`-n`, `--desktopName=`	Gibt an, welcher Desktop zu verwenden ist, wenn `autoConnectDesktop` auf „TRUE“ (WAHR) eingestellt ist und der Benutzer Zugriff auf mehrere Desktops hat. Dies ist der Name, den Sie im Dialogfeld „Desktop auswählen“ sehen würden. Der Name ist in der Regel der Poolname.
`view.defaultDesktopHeight`	Keine	Gibt die Standardhöhe des Fensters für View-Desktop in Pixel an. Verwenden Sie diese Eigenschaft in Verbindung mit `view.defaultDesktopWidth`, wenn Sie eine benutzerdefinierte Desktop-Größe (die Eigenschaft `view.defaultDesktopSize` ist auf „5“ festgelegt) angeben.

`view.defaultDesktopSize`	`--desktopSize=`	Legt die Standardgröße des Fensters für die Anzeige des View-Desktops fest:
		■ Um alle Monitore zu verwenden, setzen Sie die Eigenschaft auf **`"1"`** oder benutzen Sie das Befehlszeilenargument **`"all"`**.
		■ Um den Vollbildmodus auf allen Monitoren zu verwenden, stellen Sie die Eigenschaft auf **`"2"`** ein oder benutzen Sie das Befehlszeilenargument **`"full"`**.
		■ Um ein großes Fenster zu verwenden, stellen Sie die Eigenschaft auf **`"3"`** ein oder benutzen Sie das Befehlszeilenargument **`"large"`**.
		■ Um ein kleines Fenster zu verwenden, stellen Sie die Eigenschaft auf **`"4"`** ein oder benutzen Sie das Befehlszeilenargument **`"small"`**.
		■ Um ein benutzerdefiniertes Format zu verwenden, stellen Sie die Eigenschaft auf **`"5"`** und dann auch die Eigenschaften `view.defaultDesktopWidth` und `view.defaultDesktopHeight` ein. Alternativ geben Sie Breite mal Höhe in Pixel in der Befehlszeile als **`"widthxheight"`** ein.
		Beispiele zur Verwendung der Befehlszeilenoption:
		`--desktopSize="1280x800"`
		`--desktopSize="all"`

Tabelle 2-2. Horizon Client -Befehlszeilenoptionen und -Schlüssel für Konfigurationsdateien (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung
`view.defaultDesktopWidth`	Keine	Gibt die Standardbreite des Fensters für View-Desktop in Pixel an. Verwenden Sie diese Eigenschaft in Verbindung mit `view.defaultDesktopHeight`, wenn Sie eine benutzerdefinierte Desktop-Größe (die Eigenschaft `view.defaultDesktopSize` ist auf „5“ festgelegt) angeben.
`view.defaultDomain`	`-d`, `--domainName=`	Legt den Domänennamen fest, den Horizon Client für alle Verbindungen verwendet, und fügt den von Ihnen im Feld **Domänenname** angegebenen Namen im Dialogfeld „Authentifizierung“ hinzu.
`view.defaultLogLevel`	Keine	Legt die Protokollebene für Horizon Client-Protokolle fest. Legen Sie die Eigenschaft auf einen der folgenden Werte fest: ■ **„0“** bedeutet, dass alle Protokollereignisse protokolliert werden. ■ **„1“** bedeutet, dass Ereignisse auf Ablaufebene sowie Ereignisse, die anhand der Einstellungen 2 bis 6 erfasst werden, protokolliert werden. ■ **„2“** bedeutet, dass Debug-Ereignisse sowie Ereignisse, die anhand der Einstellungen 3 bis 6 erfasst werden, protokolliert werden. ■ **„3“** (Standard) bedeutet, dass Ereignisse auf Info-Ebene und Ereignisse, die anhand der Einstellungen 4 bis 6 erfasst werden, protokolliert werden. ■ **„4“** bedeutet, dass Warnungen, Fehler und schwerwiegende Ereignisse protokolliert werden. ■ **„5“** bedeutet, dass Fehler und schwerwiegende Ereignisse protokolliert werden. ■ **„6“** bedeutet, dass schwerwiegende Ereignisse protokolliert werden. Standard ist „3“.
`view.defaultPassword`	`-p "-"`, `--password="-"`	Für VMware Blast-, PCoIP- und `rdesktop`-Verbindungen sollten Sie immer **`"-"`** angeben, um das Kennwort von `stdin` zu lesen. Legt das Kennwort fest, das Horizon Client für alle Verbindungen verwendet, und fügt das Kennwort in das Feld **Kennwort** im Dialogfeld für die Authentifizierung ein, wenn der View-Verbindungsserver eine Kennwortauthentifizierung akzeptiert. **Hinweis** Sie können kein leeres Kennwort verwenden. Das heißt, Sie können nicht --password = "" eingeben

Tabelle 2-2. Horizon Client -Befehlszeilenoptionen und -Schlüssel für Konfigurationsdateien (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung
`view.defaultProtocol`	`--protocol=`	Gibt an, welches Anzeigeprotokoll verwendet werden soll. Geben Sie **„PCoIP“** oder **„RDP“** ein. Bei diesen Werten müssen Sie die Groß- und Kleinschreibung beachten. Wenn Sie zum Beispiel **`rdp`** eingeben, wird dieses Protokoll als Standard verwendet. Standard ist die Einstellung in View Administrator unter „Pool-Einstellungen“ für den Pool. Wenn Sie RDP verwenden und lieber FreeRDP statt `rdesktop` benutzen möchten, müssen Sie auch die Einstellung `rdpClient` verwenden.
`view.defaultUser`	`-u, --userName=`	Legt den Benutzernamen fest, den Horizon Client für alle Verbindungen verwendet, und fügt den von Ihnen im Feld **Benutzername** angegebenen Namen im Dialogfeld „Authentifizierung“ hinzu. Für den Kioskmodus kann der Kontoname auf der Client-MAC-Adresse basieren, oder er kann mit einer anerkannten Präfixzeichenfolge wie **`custom-`** beginnen.
`view.disableMaximizedApp`	`--disableMaximizedApp`	Auf **„FALSE“** (Standard) festgelegt, wird die Anwendung im Vollbildmodus gestartet.
`view.enableMMR`	Keine	Aktiviert die Multimedia-Umleitung (MMR) Geben Sie **„TRUE“** oder **„FALSE“** an. Standardwert ist „FALSE“ (FALSCH).
`view.fullScreen`	`--fullscreen`	Blendet das Hostbetriebssystem aus und öffnet die Horizon Client-Benutzeroberfläche auf einem Monitor im Vollbildmodus. Diese Option wirkt sich nicht auf den Bildschirmmodus der Desktop-Sitzung aus. Wenn Sie den Konfigurationsschlüssel einstellen, geben Sie **„TRUE“** oder **„FALSE“** ein. Standardwert ist „FALSE“ (FALSCH).

`view.kbdLayout`	`-k, --kbdLayout=`	Gibt an, welches Gebietsschema für das Tastatur-Layout verwendet werden soll.
		Hinweis `rdesktop` benutzt Gebietsschema-Codes wie **„fr“** und **„de“**, während `freerdp` IDs für das Tastatur-Layout benutzt. Um eine Liste dieser IDs zu sehen, geben Sie folgenden Befehl ein:
		`xfreerdp --kbd-list`
		Beispiel zur Verwendung der Befehlszeilenoption für rdesktop:
		`--kbdLayout="en-us"`
		`-k "fr"`
		Beispiel zur Verwendung der Befehlszeilenoption für freerdp:
		`-k "0x00010407"`

`view.kioskLogin`	`--kioskLogin`	Gibt an, dass Horizon Client zur Authentifizierung ein Kioskmoduskonto verwenden wird. Wenn Sie den Konfigurationsschlüssel einstellen, geben Sie **„TRUE“** oder **„FALSE“** ein. Standardwert ist „FALSE“ (FALSCH). Siehe Kioskmodusbeispiel im Anschluss an diese Tabelle.

Tabelle 2-2. Horizon Client -Befehlszeilenoptionen und -Schlüssel für Konfigurationsdateien (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung
`view.mmrPath`	`-m`, `--mmrPath=`	(Nur in Verbindung mit Distributionen von Drittanbietern verfügbar) Gibt den Pfad zu dem Ordner an, in dem die Wyse MMR (Multimedia-Umleitung)-Bibliotheken gespeichert sind. Beispiel zur Verwendung der Befehlszeilenoption: `--mmrPath="/usr/lib/altmmr"`
`view.monitors`	`--monitors=` *numbered list*	Ermöglicht Ihnen die Angabe, welche benachbarten Monitore für Horizon Client verwendet werden sollen. Verwenden Sie die Option `--allmonitors` (oder `view.allMonitors`), um festzulegen, dass auf allen Monitoren der Vollbildmodus verwendet werden soll, und die Option `--monitors=`*Nummerierte Liste*, um die Teilmenge der zu verwendenden Monitore festzulegen. Beispiel für die Verwendung der Befehlszeilenoption zur Festlegung, dass der erste und der zweite Monitor in einer Konfiguration aus drei horizontal nebeneinander platzierten Monitoren verwendet werden sollen: `--allmonitors --monitors="1,2" ` Um einfacher feststellen zu können, welcher physische Monitor mit einem Monitorsymbol in der Clientbenutzeroberfläche verknüpft ist, wird oben links im zur Verwendung festgelegten physischen Monitor ein Rechteck angezeigt. Das Rechteck besteht aus der Farbe und der Zahl des Symbols für den gewählten Monitor.
`view.nomenubar`	`--nomenubar`	Unterdrückt die Horizon Client-Menüleiste, wenn Client im Vollbildmodus ist, sodass die Benutzer keinen Zugriff auf Menüoptionen haben, um sich abzumelden, einen Neustart auszuführen oder die Verbindung zu einem View-Desktop zu trennen. Verwenden Sie diese Option bei der Konfiguration des Kioskmodus. Wenn Sie den Konfigurationsschlüssel einstellen, geben Sie **„TRUE“** oder **„FALSE“** ein. Standardwert ist „FALSE“ (FALSCH).
`view.nonInteractive`	`-q`, `--nonInteractive`	Verbirgt unnötige Schritte der Benutzerschnittstelle vor dem Endanwender, indem die Bildschirme übersprungen werden, die in der Kommandozeile oder bei den Konfigurationseigenschaften angegeben werden. Wenn Sie den Konfigurationsschlüssel einstellen, geben Sie **„TRUE“** oder **„FALSE“** ein. Standardwert ist „FALSE“ (FALSCH). Das Einstellen dieser Eigenschaft auf „TRUE“ (WAHR) entspricht dem Einstellen der Eigenschaften `view.autoConnectBroker` und `view.autoConnectDesktop` auf „TRUE“ (WAHR). Beispiel zur Verwendung der Befehlszeilenoption: `--nonInteractive --serverURL="https://view.company.com" --userName="user1" --password="-" --domainName="xyz" --desktopName="Windows 7"`

Tabelle 2-2. Horizon Client -Befehlszeilenoptionen und -Schlüssel für Konfigurationsdateien (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung
`view.once`	`--once`	Gibt an, dass Horizon Client bei einem Fehler nicht erneut versuchen soll, eine Verbindung herzustellen. Normalerweise sollten Sie diese Option angeben, wenn Sie den Kioskmodus verwenden, und den Fehler mit einem Exit-Code behandeln. Andernfalls kann es schwierig sein, den `vmware-view`-Prozess remote zu beenden. Wenn Sie den Konfigurationsschlüssel einstellen, geben Sie **„TRUE“** oder **„FALSE“** ein. Standardwert ist „FALSE“ (FALSCH).
`view.rdesktopOptions`	`--rdesktopOptions=`	(Verfügbar, wenn Sie das Microsoft RDP-Anzeigeprotokoll verwenden) Spezifiziert Befehlszeilenoptionen zum Weiterleiten an die Anwendung rdesktop. Informationen über Optionen von rdesktop finden Sie in der Dokumentation zu rdesktop. Beispiel zur Verwendung der Befehlszeilenoption: `--rdesktopOptions="-f -m"`
Keine	`-r`, `--redirect=`	(Verfügbar, wenn Sie das Microsoft RDP-Anzeigeprotokoll verwenden) Spezifiziert ein lokales Gerät, das rdesktop an den View-Desktop umleiten soll. Geben Sie die Geräteinformationen an, die Sie an die Option `-r` von rdesktop weiterleiten wollen. Sie können mehrere Geräteoptionen in einem einzigen Befehl einstellen. Beispiel zur Verwendung der Befehlszeilenoption: `--redirect="sound:off"`
`view.rdpClient`	`--rdpclient=`	(Verfügbar, wenn Sie das Microsoft RDP-Anzeigeprotokoll verwenden) Spezifiziert, welche Art von RDP Client benutzt werden soll. Der Standard ist `rdesktop`. Um FreeRDP zu verwenden, geben Sie `xfreerdp` ein. **Hinweis** Um FreeRDP zu verwenden, müssen Sie die richtige Version von FreeRDP mit allen verfügbaren Patches installiert haben. Weitere Informationen finden Sie unter „Installation und Konfiguration von FreeRDP“, auf Seite 50.
Keine	`--save`	Speichert den Benutzernamen und Domänennamen, die zuletzt verwendet wurden, um sich erfolgreich anzumelden, sodass Sie bei der nächsten Aufforderung, die Anmeldeinformationen einzugeben, den Benutzernamen oder den Domänenamen nicht mehr eingeben müssen.

Tabelle 2-2. Horizon Client -Befehlszeilenoptionen und -Schlüssel für Konfigurationsdateien (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung
`view.sendCtrlAltDelToLocal`	Keine	(Verfügbar, wenn Sie das VMware Blast- oder das PCoIP-Anzeigeprotokoll verwenden.) Bei Festlegung auf **„TRUE“** wird die Tastenkombination Strg-Alt-Entf an das Clientsystem gesendet, statt ein Dialogfeld zu öffnen, in dem der Benutzer zur Trennung der Verbindung mit dem View-Desktop aufgefordert wird. Standardwert ist „FALSE“ (FALSCH). **Hinweis** Wenn Sie das Microsoft RDP-Anzeigeprotokoll verwenden, erhalten Sie diese Funktionalität durch Verwendung der Option `–K`. Beispiel: `vmware–view –K`. Diese Option hat dieselbe Priorität wie die Einstellung in der Datei `/etc/vmware/view–keycombos–config`.
`view.sendCtrlAltDelToVM`	Keine	(Verfügbar, wenn Sie das VMware Blast- oder das PCoIP-Anzeigeprotokoll verwenden.) Bei Festlegung auf **„TRUE“** wird die Tastenkombination Strg-Alt-Entf an den virtuellen Desktop gesendet, statt ein Dialogfeld zu öffnen, in dem der Benutzer zur Trennung der Verbindung mit dem View-Desktop aufgefordert wird. Standardwert ist „FALSE“ (FALSCH). Diese Option hat eine höhere Priorität als die Einstellung in der Datei `/etc/vmware/view–key–combos–config`.
`view.sendCtrlAltInsToVM`	Keine	(Verfügbar, wenn Sie das VMware Blast- oder das PCoIP-Anzeigeprotokoll verwenden.) Bei Festlegung auf **„TRUE“** wird anstelle von Strg-Alt-Entf die Tastenkombination Strg+Alt+Ins an den virtuellen Desktop gesendet. Standardwert ist „FALSE“ (FALSCH). **Hinweis** Zur Verwendung dieser Funktion müssen Sie auch die Agent-GPO-Richtlinie namens „Alternative Taste zum Senden der Sicherheitssequenz verwenden“ festlegen, die in der Vorlage „`pcoip.adm`“ zur Verfügung steht. Weitere Informationen finden Sie im Thema „Anzeigen von PCoIP-Sitzungsvariablen für die Tastatur“ im Kapitel „Konfigurieren von Richtlinien“ des Dokuments *Einrichten von Desktop- und Anwendungspools für View*. Diese Option hat eine niedrigere Priorität als die Einstellung in der Datei `/etc/vmware/view–keycombos–config`.
`view.shareRemovableStorage`	Keine	Die Festlegung von **"TRUE"** aktiviert die Option **Zugriff auf Wechselmedien erlauben**. Standard ist „TRUE“.
`view.sslCipherString`	`––sslCipherString=`	Konfiguriert die Verschlüsselungsliste, um die Verwendung bestimmter kryptografischer Algorithmen zu beschränken, bevor eine verschlüsselte SSL-Verbindung hergestellt wird. Eine Liste der Verschlüsselungszeichenfolgen finden Sie unter http://www.openssl.org/docs/apps/ciphers.html. Der Standard für Horizon Client lautet „!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES“.

Tabelle 2-2. Horizon Client -Befehlszeilenoptionen und -Schlüssel für Konfigurationsdateien (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung
`view.sslProtocolString`	`--sslProtocolString=`	Konfiguriert die Verschlüsselungsliste, um die Verwendung bestimmter kryptografischer Protokolle zu beschränken, bevor eine verschlüsselte SSL-Verbindung hergestellt wird. Die unterstützten Protokolle sind SSLv3/SSLv3.0, TLSv1.0/TLSv1, TLSv1.1 und TLSv1.2. Die Verschlüsselungsliste besteht aus einer oder mehreren Protokollzeichenfolgen, die durch Doppelpunkte getrennt sind. Bei den Zeichenfolgen muss die Klein-/Großschreibung nicht beachtet werden. Der Standard lautet „TLSv1.0:TLSv1.1:TLSv1.2“.
`view.sslVerificationMode`	Keine	Stellt den Server-Zertifikatsprüfmodus ein. Geben Sie **"1"** ein, um Verbindungen abzulehnen, wenn das Zertifikat eine der Gültigkeitsprüfungen nicht besteht, **"2"**, um zu warnen, aber Verbindungen zu ermöglichen, die ein selbst signiertes Zertifikat verwenden, oder **"3"**, um nicht überprüfbare Verbindungen zuzulassen. Wenn Sie **"3"** angeben, werden keine Gültigkeitsprüfungen durchgeführt. Standard ist „2".
`view.UnauthenticatedAccessEnabled`	`--unauthenticatedAccessEnabled`	Wenn **„TRUE“** festgelegt ist, ist die Funktion für den nicht authentifizierten Zugriff standardmäßig aktiviert. Die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** ist dann in der Benutzeroberfläche verfügbar und als ausgewählt markiert. Wenn **„FALSE“** festgelegt ist, ist die Funktion für den nicht authentifizierten Zugriff deaktiviert. Die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** ist ausgeblendet und nicht ausgewählt. Wenn **""** festgelegt ist, ist die Funktion für den nicht authentifizierten Zugriff deaktiviert. Die Einstellung **Anonym mit nicht authentifiziertem Zugriff anmelden** ist dann in der Benutzeroberfläche verfügbar und nicht ausgewählt. Wenn Sie den Konfigurationsschlüssel einstellen, geben Sie **„TRUE“** oder **„FALSE“** ein. Beispiele zur Verwendung der Befehlszeilenoption: `--unauthenticatedAccessEnabled="TRUE"`
`view.UnauthenticatedAccessAccount`	`--unauthenticatedAccessAccount`	Legt das Konto fest, das verwendet werden soll, wenn für `unauthenticatedAccessEnabled` „TRUE“ festgelegt ist. Wenn für `unauthenticatedAccessEnabled` die Einstellung **„FALSE“** festgelegt ist, wird diese Konfiguration ignoriert. Das folgende Beispiel veranschaulicht die Verwendung der Befehlszeilenoption mit dem Benutzerkonto **`anonymous1`**: `--unauthenticatedAccessAccount='anonymous1'`
`view.usbAutoConnectAtStartup`	`--usbAutoConnectAtStartUp=`	Verbindet USB-Geräte automatisch, wenn Horizon Client gestartet wird. Geben Sie **„TRUE“** oder **„FALSE“** an. Standard ist **„TRUE“**.

Tabelle 2-2. Horizon Client -Befehlszeilenoptionen und -Schlüssel für Konfigurationsdateien (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung
`view.usbAutoConnectOnInsert`	`--usbAutoConnectOnInsert=`	Verbindet USB-Geräte automatisch, wenn ein USB-Gerät eingesteckt wird. Geben Sie **„TRUE“** oder **„FALSE“** an. Standard ist **„TRUE“**.
`view.xfreerdpOptions`	`--xfreerdpOptions=`	(Verfügbar, wenn Sie das Microsoft RDP-Anzeigeprotokoll verwenden) Spezifiziert Befehlszeilenoptionen zum Weiterleiten an die Anwendung `xfreerdp`. Informationen über Optionen von `xfreerdp` finden Sie in der Dokumentation zu `rdesktop`. **Hinweis** Um FreeRDP zu verwenden, müssen Sie die richtige Version von FreeRDP mit allen verfügbaren Patches installiert haben. Weitere Informationen finden Sie unter „Installation und Konfiguration von FreeRDP“, auf Seite 50.
Keine	`--enableNla`	(Trifft zu, wenn Sie FreeRDP für RDP-Verbindungen benutzen) Ermöglicht Netzwerkebenen-Authentifizierung (network-level authentication, NLA). Sie müssen diese Option in Verbindung mit der Option `--ignore-certificate` verwenden. Weitere Informationen finden Sie unter „Verwenden von FreeRDP für RDP-Verbindungen“, auf Seite 49. NLA ist standardmäßig deaktiviert, wenn Sie FreeRDP benutzen. Auf Ihrem Computer muss die korrekte Version von FreeRDP zusammen mit den entsprechenden Patches installiert sein. Weitere Informationen finden Sie unter „Installation und Konfiguration von FreeRDP“, auf Seite 50. **Hinweis** Das Programm `rdesktop` unterstützt keine NLA.
Keine	`--printEnvironmentInfo`	Zeigt Informationen über die Umgebung eines Client-Geräts, einschließlich IP-Adresse, MAC-Adresse, Rechnernamen und Domänennamen. Für den Kioskmodus können Sie für den Client anhand der MAC-Adresse ein Konto erstellen. Um die MAC-Adresse anzuzeigen, verwenden Sie diese Option mit der Option `-s`. Beispiel zur Verwendung der Befehlszeilenoption: `--printEnvironmentInfo -s view.company.com`
Keine	`--usb=`	Gibt an, welche Optionen für die USB-Umleitung verwendet werden. Siehe „Systemanforderungen für die USB-Umleitung“, auf Seite 87.
Keine	`--version`	Zeigt Versionsinformationen zu Horizon Client an.

Beispiel: Beispiel für Kioskmodus

Zu Kioskbenutzern gehören zum Beispiel Kunden an Checkin-Schaltern von Fluggesellschaften, Schüler in Klassenräumen oder Bibliotheken, medizinisches Personal an Eingabestationen für medizinische Daten oder Kunden an öffentlichen Zugangspunkten. Konten werden Client-Geräten und keinen Benutzern zugeordnet, weil sich Benutzer nicht anmelden müssen, um das Client-Gerät oder den View-Desktop zu benutzen. Dennoch müssen Benutzer für manche Anwendungen Anmeldeinformationen zur Authentifizierung bereitstellen.

Um den Kioskmodus einzurichten, verwenden Sie die Befehlszeilenschnittstelle `vdmadmin` auf der View-Verbindungsserver-Instanz und führen mehrere Verfahren durch, die im Kapitel über den Kioskmodus im Dokument *Administration von View* dokumentiert sind. Nachdem Sie den Kioskmodus eingerichtet haben, können Sie den Befehl `vmware-view` auf einem Linux-Client verwenden, um eine Verbindung zu einem View-Desktop im Kioskmodus herzustellen.

Um eine Verbindung von Linux-Clients zu View-Desktops im Kioskmodus herzustellen, müssen Sie mindestens die folgenden Konfigurationsschlüssel oder Kommandozeilenoptionen einschließen.

Konfigurationsschlüssel	Äquivalente Befehlszeilenoptionen
`view.kioskLogin`	`--kioskLogin`
`view.nonInteractive`	`-q`, `--nonInteractive`
`view.fullScreen`	`--fullscreen`
`view.nomenubar`	`--nomenubar`
`view.defaultBroker`	`-s`, `--serverURL=`

Das Auslassen einer dieser Konfigurationseinstellungen wird im Kioskmodus nicht unterstützt. Wenn der View-Verbindungsserver so eingerichtet ist, dass ein nichtstandardmäßiger Kioskbenutzername erforderlich ist, müssen Sie auch die Eigenschaft `view.defaultUser` einstellen oder Sie verwenden die Befehlszeilenoption `-u` oder `--userName=`. Wenn kein nichtstandardmäßiger Benutzername erforderlich ist und Sie keinen Benutzernamen angeben, kann Horizon Client den standardmäßigen Kioskbenutzernamen ableiten und verwenden.

Hinweis Wenn Sie den Konfigurationsschlüssel `view.sslVerificationMode` einstellen, stellen Sie sicher, dass Sie ihn in der Datei `/etc/vmware/view-mandatory-config` einstellen. Wenn der Client im Kioskmodus läuft, sieht der Client nicht in der Datei `view-preferences` nach.

Der in diesem Beispiel gezeigte Befehl führt Horizon Client auf einem Linux-Clientsystem aus und hat die folgenden Eigenschaften:

- Der Name des Benutzerkontos basiert auf der MAC-Adresse des Clients.
- Horizon Client läuft im Vollbildmodus ohne Horizon Client-Menüleiste.
- Benutzer werden automatisch mit der angegebenen View-Verbindungsserver-Instanz und dem View-Desktop verbunden und nicht zur Eingabe der Anmeldeinformationen aufgefordert.
- Wenn ein Verbindungsfehler auftritt, hängt es vom jeweiligen zurückgegebenen Fehlercode ab, ob ein Skript ausgeführt wird oder ein Kioskmonitoringprogramm den Fehler behandelt. Als Ergebnis könnte das Clientsystem zum Beispiel einen „Außer Betrieb"-Bildschirm anzeigen oder es wartet eine gewisse Zeit, bevor es versucht, erneut eine Verbindung zum View-Verbindungsserver aufzubauen.

```
./vmware-view --kioskLogin --nonInteractive --once --fullscreen --nomenubar
--serverURL="server.mycomany.com" --userName="CM-00:11:22:33:44:55:66:77" --password="mypassword"
```

Wichtig Wenn das System so konfiguriert wurde, dass vor der Zulassung einer Verbindung von Horizon Client zu einem View-Desktop und vor der Anmeldung eine Meldung angezeigt wird, muss der Benutzer diese Meldung bestätigen, bevor er auf den Desktop zugreifen kann. Verwenden Sie View Administrator und deaktivieren Sie die Anzeige von Meldungen vor der Anmeldung, um dieses Problem zu vermeiden.

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
- Domänenname
- Desktop- oder Anwendungsanzeigename
- Fenstergröße
- Aktionen, darunter „Zurücksetzen“, „Abmelden“ und „Sitzung starten“
- Anzeigeprotokoll

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

Beim Erstellen eines URI rufen Sie im Grunde genommen `vmware-view` mit der vollständigen View-URI-Zeichenfolge als Argument auf.

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 2-3. 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`**.

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 2-4. 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.

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 in der Benutzeroberfläche verfügbar und nicht ausgewählt. 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.

Diese Standardwerte können geändert werden. Siehe „Verwenden der Horizon Client-Befehlszeilenschnittstelle und -Konfigurationsdateien“, auf Seite 28.

---

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://`

Horizon Client startet und der Benutzer wird zu der Seite geleitet, auf der die Adresse eines Servers eingegeben werden kann.

10 `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. Der Dateiname ist in doppelte Anführungszeichen gesetzt, da er Leerzeichen enthält.

11 `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`.

12 `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 62.

Verwenden Sie die Eigenschaft `view.sslVerificationMode`, um den Standard-Überprüfungsmodus festzulegen:

- **`1`** implementiert `Full Verification`.
- **`2`** implementiert `Warn If the Connection May Be Insecure`.
- **`3`** implementiert `No Verification Performed`.

Um den Modus so einzustellen, dass die Endbenutzer ihn nicht ändern können, müssen Sie die Eigenschaft `view.allowSslVerificationMode` in der Datei `/etc/vmware/view-mandatory-config` auf dem Clientsystem auf **„`False`“** setzen. Siehe „Horizon Client-Konfigurationseinstellungen und -Befehlszeilenoptionen“, auf Seite 29.

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 Optionen werden auch verwendet, um den USB-Kanal (Kommunikation zwischen dem USB-Dienst-Daemon und dem Agent) zu verschlüsseln.

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 für diese Einstellungen entweder Konfigurationsdateieigenschaften oder Befehlszeilenoptionen verwenden:

- Wenn Sie Konfigurationsdateieigenschaften verwenden, nutzen Sie die Eigenschaften `view.sslProtocolString` und `view.sslCipherString`.
- Wenn Sie Befehlszeilenkonfigurationsoptionen verwenden, nutzen Sie die Optionen `--sslProtocolString` und `--sslCipherString`.

Weitere Informationen finden Sie unter „Verwenden der Horizon Client-Befehlszeilenschnittstelle und -Konfigurationsdateien“, auf Seite 28. Suchen Sie in der Tabelle unter „Horizon Client-Konfigurationseinstellungen und -Befehlszeilenoptionen“, auf Seite 29 nach der Eigenschaft und den Optionsnamen.

Konfigurieren bestimmter Tasten und Tastenkombinationen zum Senden an das lokale System

Beim Starten von Horizon Client (wenn Sie PCoIP verwenden) oder von Horizon Client 4.0 (wenn Sie VMware Blast oder PCoIP verwenden) können Sie mit einer Datei `view-keycombos-config` angeben, welche Tasten und Tastenkombinationen nicht an den Remote-Desktop weitergeleitet werden sollen.

Womöglich sollen einige Tasten oder Tastenkombinationen bei der Arbeit mit einem Remote-Desktop von Ihrem lokalen Clientsystem verarbeitet werden. Beispielsweise könnten Sie eine bestimmte Tastenkombination verwenden, um den Bildschirmschoner auf Ihrem Clientcomputer zu starten. Unter `/etc/vmware/view-keycombos-config` können Sie eine Datei erstellen und die Tastenkombinationen sowie die einzelnen Tasten angeben.

Setzen Sie jede Taste bzw. Tastenkombination in eine neue Zeile und verwenden Sie dabei das folgende Format:

<modName>scanCode
scanCode

Das erste Beispiel repräsentiert eine Tastenkombination. Das zweite Beispiel repräsentiert eine einzelne Taste. Der Wert *scanCode* ist der Tastaturabfragecode im hexadezimalen Format.

In diesem Beispiel stellt *modName* eine von vier Zusatztasten dar: `Start`, `Alt`, `Umschalt` und `Super`. Die Super-Taste ist tastaturspezifisch. Die Super-Taste ist beispielsweise normalerweise die Windows-Taste auf einer Microsoft Windows-Tastatur und die Befehlstaste auf einer Mac OS X-Tastatur. Sie können auch `<any>` als Platzhalter für *modName* verwenden. Beispielsweise steht `<any>0x153` für alle Kombinationen der Löschtaste, einschließlich der individuellen Löschtaste für die US-Tastatur. Bei dem Wert, den Sie für *modName* eingeben, müssen Sie nicht auf die Groß-/Kleinschreibung achten.

Angeben des Abfragecodes für eine Taste

Für den Wert *scanCode* ist das hexadezimale Format erforderlich. Wenn Sie feststellen möchten, welcher Code verwendet werden soll, öffnen Sie die entsprechende sprach- und tastaturspezifische Datei im Verzeichnis „`lib/vmware/xkeymap`“ auf Ihrem Clientsystem. Zusätzlich zu den in der Datei aufgeführten Tastencodes können Sie auch die folgenden Codes verwenden:

Tabelle 2-5. Multimedia-Tasten

Tastenname	Abfragecode
PREVIOUS_TRACK	0x110
NEXT_TRACK	0x119
MUTE	0x120
CALCULATOR	0x121
PLAY_PAUSE	0x122
STOP	0x124
VOLUME_DOWN	0x12e
VOLUME_UP	0x130
BROWSER_HOME	0x132
BROWSER_SEARCH	0x165
BROWSER_FAVORITES	0x166
BROWSER_REFRESH	0x167
BROWSER_STOP	0x168
BROWSER_FORWARD	0x169
BROWSER_BACK	0x16A
MY_COMPUTER	0x16B
MAIL	0x16C
MEDIA_SELECT	0x16D

Tabelle 2-6. Hangul- und Hanja-Tasten

Tastenname	Abfragecode
HANGUL_EN	0x72
HANJA_EN	0x71
HANGUL_KO	0x172
HANJA_KO	0x171
HANGUL	0xF2
HANJA	0xF1

Tabelle 2-7. „Sleep“, „Wake“ und Ein-/Ausschalttasten des Systems

Tastenname	Abfragecode
SYSTEM_SLEEP	0x15F
SYSTEM_WAKE	0x163
SYSTEM_POWER	0x15e

Die folgende Liste zeigt die Beispielinhalte einer Datei `/etc/vmware/view-keycombos-config`. Vor Codekommentaren steht das Nummernzeichen (#).

```
<ctrl>0x152      #block ctrl-insert
<alt>15          #block alt-tab
<Ctrl><Alt>0x153 #block ctrl-alt-del
<any>0x137       #block any combinations of the Print key
```

```
0x010              #block the individual Q key in a US English keyboard
                 #or block the individual A key in a French keyboard
0x03b            #block the individual F1 key
0x04f            #block the individual 1 key in a numeric keypad
```

Verwenden von FreeRDP für RDP-Verbindungen

Wenn Sie beabsichtigen, statt VMware Blast oder PCoIP RDP für Verbindungen zu View-Desktops zu verwenden, können Sie zwischen dem `rdesktop`-Client und `xfreerdp`, der unter der Apache-Lizenz freigegebenen Open-Source-Implementierung des Remote-Desktop-Protokolls (RDP), wählen.

Da das Programm `rdesktop` nicht länger aktiv entwickelt wird, kann Horizon Client auch die ausführbare Datei `xfreerdp` ausführen, wenn Ihre Linux-Maschine über die für FreeRDP erforderliche Version und die entsprechenden Patches verfügt.

Wichtig Wenn Sie vorhaben, Verbindungen mit Remote-Desktops oder Remoteanwendungen auf einem Microsoft RDS-Host herzustellen, müssen Sie `xfreerdp` verwenden oder den Lizenzierungsmodus in „pro Benutzer“ ändern, wenn dieser Host mittels des Lizenzierungsmodus „pro Gerät“ konfiguriert ist. Grund dafür ist, dass der Lizenzierungsmodus „pro Gerät“ erfordert, dass der RDP-Client eine Client-ID bereitstellt, und `rdesktop` diese ID nicht zur Verfügung stellt, wohingegen `xfreerdp` sie bereitstellt.

Auf Ihrem Computer muss die korrekte Version von FreeRDP zusammen mit den entsprechenden Patches installiert sein. Weitere Informationen finden Sie unter „Installation und Konfiguration von FreeRDP“, auf Seite 50.

Allgemeine Syntax

Sie können die Befehlszeilenschnittstelle `vmware-view` oder einige Eigenschaften in Konfigurationsdateien verwenden, um genau wie bei `rdesktop` Optionen für `xfreerdp` anzugeben.

- Um festzulegen, dass Horizon Client `xfreerdp` anstelle von `rdesktop` ausführen soll, verwenden Sie die entsprechende Befehlszeilenoption oder den entsprechenden Konfigurationsschlüssel.

Befehlszeilenoption:	`--rdpclient="xfreerdp"`
Konfigurationsschlüssel:	`view.rdpClient="xfreerdp"`

- Verwenden Sie zur Festlegung der Optionen, die an das Programm `xfreerdp` weitergeleitet werden sollen, die entsprechende Befehlszeilenoption oder den entsprechenden Konfigurationsschlüssel und geben Sie die FreeRDP-Optionen an.

Befehlszeilenoption:	`--xfreerdpOptions`
Konfigurationsschlüssel:	`view.xfreerdpOptions`

Weitere Informationen zur Befehlszeilenschnittstelle `vmware-view` und den jeweiligen Konfigurationsdateien finden Sie unter „Verwenden der Horizon Client-Befehlszeilenschnittstelle und -Konfigurationsdateien“, auf Seite 28.

Syntax für die Authentifizierung auf Netzwerkebene

Viele Konfigurationsoptionen für das Programm `rdesktop` sind mit denen für das Programm `xfreerdp` identisch. Ein wichtiger Unterschied besteht jedoch darin, dass `xfreerdp` die Authentifizierung auf Netzwerkebene (NLA) unterstützt. NLA ist standardmäßig deaktiviert. Sie müssen mit der folgenden Befehlszeilenoption die Authentifizierung auf der Netzwerkebene aktivieren.

```
--enableNla
```

Zudem müssen Sie die Option `/cert-ignore` hinzufügen, damit der Zertifikatsprüfungsprozess gelingen kann. Es folgt ein Beispiel der richtigen Syntax:

```
vmware-view --enableNla --rdpclient=xfreerdp --xfreerdpOptions="/p:Kennwort /cert-ignore /u:Benutzername /d:Domänenname /v:Server"
```

Falls das Kennwort Sonderzeichen enthält, versehen Sie die Sonderzeichen mit dem Escape-Zeichen (z. B.: **\$**).

Bestimmte Syntax für die Verwendung von FreeRDP mit Horizon Client

Beachten Sie Folgendes:

- Sie müssen Sonderzeichen, die Sie normalerweise in Anführungszeichen einschließen, mit dem Escape-Zeichen versehen. Der folgende Befehl funktioniert z. B. nicht, weil das Sonderzeichen „$“ in „pa$$word“ nicht mit dem Escape-Zeichen versehen ist:

  (nicht richtig) `vmware-view --rdpclient=xfreerdp --xfreerdpOptions="/p:'pa$$word' /u:'crt\administrator'"`

  Stattdessen müssen Sie die folgende Syntax verwenden:

  (richtig) `vmware-view --rdpclient=xfreerdp --xfreerdpOptions="/p:'pa\$\$word' /u:'crt\administrator'"`

- Wenn Endbenutzer eine Sitzung-in-Sitzung-Implementierung von Horizon Client verwenden, müssen Sie die Option `/rfx` verwenden. Ein Beispiel einer Sitzung-in-Sitzung-Implementierung ist eine Implementierung, bei der sich ein Endbenutzer auf einem Thin-Client bei Horizon Client anmeldet, sodass die Benutzeroberfläche des Horizon Client die einzige Benutzeroberfläche ist, die der Endbenutzer sieht, und der Endbenutzer dann eine verschachtelte Version von Horizon Client startet, um eine vom RDS-Host bereitgestellte Remoteanwendung zu verwenden. Wenn Sie in solchen Fällen nicht die Option `/rfx` verwenden, kann der Endbenutzer in der Desktop- und Anwendungsauswahl des verschachtelten Clients die Symbole für den Remote-Desktop und die Remoteanwendung nicht sehen.

Installation und Konfiguration von FreeRDP

Um einen FreeRDP-Client für RDP-Verbindungen zu View-Desktops verwenden zu können, muss sich auf Ihrem Linux-Computer die erforderliche Version von FreeRDP befinden.

Eine Liste der Pakete, von denen `xfreerdp` in Ubuntu abhängig ist, finden Sie unter https://github.com/FreeRDP/FreeRDP/wiki/Compilation.

Voraussetzungen

Laden Sie FreeRDP 1.1.x von GitHub unter https://github.com/FreeRDP/FreeRDP auf Ihre Linux-Clientmaschine herunter.

Vorgehensweise

1 Spielen Sie den Patch `freerdp-1.1.0.patch` unter Verwendung der folgenden Patchbefehle auf:

```
cd /client-installation-directory/patches/FreeRDP-stable-1.1
patch -p1 < freerdp-1.1.0.patch
patch -p1 < freerdp-1.1.0-tls.patch
```

In diesem Fall ist *client-installation-directory* der Pfad für `VMware-Horizon-View-Client-x.x.x-yyyyyy.i386`, wobei *x.x.x* die Versionsnummer und *yyyyyy* die Build-Nummer ist. Die Datei `freerdp-1.1.0-tls.patch` aktiviert die TLSv1.2-Verbindung in `xfreerdp`. Weitere Informationen zur Datei `freerdp-1.1.0.patch` finden Sie in der Datei `README.patches` im selben *`client-installation-directory`*`/patches`-Verzeichnis.

2 Führen Sie folgenden Befehl aus:

```
cmake –DWITH_SSE2=ON –DWITH_PULSEAUDIO=ON –DWITH_PCSC=ON –DWITH_CUPS=ON .
```

3 Führen Sie folgenden Befehl aus:

```
make
```

4 Führen Sie den folgenden Befehl aus, um die erzeugte `xfreerdp`-Binärdatei in ein Verzeichnis unter dem Ausführungspfad zu installieren, damit Horizon Client das Programm ausführen kann, indem `xfreerdp` ausgeführt wird:

```
sudo make install
```

5 (Optional) Stellen Sie sicher, dass das Modul für das virtuelle Drucken ordnungsgemäß geladen werden kann.

a Um sicherzugehen, dass `tprdp.so` von FreeRDP 1.1 geladen werden kann, führen Sie den folgenden Befehl aus:

```
sudo ln –s /usr/lib/vmware/rdpvcbridge/tprdp.so /usr/local/lib/i386–linux–
gnu/freerdp/tprdp–client.so
```

b Um Horizon Client mit aktivierter Funktion für das virtuelle Drucken zu starten, führen Sie den folgenden Befehl aus:

```
vmware–view ––rdpclient=xfreerdp ––xfreerdpOptions='/cert–ignore /vc:tprdp'
```

Hinweis Die Funktion „Virtual Printing“ steht Ihnen zur Verfügung, wenn Sie VMware Blast oder PCoIP verwenden.

Aktivieren des FIPS-Modus

Sie können den FIPS-Modus (Federal Information Processing Standard) aktivieren. Der Client verwendet dann bei der Kommunikation mit Remote-Desktops FIPS-konforme kryptografische Algorithmen.

Wichtig Wenn Sie den FIPS-Modus im Client aktivieren, muss dieser Modus auch für den Remote-Desktop aktiviert sein. Eine gemischte Anwendung, in der der FIPS-Modus nur für den Client oder nur für den Desktop aktiviert ist, wird nicht unterstützt.

Für die Aktivierung des FIPS-Modus führen Sie die folgenden Konfigurationsänderungen durch:

1 Bearbeiten Sie `/etc/vmware/config` und fügen Sie die folgenden Zeilen hinzu:

```
usb.enableFIPSMode = "TRUE"
mks.enableFIPSMode = “TRUE”
```

2 Bearbeiten Sie `/etc/vmware/view–mandatory–config` und fügen Sie die folgende Zeile hinzu:

```
View.fipsMode = ”TRUE”
```

3 Bearbeiten Sie `/etc/teradici/pcoip_admin.conf` und fügen Sie die folgende Zeile hinzu:

```
pcoip.enable_fips_mode = 1
```

Konfigurieren des PCoIP-Client-Bildcache

Bei der PCoIP-Client-Bildzwischenspeicherung wird der Bildinhalt auf dem Client gespeichert, um erneute Übertragungen zu vermeiden. Diese Funktion ist standardmäßig zur Reduzierung der Bandbreitenauslastung aktiviert.

Der PCoIP-Bildcache erfasst die räumliche sowie zeitliche Redundanz. Wenn Sie beispielsweise in einem PDF-Dokument einen Bildlauf nach unten durchführen, wird unten im Fenster neuer Inhalt angezeigt, während oben im Fenster der älteste Inhalt nicht mehr angezeigt wird. Der restliche Inhalt bleibt unverändert und wird nach oben verschoben. Der PCoIP-Bildcache kann räumliche und zeitliche Redundanz erkennen.

Da es sich während des Bildlaufs bei den an das Client-Gerät gesendeten Anzeigeinformationen in erster Linie um eine Abfolge von Cache-Indizes handelt, lassen sich durch die Verwendung eines Bildcaches deutliche Bandbreiteneinsparungen erzielen. Dieser effiziente Bildlauf hat sowohl bei LAN- als auch WAN-Verbindungen Vorteile.

- Bei LAN-Verbindungen mit relativ uneingeschränkter Bandbreite führt die clientseitige Bildzwischenspeicherung zu deutlichen Bandbreiteneinsparungen.
- Um bei WAN-Verbindungen innerhalb der Bandbreiteneinschränkungen zu bleiben, nimmt die Bildlaufleistung oft ab, wenn keine clientseitige Zwischenspeicherung verwendet wird. In dieser Situation kann die clientseitige Zwischenspeicherung zu einer Einsparung von Bandbreite führen und einen reibungslosen, äußerst schnellen Bildlauf sicherstellen.

Diese Funktion ist standardmäßig aktiviert, sodass der Client Teile der Anzeige speichert, die zuvor übermittelt wurden. Die Standard-Cachegröße beträgt 250 MB. Ein größerer Cache reduziert die Bandbreitenauslastung, erfordert jedoch auch mehr Arbeitsspeicher auf dem Client. Ein kleinerer Cache erfordert eine höhere Bandbreitenauslastung. Ein Thin Client mit nur wenig Arbeitsspeicher erfordert beispielsweise eine geringere Cachegröße.

Festlegen der Konfigurationseigenschaft

Zur Konfiguration der Cachegröße können Sie die Eigenschaft `pcoip.image_cache_size_mb` festlegen. Die folgende Einstellung konfiguriert beispielsweise die Cachegröße auf 50 MB:

```
pcoip.image_cache_size_mb = 50
```

Setzen Sie ein Leerzeichen vor und nach dem Gleichheitszeichen (=).

Wenn Sie einen Wert angeben, der kleiner ist als die Menge des verfügbaren Arbeitsspeichers geteilt durch 2, wird der Wert auf das nächstgelegene dekadische Vielfache gerundet. Der Mindestwert ist 50. Werte unter 50 werden ignoriert.

Wenn Sie einen Wert angeben, der größer ist als der verfügbare Arbeitsspeicher geteilt durch 2, wird der Wert auf die Menge des verfügbaren Arbeitsspeichers geteilt durch 2 festgelegt und auf das nächstgelegene dekadische Vielfache gerundet.

Sie können diese Eigenschaft in jeder der einzelnen Dateien festlegen. Beim Start von Horizon Client wird die Einstellung aus mehreren Speicherorten in der folgenden Reihenfolge verarbeitet:

1 `/etc/teradici/pcoip_admin_defaults.conf`

2 `~/.pcoip.rc`

3 `/etc/teradici/pcoip_admin.conf`

Ist eine Einstellung in verschiedenen Speicherorten konfiguriert, entspricht der verwendete Wert dem Wert aus dem letzten Lesevorgang der Datei.

Hinweis Sie können die folgende Eigenschaft zur visuellen Anzeige der Funktionsfähigkeit des Bildcaches festlegen:

```
pcoip.show_image_cache_hits = 1
```

In dieser Konfiguration wird Ihnen für jede Kachel (32 x 32 Pixel) in einem Bild aus dem Bildcache ein Rechteck um die Kachel herum angezeigt.

Verwalten der Remote-Desktop- und Anwendungsverbindungen 3

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 einen Server angeben und die Anmeldedaten für Ihr Benutzerkonto eingeben.

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

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 14 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.

Vorgehensweise

1 Sie können entweder ein Terminalfenster öffnen und `vmware-view` eingeben, oder die Anwendungen nach **VMware Horizon Client** durchsuchen und auf das Symbol doppelklicken.

2 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.

3 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 **OK**.

4 Wenn Sie zur Eingabe von Benutzername und Kennwort aufgefordert werden, geben Sie die Active Directory-Anmeldedaten ein.

   a Geben Sie den Benutzernamen und das Kennwort eines Benutzers ein, der berechtigt ist, mindestens einen Desktop- oder Anwendungspool zu benutzen.

     Wenn das Dropdown-Menü **Domäne** deaktiviert ist, müssen Sie den Benutzernamen im Format `Domäne\Benutzername` oder `Benutzername@Domäne` eingeben.

   b (Optional) Wählen Sie im Dropdown-Menü **Domäne** eine Domänenwert aus.

   c Klicken Sie auf **OK**.

5 Wenn die Sicherheitsanzeige des Desktops rot angezeigt und eine Warnung ausgegeben wird, reagieren Sie auf die Eingabeaufforderung.

   Normalerweise bedeutet diese Warnung, dass der Verbindungsserver keinen Zertifikat-Fingerabdruck an den Client gesendet hat. Ein Fingerabdruck ist ein Hash-Wert des öffentlichen Schlüssels des Zertifikats und wird als Abkürzung für den öffentlichen Schlüssel verwendet.

6 (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.

7 (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.

8 Doppelklicken Sie auf einen Remote-Desktop oder eine Remoteanwendung, um die Verbindung herzustellen.

Wenn Sie eine Verbindung mit einem sitzungsbasierten Remote-Desktop auf einem Microsoft RDS-Host herstellen und für den Desktop bereits die Verwendung eines anderen Anzeigeprotokolls 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 Clientfenster angezeigt.

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

- Legen Sie fest, ob der View-Verbindungsserver dahingehend konfiguriert werden soll, SSL nicht zu verwenden. Die Clientsoftware erfordert SSL-Verbindungen. Prüfen Sie, ob die globale Einstellung in View 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 View-Verbindungsserver konfiguriert ist.
- Stellen Sie eine ordnungsgemäße Funktionsweise des Sicherheitszertifikats für View-Verbindungsserver sicher. Wenn dies nicht zutrifft, wird in View Administrator möglicherweise angezeigt, dass View Agent in Desktops nicht erreichbar ist. Dies sind Hinweise auf zusätzliche Verbindungsprobleme, die durch Zertifikatprobleme verursacht werden.
- Stellen Sie sicher, dass die für die View-Verbindungsserver-Instanz festgelegten Kennzeichen Verbindungen von diesem Benutzer erlauben. Weitere Informationen finden Sie im Dokument *Administration von View*.
- Stellen Sie sicher, dass der Benutzer zum Zugriff auf diesen Desktop oder diese Anwendung berechtigt ist. Weitere Informationen finden Sie im Dokument *Einrichten von Desktop- und Anwendungspools in View*.
- Wenn Sie das RDP-Anzeigeprotokoll zur Verbindungsherstellung mit einem Remote-Desktop verwenden, müssen Sie bestätigen, dass das Remote-Betriebssystem Remote-Desktop-Verbindungen zulässt.

Verbinden mit veröffentlichten Anwendungen mithilfe eines nicht authentifizierten Zugriffs

Sie haben die Möglichkeit, mit Horizon Client eine Verbindung mit veröffentlichten Anwendungen über ein Konto für einen nicht authentifizierten Zugriff herzustellen.

Bevor Sie Endbenutzern die Möglichkeit geben, auf ihre veröffentlichten Anwendungen mithilfe eines nicht authentifizierten Zugriffs zuzugreifen, müssen Sie prüfen, ob sich eine Verbindung mit den veröffentlichten Anwendungen mit einem nicht authentifizierten Zugriff von einem Clientgerät aus herstellen lässt.

Voraussetzungen

- Stellen Sie sicher, dass der Verbindungsserver von Horizon 7 Version 7.1 für den nicht authentifizierten Zugriff konfiguriert ist.
- Vergewissern Sie sich, dass Ihre Benutzer für einen nicht authentifizierten Zugriff in Horizon Administrator erstellt wurden. Wenn es sich beim Standardbenutzer für einen nicht authentifizierten Zugriff um den einzigen Benutzer für einen nicht authentifizierten Zugriff handelt, stellt Horizon Client die Verbindung mit dem Verbindungsserver mit dem Standardbenutzer her.

Vorgehensweise

1. Sie können entweder ein Terminalfenster öffnen und `vmware-view` eingeben, oder die Anwendungen nach **VMware Horizon Client** durchsuchen und auf das Symbol doppelklicken.
2. Wählen Sie auf der Horizon Client-Startseite **Datei > Anonym mit nicht authentifiziertem Zugriff anmelden** aus der Menüleiste aus (falls noch nicht aktiviert).
3. Stellen Sie eine Verbindung mit dem Verbindungsserver her, der für einen nicht authentifizierten Zugriff konfiguriert ist.
   - Wenn der benötigte Server noch nicht hinzugefügt wurde, doppelklicken Sie auf die Schaltfläche **+ Server hinzufügen**, wenn noch keine Server vorhanden sind, oder klicken Sie auf die Schaltfläche **+ Neuer Server** in der Menüleiste, um einen neuen Server hinzuzufügen. Geben Sie den Namen des Verbindungsservers oder Sicherheitsservers ein und klicken Sie auf **Verbinden**.
   - Wenn der benötigte Server nicht auf der Startseite von Horizon Client angezeigt wird, klicken Sie mit der rechten Maustaste auf das Symbol für den Server und wählen Sie **Verbinden** aus dem eingeblendeten Kontextmenü aus.

   Es wird eventuell eine Meldung eingeblendet, die Sie bestätigen müssen, bevor das Anmeldedialogfenster angezeigt wird.
4. Legen Sie im Anmeldedialogfeld das Konto für einen nicht authentifizierten Zugriff fest, das verwendet werden soll.
   a. Wählen Sie aus der Dropdown-Liste vorhandener Konten für einen nicht authentifizierten Zugriff ein Benutzerkonto aus.

      Neben dem Standardbenutzerkonto wird `(Standard)` angezeigt.

   b. (Optional) Klicken Sie auf **Immer dieses Konto verwenden**, wenn Sie das Dialogfeld für die Serveranmeldung bei der nächsten Verbindung mit dem Server umgehen möchten.

   c. Klicken Sie auf **OK**.

Das Fenster für die Anwendungsauswahl wird mit den veröffentlichten Anwendungen angezeigt, für deren Verwendung das Konto für einen nicht authentifizierten Zugriff autorisiert ist.

Hinweis Wenn Sie die Option **Immer dieses Konto verwenden** bereits im Rahmen einer früheren Sitzung mit nicht authentifiziertem Zugriff bei der Anmeldung ausgewählt haben, werden Sie nicht zur Angabe des Kontos für die aktuelle Sitzung mit nicht authentifiziertem Zugriff aufgefordert. Um diese Option zu deaktivieren, klicken Sie mit der rechten Maustaste auf das Serversymbol auf der Startseite von Horizon Client und wählen Sie die Option **Gespeichertes Konto mit nicht authentifiziertem Zugriff löschen** aus dem eingeblendeten Kontextmenü aus.

5 Doppelklicken Sie auf die gewünschte veröffentlichte Anwendung, um diese zu starten.

Das Anwendungsfenster wird angezeigt.

6 Beenden Sie die veröffentlichte Anwendung, wenn Sie diese nicht mehr benötigen.

Das Dialogfeld „Verbindung zur Sitzung trennen?“ wird angezeigt, in dem Sie zur Bestätigung der Trennung vom Server aufgefordert werden.

Wenn der von Ihrem Horizon-Administrator festgelegte Wert für die Zeitüberschreitung der Sitzung erreicht wird, wird die Sitzung automatisch vom Server getrennt.

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.

Die Clientlaufwerksumleitung erfordert, dass die folgenden Bibliotheksdateien installiert werden. Auf einigen Clientcomputern sind diese Bibliotheksdateien womöglich nicht standardmäßig installiert.

- `libsigc-2.0.so.0`
- `libglibmm-2.4.so.1`

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 oder Registrierungseinstellungen zur Steuerung des Verhaltens der Laufwerksumleitung festzulegen. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Bei Ubuntu 16.04 x64-Distributionen ist die darin enthaltene Bibliothek `libglibmm-2.4.so.1.3.0` nicht kompatibel mit der aktuellen CDR-Implementierung (Client Drive Redirection, Clientlaufwerksumleitung). Um diese Einschränkung zu umgehen, kopieren Sie die Bibliotheksdatei `libglibmm-2.4.so.1.3.0` einer Ubuntu 14.04 x64-Distribution in Ihre Ubuntu 16.04 x64-Distribution.

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** und klicken Sie auf **Freigabe**. Alternativ wählen Sie aus der Menüleiste **Verbindungs > einstellungen** und klicken Sie auf **Freigabe**.
Vom Dialogfeld „Freigabe“, wenn Sie sich mit einem Desktop oder einer Anwendung verbinden	Klicken Sie auf **Erlauben** oder auf **Verweigern**, um die Freigabe Ihres Benutzerordners zu erlauben oder zu verhindern.
Aus einem Desktop-Betriebssystem heraus	Wählen Sie aus der Menüleiste **Verbindungs > einstellungen** und klicken Sie auf **Freigabe**.

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.
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 Benutzerordner	Aktivieren Sie das Kontrollkästchen **Geben Sie Ihren Startordner frei:** *Benutzerordner*.

Option	Aktion
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.
Dialogfeld „Freigabe“ beim Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung nicht anzeigen	Aktivieren Sie das Kontrollkästchen**Dialogfeld 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.

Freigeben von Ordnern durch Bearbeiten einer Konfigurationsdatei

Zusätzlich zur Freigabe von Ordnern über das Dialogfeld „Einstellungen“ können Sie auch Ordner durch die Bearbeitung einer Konfigurationsdatei freigeben.

Vorgehensweise

1 Erstellen Sie eine Konfigurationsdatei namens `config`, falls diese nicht an einem der folgenden Speicherorte existiert:

   - `$HOME/.vmware/`
   - `/usr/lib/vmware/`
   - `/etc/vmware/`

2 Fügen Sie jedem Ordner, den Sie freigeben möchten, die folgende Zeile hinzu:

   `tsdr.share=`*`Ordnerpfad`*

   Um beispielsweise Ordner in `/` und `/home/user1`, freizugeben, erstellen Sie die Datei `/etc/vmware/config` und fügen Sie die folgenden Zeilen hinzu:

```
tsdr.share=/
tsdr.share=/home/user1
```

Ordner, die in einer Konfigurationsdatei freigegeben werden, sind nicht im Bereich „Freigabe“ aufgelistet. Sie können die Konfigurationsdatei so konfigurieren, dass Ordner oder zusätzliche Ordner nicht mehr freigegeben 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:

- 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, das die Benutzer auf ihren Linux-Clientsystemen installieren können, finden Sie in der Ubuntu-Dokumentation.

Horizon Client verwendet die PEM-formatierten Zertifikate, die im Verzeichnis `/etc/ssl/certs` auf dem Clientsystem gespeichert sind. Informationen zum Import eines Stammzertifikats, das an diesem Speicherort gespeichert ist, finden Sie unter „Import eines Zertifikats in die systemweite Zertifikatsautorität-Datenbank“ des Dokuments unter https://help.ubuntu.com/community/OpenSSL.

Neben der Bereitstellung eines Serverzertifikats sendet der Verbindungsserver ebenfalls einen Zertifikat-Fingerabdruck an Horizon Client. Ein Fingerabdruck ist ein Hash-Wert des öffentlichen Schlüssels des Zertifikats und wird als Abkürzung für den öffentlichen Schlüssel verwendet. Wenn der Verbindungsserver keinen Fingerabdruck sendet, wird eine Warnung ausgegeben, dass es sich um eine nicht vertrauenswürdige Verbindung handelt.

Wenn Ihr Administrator dies zulässt, können Sie den Zertifikatsprüfungsmodus festlegen. Wählen Sie in der Menüleiste **Datei > Einstellungen** aus. 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.
- **Server-Identitätszertifikate nicht überprüfen**. Mit dieser Einstellung werden Zertifikate nicht überprüft.

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 bei einem Remote-Desktop angemeldet sind und zu einem anderen Remote-Desktop oder einer anderen Remoteanwendung wechseln möchten, der bzw. die bereits auf dem Client ausgeführt wird, wählen Sie den Desktop bzw. die Anwendung aus dem Menü **Ansicht** aus. ■ Wenn Sie bei einem Remote-Desktop angemeldet sind und zu einem anderen Remote-Desktop oder einer anderen Remoteanwendung wechseln möchten, der bzw. die nicht ausgeführt wird, wählen Sie in der Menüleiste **Datei > Zu Desktop- und Anwendungsliste zurückkehren** aus und starten Sie dann den Desktop bzw. die Anwendung vom Auswahlfenster aus. ■ 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- bzw. Anwendungssitzungen 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.

Vorgehensweise

- Trennen Sie die Verbindung, ohne sich abzumelden.

Option	Aktion
Horizon Client ebenfalls beenden	Klicken Sie auf die Schaltfläche **Schließen** in der Ecke des Fensters oder wählen Sie **Datei > Beenden** in der Menüleiste aus.
Einen anderen Remote-Desktop auf demselben Server auswählen	Wählen Sie **Desktop > Trennen** in der Menüleiste aus.
Einen Remote-Desktop auf einem anderen Server auswählen	Wählen Sie **Datei > Verbindung zum Server trennen** in der Menüleiste aus.

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 **Desktop > Verbindung trennen und abmelden** aus. Bei Verwendung dieser Option werden alle Dateien, die auf dem Remote-Desktop geöffnet sind, ohne vorheriges Speichern geschlossen.

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

  a Wählen Sie auf der Startseite mit den Desktop-Verknüpfungen den entsprechenden Desktop und anschließend **Desktop > Abmelden** in der Menüleiste aus.

  b Geben Sie bei Aufforderung die Anmeldeinformationen für den Zugriff auf den Remote-Desktop an.

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

Verwenden von Microsoft Windows-Desktops oder -Anwendungen auf einem Linux-System

4

Horizon Client für Linux unterstützt viele Funktionen.

Dieses Kapitel behandelt die folgenden Themen:

Funktionsunterstützungs-Matrix für Linux

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 4-1. Für Linux-Clients 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- oder Windows Server 2016-Desktop
USB-Umleitung	Begrenzt	Begrenzt	X	X	X	X
Echtzeit-Audio/Video (RTAV)	Begrenzt	Begrenzt	X	X	X	X
Scannerumleitung						
Umleitung serieller Ports						
RDP-Anzeigeprotokoll	Begrenzt	Begrenzt	X	X	X	X

Tabelle 4-1. Für Linux-Clients unterstützte Remote-Desktop-Funktionen (Fortsetzung)

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- oder Windows Server 2016-Desktop
PCoIP-Anzeigeprotokoll	Begrenzt	Begrenzt	X	X	X	X
VMware Blast-Anzeigeprotokoll			X	X	X	X
Persona-Verwaltung						
Wyse MMR	Nur Partner-Clientsysteme, und nur mit RDP	Nur Partner-Clientsysteme, und nur mit RDP				
Windows Media MMR			X	X	X	
Standortbasiertes Drucken	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
Clientlaufwerksumleitung			X	X	X	X

Windows 10-Desktops erfordern View Agent 6.2 oder höher. Windows Server 2012 R2-Desktops erfordern View Agent 6.1 oder höher. Windows Server 2016-Desktops erfordern Horizon Agent 7.0.2 oder höher.

VMware Blast erfordert 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.

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 4-2. 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
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)
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-Desktops mit Horizon Client für Linux unterstützt werden, gelten die folgenden Einschränkungen.

Tabelle 4-3. Anforderungen für Sonderfunktionen

Funktion	Anforderungen
Echtzeit-Audio/Video	■ Bei Clientsoftware von Drittanbietern ist für diese Funktion View 5.2 mit Feature Pack 2 oder höher erforderlich. ■ Für Horizon Client von VMware ist für diese Funktion View Agent 6.0.2 oder höher erforderlich. Erfordert das VMware Blast- oder PCoIP-Anzeigeprotokoll.
Virtuelles und standortbasiertes Drucken für Windows Server 2008 R2 Desktops, RDS-Desktops (auf RDS-Hosts auf virtueller Maschine) und Remoteanwendungen	■ Bei Clientsoftware von Drittanbietern ist für diese Funktion Horizon 6.0.1 mit View oder höher erforderlich. ■ Für Horizon Client von VMware ist für diese Funktion View Agent 6.0.2 oder höher erforderlich. Erfordert das VMware Blast- oder PCoIP-Anzeigeprotokoll.
USB-Umleitung	■ Bei Clientsoftware von Drittanbietern ist für diese Funktion View 5.1 oder höher erforderlich. ■ Für Horizon Client von VMware ist für diese Funktion View Agent 6.0.2 oder höher erforderlich. Erfordert das VMware Blast- oder PCoIP-Anzeigeprotokoll.
Smartcards	Für Desktops virtueller Einzelbenutzer-Maschinen ist für diese Funktion View Agent 6.0.2 oder höher erforderlich. Für durch RDS-Hosts bereitgestellte sitzungsbasierte Desktops ist für diese Funktion View Agent 6.1 oder höher erforderlich.
Clientlaufwerksumleitung	View Agent 6.1.1 oder höher.

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*.

Hinweis Welche Funktionen für die einzelnen Thin Client-Geräte verfügbar sind, richtet sich jeweils nach dem Hersteller und Modell sowie nach der vom jeweiligen Unternehmen gewählten Konfiguration. Informationen über Hersteller und Modelle für Thin Client-Geräte finden Sie im *VMware-Kompatibilitätshandbuch* unter http://www.vmware.com/resources/compatibility/search.php?deviceCategory=vdm.

Weitere Erläuterungen zu diesen Funktionen und deren Einschränkungen finden Sie im Dokument *Planung von View*.

Funktionsunterstützung für Linux-Desktops

Einige Linux-Gastbetriebssysteme werden unterstützt, wenn Sie über View Agent 6.1.1 oder höher verfügen. Im Dokument *Einrichten von Horizon 6 for Linux-Desktops*, das Bestandteil der Dokumentation von Horizon 6, Version 6.1, ist, finden Sie eine Liste unterstützter Linux-Betriebssysteme sowie Informationen zu den unterstützten Funktionen.

Internationalisierung

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

Wenn Sie ein Linux-Clientsystem mit Ubuntu 10.4 verwenden und die Benutzeroberfläche des Clients in einer anderen Sprache als Englisch angezeigt werden soll, müssen Sie das Clientsystem für ein Gebietsschema mit UTF-8-Codierung einrichten.

Tastaturen und Monitore

Sie können mehrere Monitore und beliebige Tastaturtypen bei einem Remote-Desktop verwenden. Durch bestimmte Einstellungen wird das bestmögliche Benutzererlebnis sichergestellt.

Empfohlene Vorgehensweisen zum Verwenden mehrerer Monitore

Es gibt folgende Empfehlungen zur erfolgreichen Verwendung mehrerer Monitore bei einem Remote-Desktop:

- Definieren Sie den primären Monitor als den Monitor ganz links unten.
- Aktivieren Sie Xinerama. Wenn Sie Xinerama nicht aktivieren, wird das primäre Anzeigegerät möglicherweise nicht korrekt identifiziert.
- Die Menüleiste wird auf dem Monitor ganz links oben angezeigt. Wenn beispielsweise zwei Monitore nebeneinander vorhanden sind und die Oberkante des linken Monitors niedriger als die Oberkante des rechten Monitors ist, wird die Menüleiste auf dem rechten Monitor angezeigt, da der rechte Monitor weiterhin ganz links oben ist.
- Sie können bis zu vier Monitore verwenden, sofern Sie über ausreichend Video-RAM verfügen.

  Um mehr als zwei Monitore zum Anzeigen Ihres Remote-Desktops auf einem Ubuntu-Clientsystem zu verwenden, müssen Sie die Einstellung `kernel.shmmax` korrekt festlegen. Verwenden Sie die folgende Formel:

  maximale horizontale Auflösung X *maximale vertikale Auflösung* X *maximale Anzahl an Monitoren* X 4

  Wenn Sie beispielsweise `kernel.shmmax` manuell auf 65536000 einstellen, können Sie vier Monitore mit einer Bildschirmauflösung von 2560 x 1600 verwenden.
- Horizon Client verwendet die Monitorkonfiguration, die beim Start von Horizon Client aktiviert ist. Wenn Sie bei der Monitoranzeige vom Querformat zum Hochformat wechseln oder einen zusätzlichen Monitor an das Clientsystem anschließen, während Horizon Client ausgeführt wird, müssen Sie Horizon Client neu starten, um die neue Monitorkonfiguration verwenden zu können.

Horizon Client unterstützt die folgenden Monitorkonfigurationen:

- 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.
- Wenn Sie über eine Version von Horizon Client vor Version 4.0 verfügen und mehr als zwei Monitore verwenden, muss für diese Monitore der gleiche Modus und die gleiche Auflösung aktiviert sein. Wenn Sie also drei Monitore verwenden, müssen sich alle drei entweder im Querformat oder im Hochformat befinden und die gleiche Bildschirmauflösung verwenden.
- Monitore können nur dann nebeneinander, in Zweiergruppen oder vertikal gestapelt platziert werden, wenn Sie zwei Monitore verwenden.

- Wenn Sie angeben, dass Sie alle Monitore verwenden möchten, und das VMware Blast- oder PCoIP-Anzeigeprotokoll verwenden, können Sie eine zu verwendende Teilmenge von benachbarten Monitoren festlegen, indem Sie im Desktop-Auswahlfenster mit der rechten Maustaste auf den Desktop klicken, in der Dropdown-Liste **Anzeige** die Option **Vollbild - Alle Monitore** auswählen und anschließend die Monitore, die Sie verwenden möchten, durch Klicken auswählen.

  Hinweis Bei einem Ubuntu-Clientsystem müssen Sie den Monitor ganz links oben als einen der Monitore auswählen. Beispiel: Wenn Sie vier Monitore in Zweiergruppen gestapelt haben, müssen Sie entweder die beiden oberen Monitore oder die beiden Monitore ganz links auswählen.

Bildschirmauflösung

Berücksichtigen Sie die folgenden Regeln beim Festlegen von Bildschirmauflösungen:

- Wenn Sie einen Remote-Desktop auf einem sekundären Monitor öffnen und dann die Bildschirmauflösung auf diesem Monitor ändern, geht der Remote-Desktop zum primären Monitor über.
- Mit PCoIP können Sie beim Einsatz von 2 Monitoren die Auflösung für jeden Monitor einzeln anpassen, wobei eine Auflösung von bis zu 2560 x 1600 pro Bildschirm möglich ist. Wenn Sie mehr als zwei Monitore verwenden, müssen die Monitore alle die gleiche Bildschirmauflösung verwenden.
- 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.

- Mit RDP können Sie bei der Verwendung mehrerer Monitore die Auflösung für jeden Monitor nicht separat festlegen.

Tastatureinschränkungen

Meistens funktionieren Tastaturen bei einem Remote-Desktop genauso gut wie bei einem physischen Computer. Im Folgenden finden Sie eine Aufstellung der Einschränkungen, die abhängig von der Art der Peripheriegeräte und der Software auf dem Clientsystem auftreten können:

- Wenn Sie das PCoIP-Anzeigeprotokoll verwenden und der Remote-Desktop erkennen soll, welche Tastaturbelegung Ihr Clientsystem verwendet, z. B. eine japanische oder eine deutsche Tastatur, müssen Sie in View Agent ein GPO festlegen. Verwenden Sie die Richtlinie **Synchronisierung der Standardeingabesprache für PCoIP-Benutzer aktivieren**, die in der ADM-Vorlagendatei für View-PCoIP-Sitzungsvariablen zur Verfügung steht. Weitere Informationen finden Sie im Dokument *Einrichten von Desktop- und Anwendungspools für View*.

- Möglicherweise funktionieren nicht alle Multimedia-Tasten einer Multimedia-Tastatur. So funktionieren beispielsweise u. U. die Musik- und Computer-Taste nicht.
- Für den Fall, dass Sie über RDP eine Verbindung zu einem Desktop herstellen und Sie über den Fluxbox-Fenster-Manager verfügen, funktioniert die Tastatur nach einem Zeitraum mit Inaktivität möglicherweise nicht mehr, wenn ein Bildschirmschoner auf dem Remote-Desktop ausgeführt wird.

  Unabhängig vom verwendeten Fenster-Manager empfiehlt VMware, den Bildschirmschoner auf dem Remote-Desktop zu deaktivieren und keinen Ruhezustandstimer einzustellen.

Verbinden von USB-Geräten

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

Dank 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.

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 einstellen, dass die USB-Geräte automatisch mit Ihrem Remote-Desktop verbunden werden. Anderenfalls wird das USB-Gerät beim Versuch der manuellen Umleitung über ein Menüelement nur umgeleitet, wenn Sie das Gerät trennen und es anschließend wieder verbinden.
- 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 74.
- 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. Weitere Informationen finden Sie im Thema „Konfiguration der Filterrichtlinieneinstellungen für USB-Geräte“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Wichtig Dieser Vorgang beschreibt die Verwendung des Horizon Client-Menüs zur Verbindung von USB-Geräten und der automatischen Konfiguration von verbundenen USB-Geräten. Sie können auch eine USB-Umleitung konfigurieren, indem Sie eine Konfigurationsdatei verwenden oder eine Gruppenrichtlinie erstellen. Weitere Informationen zur Verwendung einer Konfigurationsdatei finden Sie unter „Systemanforderungen für die USB-Umleitung“, auf Seite 87. Weitere Informationen zur Erstellung von Gruppenrichtlinien finden Sie im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Voraussetzungen

- Um USB-Geräte mit einem Remote-Desktop verwenden zu können, muss der View-Administrator die USB-Funktion für den Remote-Desktop aktiviert haben.

  Diese Aufgabe schließt die Installation der Komponente **USB-Umleitung** des Agenten ein und kann auch die Erstellung von Einstellungsrichtlinien hinsichtlich der USB-Umleitung umfassen. Wenn Sie Verbindungsserver und Agent 5.3.x verwenden, finden Sie weitere Informationen im Dokument *View-Administration*. Für den Verbindungsserver und Agent 6.0 oder höher erhalten Sie Erläuterungen im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

- 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 ein USB-Gerät manuell mit einem Remote-Desktop.

  a Schließen Sie das USB-Gerät an Ihr lokales Clientsystem an.

  b Klicken Sie in der 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 zur automatischen Verbindung von USB-Geräten mit dem Remote-Desktop, wenn Horizon Client gestartet wird.

  Diese Option ist standardmäßig ausgewählt.

  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 Horizon Client-Menüleiste auf **USB-Gerät verbinden**.

  c Wählen Sie **Beim Start automatisch verbinden** aus.

  d Schließen Sie das USB-Gerät an und starten Sie Horizon Client neu.

  USB-Geräte, die Sie nach dem Start von Horizon Client an Ihr lokales System anschließen, werden an den Remote-Desktop umgeleitet. 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 dahingehend, dass USB-Geräte automatisch mit dem Remote-Desktop verbunden werden, wenn Sie diese an das lokale System anschließen.

  Mit dieser Option haben Sie die Möglichkeit, Geräte mit MTP-Treibern zu verbinden, so zum Beispiel Android-basierte Samsung-Smartphones und -Tablets. Diese Option ist standardmäßig ausgewählt.

  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 Horizon Client-Menüleiste auf **USB-Gerät verbinden**.

  c Wählen Sie **Nach Einführung automatisch verbinden** aus.

  d 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.

Sie können die automatische Verbindung von USB-Geräten auch konfigurieren, indem Sie die Konfigurationsdateioptionen `view.usbAutoConnectAtStartup` und `view.usbAutoConnectOnInsert` verwenden. Weitere Informationen dazu finden Sie unter „Horizon Client-Konfigurationseinstellungen und -Befehlszeilenoptionen“, auf Seite 29.

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 *Einrichten von Desktop- und Anwendungspools in View*.

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.

Hinweis Diese Funktion ist nur mit der von Drittanbietern bereitgestellten Horizon Client-Version für Linux oder mit der Horizon Client-Software verfügbar, die über die VMware-Website für Produkt-Downloads abrufbar ist.

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, muss Ihr Administrator den Client nicht konfigurieren, um die Geräte automatisch über die USB-Umleitung weiterzuleiten. Wenn die Webcam über die USB-Umleitung verbunden wird, reicht die Leistung für einen Video-Chat nicht aus.

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 eines Standardmikrofons auf einem Linux-Clientsystem

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

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

Dieses Verfahren beschreibt die Auswahl eines Standardmikrofons über die Benutzeroberfläche des Clientsystems. Administratoren können auch ein bevorzugtes Mikrofon konfigurieren, indem sie eine Konfigurationsdatei bearbeiten. Siehe „Auswählen einer bevorzugten Webcam oder eines Mikrofons auf einem Linux-Clientsystem“, auf Seite 75.

Voraussetzungen

- Stellen Sie sicher, dass 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 Remote-Desktops verwendet wird.

Vorgehensweise

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

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

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

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

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

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

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

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

Um die Eigenschaften in der Datei „`/etc/vmware/config`“ und ein bevorzugtes Gerät festzulegen, müssen Sie die Werte bestimmter Felder ermitteln. Sie können in der Protokolldatei nach den Werten dieser Felder suchen.

- Für Webcams legen Sie für die Eigenschaft `rtav.srcWCamId` den Wert des Felds `UserId` und für die Eigenschaft `rtav.srcWCamName` den Wert des Felds `Name` fest.

  Die Eigenschaft `rtav.srcWCamName` besitzt eine höhere Priorität als die Eigenschaft `rtav.srcWCamId`. Beide Eigenschaften müssen sich auf dieselbe Webcam beziehen. Wenn die Eigenschaften unterschiedliche Webcams betreffen, wird die durch `rtav.srcWCamName` angegebene Webcam verwendet, sofern vorhanden. Andernfalls wird die durch `rtav.srcWCamId` angegebene Webcam verwendet. Falls beide Webcams nicht gefunden werden, wird die standardmäßige Webcam verwendet.

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

Voraussetzungen

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

- Stellen Sie sicher, dass auf Ihrem Clientsystem eine USB-Webcam installiert und betriebsbereit ist.

- Stellen Sie sicher, dass ein USB-Mikrofon oder ein anderer Mikrofontyp auf Ihrem Clientsystem installiert und betriebsbereit ist.
- Stellen Sie sicher, dass das VMware Blast-Anzeigeprotokoll oder das PCoIP-Anzeigeprotokoll für Ihre Remote-Desktops verwendet wird.

Vorgehensweise

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

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

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

   c Starten Sie einen Anruf und beenden Sie ihn dann.

   Auf diese Weise wird eine Protokolldatei erstellt.

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

a Öffnen Sie die Debug-Protokolldatei mit einem Texteditor.

Die Protokolldatei mit Protokollmeldungen zu Audio-Video in Echtzeit befindet sich unter `/tmp/vmware-<username>/vmware-RTAV-<pid>.log`. Das Clientprotokoll befindet sich unter `/tmp/vmware-<username>/vmware-view-<pid>.log`.

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

Das folgende Beispiel zeigt einen Auszug der Webcam-Auswahl:

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

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

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

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

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

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

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

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

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

Kopieren Sie als Beispiel für eine Webcam `Microsoft® LifeCam HD-6000 für Notebooks` und `Microsoft® LifeCam HD-6000 for Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6`, um die Microsoft-Webcam als bevorzugte Webcam festzulegen, und legen Sie die Eigenschaften wie folgt fest:

```
rtav.srcWCamName = “Microsoft® LifeCam HD-6000 for Notebooks”
rtav.srcWCamId = “Microsoft® LifeCam HD-6000 for Notebooks#/sys/devi-
ces/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6”
```

In diesem Beispiel könnten Sie für die Eigenschaft `rtav.srcWCamId` auch „`Microsoft`“ festlegen. Die Eigenschaft `rtav.srcWCamId` unterstützt sowohl teilweise als auch exakte Übereinstimmungen. Die Eigenschaft `rtav.srcWCamName` unterstützt nur eine exakte Übereinstimmung.

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

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

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

5 Melden Sie sich von der Desktop-Sitzung ab und starten Sie eine neue Sitzung.

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*.

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.

Wichtig Die Funktion „Virtuelles Drucken“ steht nur mit Horizon Client 3.2 oder höher, abrufbar über die VMware-Website für Produkt-Downloads, oder mit der Horizon Client-Version für Linux, die von Drittanbietern bereitgestellt wird, zur Verfügung.

Für diese Funktion gelten zudem die folgenden Anforderungen:

- Auf dem Remote-Desktop muss View Agent 6.0.2 oder höher oder Horizon Agent 7.0 oder höher installiert sein.
- Sie müssen das VMware Blast- oder PCoIP-Anzeigeprotokoll verwenden.

Weitere Informationen zu den Thin Client- und Zero Client-Partnern von VMware finden Sie im *VMware-Kompatibilitätshandbuch* unter http://www.vmware.com/resources/compatibility/search.php?deviceCategory=vdm. Für eine Clientsoftware von Drittanbietern müssen Sie das VMware Blast-, PCoIP- oder FreeRDP-Anzeigeprotokoll verwenden. Diese Funktion arbeitet nicht mit rdesktop.

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:\Programme\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**.

Kopieren und Einfügen von Text

Sie haben die Möglichkeit, Text in und aus Remote-Desktops und -anwendungen zu kopieren. Ihr View-Administrator kann diese Funktion so einstellen, dass Kopier- und Einfügevorgänge nur von Ihrem Clientsystem zu einem Remote-Desktop bzw. einer Anwendung oder nur von einem Remote-Desktop bzw. einer Anwendung zu Ihrem Clientsystem zugelassen werden oder beide bzw. keiner der beiden Vorgänge möglich sind.

Diese Funktion ist verfügbar, wenn Sie das VMware Blast-Anzeigeprotokoll oder das PCoIP-Anzeigeprotokoll verwenden. Remoteanwendungen werden mit Horizon 6.0 oder höher unterstützt.

Die Administratoren konfigurieren die Möglichkeit zum Kopieren/Einfügen durch die Verwendung von Gruppenrichtlinienobjekten (GPOs), die View Agent oder Horizon Agent auf den Remote-Desktops zugeordnet sind. Weitere Informationen finden Sie im Kapitel zur Konfiguration von Richtlinien unter *Einrichten von Desktops und Anwendungen im View*-Dokument.

Sie können Text aus Horizon Client auf einen Remote-Desktop bzw. in eine Remoteanwendung kopieren und umgekehrt. Beim eingefügten Text handelt es sich aber immer um einfachen Text.

Sie können keine Grafiken kopieren und einfügen. Sie können außerdem 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.

Fügen Sie zum Festlegen des Zwischenablagespeichers des Clients einer der folgenden drei Konfigurationsdateien den folgenden Parameter hinzu: `~/.vmware/config`, `/usr/lib/vmware/config` oder `/etc/vmware/config`.

`mksvchan.clipboardSize=`*`Wert`*

Wert stellt die Größe des Zwischenablagespeichers für den Client in Kilobyte (KB) dar. Sie können einen maximalen Wert von 16.384 KB angeben. Wenn Sie 0 oder keinen Wert eingeben, gilt für den Client die Standardgröße des Zwischenablagespeichers von 8.192 KB (8 MB).

Horizon Client sucht in den Konfigurationsdateien in der folgenden Reihenfolge nach der Größe des Zwischenablagespeichers und hält an, sobald ein Wert gefunden wird, der nicht 0 entspricht.

1 `~/.vmware/config`

2 `/usr/lib/vmware/config`

3 `/etc/vmware/config`

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.

Fehlerbehebung für Horizon Client 5

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.

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 **Neu starten**.

Option	Aktion
Aus dem Desktop heraus	Wählen Sie **Verbindung > Desktop neu starten** aus der Menüleiste aus.
Im Desktop-Auswahlfenster	Wählen Sie den Remote-Desktop und anschließend in der Menüleiste **Verbindung > 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 84.

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

- Verwenden Sie den **Zurücksetzen**-Befehl.

Option	Aktion
Einen Remote-Desktop aus dem Desktop heraus zurücksetzen	Wählen Sie in der Menüleiste **Verbindung > Zurücksetzen** aus.
Einen Remote-Desktop im Fenster für die Desktop- und Anwendungsauswahl zurücksetzen	Wählen Sie den Remote-Desktop und anschließend in der Menüleiste **Verbindung > Zurücksetzen** aus.
Remoteanwendungen im Fenster für die Desktop- und Anwendungsauswahl zurücksetzen	Klicken Sie in der oberen rechten Ecke des Fensters auf die Schaltfläche **Einstellungen** (Zahnradsymbol), wählen Sie im linken Fensterbereich **Anwendungen** aus, klicken Sie auf **Zurücksetzen** und dann auf **Weiter**.

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 für Linux

Manchmal können Sie Probleme mit Horizon Client einfach dadurch beheben, dass Sie die Horizon Client-Anwendung deinstallieren und anschließend neu installieren.

Das Verfahren, das Sie zum Deinstallieren von Horizon Client für Linux verwenden, hängt von der Version und davon ab, welches Verfahren Sie für die Installation der Clientsoftware verwendet haben.

Voraussetzungen

Stellen Sie sicher, dass Sie auf dem Linux-Clientsystem über die Berechtigung zum Stammzugriff verfügen.

Vorgehensweise

- Wenn Sie über Horizon Client 3.1 oder eine ältere Version verfügen, oder wenn Sie den Client über das Ubuntu Software Center installiert haben, wählen Sie **Anwendungen > Ubuntu Software Center** und im Abschnitt **Installierte Software** die Option **vmware-view-client** aus und klicken auf **Entfernen**.
- Wenn Sie über Horizon Client 3.2 oder eine neuere Version verfügen, die Sie über die VMware-Website für Produkt-Downloads installiert haben, wechseln Sie zu dem Verzeichnis, in dem sich die Datei mit dem Installationsprogramm befindet und führen den Installationsbefehl mit der Option `–u` aus.

  ```
  sudo env VMWARE_KEEP_CONFIG=yes \

  ./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle –u vmware-horizon-client
  ```

  Im Dateinamen steht *x.x.x* für die Versionsnummer, *yyyyyyy* für die Build-Nummer und *arch* entweder für `x86` oder für `x64`. Mit der Einstellung `VMWARE_KEEP_CONFIG=yes` legen Sie fest, dass die Konfigurationseinstellungen bei Deinstallation des Clients beibehalten werden. Wenn für diese Umgebungsvariable keine Einstellung festgelegt ist, werden Sie aufgefordert anzugeben, ob die Konfigurationseinstellungen gespeichert werden sollen.

Weiter

Sie können den Client erneut oder eine neue Version installieren. Siehe „Installieren oder Aktualisieren von Horizon Client für Linux über die VMware-Website für Produkt-Downloads“, auf Seite 17.

Konfigurieren der USB-Umleitung auf dem Client

6

Mit der Funktion der USB-Umleitung können Sie auf dem Clientsystem mithilfe einer Konfigurationsdatei die USB-Geräte angeben, die sich an einen Remote-Desktop umleiten lassen.

Beispielsweise haben Sie die Möglichkeit, die USB-Gerätetypen zu beschränken, die Horizon Client für die Umleitung bereitstellt, festzulegen, dass View Agent die Weiterleitung bestimmter USB-Geräte von einem Clientcomputer verhindert und anzugeben, ob Horizon Client USB-Verbundgeräte in eigene Komponenten für die Umleitung aufschlüsseln soll.

Dieses Kapitel behandelt die folgenden Themen:

Systemanforderungen für die USB-Umleitung

Die Funktion zur USB-Umleitung ist nur mit bestimmten Versionen der Clientsoftware verfügbar.

Darüber hinaus hat die Funktion der USB-Umleitung für die Horizon Client-Software, die von Drittanbietern zur Verfügung gestellt wird, folgende Anforderungen:

- Bei View Agent und dem View-Verbindungsserver muss es sich um View-Version 5.1 oder höher handeln.
- Die in diesem Dokument beschriebenen USB-Filterfunktionen und die Funktionen zur Geräteaufschlüsselung sind ab dem View-Verbindungsserver 5.1 und höher verfügbar.

Weitere Informationen über VMware Thin-Client- und Zero-Client-Partner finden Sie im VMware-Kompatibilitätsleitfaden. Um die für Drittanbieter verfügbaren USB-Komponenten zu verwenden, müssen bestimmte Dateien an bestimmten Speicherorten installiert werden und bestimmte Prozesse müssen so konfiguriert werden, dass sie vor Horizon Client gestartet werden. Diese Details gehen über den Rahmen dieses Dokuments hinaus.

Für Horizon Client gelten für die Funktion der USB-Umleitung die folgenden Anforderungen:

- Auf dem Remote-Desktop muss View Agent 6.0.2 oder später installiert sein.
- Sie müssen das VMware Blast- oder PCoIP-Anzeigeprotokoll verwenden.

Wenn Sie Horizon 6.0.1 und höher verwenden, können Sie USB 3.0-Geräte an USB 3.0-Ports anschließen. Für USB 3.0-Geräte wird nur ein Stream unterstützt. Da die Unterstützung mehrerer Streams noch nicht implementiert ist, wurde die Leistung von USB-Geräten nicht verbessert. Beachten Sie, dass auf dem Linux-Clientsystem i386-Prozessoren unterstützt werden, armel- und armhf-Architekturen jedoch nicht. Der Version des Linux-Kernels muss 2.6.35 oder höher sein.

USB-spezifische Protokolldateien

Horizon Client sendet USB-Informationen an die Protokolldateien.

Zur Fehlersuche können Sie mithilfe der folgenden Befehle den Informationsumfang erhöhen, der an USB-spezifische Protokolle gesendet wird:

```
vmware-usbarbitrator --verbose
```

```
vmware-view-usbd -o log:trace
```

Verwenden Sie den folgenden Befehl, um eine Liste der Nutzungsinformationen abzurufen:

```
vmware-usbarbitrator -h
```

Einstellen der USB-Konfigurationseigenschaften

Sie können USB-Konfigurationseigenschaften in den Konfigurationsdateien `/etc/vmware/config`, `/usr/lib/vmware/config` und `~/.vmware/config` festlegen.

Der Dienst `vmware-view-usbd` wertet diese Konfigurationsdateien in der folgenden Reihenfolge aus:

1. `/etc/vmware/config`. Wenn USB-Konfigurationseigenschaften in dieser Datei eingerichtet sind, werden diese Eigenschaften verwendet.
2. `/usr/lib/vmware/config`. Wenn die USB-Eigenschaften nicht in `/etc/vmware/config` zu finden sind, wird die Datei `/usr/lib/vmware/config` geprüft.
3. `~/.vmware/config`. Wenn in den anderen Dateien keine USB-Eigenschaften gefunden werden, wird die Datei `~/.vmware/config` überprüft.

Verwenden Sie die folgende Syntax, um die USB-Konfigurationseigenschaften in den Konfigurationsdateien festzulegen.

```
viewusb.Eigenschaft1 = "Wert1"
```

Mit den USB-Konfigurationseigenschaften können Sie festlegen, dass bestimmte Gerätetypen umgeleitet werden sollen. Es sind auch Eigenschaften zum Filtern verfügbar, mit denen Sie bestimmte Gerätetypen ausschließen oder einbeziehen können. Für Linux-Clients der Version 1.7 und höher sowie für Windows-Clients stehen auch Eigenschaften für das Aufteilen von Composite-Geräten zur Verfügung.

Manche Eigenschaftswerte erfordern für ein USB-Gerät die VID (Hersteller-ID) und die PID (Produkt-ID). Die korrekte VID und PID finden Sie, indem Sie im Internet nach dem Produktnamen plus `VID` und `PID` suchen. Alternativ können Sie in der Datei `/tmp/vmware-root/vmware-view-usbd-*.log` nachsehen, nachdem Sie das USB-Gerät an das lokale System angeschlossen haben, während Horizon Client ausgeführt wird. Um den Speicherort der Datei festzulegen, verwenden Sie die Eigenschaft `view-usbd.log.fileName` in der Datei `/etc/vmware/config`, zum Beispiel:

```
view-usbd.log.fileName = "/tmp/usbd.log"
```

Wichtig Stellen Sie beim Umleiten von Audiogeräten sicher, dass die Kernelversion Ihres Ubuntu-Systems 3.2.0-27.43 oder höher beträgt. Ubuntu 12.04 enthält die Kernelversion 3.2.0-27.43. Wenn Sie nicht auf diese Kernelversion aktualisieren können, können Sie alternativ den Hostzugriff auf das Audiogerät deaktivieren. Sie können beispielsweise die Zeile „`blacklist snd-usb-audio`“ am Ende der Datei „`/etc/modprobe.d/blacklist.conf`“ einfügen. Falls Ihr System eine dieser Voraussetzungen nicht erfüllt, kann das Clientsystem abstürzen, wenn Horizon Client versucht, das Audiogerät umzuleiten. Standardmäßig werden Audiogeräte umgeleitet.

Die nachfolgende Tabelle stellt die verfügbaren USB-Konfigurationseigenschaften dar.

Tabelle 6-1. Konfigurationseigenschaften für die USB-Umleitung

Name und Eigenschaft der Richtlinie	Beschreibung
Autom. Gerätesplitten zulassen Eigenschaft: `viewusb.AllowAutoDeviceSplitting`	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 (Vid/Pid-Gerät vom Splitten ausschließen) Eigenschaft: `viewusb.SplitExcludeVidPid`	Schließt ein Composite USB-Gerät vom Splitten aus, das durch Anbieter- und Produkt-IDs angegeben ist. Das Format der Einstellung lautet `vid-`*xxx1*`_pid-`*yyy1*`[;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 (Vid/Pid-Gerät splitten) Eigenschaft: `viewusb.SplitVidPid`	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** Enthält das Verbundgerät Komponenten, die automatisch ausgeschlossen werden, z. B. Maus- und Tastaturkomponenten, dann schließt View die Komponenten, die Sie nicht ausdrücklich ausgeschlossen haben, nicht automatisch ein. Sie müssen eine Filterrichtlinie wie z. B. `Include Vid/Pid Device` angeben, um diese Komponenten einzuschließen. Der Standardwert ist nicht definiert.
Allow Audio Input Devices (Audioeingabegeräte zulassen) Eigenschaft: `viewusb.AllowAudioIn`	Lässt zu, dass Audioeingabegeräte umgeleitet werden. Der Standardwert ist nicht definiert, was **`Falsch`** entspricht, da für Audioeingabe- und Videogeräte die Audio/Video-Echtzeitfunktion verwendet wird, und die USB-Umleitung für diese Geräte standardmäßig nicht verwendet wird.
Allow Audio Output Devices (Audioausgabegeräte zulassen) Eigenschaft: `viewusb.AllowAudioOut`	Lässt zu, dass Audioausgabegeräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.

Tabelle 6-1. Konfigurationseigenschaften für die USB-Umleitung (Fortsetzung)

Name und Eigenschaft der Richtlinie	Beschreibung
HID zulassen Eigenschaft: `viewusb.AllowHID`	Ermöglicht die Umleitung anderer Eingabegeräte neben Tastaturen und Mäusen. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`true`** ist.
Allow HIDBootable (HIDBootable zulassen) Eigenschaft: `viewusb.AllowHIDBootable`	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.
Ausfallsicherung der Dienstbeschreibung zulassen Eigenschaft: `viewusb.AllowDevDescFailsafe`	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 Keyboard and Mouse Devices (Tastatur- und Mausgeräte zulassen) Eigenschaft: `viewusb.AllowKeyboardMouse`	Lässt zu, dass Tastaturen mit eingebauten Zeigegeräten (Maus, Trackball oder Touchpad) umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
Allow Smart Cards (SmartCards zulassen) Eigenschaft: `viewusb.AllowSmartcard`	Lässt zu, dass SmartCard-Geräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
Allow Video Devices (Videogeräte zulassen) Eigenschaft: `viewusb.AllowVideo`	Lässt zu, dass Videogeräte umgeleitet werden. Der Standardwert ist nicht definiert, was **`Falsch`** entspricht, da für Audioeingabe- und Videogeräte die Audio/Video-Echtzeitfunktion verwendet wird, und die USB-Umleitung für diese Geräte standardmäßig nicht verwendet wird.
Disable Remote Configuration Download (Remote-Konfigurations-Download deaktivieren) Eigenschaft: `viewusb.DisableRemoteConfig`	Deaktiviert die Verwendung der View Agent-Einstellungen beim Durchführen der USB-Gerätefilterung. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
Exclude All Devices (Alle Geräte ausschließen) Eigenschaft: `viewusb.ExcludeAllDevices`	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` in View Agent auf **`true`** setzen und diese Einstellung an Horizon Client weitergegeben wird, überschreibt die View Agent-Einstellung die Horizon Client-Einstellung. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
Exclude Device Family (Gerätefamilie ausschließen) Eigenschaft: `viewusb.ExcludeFamily`	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 View die Gerätefamilie jeder Schnittstelle eines Composite USB-Gerätes, um zu entscheiden, welche Schnittstelle ausgeschlossen werden sollte. Wenn Sie das automatische Gerätesplitten deaktiviert haben, prüft View die Gerätefamilie des gesamten Composite USB-Gerätes. Der Standardwert ist nicht definiert.

Tabelle 6-1. Konfigurationseigenschaften für die USB-Umleitung (Fortsetzung)

Name und Eigenschaft der Richtlinie	Beschreibung
Exclude Vid/Pid Device (Vid/Pid-Gerät ausschließen) Eigenschaft: `viewusb.ExcludeVidPid`	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 (Pfad ausschließen) Eigenschaft: `viewusb.ExcludePath`	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 (Gerätefamilie einschließen) Eigenschaft: `viewusb.IncludeFamily`	Bestimmt Gerätefamilien, die umgeleitet werden können. Das Format der Einstellung lautet *Familienname_1*`[;`*Familienname_2*`]...` Beispiel: **`storage`** Der Standardwert ist nicht definiert.
Include Path (Pfad einschließen) Eigenschaft: `viewusb.IncludePath`	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 (Vid/Pid-Gerät einschließen) Eigenschaft: `viewusb.IncludeVidPid`	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.

Beispiele der USB-Umleitung

Für jedes Beispiel wird eine Beschreibung der Auswirkung auf die USB-Umleitung gezeigt.

- Beziehen Sie die meisten Geräte der Familie der Mausgeräte ein.

  ```
  viewusb.IncludeFamily = "mouse"
  viewusb.ExcludeVidPid = "Vid-0461_Pid-0010;Vid-0461_Pid-4d20"
  ```

  Die erste Eigenschaft in diesem Beispiel weist Horizon Client an, es zuzulassen, dass Mausgeräte zu einem View-Desktop umgeleitet werden. Die zweite Eigenschaft überschreibt die erste und weist Horizon Client an, zwei bestimmte Mausgeräte lokal zu halten und nicht umzuleiten.

- Schalten Sie die automatische Geräteaufteilung an, aber schließen Sie ein bestimmtes Gerät aus der Aufteilung aus. Für ein bestimmtes anderes Gerät behalten Sie eine seiner Komponenten lokal und leiten die anderen Komponenten auf den Remote-Desktop um:

  ```
  viewusb.AllowAutoDeviceSplitting = "True"
  viewusb.SplitExcludeVidPid = "Vid-03f0_Pid-2a12"
  viewusb.SplitVidPid = "Vid-0911_Pid-149a(exintf:03)"
  viewusb.IncludeVidPid = "Vid-0911_Pid-149a"
  ```

USB-Verbundgeräte bestehen aus einer Kombination von zwei oder mehr Geräten, so zum Beispiel einem Videoeingabegerät und einem Speichergerät. Die erste Eigenschaft in diesem Beispiel aktiviert die automatische Aufteilung von Composite-Geräten. Die zweite Eigenschaft schließt das angegebene USB-Composite-Gerät (`Vid-03f0_Pid-2A12`) von der Aufteilung aus.

Die dritte Zeile weist Horizon Client dazu an, die Komponenten eines anderen Verbundgeräts (`Vid-0911_Pid-149a`) als separate Geräte zu behandeln, die folgende Komponente jedoch von der Umleitung auszuschließen: Die Komponente, deren Schnittstellennummer 03 lautet. Diese Komponente wird lokal beibehalten.

Da dieses Verbundgerät eine Komponente enthält, die im Regelfall standardmäßig ausgeschlossen wird, z. B. eine Maus oder eine Tastatur, ist die vierte Zeile notwendig, damit andere Komponenten des Verbundgeräts `Vid-0911_Pid-149a` zum View-Desktop umgeleitet werden können.

Die ersten drei Eigenschaften beziehen sich auf die Aufschlüsselung. Die letzte Eigenschaft bezieht sich auf das Filtern. Filtereigenschaften werden vor den Aufschlüsselungseigenschaften verarbeitet.

Wichtig Diese Konfigurationseinstellungen des Clients können mit den entsprechenden für View Agent auf dem Remote-Desktop eingestellten Richtlinien zusammengeführt oder von diesen überschrieben werden. Informationen darüber, wie die Eigenschaften der USB-Aufteilung und Filterung auf dem Client mit den View Agent-USB-Richtlinien zusammenarbeiten, finden Sie in den Themen über die Verwendung von Richtlinien zur Steuerung der USB-Umleitung im Dokument *Verwaltung von View*.

USB-Gerätefamilien

Beim Erstellen von USB-Filterregeln für Horizon Client oder View Agent oder Horizon Agent können Sie eine bestimmte Familie angeben.

Hinweis Einige Geräte zeigen keine Gerätefamilie an.

Tabelle 6-2. USB-Gerätefamilien

Gerätefamilienname	Beschreibung
`audio`	Ein Audioeingabe- oder Audioausgabegerät beliebigen Typs.
`audio-in`	Audioeingabegeräte, z. B. Mikrofone.
`audio-out`	Audioausgabegeräte, z. B. Lautsprecher und Kopfhörer.
`bluetooth`	Per Bluetooth verbundene Geräte.
`comm`	Kommunikationsgeräte wie Modems und kabelgebundene Netzwerkadapter.
`hid`	Eingabegeräte (Human Interface Devices) außer Tastaturen und Zeigegeräten.
`hid-bootable`	Eingabegeräte (Human Interface Devices), die beim Start verfügbar sind, außer Tastaturen und Zeigegeräte.
`imaging`	Bildverarbeitungsgeräte, z. B. Scanner.
`keyboard`	Tastaturgerät.
`mouse`	Zeigegerät, z. B. eine Maus.
`other`	Familie nicht angegeben.
`pda`	PDA (Personal Digital Assistant)
`physical`	Force-Feedback-Geräte, z. B. Force-Feedback-Joysticks.
`printer`	Druckergeräte.
`security`	Sicherheitsgeräte, z. B. Fingerabdruckleser.
`smart-card`	SmartCard-Geräte.

Tabelle 6-2. USB-Gerätefamilien (Fortsetzung)

Gerätefamilien-name	Beschreibung
`storage`	Massenspeichergeräte wie z. B. Flash-Laufwerke und externe Festplattenlaufwerke.
`unknown`	Familie nicht bekannt.
`vendor`	Geräte mit herstellerspezifischen Funktionen.
`video`	Videoeingabegeräte.
`wireless`	Drahtlose Netzwerkadapter.
`wusb`	Drahtlose USB-Geräte.

Index