Verwendung von VMware Horizon View Client für Linux

Januar 2014

Horizon View

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

DE-001162-03

vmware®

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

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

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

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

docfeedback@vmware.com

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

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

Inhalt

Verwendung von VMware Horizon View Client für Linux

Dieses Handbuch, *Verwendung von VMware Horizon View Client für Linux*, enthält Informationen zur Installation und Verwendung der Software VMware® Horizon View™ auf einem Linux-Clientsystem, um zu einem View-Desktop im Rechenzentrum zu verbinden.

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

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

Hinweis Dieses Dokument bezieht sich auf Horizon View Client für Linux, das VMware auf Ubuntu verfügbar macht. Darüber hinaus bieten verschiedene VMware-Partner Thin Client-Geräte für Horizon View-Bereitstellungen an. Die Funktionen, die für die einzelnen Thin Client-Geräte verfügbar sind, sowie die unterstützten Betriebssysteme werden vom Hersteller und Modell sowie der vom jeweiligen Unternehmen gewählten Konfiguration bestimmt. Informationen zu Herstellern und Modellen für Thin 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 View Client gestaltet sich ähnlich wie die Installation der meisten anderen Anwendungen.

Systemanforderungen

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

HINWEIS Diese Systemanforderungen betreffen den Horizon View Client für Linux, den VMware auf Ubuntu zur Verfügung stellt. Darüber hinaus bieten verschiedene VMware-Partner Thin Client-Geräte für Horizon View-Bereitstellungen an. Die Funktionen, die für die einzelnen Thin Client-Geräte verfügbar sind, sowie die unterstützten Betriebssysteme werden vom Hersteller und Modell sowie der vom jeweiligen Unternehmen gewählten Konfiguration bestimmt. Informationen zu Herstellern und Modellen für Thin Client-Geräte finden Sie im VMware-Kompatibilitätsleitfaden, der auf der VMware-Website zur Verfügung steht.

Modell	Intel-basierter Desktop- oder Laptop-Computer
Arbeitsspeicher	Mindestens 2GB Arbeitsspeicher (RAM)
Betriebssysteme	■ View Client 2.0 und höher: 32 Bit Ubuntu Linux 12.04 ■ View Client 1.6 und 1.7: 32 Bit Ubuntu Linux 10.04 oder 12.04 ■ View Client 1.5: 32 Bit Ubuntu Linux 10.04 oder 10.10
View-Verbindungsserver, Sicherheitsserver und View Agent	Aktuelle Wartungsversion von VMware View 4.6.x und spätere 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.
Anzeigeprotokoll für Horizon View	PCoIP oder RDP **WICHTIG** Horizon View Client für Linux unterstützt zwar das RDP-Anzeigeprotokoll, aber der im Lieferumfang von Ubuntu enthaltene RDP-Client ist möglicherweise nicht mit Horizon View Client kompatibel.
Bildschirmauflösung auf Client-System	Minimum: 1024 x 768 Pixel

Hardwareanforderungen für PCoIP	■ x86-basierter Prozessor mit SSE2-Erweiterungen, mit einer Prozessorgeschwindigkeit von 800 MHz oder höher.
	■ Verfügbarer RAM über den Systemanforderungen zur Unterstützung verschiedener Monitorkonfigurationen. Im Allgemeinen gilt die folgende Formel:
	`20 MB + (24 * (Anzahl der Monitore) * (Breite des Monitors) * (Höhe des Monitors))`
	Als grobes Maß können Sie die folgenden Berechnungen verwenden:
	`1 Monitor: 1600 x 1200: 64 MB`
	`2 Monitore: 1600 x 1200: 128MB`
	`3 Monitore: 1600 x 1200: 256MB`

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

Softwareanforderungen für Microsoft RDP

- Für Ubuntu 12.04 ist rdesktop 1.7.0 zu verwenden.
- Für Ubuntu 10.04 ist rdesktop 1.6.0 zu verwenden.

Software-Voraussetzungen 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 36.

Systemanforderungen für Echtzeit-Audio/Video

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

Horizon View-Remote-Desktop

Auf den Desktops muss View Agent 5.2 oder später installiert sein. Auf den Desktops muss außerdem die entsprechende Version von Remote Experience Agent installiert sein. Wenn View Agent 5.3 installiert ist, müssen Sie auch Remote Experience Agent aus dem Horizon View 5.3 Feature Pack 1 installieren. Weitere Informationen finden Sie im Dokument *Installation und Verwaltung von VMware Horizon View Feature Pack* für VMware Horizon View-

Horizon View Client-Software

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

Horizon View Client-Computer oder Clientzugriffsgerät

- Echtzeit-Audio/Video wird auf x86-Geräten unterstützt. Auf ARM-Prozessoren wird diese Funktion nicht unterstützt. Der Clientsystem-Prozess muss über mindestens zwei Kerne verfügen.
- Horizon View Client erfordert die folgenden Bibliotheken:
  - `Video4Linux2`
  - `libv4l`
  - `Pulse Audio`

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

  ```
  libuuid.so.1
  libv4l2.so.0
  libspeex.so.1
  libudev.so.0
  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 View 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 View Agent installiert ist.

Anzeigeprotokoll für Horizon View	PCoIP Echtzeit-Audio/Video wird in RDP-Desktop-Sitzungen nicht unterstützt.

Unterstützte Desktop-Betriebssysteme

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

Eine Liste mit unterstützten Gastbetriebssystemen finden Sie unter dem Thema „Unterstützte Betriebssysteme für View Agent“ in der Dokumentation „Installation von Horizon View 4.6.x oder 5.x“.

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.

Diese Funktion ist verfügbar, wenn sie zusammen mit der richtigen Version des VMware Horizon View-Feature Packs verwendet wird.

- Anforderungen für Multicast-Unterstützung: VMware Horizon View- 5.2 Feature Pack 2 oder später.
- Anforderungen für Unicast-Unterstützung: VMware Horizon View- 5.3 Feature Pack 1 oder später.

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

- Für eine Unicast-Unterstützung müssen Sie die Clientsysteme Horizon View Client 2.1 oder später verwenden. Für eine Unicast-Unterstützung müssen Sie die Clientsysteme Horizon View Client 2.2 oder später verwenden.

  HINWEIS Diese Funktion wird nur für die von Partnern bereitgestellte Horizon View Client-Version und ausschließlich auf x86 Thin Client-Geräten 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.0`“ oder stellen Sie sicher, dass diese Datei bereits installiert ist.

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

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

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

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

Eine Liste der View-Desktop-Anforderungen für die Flash-URL-Umleitung sowie Anweisungen zum Konfigurieren einer Webseite zur Bereitstellung des Multicast- oder Unicast-Streaming finden Sie im Dokument *Installation und Verwaltung von VMware Horizon View Feature Pack*.

Vorbereiten des View-Verbindungsservers für Horizon View Client

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

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

- Wenn Sie einen Sicherheitsserver verwenden, wie von VMware empfohlen, stellen Sie sicher, dass Sie die aktuellen Wartungsversionen für einen View-Verbindungsserver der Version 4.6.x und für einen View-Sicherheitsserver der Version 4.6.x oder höher verwenden. Siehe die Dokumentation *Installation von VMware Horizon View-*.
- Wenn Sie eine sichere Tunnelverbindung für Clientgeräte verwenden möchten und die sichere Verbindung mit einem DNS-Hostnamen für den View-Verbindungsserver oder einen Sicherheitsserver konfiguriert ist, muss sichergestellt werden, dass das Clientgerät diesen DNS-Namen auflösen kann.

  Navigieren Sie zur Aktivierung oder Deaktivierung der sicheren Tunnelverbindung in View Administrator auf das Dialogfeld View-Verbindungsserver-Einstellungen bearbeiten und setzen Sie einen Haken in das Kontrollkästchen **Sichere Tunnelverbindung zum Desktop verwenden**.
- Vergewissern Sie sich, dass ein Desktop-Pool erstellt wurde und das Benutzerkonto, das Sie verwenden möchten, über die Rechte zum Zugriff auf diesen Remote-Desktop verfügt. Siehe Hilfethemen zur Erstellung von Desktop-Pools in der Dokumentation *Verwaltung von VMware Horizon View-*.
- Zum Verwenden der zweistufigen Authentifizierung für Horizon View Client, z. B. der RSA SecurID- oder RADIUS-Authentifizierung, müssen Sie diese Funktion auf dem View-Verbindungsserver aktivieren. Die RADIUS-Authentifizierung ist bei View-Verbindungsservern mit View 5.1 oder höher verfügbar. Weitere Informationen finden Sie in den Themen über zweistufige Authentifizierung in der Dokumentation *Verwaltung von VMware Horizon View-*.

Installation von Horizon View Client für Linux

Endbenutzer öffnen Horizon View Client, um von einem physischen Computer eine Verbindung zu Remote-Desktops herstellen zu können. Horizon View Client für Linux läuft auf Ubuntu 12.04-Systemen und wird mit dem Synaptic Package Manager installiert.

Wichtig Kunden, die Linux-basierte Thin Clients verwenden, müssen sich wegen Updates für Horizon View 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“, 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“, auf Seite 8.

Vorgehensweise

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

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

   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 Laden Sie das Paket folgendermaßen aus dem Ubuntu Software Center herunter.

   a Wählen Sie in der Ubuntu-Menüleiste **System > Verwaltung > Synaptic Package Manager**.

   b Klicken Sie auf **Suche** und suchen Sie nach **`vmware`**.

   c In der Liste der gefundenen Pakete wählen Sie das Kontrollkästchen neben **vmware-view-client** und dann wählen Sie **Für Installation markieren**.

   d Klicken Sie in der Symbolleiste auf **Anwenden**.

   Wenn Sie Ubuntu 12.04 als Betriebssystem verwenden, wird die neueste Version von Horizon View Client installiert. Wenn Sie Ubuntu 10.04 als Betriebssystem verwenden, wird View Client für Linux 1.7 installiert.

3 Um zu ermitteln, ob diese Installation erfolgreich war, überprüfen Sie, ob das Symbol **VMware Horizon View** im Menü **Anwendungen > Internet** angezeigt wird.

Weiter

Starten Sie Horizon View Client und stellen Sie sicher, dass Sie sich am richtigen virtuellen Desktop anmelden können. Siehe „Erstmaliges Anmelden an einem Remote-Desktop“, auf Seite 39.

Konfigurieren der im View Portal angezeigten View Client-Download-Links

Standardmäßig enthält die Portalseite, die angezeigt wird, wenn Sie einen Browser öffnen und die URL einer View-Verbindungsserverinstanz eingeben, Links zur VMware-Download-Site, um Horizon View Client herunterzuladen. Die Standard können geändert werden.

Die Standardlinks für Horizon View Client auf der Portalseite sorgen dafür, dass Sie zu den derzeit kompatiblen Horizon View Client-Installationsprogrammen umgeleitet werden. In einigen Fällen sollen die Links jedoch auf einen internen Webserver verweisen oder Sie möchten bestimmte Clientversionen auf Ihrem eigenen View-Verbindungsserver zur Verfügung stellen. Sie können die Seite neu konfigurieren, sodass sie auf eine andere URL verweist.

Wenn Sie Links für Mac OS X-, Linux- und Windows-Clientsysteme erstellen, wird der entsprechende Link zum jeweiligen Betriebssystem auf der Portalseite angezeigt. Wenn Sie beispielsweise die Portalseite auf einem Windows-System öffnen, werden die Links für die Windows-Installationsprogramme angezeigt. Sie können auch separate Links für die 32-Bit- und 64-Bit-Installationsprogramme erstellen. Sie können auch Links für iOS- und Android-Systeme erstellen. Diese Betriebssysteme werden jedoch nicht automatisch erkannt, sodass Sie beispielsweise beim Öffnen der Portalseite auf einem iPad die Links für iOS und Android sehen, sofern Sie Links für die beiden erstellt haben.

Wichtig Wenn Sie die Portalseiten-Links anpassen, wie in diesem Thema beschrieben, und später VMware Horizon View HTML Access auf dem Server installieren, wird Ihre benutzerdefinierte Portalseite durch eine HTML-Zugriff-Seite ersetzt. Informationen zum Anpassen dieser Seite finden Sie unter *Verwendung von VMware Horizon View HTML Access*.

Voraussetzungen

- Laden Sie die Installationsdateien für die Horizon View Client-Typen herunter, die Sie in Ihrer Umgebung einsetzen möchten. Die URL für die Client-Download-Seite ist https://www.vmware.com/go/viewclients.
- Legen Sie fest, auf welchem HTTP-Server die Installationsdateien liegen sollen. Die Dateien können sich auf einer View-Verbindungsserver-Instanz oder auf einem anderen HTTP-Server befinden.

Vorgehensweise

1 Erstellen Sie auf dem HTTP-Server, auf dem sich die Installationsdateien befinden sollen, einen Ordner für die Dateien des Installationsprogramms.

   Um die Dateien beispielsweise in einen Ordner `downloads` im Standardinstallationsverzeichnis auf dem View-Verbindungsserver-Host zu stellen, verwenden Sie den folgenden Pfad:

   ```
   C:\Programme\VMware\VMware View\Server\broker\webapps\downloads
   ```

   Die Links zu den Dateien würden dann URLs mit dem Format `https://`*`Servername`*`/downloads/`*`Client-Installer-Dateiname`* verwenden. Ein Server mit dem Namen `view.mycompany.com` kann die folgende URL für View Client für Windows verwenden: `https://view.mycompany.com/downloads/VMware-Horizon-View-Client.exe`. Bei diesem Beispiel befindet sich der Ordner mit dem Namen `downloads` im Stammordner `webapps`.

2 Kopieren Sie die Installationsdateien in den Ordner.

   Wenn sich der Ordner auf einem View-Verbindungsserver-Dienst neu befindet, können Sie alle Dateien in diesem Ordner ersetzen, ohne den VMware View-Verbindungsserver-Dienst neu starten zu müssen.

3 Kopieren Sie auf dem View-Verbindungsserver die Datei `portal-links.properties` und die Datei `portal.properties`, die sich unter *`Installationspfad`*`\Server\Extras\PortalExamples` befinden.

4 Legen Sie einen Ordner `portal` im Verzeichnis `C:\ProgramData\VMware\VDM` an, und kopieren Sie die Dateien `portal-links.properties` und `portal.properties` in den Ordner `portal`.

5 Bearbeiten Sie die Datei `C:\ProgramData\VMware\VDM\portal\portal-links.properties` so, dass sie auf den neuen Speicherort der Installationsdateien verweist.

   Sie können die Zeilen in dieser Datei bearbeiten und ihnen weitere hinzufügen, falls Sie weitere Links erstellen müssen. Sie können auch Zeilen löschen.

   Die folgenden Beispiele zeigen Eigenschaften zum Erstellen von zwei Links für View Client für Windows sowie zwei Links für View Client für Linux:

   ```
   link.win=https://<varname id="VARNAME_B2B27F517DB04754B1CCF5F1411BA59E">server-name</varname>/downloads/VMware-Horizon-View-Client-x86_64-<varname id="VARNAME_7CD50CBABC614BCD976B2575FEDEF1F2">y.y.y-XXXX</varname>.exe#win
   link.win.1=https://<varname id="VARNAME_8243922EA8B44DC3A2E9A360C4DDC304">server-name</varname>
   ```

```
me>/downloads/VMware-Horizon-View-Client-<varname id="VARNA-
ME_9D2A6519E01D4ADA9B701FDB8785B141">y.y.y-XXXX</varname>.exe#win
link.linux=https://<varname id="VARNAME_C62EA29FFF1047D1A350C57AD8006223">server-name</varna-
me>/downloads/VMware-Horizon-View-Client-x86_64-<varname id="VARNA-
ME_B664011E02154BBD9479411042551944">y.y.y-XXXX</varname>.rpm#linux
link.linux.1=https://<varname id="VARNAME_C498001B66334F39A59E2610D499EAA8">server-name</var-
name>/downloads/VMware-Horizon-View-Client-<varname id="VARNA-
ME_D5652EFD7B75490F873921D2AFF8D9B0">y.y.y-XXXX</varname>.tar.gz#linux
```

Bei diesem Beispiel gibt *y.y.y-XXXX* die Versions- und Build-Nummer an. Der Text `win` am Ende der Zeile weist darauf hin, dass dieser Link im Browser angezeigt werden soll, wenn der Client über ein Windows-Betriebssystem verfügt. Verwenden Sie `win` für Windows, `linux` für Linux und `mac` für Mac OS X. Verwenden Sie für andere Betriebssysteme `unknown`.

6 Bearbeiten Sie für Text die Datei `C:\ProgramData\VMware\VDM\portal\portal.properties` so, dass sie den anzuzeigenden Text für die Links angibt.

Diese Zeilen stehen im Abschnitt der Datei namens `# keys based on key names in portal-links.properties` zur Verfügung.

Das folgende Beispiel zeigt den Text, der den für `link.win` und `link.win.1` angegebenen Links entspricht:

```
text.win=View Client for Windows 32 bit Client users
text.win.1=View Client for Windows 64 bit Client users
```

7 Starten Sie den VMware View-Verbindungsserver-Dienst neu.

Wenn Endbenutzer den View-Verbindungsserver öffnen, sehen sie Links mit dem von Ihnen angegebenen Text. Die Links verweisen auf die von Ihnen angegeben Stellen.

Durch VMware gesammelte Horizon View Client -Daten

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

HINWEIS Diese Funktion ist nur verfügbar, wenn Ihre Horizon View-Bereitstellung den View-Verbindungsserver der Version 5.1 oder einer höheren Version verwendet. Client-Informationen werden für Clients mit View Client 1.7 und höher gesendet.

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 View Client-Informationen werden erst an den View-Verbindungsserver und dann an VMware gesendet, zusammen mit den Daten der Horizon View-Server, Desktop-Pools und Remote-Desktops.

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

Zur Teilnahme am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit kann der Administrator, der die Installation des View-Verbindungsservers durchführt, bei der Ausführung des Installations-Assistenten für den View-Verbindungsserver diese Option „abonnieren“ oder nach der Installation eine entsprechende Option in View Administrator festlegen.

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

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Unternehmen, das die die Horizon View Client-Anwendung entwickelte	No (Nein)	VMware
Produktname	No (Nein)	VMware Horizon View Client
Client-Produktversion	No (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	No (Nein)	Beispiele hierfür sind: ■ i386 ■ x86_64 ■ arm
Client-Build-Name	No (Nein)	Beispiele hierfür sind: ■ VMware-Horizon-View-Client-Win32-Windows ■ VMware-Horizon-View-Client-Linux ■ VMware-Horizon-View-Client-iOS ■ VMware-Horizon-View-Client-Mac ■ VMware-Horizon-View-Client-Android ■ VMware-Horizon-View-Client-WinStore
Host-Betriebssystem	No (Nein)	Beispiele hierfür sind: ■ Windows 8.1 ■ Windows 7, Service Pack 1 für 64 Bit (Build 7601) ■ iPhone OS 5.1.1 (9B206) ■ Ubuntu 10.04.4 LTS ■ Mac OS X 10.7.5 (11G63)
Host-Betriebssystemkernel	No (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	No (Nein)	Beispiele hierfür sind: ■ x86_64 ■ i386 ■ armv71 ■ ARM
Hostsystem-Modell	No (Nein)	Beispiele hierfür sind: ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision WorkStation T3400 (A04 03/21/2008)
Hostsystem-CPU	No (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)

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

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Anzahl der Cores bzw. Kerne im Prozessor des Hostsystems	No (Nein)	Beispiel: 4
MB Arbeitsspeicher auf dem Hostsystem	No (Nein)	Beispiele hierfür sind: ■ 4096 ■ unbekannt (für Windows Store)

Konfigurieren von Horizon View Client für Endbenutzer

2

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

In der folgenden Tabelle werden einige Konfigurationseinstellungen beschrieben, die Sie auf verschiedene Weise festlegen können. Für viele andere Konfigurationseinstellungen müssen Sie einen ganz bestimmten Mechanismus verwenden. Beispielsweise müssen Sie für die Einstellung „Disable Toast Notifications“ (Toastnachrichten deaktivieren) eine Gruppenrichtlinieneinstellung verwenden.

Tabelle 2-1. Allgemeine Konfigurationseinstellungen

Einstellung	Konfigurationsmechanismen
Adresse des View-Verbindungsservers	URI, Gruppenrichtlinie, Befehlszeile, Windows-Registrierung
Active Directory-Benutzername	URI, Gruppenrichtlinie, Befehlszeile, Windows-Registrierung
Als aktueller Benutzer anmelden	Gruppenrichtlinie, Befehlszeile
Domänenname	URI, Gruppenrichtlinie, Befehlszeile, Windows-Registrierung
Desktopanzeigename	URI, Gruppenrichtlinie, Befehlszeile
Fenstergröße	URI, Gruppenrichtlinie, Befehlszeile
Anzeigeprotokoll	URI, Befehlszeile
Optionen zur Umleitung von USB-Geräten	URI, Gruppenrichtlinie, Befehlszeile
Konfigurieren der Zertifikatsprüfung	Gruppenrichtlinie, Windows-Registrierung
Konfigurieren von SSL-Protokollen und kryptografischen Algorithmen	Gruppenrichtlinie, Windows-Registrierung

Dieses Kapitel behandelt die folgenden Themen:

Verwenden von URIs zur Konfiguration von Horizon View 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 View Client, zur Verbindung mit dem View-Verbindungsserver oder zum Start eines bestimmten Desktops mit bestimmten Konfigurationsoptionen klicken.

Sie können die Anmeldung am Remote-Desktop 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 View-Verbindungsservers
- Portnummer für den View-Verbindungsserver
- Active Directory-Benutzername
- Domänenname
- Desktopanzeigename
- Fenstergröße
- Desktop-Aktionen, darunter „Zurücksetzen“, „Abmelden“ und „Sitzung starten“
- Anzeigeprotokoll

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

HINWEIS Sie können URIs nur zum Start von Horizon View Client verwenden, wenn die Clientsoftware bereits auf den Clientcomputern der Endbenutzer installiert ist.

Syntax für die Erstellung von vmware-view-URIs

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

Spezifikationen für VMware Horizon View-URIs

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 View Client die folgende Syntax:

```
vmware-view://[<varname id="VARNAME_E0F8F9951BC4471D9871655A18782C9E">authority-part</varname>]
[/<varname id="VARNAME_7B21DCA6CDE942BBB914ADD20452590B">path-part</varname>][?<varname id="VAR-
NAME_217F9AF17A3745369FD8E2154505D735">query-part</varname>]
```

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. Die Servernamen müssen der DNS-Syntax entsprechen.

Verwenden Sie zur Angabe eines Benutzernamens die folgende Syntax:

```
user1@<varname id="VARNAME_640D14F5E64B44E189F204DC09A8248B">server-address</varname>
```

Beachten Sie dabei, dass Sie keine UPN-Adresse angeben können. Hierzu zählt auch die Domäne. Zur Angabe des Domänennamens können Sie den Abfrageteil `domainName` im URI verwenden.

Verwenden Sie zur Angabe einer Portnummer die folgende Syntax:

```
<varname id="VARNAME_1BAB6153D2834B1490509093A1961D1F">server-address</varname>:<varname id="VARNAME_2296A4E54893485C852FFE94067114D7">port-number</varname>
```

path-part

Gibt den Desktop an. Verwenden Sie den Anzeigenamen des Desktops. 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 Desktopaktionen 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:

```
<varname id="VARNAME_48A6B3A0E1184943BC1206017B78B9D5">query1</varname>=<varname id="VARNAME_9B9916FF3D3540D4AA5622F9C828F072">value1</varname>[&<varname id="VARNAME_6BCA2912EC454A5683D586754BF89DCE">query2</varname>=<varname id="VARNAME_F698C39E83D34D639C943ACDF828BAFE">value2</varname>...]
```

Unterstützte Abfragen

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

action

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

Wert	Beschreibung
`browse`	Zeigt eine Liste der verfügbaren, auf dem angegebenen Server gehosteten Desktops an. Bei Verwendung dieser Aktion müssen Sie keinen Desktop angeben.
`start-session`	Startet den angegebenen Desktop. Wenn keine „action“-Abfrage bereitgestellt wird und der Desktopname angegeben wird, ist `start-session` die Standardaktion.
`zurücksetzen`	Fährt den angegebenen Desktop herunter und startet ihn neu. Nicht gespeicherte Daten gehen verloren. Das Zurücksetzen eines Remote-Desktops entspricht dem Betätigen der Reset-Taste auf einem physischen PC.
`logoff`	Meldet den Benutzer vom Gastbetriebssystem auf dem Remote-Desktop ab.
`rollback`	Verwirft die Änderungen, die am angegebenen Desktop vorgenommen wurden, während dieser zur Verwendung im lokalen Modus auf einem Windows-PC oder Laptop ausgecheckt wurde.

connectUSBOnInsert

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

connectUSBOnStartup

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

desktopLayout

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

Tabelle 2-3. Gültige Werte für desktopLayout-Abfrage

Wert	Beschreibung
`fullscreen`	Vollbild auf einem Monitor. Hierbei handelt es sich um die Standardeinstellung.
`multimonitor`	Vollbild auf allen Monitoren.
`windowLarge`	Großes Fenster.

Tabelle 2-3. Gültige Werte für desktopLayout-Abfrage (Fortsetzung)

Wert	Beschreibung
`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 sind **`RDP`** und **`PCoIP`**. Zur Angabe von PCoIP verwenden Sie beispielsweise die Syntax **`desktopProtocol=PCoIP`**.

domainName Die Domäne, die mit dem Benutzer verknüpft ist, der eine Verbindung zum Remote-Desktop herstellt.

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 starten.

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 View Client wird gestartet und stellt eine Verbindung mit dem Server `view.mycompany.com` 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 View Client-Befehlszeilenschnittstelle und -Konfigurationsdateien“, auf Seite 22.

---

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 View-Verbindungsserver verwendet. (Der standardmäßige Port lautet 443.) Da eine Desktop-ID bereitgestellt wird, wird der Desktop gestartet, obwohl die Aktion `start-session` nicht im URI enthalten ist.

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

Horizon View Client wird gestartet und stellt eine Verbindung mit dem Server `view.mycompany.com` 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://fred@view.mycompany.com/Finance%20Desktop?domainName=mycompany`

Horizon View Client wird gestartet und stellt eine Verbindung mit dem Server `view.mycompany.com` 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.

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

Horizon View Client wird gestartet und der Benutzer wird an die Anmeldeaufforderung für die Verbindung mit dem Server `view.mycompany.com` weitergeleitet.

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

Horizon View Client wird gestartet und stellt eine Verbindung mit dem Server `view.mycompany.com` her. Das Anmeldefeld fordert den Benutzer zur Eingabe von Benutzernamen, Domänennamen und Kennwort auf. Nach einer erfolgreichen Anmeldung zeigt Horizon View Client ein Dialogfeld an, in dem der Benutzer aufgefordert wird, das Zurücksetzen für „Primary Desktop“ zu bestätigen. Nach dem Zurücksetzen wird je nach Clienttyp eine Meldung angezeigt, die über den Erfolg des Zurücksetzens informiert.

Hinweis Diese Aktion ist nur verfügbar, wenn die Funktion vom View-Administrator für den Endbenutzer aktiviert wurde.

---

7 `vmware-view://`

Horizon View Client wird gestartet und der Benutzer wird zu der Seite weitergeleitet, auf der die Adresse einer View-Verbindungsserver-Instanz eingegeben werden kann.

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>
```

Verwenden der View Client-Befehlszeilenschnittstelle und -Konfigurationsdateien

Sie können View 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 View 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 View 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 View Client alle geänderten Einstellungen in der Datei `~/.vmware/view-preferences` gespeichert.

Eigenschaften, die ein Ändern der Standardeinstellungen durch die Benutzer verhindern

Für jede Eigenschaft können Sie eine entsprechende `view.allow`-Eigenschaft festlegen, durch die gesteuert wird, ob eine Änderung der Einstellung durch die Benutzer zulässig ist. Wenn Sie zum Beispiel die Eigenschaft `view.allowDefaultBroker` in der Datei `/etc/vmware/view-mandatory-config` auf „FALSE“ festlegen, können die Benutzer bei Verwendung von View Client den Namen im Feld **Servername** nicht ändern.

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-`*`Optionen`*

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 nicht in View Client wirksam. Sie können eine Proxyausnahme für die View-Verbindungsserver-Instanz konfigurieren.

View 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, wie die für USB-Umleitung und MMR, werden nur in der Version von View Client von Drittanbietern zur Verfügung gestellt. Weitere Informationen über die Thin Client- und Zero Client-Partner von VMware finden Sie im *VMware-Kompatibilitätshandbuch* unter http://www.vmware.com/resources/compatibility/search.php?deviceCategory=vdm.

Tabelle 2-4. View Client-Befehlszeilenoptionen und -Schlüssel für Konfigurationsdateien

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung
`view.allMonitors`	`--allmonitors`	Blendet das Host-Betriebssystem aus und öffnet die View Client-Benutzeroberfläche im Vollbildmodus auf allen Monitoren, die verbunden werden, sobald View Client gestartet wird. Wenn Sie den Konfigurationsschlüssel einstellen, geben Sie **„TRUE“** oder **„FALSE“** ein. Standardwert ist „FALSE“ (FALSCH).

`view.allowDefaultBroker`	`-l`, `--lockServer`
	Beispiel:
	`--lockServer -s view.company.com`
		Mit dieser Befehlszeilenoption oder dem Einstellen der Eigenschaft auf „FALSE“ (FALSCH) wird das Feld **Servername** 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.

`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“** ein. 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 2-4. View 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“** ein. 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.defaultBroker`	`-s, --serverURL=`
	Beispiele:
	`--serverURL=https://view.company.com`
	`-s view.company.com`
	`--serverURL=view.company.com:1443`
		Fügt den Namen hinzu, den Sie im Feld **Servername** im View 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.

`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.

Tabelle 2-4. View Client-Befehlszeilenoptionen und -Schlüssel für Konfigurationsdateien (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung

`view.defaultDesktopSize`	`--desktopSize=`
	Beispiele:
	`--desktopSize="1280x800"`
	`--desktopSize="all"`
		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.

`view.defaultDesktopWidth`	Keine	Gibt die Standardbreite des Fensters für View-Desktop in Pixel an.
`view.defaultDomain`	`-d`, `--domainName=`	Stellt den Domänennamen ein, den View Client für alle Verbindungen verwendet, und fügt den von Ihnen im Feld **Domänenname** angegebenen Namen dem Dialogfeld „View Client-Authentifizierung“ hinzu.
`view.defaultPassword`	`-p "-"`, `--password="-"`	Für PCoIP- und `rdesktop`-Verbindungen sollten Sie immer **`"-"`** angeben, um das Kennwort von `stdin` zu lesen. Stellt das Kennwort ein, das View Client für alle Verbindungen verwendet, und fügt das Kennwort in das Feld **Kennwort** im Dialogfeld „View Client-Authentifizierung“ ein, wenn der View-Verbindungsserver eine Kennwort-Authentifizierung akzeptiert. **Hinweis** Sie können kein leeres Kennwort verwenden. Das heißt, Sie können nicht --password = "" eingeben

Tabelle 2-4. View 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=`	Stellt den Benutzernamen ein, den View Client für alle Verbindungen verwendet, und fügt den von Ihnen im Feld **Benutzername** angegebenen Namen dem Dialogfeld „View Client-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.fullScreen`	`--fullscreen`	Blendet das Host-Betriebssystem aus und öffnet die View 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=`
	`rdesktop`-Beispiele:
	`--kbdLayout="en-us"`
	`-k "fr"`
	`FreeRDP`-Beispiel:
	`-k "0x00010407"`
		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`

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

`view.mmrPath`	`-m, --mmrPath=`
	Beispiel:
	`--mmrPath="/usr/lib/altmmr"`
		(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.

Tabelle 2-4. View Client-Befehlszeilenoptionen und -Schlüssel für Konfigurationsdateien (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung
`view.nomenubar`	`--nomenubar`	Unterdrückt die View Client-Menüleiste, wenn View 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`
	Beispiel:
	`--nonInteractive --serverURL="https://view.company.com" --userName="user1" --password="-" --domainName="xyz" --desktopName="Windows 7"`
		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).

`view.once`	`--once`	Gibt an, dass View Client bei einem Fehler nicht erneut versuchen soll, eine Verbindung herzustellen. Verwenden Sie `--once`, wenn Sie zum View 4.6 Client einen ähnlichen Workflow haben möchten. Diese Option erzwingt die Beendigung des View Client, nachdem der Benutzer die Verbindung getrennt oder sich von einem Desktop abgemeldet hat. Normalerweise sollten Sie diese Option angeben, wenn Sie den Kioskmodus verwenden, und den Fehler mit einem Exit-Code behandeln. Anderenfalls 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=`
	Beispiel:
	`--rdesktopOptions="-f -m"`
		(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.

Tabelle 2-4. View Client-Befehlszeilenoptionen und -Schlüssel für Konfigurationsdateien (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung

Keine	`–r, ––redirect=`
	Beispiel:
	`––redirect="sound:off"`
		(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.

`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 36.
Keine	`––save`	(Verfügbar mit View Client 2.2. oder später) 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 Domänenanmen nicht mehr manuell eingeben müssen.
`view.sendCtrlAltDelToLocal`	Keine	(Verfügbar, wenn Sie das PCoIP-Anzeigeprotokoll und View Client 2.1 oder höher verwenden) Bei Festlegung auf **„TRUE“** wird die Tastenkombination Strg-Alt-Del 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`. Sie können diese Tastenkombination auch konfigurieren, indem Sie „`view–keycombos–config file`“ wie in „Konfigurieren bestimmter Tasten und Tastenkombinationen zum Senden an das lokale System“, auf Seite 32 beschrieben verwenden.

Tabelle 2-4. View Client-Befehlszeilenoptionen und -Schlüssel für Konfigurationsdateien (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung
`view.sendCtrlAltInsToVM`	Keine	(Verfügbar, wenn Sie das PCoIP-Anzeigeprotokoll und View Client 2.1 oder höher verwenden) Bei Festlegung auf **„TRUE“** wird anstelle von Strg-Alt-Del die Tastenkombination Strg+Alt+Ins an den virtuellen Desktop gesendet. Der Standardwert ist „FALSE“. **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 *Verwaltung von VMware Horizon View-*.
`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.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 36.
Keine	`--enableNla`	(Trifft zu, wenn Sie FreeRDP für RDP-Verbindungen benutzen) Ermöglicht Netzwerkebenen-Authentifizierung (network-level authentication, NLA). 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 36. **Hinweis** Das Programm `rdesktop` unterstützt keine NLA.

Tabelle 2-4. View Client-Befehlszeilenoptionen und -Schlüssel für Konfigurationsdateien (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung

Keine	`--printEnvironmentInfo`
	Beispiel:
	`--printEnvironmentInfo -s view.company.com`
		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`.

Keine	`--usb=`	(Nur mit Distributionen von Drittanbietern und nur für View Client 1.5 verfügbar) Spezifiziert, welche Optionen für die USB-Umleitung benutzt werden. Siehe „Verwenden der Befehlszeilenoption aus View Client 1.5 zur Umleitung von USB-Geräten“, auf Seite 63. Um USB-Optionen mit View Client 1.6 und später zu konfigurieren, siehe Kapitel 6, „Konfigurieren der USB-Umleitung auf dem Client“, auf Seite 57.
Keine	`--version`	Zeigt Versionsinformationen von View Client.

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 *Verwaltung von VMware Horizon 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 ein nichtstandardmäßiger Benutzernamen nicht erforderlich ist und Sie keinen Benutzernamen angeben, kann View 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 View Client auf einem Linux-Clientsystem aus und hat die folgenden Eigenschaften:

- Der Name des Benutzerkontos basiert auf der MAC-Adresse des Clients.
- View Client läuft im Vollbildmodus ohne View 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 View 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.

Konfigurieren bestimmter Tasten und Tastenkombinationen zum Senden an das lokale System

Wenn Sie das PCoIP-Anzeigeprotokoll und Horizon View Client 2.2 oder höher verwenden, können Sie eine Datei „`view–keycombos–config`“ erstellen, um anzugeben, welche Tastenkombinationen nicht an den Remote-Desktop weitergeleitet werden sollen. Bei Verwendung von Horizon View Client 2.3 können Sie auch einzelne Tasten angeben.

Womöglich sollen einige Tasten oder Tastenkombinationen bei der Arbeit mit einem Remote-Desktop von Ihrem lokalen Clientsystem verarbeitet werden. So können Sie zum Beispiel eine bestimmte Tastenkombination verwenden, um den Bildschirmschoner auf Ihrem Clientcomputer zu starten. Ab Horizon View Client 2.2 können Sie eine Datei unter „`/etc/vmware/view–keycombos–config`“ erstellen und die Tastenkombinationen festlegen. Bei Verwendung von Horizon View Client 2.3 oder höher können Sie auch einzelne Tasten angeben.

Setzen Sie jede Taste oder Tastenkombination in eine neue Zeile und verwenden Sie dabei das in der folgenden Tabelle dargestellte Format.

Tabelle 2-5. Format für die Festlegung von Tasten, die nicht an Remote-Desktops weitergeleitet werden dürfen

Client-Version	Format
Horizon View Client 2.2	`<<varname id="VARNAME_2FEB13F2EAB54854AB592728157B01DA">modNa–me</varname>><varname id="VARNA–ME_5599ABEB8A9C40008FC8DBB35ADD0553">keyName</varname>` **Wichtig** Diese Funktion gilt für Tastenkombinationen und nicht für einzelne Tasten. So können Sie beispielsweise nicht nur <*modName*> oder nur *keyName* angeben.

Horizon View Client 2.3 oder höher	`<<varname id="varname_8B31DEC6FAAD4DF2A2459399C4FFF8CA">modNa–me</varname>><varname id="varna–me_2775AC593B6F46689C5FF2164A58AA80">scanCode</varname>`
	`<varname id="varname_3947E08F92424A659F8F601D8399F92B">scanC–ode</varname>`
	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 ist *modName* eine der vier Zusatztasten: `Ctrl`, `Alt`, `Shift` 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. Bei Verwendung von Horizon View Client 2.3 oder höher können Sie 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 in Horizon View Client 2.3 oder höher

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.

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
```

Angeben eines Tastennamens in Horizon View Client 2.2

Bei dem *keyName*-Wert müssen Sie auf die Groß-/Kleinschreibung achten und er kann aus Folgendem bestehen: Zahlen `0` bis `9`, Funktionstasten `F1` bis `F12`, groß- oder kleingeschriebene Buchstaben `A` bis `Z` oder jede andere in der folgenden Liste aufgeführte Taste.

Hinweis Durch das Präfix „`KP`“, z. B.`KP_Enter`, werden in der folgenden Liste die Tasten der numerischen Tastatur gekennzeichnet.

BackSpace	Ausführen	KP_Page_Down	quotedbl	asciicircum
Tab	Einfügen	KP_End	numbersign	underscore
Linefeed	Rückgängig	KP_Begin	dollar	grave
Clear	Wiederholen	KP_Insert	percent	quoteleft

Return	Menü	KP_Delete	ampersand	braceleft
Pause	Suchen	KP_Equal	apostrophe	bar
Scroll_Lock	Abbrechen	KP_Multiply	quoteright	braceright
Sys_Req	Hilfe	KP_Add	quoteleft	asciitilde
Escape	Break	KP_Separator	parenleft	
Löschen	Num_Lock	KP_Subtract	parenright	
Multi_key	KP_Space	KP_Decimal	asterisk	
Codeinput	KP_Tab	KP-Divide	plus	
Startseite	KP_Enter	KP_0	comma	
Left	KP_F1	KP_1	minus	
Up	KP_F2	KP_2	period	
Right	KP_F3	KP_3	slash	
Down	KP_F4	KP_4	colon	
Prior	KP_Home	KP_5	less	
Page_Up	KP_Left	KP_6	equal	
Next	KP_UP	KP_7	greater	
Page_Down	KP_Right	KP_8	question	
End	KP_Down	KP_9	at	
Begin	KP_Prior	Caps_Lock	bracketleft	
Wählen Sie	KP_Page_Up	space	backslash	
Print	KP_Next	exclam	bracketright	

Die folgende Liste zeigt die Beispielinhalte einer Datei „`/etc/vmware/view-keycombos-config`“:

```
<ctrl><alt>Delete
<alt>Tab
<alt>1
<alt>h
<ctrl>1
<ctrl>S
<ctrl>h
<super>h
<shift>h
<ctrl>space
<Ctrl>KP_Enter
<Ctrl>Up
```

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 View-Verbindungsserver und Horizon View 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 „Zertifikatsprüfungsmodi für Horizon View Client“, auf Seite 41.

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

- **`1`** implementiert `Vollständige Überprüfung`.
- **`2`** implementiert `Warnen, wenn die Verbindung nicht sicher sein könnte`.
- **`3`** implementiert `Es wird keine Überprüfung durchgeführt`.

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 „View Client-Konfigurationseinstellungen und -Befehlszeilenoptionen“, auf Seite 24.

Verwenden von FreeRDP für RDP-Verbindungen

Wenn Sie beabsichtigen, anstelle von PCoIP RDP für Verbindungen zu View-Desktops zu verwenden, können Sie entweder einen `rdesktop`-Client oder `xfreerdp`, die unter der Apache-Lizenz veröffentlichte Open-Source-Implementierung des Remotedesktopprotokolls (RDP), verwenden.

Da das Programm `rdesktop` nicht länger aktiv entwickelt wird, können View Client 1.7 und alle neueren Versionen auch die ausführbare Datei `xfreerdp` ausführen, wenn Ihr Linux-Computer über die für FreeRDP erforderliche Version und die entsprechenden Patches verfügt.

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

- Um festzulegen, dass View Client `xfreerdp` anstelle von `rdesktop` ausführt, müssen Sie die entsprechende Befehlszeilenoption oder den entsprechenden Konfigurationsschlüssel verwenden.

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`

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. Zur Aktivierung der Authentifizierung auf Netzwerkebene muss die folgende Befehlszeilenoption verwendet werden:

```
--enableNla
```

Weitere Informationen zur Befehlszeilenschnittstelle `vmware-view` und den jeweiligen Konfigurationsdateien finden Sie unter „Verwenden der View Client-Befehlszeilenschnittstelle und -Konfigurationsdateien“, auf Seite 22.

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 36.

Installation und Konfiguration von FreeRDP

Um einen FreeRDP-Client für RDP-Verbindungen zu View-Desktops verwenden zu können, müssen auf Ihrem Linux-Computer die erforderliche Version und die entsprechenden Patches für FreeRDP aufgespielt sein.

Es muss FreeRDP 1.0.x installiert sein und Sie müssen die entsprechenden Patches installieren, damit die Optionen `--from-stdin` und `-X` ordnungsgemäß funktionieren.

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

Vorgehensweise

1 Laden Sie auf die Linux-Clientmaschinen FreeRDP 1.0.x von GitHub unter https://github.com/FreeRDP/FreeRDP herunter.

2 Bei der Installation von FreeRDP 1.0.1 müssen Sie das Patching mit der Datei „`freerdp-1.0.1.patch`“ durchführen und den folgenden Patch-Befehl verwenden:

```
patch -p1 < freerdp-1.0.1.patch
```

3 Zur Erstellung und Installation von FreeRDP öffnen Sie ein Terminalfenster und führen Sie die folgenden Befehle aus.

   a Führen Sie folgenden Befehl aus:

   ```
   cmake -DWITH_SSE2=ON -DWITH_PULSEAUDIO=ON -DWITH_PCSC=ON .
   ```

   b Führen Sie folgenden Befehl aus:

   ```
   make
   ```

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

   ```
   sudo make install
   ```

Konfigurieren der USB-Umleitung auf dem Client

Sie können eine Konfigurationseigenschaft so einstellen, dass der Client nur durch FIPS (Federal Information Processing Standard) 140-2 zugelassene kryptografische Algorithmen und Protokolle verwendet, um eine Remote-PCoIP-Verbindung herzustellen.

Hinweis Der View PCoIP FIPS-Modus unterstützt keine AES-256-Verschlüsselungs-Algorithmen.

Diese Einstellung gilt sowohl für den Server als auch für den Client. Sie können entweder einen oder beiden Endpunkte für den Betrieb im FIPS-Modus konfigurieren. Einen Endpunkt zu konfigurieren, um ihn im FIPS-Modus zu betreiben, schränkt die verfügbaren Verschlüsselungsalgorithmen für die Verhandlung der Sitzung ein.

Wichtig Wenn Sie den FIPS-Modus auf einem Endpunkt aktivieren, aber der andere Endpunkt keine von FIPS 140-2 zugelassenen kryptografischen Algorithmen unterstützt, schlägt die Verbindung fehl.

Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, wird der FIPS-Modus nicht verwendet.

Einstellen der Konfigurationseigenschaft

Um den FIPS-Modus zu aktivieren oder zu deaktivieren, können Sie die Eigenschaft `pcoip.enable_fips_mode` einrichten. Wenn Sie die Eigenschaft auf **`1`** einstellen, ist der FIPS-Modus eingeschaltet, wenn Sie die Eigenschaft auf **`0`** einstellen, ist der FIPS-Modus ausgeschaltet. Zum Beispiel schaltet die folgende Einstellung den FIPS-Modus ein:

```
pcoip.enable_fips_mode = 1
```

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

Sie können diese Eigenschaft in einer von mehreren Dateien einstellen. Wenn View Client startet, wird die Einstellung von verschiedenen Standorten aus in der folgenden Reihenfolge verarbeitet:

1 `/etc/teradici/pcoip_admin_defaults.conf`

2 `~/.pcoip.rc`

3 `/etc/teradici/pcoip_admin.conf`

Wenn eine Einstellung an mehreren Stellen definiert ist, wird der Wert aus der zuletzt gelesenen Datei verwendet.

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.

Wichtig Diese Funktion ist nur verfügbar, wenn View Agent und der View-Verbindungsserver über die View-Version 5.0 oder höher verfügen.

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. Sie können die Client-Bildcachegröße für View Client 1.7 und höher von mindestens 50 MB auf maximal 1024 MB anheben. Die maximale Größe in den älteren Versionen beträgt 300 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 eine Zahl unter 50 angeben, wird die Zahl in 50 geändert. Wenn Sie eine Zahl angeben, die den Maximalwert überschreitet, wird die Zahl in den Maximalwert geändert.

Sie können diese Eigenschaft in jeder der einzelnen Dateien festlegen. Beim Start von View 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.

Verwaltung der Serververbindungen und Desktops 3

Mit Horizon View Client können Sie eine Verbindung zu einem View-Verbindungsserver oder Sicherheitsserver herstellen und sich bei einem Remote-Desktop an- oder abmelden. Zur Fehlersuche können Sie auch einen Ihnen zugewiesen Remote-Desktop zurücksetzen.

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

- Erstmaliges Anmelden an einem Remote-Desktop auf Seite 39

  Bevor Endbenutzer auf ihre Remote-Desktops zugreifen, sollten Sie testen, ob Sie sich über ein Clientsystem an einem Remote-Desktop anmelden können.

- Zertifikatsprüfungsmodi für Horizon View Client auf Seite 41

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

- Wechseln zwischen Desktops auf Seite 42

  Wenn Sie mit einem Desktop verbunden sind, können Sie zu einem anderen Desktop wechseln.

- Abmelden oder Trennen von Desktops auf Seite 42

  Wenn Sie die Verbindung zu einem Remote-Desktop trennen, ohne sich abzumelden, bleiben die Anwendungen geöffnet.

- Rollback eines Desktops auf Seite 43

  Bei einem Rollback werden alle an einem virtuellen Desktop vorgenommenen Änderungen verworfen, den Sie zur Verwendung im lokalen Modus auf einem Windows-PC oder -Laptop ausgecheckt haben.

Erstmaliges Anmelden an einem Remote-Desktop

Bevor Endbenutzer auf ihre Remote-Desktops zugreifen, sollten Sie testen, ob Sie sich über ein Clientsystem an einem Remote-Desktop anmelden können.

Voraussetzungen

- Besorgen Sie sich die zur Anmeldung benötigten Informationen, so etwa den Active Directory-Benutzernamen und das Active Directory-Kennwort, den RSA SecurID-Benutzernamen und -Passcode oder den RADIUS-Authentifizierungsbenutzernamen oder -Passcode.
- Besorgen Sie sich den Domänennamen für die Anmeldung.
- Führen Sie die unter „Vorbereiten des View-Verbindungsservers für Horizon View Client“, auf Seite 11 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 diesen Remote-Desktop gewährt. 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 View Agent-Gruppenrichtlinieneinstellung AllowDirectRDP aktiviert ist.
- Wenn Ihr Administrator dies zulässt, können Sie den Zertifikatsprüfungsmodus für das von View Server vorgelegte SSL-Zertifikat konfigurieren. Siehe „Zertifikatsprüfungsmodi für Horizon View Client“, auf Seite 41.

Vorgehensweise

1 Öffnen Sie entweder ein Terminal-Fenster und geben Sie **`vmware-view`** ein oder wählen Sie **Anwendungen > Internet > VMware Horizon View Client** in der Ubuntu-Menüleiste.

2 Geben Sie den Servernamen und eine Portnummer ein, falls dies erforderlich ist, und klicken Sie dann auf **Weiter**.

  Ein Beispiel für die Verwendung eines nicht standardmäßigen Ports ist **`view.company.com:1443`**.

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

4 Geben Sie Ihren Benutzernamen und das Kennwort ein, wählen Sie eine Domäne aus und klicken Sie auf **OK**.

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

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

  Normalerweise bedeutet diese Warnung, dass der View-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. View-Verbindungsserver der Version 4.6.1, 5.0.1 und höher senden Fingerabdruck-Informationen, frühere Versionen jedoch nicht.

6 (Optional) Wählen Sie das zu verwendende Anzeigeprotokoll und die zu verwendende Fenstergröße aus.

Option	Beschreibung
Anzeigeprotokoll	Die Standardeinstellung ist **PCoIP**. Wenn Sie stattdessen das Microsoft RDP-Anzeigeprotokoll verwenden möchten, müssen Sie zum Umschalten auf **PCoIP** unter dem Desktop-Namen klicken und **Microsoft RDP** auswählen.
Fenstergröße	Die Standardeinstellung ist **Vollbild - Alle Monitore**. Klicken Sie zur Auswahl einer anderen Fenstergröße auf eine der anderen Optionen unter dem Desktop-Namen, z. B. auf **Großer Bildschirm** oder **Benutzerdefinierte Größe**.

7 Doppelklicken Sie auf eine Remote-Desktop-Verknüpfung, um die Verbindung herzustellen.

Nachdem die Verbindung hergestellt wurde, wird das Clientfenster angezeigt. Wenn Horizon View Client keine Verbindung mit dem Desktop herstellen kann, führen Sie die folgenden Aufgaben aus:

- Legen Sie fest, ob der View-Verbindungsserver dahingehend konfiguriert werden soll, SSL nicht zu verwenden. Horizon View Client 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.
- Stellen Sie sicher, dass die für die View-Verbindungsserver-Instanz festgelegten Kennzeichen Verbindungen von diesem Benutzer erlauben. Weitere Informationen finden Sie im Dokument *Verwaltung von VMware Horizon View-*.
- Stellen Sie sicher, dass der Benutzer zum Zugriff auf diesen Desktop berechtigt ist. Weitere Informationen finden Sie im Dokument *Verwaltung von VMware Horizon View-*.
- Wenn Sie das RDP-Anzeigeprotokoll zur Verbindungsherstellung mit einem Remote-Desktop verwenden, müssen Sie bestätigen, dass der Clientcomputer Remote-Desktop-Verbindungen zulässt.

Zertifikatsprüfungsmodi für Horizon View 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 View-Verbindungsserver und Horizon View 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 View Client an einen Server mit einem Zertifikat umleitet, das nicht mit dem in Horizon View 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 Anweisungen zur Verteilung eines selbstsignierten Stammzertifikats, das die Benutzer auf ihren Linux-Clientsystemen installieren können, finden Sie in der Ubuntu-Dokumentation.

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

Neben der Bereitstellung eines Serverzertifikats sendet der View-Verbindungsserver der Version 4.6.1, 5.0.1 und höher ebenfalls einen Zertifikat-Fingerabdruck an Horizon View Client. Ein Fingerabdruck ist ein Hash-Wert des öffentlichen Schlüssels des Zertifikats und wird als Abkürzung für den öffentlichen Schlüssel verwendet. Wenn View Server 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 **Datei > Einstellungen** in der VMware Horizon View--Client-Menüleiste oder in der View-Desktop-Menüleiste. 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 Namen des View-Verbindungsservers übereinstimmen, den Sie in Horizon View Client eingegeben haben.
- **Server-Identitätszertifikate nicht überprüfen**. Bei Aktivierung dieser Option führt View keine Zertifikatsüberprüfung durch.

Wechseln zwischen Desktops

Wenn Sie mit einem Desktop verbunden sind, können Sie zu einem anderen Desktop wechseln.

Vorgehensweise

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

Option	Aktion
Einen anderen Remote-Desktop auf demselben Server auswählen	Wählen Sie **Desktop > Trennen** aus der Menüleiste.
Einen Remote-Desktop auf einem anderen Server auswählen	Wählen Sie **Datei > Verbindung zu Server trennen** aus der Menüleiste aus.

Abmelden oder Trennen von Desktops

Wenn Sie die Verbindung zu einem Remote-Desktop trennen, ohne sich abzumelden, bleiben die Anwendungen geöffnet.

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

HINWEIS Der View-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 zu einem Desktop.

Option	Aktion
Aus dem Desktop-Betriebssystem heraus	Melden Sie sich über das Windows-**Start**-Menü ab.
Über die Menüleiste	Wählen Sie **Desktop > Trennen und Abmelden**. 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.
  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.

Rollback eines Desktops

Bei einem Rollback werden alle an einem virtuellen Desktop vorgenommenen Änderungen verworfen, den Sie zur Verwendung im lokalen Modus auf einem Windows-PC oder -Laptop ausgecheckt haben.

Sie können ein Rollback eines Remote-Desktops nur dann durchführen, wenn Ihr View-Administrator diese Funktion aktiviert hat und auch nur dann, wenn Sie den Desktop ausgecheckt haben.

VORSICHT Wenn Änderungen am Desktop im lokalen Modus vorgenommen wurden und diese Änderungen nicht vor dem Rollback zurück auf den View Server repliziert wurden, gehen sie verloren.

Voraussetzungen

- Besorgen Sie sich die zur Anmeldung benötigten Informationen, so etwa den Active Directory-Benutzernamen und das Active Directory-Kennwort, den RSA SecurID-Benutzernamen und -Passcode oder den RADIUS-Authentifizierungsbenutzernamen oder -Passcode.
- Sichern Sie den Desktop auf dem Server, um Daten oder Dateien zu speichern.

  Sie können View Administrator zum Replizieren von Daten auf dem Server verwenden, oder, falls die Richtlinie dies zulässt, View Client with Local Mode auf dem Windows-Client verwenden, auf dem der Desktop aktuell ausgecheckt ist.

Vorgehensweise

1 Wenn auf der Startseite von Horizon View Client die **View-Verbindungsserver**-Eingabeaufforderung angezeigt wird, geben Sie den Namen des Servers ein und klicken Sie auf **Fortfahren**.

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

   b Geben Sie im Anmeldedialogfeld Ihren Benutzernamen und Ihr Kennwort ein.

2 Wählen Sie auf der Horizon View Client-Startseite, auf der Remote-Desktop-Verknüpfungen angezeigt werden, den entsprechenden Desktop aus und wählen Sie anschließend **Desktop > Rollback für Desktop durchführen** aus der Menüleiste.

Nach der Durchführung des Rollbacks auf dem Remote-Desktop können Sie sich über den Linux-Client am Remote-Desktop anmelden.

Verwendung eines Microsoft Windows-Desktops auf einem Linux-System

4

View Client für Linux unterstützt einige der Funktionen, die in View Client für Windows enthalten sind.

Dieses Kapitel behandelt die folgenden Themen:

Funktionsunterstützungs-Matrix für Linux

Einige Funktionen werden auf manchen View Clients unterstützt, auf anderen nicht. Zum Beispiel wird der lokale Modus nur auf View Client für Windows unterstützt.

Tabelle 4-1. Auf Windows-Desktops für Linux-Clients unterstützte Funktionen

Funktion	Windows 8.x-Desktop	Windows 7-Desktop	Windows Vista-Desktop	Windows XP-Desktop	Windows Server 2008 R2-Desktop
RSA SecurID oder RADIUS	X	X	X	X	X
Einmaliges Anmelden	X	X	X	X	X
RDP-Anzeigeprotokoll	X	X	X	X	X
PCoIP-Anzeigeprotokoll	X	X	X	X	X
USB-Zugriff	Nur Partner-Clientsysteme	Nur Partner-Clientsysteme	Nur Partner-Clientsysteme	Nur Partner-Clientsysteme	Nur Partner-Clientsysteme
Echtzeit-Audio/Video (RTAV)	Nur Partner-Clientsysteme	Nur Partner-Clientsysteme	Nur Partner-Clientsysteme	Nur Partner-Clientsysteme	Nur Partner-Clientsysteme
Wyse MMR			Nur Partner-Clientsysteme, und nur mit RDP	Nur Partner-Clientsysteme, und nur mit RDP	
Windows 7 MMR					

Tabelle 4-1. Auf Windows-Desktops für Linux-Clients unterstützte Funktionen (Fortsetzung)

Funktion	Windows 8.x-Desktop	Windows 7-Desktop	Windows Vista-Desktop	Windows XP-Desktop	Windows Server 2008 R2-Desktop
Virtuelles Drucken	Nur Partner-Clientsysteme	Nur Partner-Clientsysteme	Nur Partner-Clientsysteme	Nur Partner-Clientsysteme	
Standortbasiertes Drucken	X	X	X	X	
Smartcards	Nur Partner-Clientsysteme, und nur mit PCoIP	Nur Partner-Clientsysteme	Nur Partner-Clientsysteme	Nur Partner-Clientsysteme	Nur Partner-Clientsysteme
Mehrere Monitore	X	X	X	X	X
Lokaler Modus					

Für Funktionen, die auf Windows-Desktops für Linux View Client unterstützt werden, gelten die folgenden Einschränkungen.

- Windows 8.x-Desktops werden nur unterstützt, wenn Sie über Server und Desktops mit Horizon View 5.2 oder höher verfügen.
- Die Echtzeit-Audio/Video-Funktion wird nur unterstützt, wenn Sie über Horizon View 5.2 mit Feature Pack 2 oder später verfügen.
- Windows 2008 R2-Desktops werden nur unterstützt, wenn Sie über Server und Desktops mit Horizon View 5.3 oder später verfügen.

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

Hinweis Diese Funktionsunterstützungsmatrix gilt für den View Client für Linux, den VMware für Ubuntu verfügbar macht. Darüber hinaus bieten verschiedene VMware-Partner Thin Client-Geräte für Horizon View-Bereitstellungen an. Die Funktionen, die für die einzelnen Thin Client-Geräte verfügbar sind, werden vom Hersteller und Modell sowie der vom jeweiligen Unternehmen gewählten Konfiguration bestimmt. 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.

Internationalisierung

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

Wenn Sie ein Linux-Clientsystem mit Ubuntu 10.4 verwenden und die View Client-Benutzeroberfläche 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.

- 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 View Client verwendet die Monitorkonfiguration, die beim Start von Horizon View Client aktiviert ist. Wenn Sie bei der Monitoranzeige vom Querformat zum Hochformat wechseln oder einen zusätzlichen Monitor an das Clientsystem anschließen, während Horizon View Client ausgeführt wird, müssen Sie Horizon View Client neu starten, um die neue Monitorkonfiguration verwenden zu können.

Horizon View 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 mehr als zwei Monitore verwenden, müssen sich die Monitore alle im gleichen Modus befinden und über die gleiche Bildschirmauflösung verfügen. 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.

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 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 *Verwaltung von VMware Horizon 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.

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.

Diese Funktion steht bei Verwendung von VMware Horizon View- 5.2 Feature Pack 2 oder später zur Verfügung. Informationen über das Einrichten der Echtzeit-Audio/Video-Funktion und über das Konfigurieren der Frame-Rate und Bildauflösung in einem Remote-Desktop finden Sie im Handbuch *Installation und Verwaltung von VMware Horizon View Feature Pack*. 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 steht nur mit der Version von Horizon View Client für Linux zur Verfügung, die von Drittanbietern bereitgestellt wird.

In diesen Fällen können Sie Ihre Webcam verwenden

Wenn Ihr Horizon View-Administrator die Echtzeit-Audio/Video-Funktion konfiguriert hat und Sie das PCoIP-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.

Während der Einrichtung von Anwendungen wie z. B. Skype, Webex oder Google Hangouts auf Ihrem Remote-Desktop können Sie VMware Virtual Microphone und VMware Virtual Webcam als Eingabegeräte und VMware Virtual Audio als Ausgabegerät in den Menüs der Anwendung 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, kann Ihr Administrator eine bevorzugte Webcam konfigurieren, die auf Ihrem Remote-Desktop verwendet wird. Stimmen Sie sich mit Ihrem Horizon View-Administrator ab, wenn Sie sich bezüglich der Webcamauswahl nicht sicher sind.

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 49.

Voraussetzungen

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

Vorgehensweise

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

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

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

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

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

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

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

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

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

- Für Webcams legen Sie die Eigenschaft „`rtav.srcWCamId`“ auf den Wert der in der Protokolldatei gefundenen Webcam-Beschreibung fest, wie im Folgenden beschrieben.
- Für Audiogeräte legen Sie die Eigenschaft „`rtav.srcAudioInId`“ auf den Wert des PULSE-Audio-Felds „`device.description`“ fest.

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

Voraussetzungen

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

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

Vorgehensweise

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

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

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

   c Starten Sie einen Anruf und beenden Sie ihn dann.

      Auf diese Weise wird eine Protokolldatei erstellt.

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

a Öffnen Sie die Debug-Protokolldatei mit einem Texteditor.

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

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

Das folgende Beispiel zeigt einen Auszug der Webcam-Auswahl:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5 Starten Sie einen neuen Anruf.

Festlegen von Druckeinstellungen für die virtuelle Druckfunktion

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 virtuelle Druckfunktion steht nur mit der Version von Horizon View Client für Linux zur Verfügung, die von Drittanbietern bereitgestellt wird. Weitere Informationen über die Thin Client- und Zero Client-Partner von VMware finden Sie im *VMware-Kompatibilitätshandbuch* unter http://www.vmware.com/resources/compatibility/search.php?deviceCategory=vdm. Für diese Funktion gelten zudem die folgenden Anforderungen:

- Die Version von Horizon View Client für Linux muss 2.1 oder später sein.
- Bei View Agent und dem View-Verbindungsserver muss es sich um Horizon View-Version 5.2 oder später handeln.
- Sie müssen das PCoIP-Anzeigeprotokoll oder FreeRDP verwenden. Diese Funktion arbeitet nicht mit rdesktop.

Nachdem dem lokalen Computer ein Drucker hinzugefügt wurde, fügt Horizon View 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 der für Windows XP und Windows Vista, ist aber nicht vollständig gleich.

Voraussetzungen

Stellen Sie sicher, dass die virtuelle Druckfunktion von View Agent auf dem Remote-Desktop installiert ist. Die Treiber befinden sich im Remote-Desktop-Dateisystem unter `C:\Programme\Gemeinsame Dateien\VMware\Drivers\Virtual Printer`.

Die Installation von View Agent ist eine der Aufgaben, die im Rahmen der Vorbereitung einer virtuellen Maschine auf die Verwendung als Remote-Desktop durchgeführt werden muss. Weitere Informationen finden Sie im Dokument *Verwaltung von VMware Horizon View*.

Vorgehensweise

1 Klicken Sie auf einem Remote-Desktop mit 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.

  Auf dem Remote-Desktop werden virtuelle Drucker als <*Druckername*>#:<*Nummer*> 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 können standardmäßig Text von Ihrem Clientsystem auf einen Remote-View-Desktop kopieren und einfügen. Wenn Ihr Administrator die Funktion aktiviert, können Sie auch formatierten Text und Bilder zwischen einem Remote-View-Desktop und Ihrem Clientsystem oder zwischen zwei View-Desktops kopieren und einfügen. Hierfür gelten allerdings einige Einschränkungen.

Wenn Sie das PCoIP-Anzeigeprotokoll sowie einen View-Desktop vom Typ 5.x oder eine neuere Version verwenden, kann Ihr View-Administrator diese Funktion so einstellen, dass Kopier- und Einfügevorgänge nur von Ihrem Clientsystem auf einen View-Desktop oder nur von einem View-Desktop zu Ihrem Clientsystem oder beide Vorgänge zugelassen werden bzw. keiner der beiden Vorgänge zugelassen wird.

Die Administratoren konfigurieren die Möglichkeit zum Kopieren/Einfügen durch die Verwendung von Gruppenrichtlinienobjekten (GPOs), die View Agent auf den View-Desktops zugeordnet sind. Weitere Informationen finden Sie unter dem Thema über allgemeine Sitzungsvariablen von View PCoIP im Dokument *Verwaltung von VMware Horizon View-* im Kapitel über die Konfigurationsrichtlinien.

Sie können Klartext oder formatierten Text aus View Client zu einem View-Desktop kopieren oder umgekehrt, aber der eingefügte Text ist Klartext.

Sie können keine Grafiken kopieren und einfügen. Das Kopieren und Einfügen von Dateien zwischen einem View-Desktop und dem Dateisystem auf Ihrem Client-Computer ist nicht möglich.

Fehlerbehebung für Horizon View Client 5

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

Dieses Kapitel behandelt die folgenden Themen:

Zurücksetzen eines Desktops

Eventuell muss der Desktop zurückgesetzt werden, wenn das Desktop-Betriebssystem nicht mehr reagiert. Beim Zurücksetzen wird der Desktop heruntergefahren und neu gestartet. Nicht gespeicherte Daten gehen verloren.

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 ohne vorheriges Speichern geschlossen.

Sie können den Desktop nur zurücksetzen, wenn Ihr View-Administrator diese Funktion aktiviert hat.

Vorgehensweise

- Verwenden Sie den **Desktop zurücksetzen**-Befehl.

Option	Aktion
Aus dem Desktop-Betriebssystem heraus	Wählen Sie **Desktop > Desktop zurücksetzen** aus der Menüleiste.
Vom Startbildschirm aus (mit Desktop-Symbolen)	Wählen Sie zuerst den Desktop und anschließend **Desktop > Desktop zurücksetzen** aus der Menüleiste aus.

Das Betriebssystem im Remote-Desktop wird neu gestartet. Horizon View Client wird vom Desktop getrennt.

Weiter

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

Deinstallieren von Horizon View Client

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

Die Vorgehensweise beim Deinstallieren von Horizon View Client entspricht der Vorgehensweise bei der Deinstallation anderer Anwendungen.

Wählen Sie z. B. **Anwendungen > Ubuntu Software-Center** und im Abschnitt **Installierte Software vmware-view-client**. Klicken Sie dann auf **Entfernen**.

Nachdem Sie die Deinstallation durchgeführt haben, können Sie die Anwendung von neuem installieren.

Siehe „Installation von Horizon View Client für Linux“, auf Seite 11.

Konfigurieren der USB-Umleitung auf dem Client

6

Mit View Client 1.6 können Sie auf dem Clientsystem eine Konfigurationsdatei zur Angabe der USB-Geräte verwenden, die an einen View-Desktop umgeleitet werden können. Beachten Sie, dass die USB-Komponente nur mit der Drittanbieterversion von View Client für Linux zur Verfügung gestellt wird.

Zum Erreichen der folgenden Ziele können Sie sowohl für View Agent auf dem Remote-Desktop als auch für View Client auf dem lokalen System einzelne USB-Richtlinien konfigurieren:

- Legen Sie bestimmte Einschränkungen für die USB-Gerättypen fest, die View Client zur Umleitung bereitstellt.
- Veranlassen Sie, dass View Agent das Weiterleiten bestimmter USB-Geräte von einem Clientcomputer aus verhindert.
- (View Client 1.7 und höher) Definieren Sie, ob View Client USB-Verbundgeräte für die Umleitung in separate Komponenten aufschlüsseln soll oder nicht.

Wichtig Die Funktion zur USB-Umleitung ist nur verfügbar, wenn View Agent und der View-Verbindungsserver über die View-Version 4.6.1 oder höher verfügen und die Version von View Client verwendet wird, die von Drittanbietern vertrieben wird. Die in diesen Hilfethemen 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 von View Client 1.6 und höher verfügbaren USB-Komponenten zu verwenden, müssen bestimmte Dateien an bestimmten Orten installiert werden, und bestimmte Prozesse müssen so konfiguriert werden, dass sie vor View Client gestartet werden. Diese Details gehen über den Rahmen dieses Dokuments hinaus.

Dieses Kapitel behandelt die folgenden Themen:

Einstellen der USB-Konfigurationseigenschaften

Sie können diese Eigenschaft in einer von mehreren Konfigurationsdateien einstellen.

1 `/etc/vmware/config`. Der Dienst `vmware-view-usbd` untersucht zunächst diese Datei. 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 diese Eigenschaften in der Konfigurationsdatei einzurichten.

```
viewusb.property1 = "value1"
```

HINWEIS Mit diesen Eigenschaften können Sie bestimmen, dass bestimmte Gerätearten umgeleitet werden sollen oder nicht. Es stehen auch Filtereigenschaften zur Verfügung, sodass Sie einige Gerätearten ausschließen und andere einschließen 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 Werte 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 Protokolldatei `/tmp/vmware-root/vmware-view-usbd-*.log` nachsehen, nachdem Sie das USB-Gerät bei laufendem View Client an das lokale System angeschlossen haben. 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 im Hinblick auf die Umleitung von Audiogeräten sicher, dass die Kernelversion Ihres Ubuntu-Systems 3.2.0-27.43 oder später ist. Ubuntu 12.04 besitzt einen Kernel der Version 3.2.0-27.43. Wenn Sie nicht auf diese Kernelversion aktualisieren können, können Sie alternativ den Host-Zugriff 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 View Client versucht, das Audiogerät umzuleiten. Standardmäßig werden Audiogeräte umgeleitet.

Tabelle 6-1. Konfigurationseigenschaften für die USB-Umleitung

Name und Eigenschaft der Richtlinie	Beschreibung
Automatische Geräteaufschlüsselung zulassen Eigenschaft: `viewusb.AllowAutoDeviceSplitting`	(View Client 1.7 und höher) Automatische Aufschlüsselung von USB-Verbundgeräten zulassen. Der Standardwert ist nicht definiert; dies entspricht **`false`**.
VID/PID-Gerät von Aufschlüsselung ausnehmen Eigenschaft: `viewusb.SplitExcludeVidPid`	(View Client 1.7 und höher) Ein USB-Verbundgerät, das durch die Hersteller- und Produkt-ID gekennzeichnet ist, von der Aufschlüsselung ausschließen. Das Format der Einstellung lautet `vid-`*xxx1*`_pid-`*yyy1*`[;vid-`*xxx2*`_pid-`*yyy2*]... Sie müssen die ID-Nummern im hexadezimalen Format angeben. Anstelle einzelner Ziffern in einer ID können Sie auch das Platzhalterzeichen (**`*`**) verwenden. Beispiel: **`vid-0781_pid-55**`** Der Standardwert ist nicht definiert.

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

Name und Eigenschaft der Richtlinie	Beschreibung
VID/PID-Gerät aufschlüsseln Eigenschaft: `viewusb.SplitVidPid`	(View Client 1.7 und höher) Die Komponenten eines USB-Verbundgeräts, das durch die Hersteller- und Produkt-ID gekennzeichnet ist, als separate Geräte behandeln. Das Format der Einstellung lautet `vid-`*xxxx*`_pid-`*yyyy*`([exintf:`*zz*`[;exintf:`*ww*`]])[;...]` Sie können das Schlüsselwort `exintf` verwenden, um einzelne Komponenten von der Umleitung auszuschließen, indem Sie deren Schnittstellennummer angeben. Die ID-Nummern müssen im hexadezimalen und die Schnittstellennummern im dezimalen Format angegeben werden (einschließlich aller führenden Nullen). Anstelle einzelner Ziffern in einer ID können Sie auch das Platzhalterzeichen (*****) 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.
Audioeingabegeräte zulassen Eigenschaft: `viewusb.AllowAudioIn`	Ermöglicht die Umleitung von Audioeingabegeräten. Der Standardwert ist nicht definiert, was so viel wie **`false`** in View Client 2.2 oder später und **`true`** in View Client 2.1 und früher bedeutet. Der Standard wurde geändert, da bei View Client 2.2 die Echtzeit-Audio/Video-Funktion für Audioeingabe- und Videogeräte verwendet wird und da die USB-Umleitung standardmäßig nicht für diese Geräte verwendet wird.
Audioausgabegeräte zulassen Eigenschaft: `viewusb.AllowAudioOut`	Ermöglicht die Umleitung von Audioausgabegeräten. Der Standardwert ist nicht definiert; dies entspricht **`false`**.
HID zulassen Eigenschaft: `viewusb.AllowHID`	Ermöglicht die Umleitung anderer Eingabegeräte neben Tastaturen und Mäusen. Der Standardwert ist nicht definiert; dies entspricht **`true`**.
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; dies entspricht **`true`**.
Ausfallsicherung der Dienstbeschreibung zulassen Eigenschaft: `viewusb.AllowDevDescFailsafe`	Ermöglicht die Umleitung der Geräte, auch wenn View 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; dies entspricht **`false`**.
Tastatur- und Mausgeräte zulassen Eigenschaft: `viewusb.AllowKeyboardMouse`	Ermöglicht die Umleitung von Tastaturen mit integrierten Zeigegeräten (zum Beispiel Maus, Trackball, Touchpad). Der Standardwert ist nicht definiert; dies entspricht **`false`**.
Smartcards zulassen Eigenschaft: `viewusb.AllowSmartcard`	Ermöglicht die Umleitung von Smartcard-Geräten. Der Standardwert ist nicht definiert; dies entspricht **`false`**.
Videogeräte zulassen Eigenschaft: `viewusb.AllowVideo`	Ermöglicht die Umleitung von Videogeräten. Der Standardwert ist nicht definiert, was so viel wie **`false`** in View Client 2.2 oder später und **`true`** in View Client 2.1 und früher bedeutet. Der Standard wurde geändert, da bei View Client 2.2 die Echtzeit-Audio/Video-Funktion für Audioeingabe- und Videogeräte verwendet wird und da die USB-Umleitung standardmäßig nicht für diese Geräte verwendet wird.

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

Name und Eigenschaft der Richtlinie	Beschreibung
Herunterladen der Remote-Konfiguration deaktivieren Eigenschaft: `viewusb.DisableRemoteConfig`	Deaktiviert die Verwendung der View Agent-Einstellungen beim Ausführen eines USB-Gerät-Filterungsvorgangs. Der Standardwert ist nicht definiert; dies entspricht **`false`**.
Alle Geräte ausschließen Eigenschaft: `viewusb.ExcludeAllDevices`	Schließt alle USB-Geräte von der Umleitung aus. Ist diese Option auf **`true`** gesetzt, können Sie die Umleitung bestimmter Geräte oder Gerätefamilien über andere Richtlinieneinstellungen zulassen. Ist diese Option auf **`false`** gesetzt, können Sie die Umleitung bestimmter Geräte oder Gerätefamilien über andere Richtlinieneinstellungen verhindern. Wenn Sie den Wert von `Exclude All Devices` in View Agent auf **`true`** setzen und diese Einstellung an View Client weitergegeben wird, überschreibt die View Agent-Einstellung die View Client-Einstellung. Der Standardwert ist nicht definiert; dies entspricht **`false`**.
Gerätefamilie ausschließen Eigenschaft: `viewusb.ExcludeFamily`	Schließt bestimmte Gerätefamilien von der Umleitung aus. Das Format der Einstellung lautet *family_name_1*[`;`*family_name_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 die automatische Geräteaufschlüsselung deaktiviert haben, untersucht View die Gerätefamilie des gesamten USB-Verbundgeräts. Der Standardwert ist nicht definiert.
VID/PID-Gerät ausschließen Eigenschaft: `viewusb.ExcludeVidPid`	Schließt Geräte mit definierten Hersteller- und Produkt-IDs von der Umleitung aus. Das Format der Einstellung lautet `vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]... Sie müssen die ID-Nummern im hexadezimalen Format angeben. Anstelle einzelner Ziffern in einer ID können Sie auch das Platzhalterzeichen (**`*`**) verwenden. Beispiel: **`vid-0781_pid-****;vid-0561_pid-554c`** Der Standardwert ist nicht definiert.
Pfad ausschließen Eigenschaft: `viewusb.ExcludePath`	Schließt Geräte unter bestimmten Hubs oder Portpfaden von der Umleitung aus. Das Format der Einstellung lautet `bus-`*x1*[`/`*y1*]...`_port-`*z1*[`;bus-`*x2*[`/`*y2*]...`_port-`*z2*]... Sie müssen die Bus- und Portnummern im hexadezimalen Format angeben. Das Platzhalterzeichen kann in Pfaden nicht verwendet werden. Beispiel: **`bus-1/2/3_port-02;bus-1/1/1/4_port-ff`** Der Standardwert ist nicht definiert.
Gerätefamilie einschließen Eigenschaft: `viewusb.IncludeFamily`	Schließt Gerätefamilien ein, die umgeleitet werden können. Das Format der Einstellung lautet *family_name_1*[`;`*family_name_2*]... Beispiel: **`storage (Speicher)`** Der Standardwert ist nicht definiert.
Pfad einschließen Eigenschaft: `viewusb.IncludePath`	Schließt Geräte unter bestimmten Hubs oder Portpfaden ein, die umgeleitet werden können. Das Format der Einstellung lautet `bus-`*x1*[`/`*y1*]...`_port-`*z1*[`;bus-`*x2*[`/`*y2*]...`_port-`*z2*]... Sie müssen die Bus- und Portnummern im hexadezimalen Format angeben. Das Platzhalterzeichen kann in Pfaden nicht verwendet werden. Beispiel: **`bus-1/2_port-02;bus-1/7/1/4_port-0f`** Der Standardwert ist nicht definiert.
VID/PID-Gerät einschließen Eigenschaft: `viewusb.IncludeVidPid`	Schließt Geräte mit definierten Hersteller- und Produkt-IDs ein, die umgeleitet werden können. Das Format der Einstellung lautet `vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]... Sie müssen die ID-Nummern im hexadezimalen Format angeben. Anstelle einzelner Ziffern in einer ID können Sie auch das Platzhalterzeichen (**`*`**) verwenden. Beispiel: **`vid-0561_pid-554c`** Der Standardwert ist nicht definiert.

Zusätzliche Beispiele

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

1 Einfügen der meisten Geräte der Familie der Mausgeräte:

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

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

2 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 Remotedesktop 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 View 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 Remotedesktop eingestellten Richtlinien zusammengeführt oder von diesen überschrieben werden. Informationen darüber, wie die 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 VMware Horizon View-*.

USB-Gerätefamilien

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

Tabelle 6-2. USB-Gerätefamilien

Gerätefamilienname	Beschreibung
`audio (Audiowiedergabe)`	Ein Audioeingabe- oder Audioausgabegerät beliebigen Typs.
`audio-in (Audio-Eingabe)`	Audioeingabegeräte, z. B. Mikrofone.

Tabelle 6-2. USB-Gerätefamilien (Fortsetzung)

Gerätefamilien-name	Beschreibung
audio-out (Audio-Ausgabe)	Audioausgabegeräte, z. B. Lautsprecher und Kopfhörer.
bluetooth (Bluetooth)	Per Bluetooth verbundene Geräte.
comm	Kommunikationsgeräte wie Modems und kabelgebundene Netzwerkadapter.
hid (Eingabegeräte (Human Interface Devices))	Eingabegeräte (Human Interface Devices) außer Tastaturen und Zeigegeräten.
hid-bootable (Eingabegeräte startfähig)	Eingabegeräte (Human Interface Devices), die beim Start verfügbar sind, außer Tastaturen und Zeigegeräte.
imaging (Bildverarbeitung)	Bildverarbeitungsgeräte, z. B. Scanner.
keyboard (Tastatur)	Tastaturgerät.
mouse (Maus)	Zeigegerät, z. B. eine Maus.
Andere	Familie nicht angegeben.
pda (PDA)	PDA (Personal Digital Assistant)
physical (physisch)	Force-Feedback-Geräte, z. B. Force-Feedback-Joysticks.
printer (Drucker)	Druckergeräte.
security (Sicherheit)	Sicherheitsgeräte, z. B. Fingerabdruckleser.
smart-card (Smartcard)	SmartCard-Geräte.
Speicher	Massenspeichergeräte wie z. B. Flash-Laufwerke und externe Festplattenlaufwerke.
unknown (unbekannt)	Familie nicht bekannt.
vendor (Hersteller)	Geräte mit herstellerspezifischen Funktionen.
video (Video)	Videoeingabegeräte.
wireless (drahtlos)	Drahtlose Netzwerkadapter.
wusb	Drahtlose USB-Geräte.

Hinweis In den Versionen vor View 5.1 bezog View Client für Windows die Informationen zur Gerätefamilie von dem Gerätetreiber, den Sie auf dem Clientcomputer installierten. Unter View 5.1 müssen Sie den Gerätetreiber nicht auf einem Windows-Clientcomputer installieren. View Client liest die Gerätefamilie vom Gerät selbst und nicht vom Gerätetreiber. Die Firmware auf einem USB-Gerät definiert normalerweise die Familie des Geräts und seine beabsichtigte Funktionalität, jedoch geben nicht alle Geräte den richtigen Wert für die Familie an.

Linuxbasierte Thin Clients beziehen die Information zur Gerätefamilie schon immer vom Gerät selbst.

Verwenden der Befehlszeilenoption aus View Client 1.5 zur Umleitung von USB-Geräten

Sie können die Befehlszeilenoption `--usb=` des Befehls `vmware-view` verwenden, um zu konfigurieren, welche USB-Geräte auf einen View-Desktop umgeleitet werden können. Beachten Sie, dass die USB-Befehlszeilenoption nur für die von anderen Anbietern bereitgestellte Version von View Client für Linux und nur für View Client 1.5 verfügbar ist.

WICHTIG Wenn Sie mit View Client 1.6 oder höher arbeiten, müssen Sie statt der Befehlszeilenoption `--usb=` zur Konfiguration der USB-Umleitung eine Konfigurationsdatei verwenden. Siehe Kapitel 6, „Konfigurieren der USB-Umleitung auf dem Client“, auf Seite 57.

Die Argumente der Option `--usb=` werden an den USB-Umleitungsbefehl `vmware-view-usb` gesendet.

Mit dem folgenden Beispiel wird die Protokollierung auf Ablaufebene aktiviert:

```
vmware-view --usb=log:trace
```

Sie können mehrere Instanzen der Option `--usb` für jede einzustellende Option `vmware-view-usb` angeben. Mit dem folgenden Beispiel wird die Protokollierung auf Debugging-Ebene aktiviert und ein durch seine ID angegebenes Gerät ausgeschlossen:

```
 vmware-view --usb=log:debug
--usb=exid:vid0012pid0034
```

In der folgenden Tabelle werden die mit der Option `--usb` verwendbaren Argumente aufgelistet.

Tabelle 6-3. USB-Umleitungsoptionen

Option	Beschreibung
`disable-boot-fwd`	Deaktiviert die Erkennung und Filterung des Startgeräts durch den View-USB-Client. Durch Festlegen dieser Option werden alle USB-Geräte weitergeleitet, auch das Gerät, über welches das Clientsystem gestartet wird.

`ex:`*Gerät1*`[,`*Gerät2*`]...`	Schließt eine Liste benannter Geräte von der Weiterleitung ein. Beispiel:
	`vmware-view`
	`--usb=ex:"flash 1"`

`exfa:`*Gerätefamilie1*`[,`*Gerätefamilie2*`]...`	Schließt eine Liste benannter Gerätefamilien von der Weiterleitung aus. Beispiel:
	`vmware-view`
	`--usb=exfa:storage`

`exid:`*Geräte-ID1*`[,`*Geräte-ID2*`]...`	Schließt eine Liste von Geräten von der Weiterleitung aus. Die Geräte werden dabei durch die Hexadezimalwerte ihrer Hersteller- und Produkt-IDs angegeben, und zwar in dem Format `vid`*xxxx*`pid`*xxxx*. . Zum Beispiel:
	`vmware-view`
	`--usb=exid:vid1e2fpid5a1e`

`expt:`*Gerätpfad1*`[,`*Gerätepfad2*`]...`	Schließt eine Liste von Geräten von der Weiterleitung aus. Die Geräte werden dabei durch die Dezimalwerte ihrer Bus- und Portwerte angegeben, und zwar im Format `bus`*n*`port`*n*. Zum Beispiel: `vmware-view --usb=expt:bus1port4,bus5port3`

`in:`*Gerät1*`[,`*Gerät2*`]...`	Schließt eine Liste benannter Geräte in die Weiterleitung ein. Beispiel:
	`vmware-view`
	`--usb=in:"flash 1"`

`infa:`*Gerätefamilie1*`[,`*Gerätefamilie2*`]...`	Schließt eine Liste benannter Gerätefamilien in die Weiterleitung ein. Beispiel:
	`vmware-view`
	`--usb=infa:storage`

Tabelle 6-3. USB-Umleitungsoptionen (Fortsetzung)

Option	Beschreibung

`inid:`*Geräte-ID1*`[,`*Geräte-ID2*`]...`	Schließt eine Liste von Geräten in die Weiterleitung ein. Die Geräte werden dabei durch die Hexadezimalwerte ihrer Hersteller- und Produkt-IDs angegeben, und zwar im Format `vid`*xxxx*`pid`*xxxx*. . Beispiel:
	`vmware-view`
	`--usb=inid:vid27f8pid2a1b`

`inpt:`*Gerätpfad1*`[,`*Gerätpfad2*`]...`	Schließt eine Liste von Geräten in die Weiterleitung ein. Die Geräte werden dabei durch die Dezimalwerte ihrer Bus- und Portwerte angegeben, und zwar im Format `bus`*n*`port`*n*. Zum Beispiel:
	`vmware-view`
	`--usb=inpt:bus3port1,bus4port2`

`log:{debug|error|info|trace}`	Legt die Protokollierungsebene für `vmware-view-usb:trace`, `debug`, `info` (Standardeinstellung) oder `error` nach abnehmender Detailtiefe fest. Die Protokolldatei (`backendLog.txt`) wird in `/tmp/vmware-`*`username`*`/vmware-view-usb-`*`pid`*`.log` geschrieben. Beispiel:
	`vmware-view`
	`--usb=log:error`

Die Rangfolge zum Ein- oder Ausschließen von Geräten lautet, in absteigender Reihenfolge, wie folgt:

1 `expt` (schließt durch Bus und Port identifizierte Geräte aus)

2 `inpt` (schließt durch Bus und Port identifizierte Geräte ein)

3 `ex` (schließt eine Liste benannter Geräte aus)

4 `in` (schließt eine Liste benannter Geräte ein)

5 `exid` (schließt durch Hersteller- und Produkt-ID identifizierte Geräte aus)

6 `inid` (schließt durch Hersteller- und Produkt-ID identifizierte Geräte ein)

7 `exfa` (schließt eine Liste benannter Gerätefamilien aus)

8 `infa` (schließt eine Liste benannter Gerätefamilien ein)

Im folgenden Beispiel werden alle Speicherfamiliengeräte mit Ausnahme eines Geräts ausgeschlossen, das durch seine ID definiert wird:

```
vmware-view --usb=exfa:storage
--usb=inid:vid1812pid1492
```

Im Folgenden finden Sie eine Liste mit Klassen von USB-Gerätefamilien, die Sie für die Optionen `infa` und `exfa` verwenden können.

`audio (Audio)`	`printer (Drucker)`
`bluetooth (Bluetooth)`	`security (Sicherheit)`
`comm (Komm)`	`smart-card (Smartcard)`
`hid (Eingabegeräte (Human Interface Devices))`	`storage (Speicher)`
`hid-bootable (Eingabegeräte startfähig)`	`unknown (unbekannt)`
`hub (Hub)`	`vendor (Hersteller)`
`imaging (Bildverarbeitung)`	`video (Video)`
`other (andere)`	`wireless (drahtlos)`
`pda (PDA)`	`wusb`
`physical (physisch)`	

Index

U

V

W

X

Z