

Verwendung von VMware View Client für Linux

September 2012
View Client für Linux

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-000780-02

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

Copyright © 2012 VMware, Inc. Alle Rechte vorbehalten. Dieses Produkt ist durch Urheberrechtsgesetze, internationale Verträge und mindestens eines der unter <http://www.vmware.com/go/patents-de> aufgeführten Patente geschützt.

VMware ist eine eingetragene Marke oder Marke der VMware, Inc. in den USA und/oder anderen Ländern. Alle anderen in diesem Dokument erwähnten Bezeichnungen und Namen sind unter Umständen markenrechtlich geschützt.

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

- 1 Verwendung von VMware View Client für Linux 5
- 2 Systemanforderungen und Installation 7
 - Systemanforderungen für Linux-Clients 7
 - Unterstützte View-Desktop-Betriebssysteme 8
 - Vorbereitung des View-Verbindungsservers für View Client 8
 - Installation von View Client für Linux 9
- 3 Konfigurieren von View Client für die Endbenutzer 11
 - Verwenden von URIs zur Konfiguration von View Client 11
 - Verwenden der View Client-Befehlszeilenschnittstelle und -Konfigurationsdateien 15
 - Aktivieren des FIPS-Modus auf dem Client 23
 - Konfigurieren des PCoIP-Client-Bildcache 24
- 4 Verwaltung der Serververbindungen und Desktops 27
 - Erstmalige Anmeldung an einem View-Desktop 27
 - Zertifikatsprüfungsmodi für View Client 29
 - Wechseln zwischen Desktops 30
 - Abmelden oder Trennen von Desktops 30
 - Rollback eines Desktops 31
- 5 Verwendung eines Microsoft Windows-Desktops auf einem Linux-System 33
 - Funktionsunterstützungs-Matrix 33
 - Internationalisierung 34
 - Tastaturen und Monitore 34
 - Kopieren und Einfügen von Text 35
- 6 Fehlerbehebung für View Client 37
 - Zurücksetzen eines Desktops 37
 - Deinstallation von View Client 38
- 7 Konfigurieren der USB-Umleitung auf dem Client 39
 - Festlegen der USB-Konfigurationseigenschaften 39
 - USB-Gerätefamilien 42
 - Verwenden der Befehlszeilenoption aus View Client 1.5 zur Umleitung von USB-Geräten 43
- Index 47

Verwendung von VMware View Client für Linux

1

Dieses Handbuch, *Verwendung von VMware View Client für Linux*, bietet Informationen über die Installation und Verwendung der VMware® View™-Software auf einem Linux-Clientsystem zur Verbindungsherstellung mit einem View-Desktop im Rechenzentrum.

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

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

HINWEIS Dieses Dokument gehört zu der View Client für Linux-Instanz, die VMware auf Ubuntu zur Verfügung stellt. Darüber hinaus bieten verschiedene VMware-Partner Thin Client-Geräte für VMware View-Bereitstellungen. Die Funktionen, die für das jeweilige Thin Client-Gerät verfügbar sind, sowie die unterstützten Betriebssysteme, werden durch den Hersteller, das Modell und die Konfiguration festgelegt, die ein Unternehmen verwendet. Informationen über Hersteller und Modelle für Thin Client-Geräte finden Sie im [VMware-Kompatibilitätshandbuch](#), das auf der VMware-Website zur Verfügung steht.

Systemanforderungen und Installation

2

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

- [Systemanforderungen für Linux-Clients](#) auf Seite 7
Sie können View Client für Linux auf PCs installieren, die das Betriebssystem Ubuntu Linux 10.04 oder 12.04 verwenden.
- [Unterstützte View-Desktop-Betriebssysteme](#) auf Seite 8
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.
- [Vorbereitung des View-Verbindungsservers für View Client](#) auf Seite 8
Administratoren müssen bestimmte Aufgaben durchführen, um Endbenutzern die Verbindung zu den View-Desktops zu ermöglichen.
- [Installation von View Client für Linux](#) auf Seite 9
Endbenutzer öffnen View Client, um von einem physischen Computer eine Verbindung mit virtuellen Desktops herzustellen. View Client für Linux wird mit Ubuntu 10.04- oder 12.04-Systemen ausgeführt. Sie können es mithilfe von Synaptic Package Manager installieren.

Systemanforderungen für Linux-Clients

Sie können View Client für Linux auf PCs installieren, die das Betriebssystem Ubuntu Linux 10.04 oder 12.04 verwenden.

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

Modell	Intel-basierter Desktop- oder Laptopcomputer
Arbeitsspeicher	Mindestens 2 GB Arbeitsspeicher (RAM)
Betriebssysteme	View Client 1.6: Ubuntu Linux 10.04 oder 12.04 mit 32 Bit View Client 1.5: Ubuntu Linux 10.04 oder 10.10 mit 32 Bit
View-Verbindungs- server , Sicherheitsserver und View Agent	4.6.1 oder höher 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 VMware View

PCoIP oder RDP

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:

$$20\text{MB} + (24 * (\# \text{ monitors}) * (\text{monitor width}) * (\text{monitor height}))$$

Als grobes Maß können Sie die folgenden Berechnungen verwenden:

1 monitor: 1600 x 1200: 64MB

2 monitors: 1600 x 1200: 128MB

3 monitors: 1600 x 1200: 256MB

Hardwareanforderungen für RDP

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

Unterstützte View-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 der unterstützten Gastbetriebssysteme finden Sie im Hilfethema „Unterstützte Betriebssysteme für View Agent“ der Dokumentation zur Installation von VMware View 4.6.x oder 5.x.

Vorbereitung des View-Verbindungsservers für View Client

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

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

- Stellen Sie bei Verwendung eines Sicherheitsservers, wie von VMware empfohlen, sicher, dass ein View-Verbindungsserver der Version 4.6.1 oder höher und ein View-Sicherheitsserver der Version 4.6.1 oder höher verwendet werden. Siehe die Dokumentation *Installation von VMware View* zu View 4.6 oder höher.
- 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]**.

- Stellen Sie sicher, dass ein virtueller Desktop-Pool erstellt wurde und das zu verwendende Benutzerkonto über Zugriffsberechtigungen für diesen View-Desktop verfügt. Siehe die Hilfethemen zur Erstellung von Desktop-Pools in der Dokumentation *VMware View-Verwaltung*.

- Zum Verwenden der zweistufigen Authentifizierung für 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 im Thema zur zweistufigen Authentifizierung der Dokumentation *Verwaltung von VMware View*.

Installation von View Client für Linux

Endbenutzer öffnen View Client, um von einem physischen Computer eine Verbindung mit virtuellen Desktops herzustellen. View Client für Linux wird mit Ubuntu 10.04- oder 12.04-Systemen ausgeführt. Sie können es mithilfe von Synaptic Package Manager installieren.

Voraussetzungen

- Stellen Sie sicher, dass das Clientsystem ein unterstütztes Betriebssystem verwendet. Siehe „[Systemanforderungen für Linux-Clients](#)“, auf Seite 7.
- 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 vorab sicherstellen, dass der entsprechende RDP-Client installiert ist. Siehe „[Systemanforderungen für Linux-Clients](#)“, auf Seite 7.

Vorgehensweise

- 1 Aktivieren Sie Canonical Partners auf Ihrem Linux-Laptop oder -PC.
 - a Wählen Sie aus der Ubuntu-Menüleiste die Optionen **[System] > [Verwaltung] > [Update-Manager]** aus.
 - b Klicken Sie auf die Schaltfläche **[Einstellungen]** und geben Sie das Kennwort zur Durchführung administrativer Aufgaben an.
 - c Klicken Sie im Softwarequellen-Dialogfeld auf die Registerkarte **[Andere Software]** und markieren Sie das Kontrollkästchen **[Canonical Partners]**, um das Archiv für die Software auszuwählen, die Canonical für seine Partner paketiert.
 - d Klicken Sie auf **[Schließen]** und folgen Sie den Anweisungen zur Aktualisierung der Liste der Pakete.
- 2 Wählen Sie aus der Ubuntu-Menüleiste die Optionen **[System] > [Verwaltung] > [Synaptic Package Manager]** aus.
- 3 Klicken Sie auf **[Suchen]** und suchen Sie nach **vmware**.
- 4 Markieren Sie in der zurückgegebenen Liste der Pakete das Kontrollkästchen neben **[vmware-view-client]** und wählen Sie **[Für Installation markieren]** aus.
Markieren Sie nicht das Kontrollkästchen für den geöffneten Client.
- 5 Klicken Sie auf **[Anwenden]** in der Symbolleiste.
VMware View Client für Linux wurde installiert.
- 6 Um festzustellen, ob die Installation erfolgreich war, sollten Sie sicherstellen, dass das Anwendungssymbol **[VMware View]** im Menü **[Anwendungen] > [Internet]** angezeigt wird.

Weiter

Starten Sie View Client und stellen Sie sicher, dass Sie sich am korrekten virtuellen Desktop anmelden können. Siehe „[Erstmalige Anmeldung an einem View-Desktop](#)“, auf Seite 27.

Konfigurieren von View Client für die Endbenutzer

3

View Client bietet mehrere Konfigurationsmechanismen zur Vereinfachung der Anmeldung und Desktopauswahl und Verbesserung der Benutzererfahrung, jedoch auch zur Durchsetzung der Sicherheitsrichtlinien.

Dieses Kapitel behandelt die folgenden Themen:

- [„Verwenden von URIs zur Konfiguration von View Client“](#), auf Seite 11
- [„Verwenden der View Client-Befehlszeilenschnittstelle und -Konfigurationsdateien“](#), auf Seite 15
- [„Aktivieren des FIPS-Modus auf dem Client“](#), auf Seite 23
- [„Konfigurieren des PCoIP-Client-Bildcache“](#), auf Seite 24

Verwenden von URIs zur Konfiguration von View Client

Unter Verwendung sogenannter Uniform Resource Identifiers (URIs) können Sie eine Webseite oder E-Mail mit verschiedenen Verknüpfungen erstellen, auf die die Endbenutzer zum Start von View Client, zur Verbindung mit dem View-Verbindungsserver oder zum Start eines bestimmten Desktops mit bestimmten Konfigurationsoptionen klicken.

Mit View Client 1.6 und höher können Sie die Anmeldung am View-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
- Desktopaktionen, darunter „Zurücksetzen“, „Abmelden“ und „Rollback ausführen“
- Anzeigeprotokoll

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

HINWEIS Sie können URIs nur zum Start von View Client verwenden, wenn View Client 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 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 View Client die folgende Syntax:

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

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

WICHTIG In allen Teilen müssen Nicht-ASCII-Zeichen vorab gemäß UTF-8 codiert werden [STD63]. Anschließend muss jedes Oktett der entsprechenden UTF-8-Sequenz als Prozentwert codiert werden, damit es als URI-Zeichen dargestellt werden kann.

Informationen zur Codierung von ASCII-Zeichen finden Sie in der URL-Codierungsreferenz unter http://www.w3schools.com/tags/ref_urlencode.asp.

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@server-address
```

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:

```
server-address:port-number
```

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:

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

Unterstützte Abfragen

In diesem Abschnitt werden die Abfragen aufgeführt, die für diesen 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 View Client*.

action

Tabelle 3-1. 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.
reset	Führt den angegebenen Desktop herunter und startet ihn neu. Nicht gespeicherte Daten gehen verloren. Das Zurücksetzen eines View-Desktops kommt dem Betätigen der Schaltfläche „Zurücksetzen“ auf einem physischen PC gleich.
logoff	Meldet den Benutzer vom Gastbetriebssystem auf dem View-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 View Client-Versionen von Drittanbietern verfügbar.) Verbindet ein USB-Gerät mit dem Desktop im Vordergrund, wenn Sie das Gerät anschließen. 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 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 View-Desktops fest. Zur Verwendung dieser Abfrage müssen Sie die Abfrage action auf start-session setzen oder ohne die Abfrage action arbeiten.

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

Wert	Beschreibung
windowSmall	Kleines Fenster.
WxH	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 sich mit dem View-Desktop verbindet.

Beispiele für vmware-view-URIs

Sie können mithilfe des `vmware-view`-URI-Schemas Hypertext-Verknüpfungen oder -Schaltflächen generieren und diese Verknüpfungen in E-Mails oder auf eine Webseite einfügen. Ihre Endbenutzer können dann über diese Links zum Beispiel einen bestimmten View-Desktop mit den von Ihnen angegebenen Startoptionen starten.

URI-Syntaxbeispiele

Auf jedes URI-Beispiel folgt eine Beschreibung des Inhalts, der dem Endbenutzer nach dem Klick auf die URI-Verknüpfung angezeigt wird.

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

View Client wird gestartet und stellt eine Verbindung mit dem Server `view.mycompany.com` her. Im Anmeldefeld wird der Benutzer zur Angabe des Benutzernamens, des Domänennamens und des Kennworts aufgefordert. Nach erfolgreicher Anmeldung verbindet sich der Client mit dem Desktop, dessen Anzeigename als **[Primärer Desktop]** angezeigt wird, und der Benutzer wird am Gastbetriebssystem angemeldet.

HINWEIS Es wird das Standard-Anzeigeprotokoll und die Standard-Fenstergröße verwendet. Das Standard-Anzeigeprotokoll ist PCoIP. Die Standard-Fenstergröße ist „Vollbild“.

Sie können die Standardeinstellungen ändern. Siehe „[Verwenden der View Client-Befehlszeilenschnittstelle und -Konfigurationsdateien](#)“, auf Seite 15.

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

Dieser URI hat den gleichen Effekt wie das vorangehende Beispiel, verwendet jedoch den nicht standardmäßigen Port 7555 für den View-Verbindungsserver. (Der Standard-Port ist 443.) Da ein Desktop-Bezeichner angegeben 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`

View Client wird gestartet und stellt eine Verbindung mit dem Server `view.mycompany.com` her. Im Anmeldefeld wird in das Textfeld **[Benutzername]** automatisch der Name **[fred]** eingetragen. Der Benutzer muss den Domänennamen und das Kennwort angeben. Nach erfolgreicher Anmeldung verbindet sich der Client mit dem Desktop, dessen Anzeigename als **[Finance Desktop]** angezeigt wird, und der Benutzer wird am Gastbetriebssystem angemeldet. Die Verbindung verwendet das PCoIP-Anzeigeprotokoll.

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

View Client wird gestartet und stellt eine Verbindung mit dem Server `view.mycompany.com` her. Im Anmeldefeld wird in das Textfeld **[Benutzername]** automatisch der Name **[fred]** eingegeben, und in das Textfeld **[Domäne]** wird **[mycompany]** eingetragen. Der Benutzer muss nur ein Kennwort eingeben. Nach erfolgreicher Anmeldung verbindet sich der Client mit dem Desktop, dessen Anzeigename als **[Finance Desktop]** angezeigt wird, und der Benutzer wird am Gastbetriebssystem angemeldet.

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

View Client wird gestartet, und der Benutzer wird zur Anmeldeaufforderung weitergeleitet, die zur Verbindung mit dem Server `view.mycompany.com` verwendet wird.

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

View Client wird gestartet und stellt eine Verbindung mit dem Server `view.mycompany.com` her. Im Anmeldefeld wird der Benutzer zur Angabe des Benutzernamens, des Domänennamens und des Kennworts aufgefordert. Nach erfolgreicher Anmeldung zeigt View Client ein Dialogfeld an, das den Benutzer zur Bestätigung des Zurücksetzungsvorgangs für den primären Desktop auffordert. Nach dem Zurücksetzen wird dem Benutzer je nach View Client-Typ über eine Meldung angezeigt, ob das Zurücksetzen erfolgreich war.

HINWEIS Diese Aktion ist nur verfügbar, wenn der View-Administrator diese Funktion für Endbenutzer aktiviert hat.

7 `vmware-view://`

View Client wird gestartet, und der Benutzer wird zu der Seite weitergeleitet, auf der er die Adresse einer View-Verbindungsserverinstanz eingeben muss.

HTML-Code-Beispiele

Sie können URIs zur Generierung von Hypertext-Verknüpfungen und -Schaltflächen verwenden, die Sie in E-Mails oder auf Webseiten einfügen können. In den folgenden Beispielen wird gezeigt, wie der URI aus dem ersten URI-Beispiel zur Codierung einer Hypertext-Verknüpfung mit dem Namen **[Test-Verknüpfung]** und einer Schaltfläche mit dem Namen **[Test-Schaltfläche]** verwendet werden kann.

```
<html>
<body>

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

Zur Verbesserung der Benutzerfreundlichkeit verfügen so gut wie alle Konfigurationseinstellungen sowohl über die Eigenschaft *key=value* als auch über einen entsprechenden Befehlszeilenoptionsnamen. Für einige Einstellungen ist zwar eine Befehlszeilenoption verfügbar, doch es kann keine entsprechende Eigenschaft in einer Konfigurationsdatei festgelegt werden. Für einige andere Einstellungen muss eine Eigenschaft festgelegt werden, da keine Befehlszeilenoption verfügbar ist.

WICHTIG Einige Befehlszeilenoptionen und Konfigurationsschlüssel, z. B. die für die USB-Umleitung und MMR, stehen nur für die von anderen Anbietern bereitgestellte Version von View Client zur Verfügung. Weitere Informationen zu diesen Partnern finden Sie im [VMware-Kompatibilitätshandbuch](#).

Tabelle 3-3. View Client-Befehlszeilenoptionen und -Konfigurationsdateischlüssel

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung
view.allMonitors	--allmonitors	Blendet das Betriebssystem des Hosts aus und öffnet die View Client-Benutzeroberfläche auf allen Monitoren, die beim Start von View Client verbunden sind, im Vollbildmodus. Geben Sie beim Festlegen des Konfigurationsschlüssels „TRUE“ oder „FALSE“ an. Die Standardeinstellung ist „FALSE“.
view.allowDefaultBroker	-l, --lockServer Beispiel: --lockServer -s view.company.com	Durch Verwendung dieser Befehlszeilenoption oder Festlegen der Eigenschaft auf „FALSE“ wird das Feld [Servername] deaktiviert, außer wenn der Client noch nie eine Verbindung zu einem Server hergestellt hat und keine Serveradresse in der Befehlszeile oder Einstellungsdatei angegeben ist.
view.autoConnectBroker	Keine	Stellt automatisch eine Verbindung mit der zuletzt verwendeten View Server-Instanz her, außer wenn die Konfigurationseigenschaft <code>view.defaultBroker</code> festgelegt ist oder die Befehlszeilenoption <code>--serverURL=</code> verwendet wird. Geben Sie „TRUE“ oder „FALSE“ an. Die Standardeinstellung ist „FALSE“. Das Festlegen dieser Eigenschaft und der Eigenschaft <code>view.autoConnectDesktop</code> auf „TRUE“ ist gleichbedeutend mit dem Festlegen der Eigenschaft <code>view.nonInteractive</code> auf „TRUE“.
view.autoConnectDesktop	Keine	Stellt automatisch eine Verbindung mit dem zuletzt verwendeten View-Desktop her, außer wenn die Konfigurationseigenschaft <code>view.defaultDesktop</code> festgelegt ist oder die Befehlszeilenoption <code>--desktopName=</code> verwendet wird. Geben Sie „TRUE“ oder „FALSE“ an. Die Standardeinstellung ist „FALSE“. Das Festlegen dieser Eigenschaft und der Eigenschaft <code>view.autoConnectBroker</code> auf „TRUE“ ist gleichbedeutend mit dem Festlegen der Eigenschaft <code>view.nonInteractive</code> auf „TRUE“.

Tabelle 3-3. View Client-Befehlszeilenoptionen und -Konfigurationsdateischlüssel (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung
view.defaultBroker	-s, --serverURL= Beispiele: --serverURL=https://view.company.com -s view.company.com --serverURL=view.company.com:1443	Fügt den von Ihnen im Feld [Servername] angegebenen Namen in View Client hinzu. Geben Sie einen vollqualifizierten Domänennamen an. Sie können zudem auch eine Portnummer angeben, wenn Sie nicht den Standardport 443 verwenden. Als Standard ist der zuletzt verwendete Wert eingestellt.
view.defaultDesktop	-n, --desktopName=	Gibt an, welcher Desktop verwendet werden soll, wenn <code>autoConnectDesktop</code> auf „TRUE“ festgelegt ist und der Benutzer Zugriff auf mehrere Desktops hat. Dies ist der Name, der Ihnen im Dialogfeld zur Desktop-Auswahl angezeigt wird. Der Name entspricht üblicherweise dem Poolnamen.
view.defaultDesktopHeight	Keine	Gibt die Standardhöhe des Fensters für den View-Desktop in Pixel an.
view.defaultDesktopSize	--desktopSize= Beispiele: --desktopSize="1280x800" --desktopSize="all"	Legt die Standardgröße des Fensters für den View-Desktop fest: <ul style="list-style-type: none"> ■ Zur Verwendung aller Monitore müssen Sie die Eigenschaft auf „1“ festlegen oder das Befehlszeilenargument „all“ verwenden. ■ Zur Verwendung des Vollbildmodus auf einem Monitor müssen Sie die Eigenschaft auf „2“ festlegen oder das Befehlszeilenargument „full“ verwenden. ■ Zur Verwendung eines großen Fensters müssen Sie die Eigenschaft auf „3“ festlegen oder das Befehlszeilenargument „large“ verwenden. ■ Zur Verwendung eines kleinen Fensters müssen Sie die Eigenschaft auf „4“ festlegen oder das Befehlszeilenargument „small“ verwenden. ■ Zur Festlegung einer benutzerdefinierten Größe müssen Sie die Eigenschaft auf „5“ festlegen und anschließend auch die Eigenschaften <code>view.defaultDesktopWidth</code> und <code>view.defaultDesktopHeight</code> festlegen. Alternativ können Sie die Breite mal Höhe in Pixel in der Befehlszeile mit "widthxheight" angeben.
view.defaultDesktopWidth	Keine	Gibt die Standardbreite des Fensters für den View-Desktop in Pixel an.
view.defaultDomain	-d, --domainName=	Legt den Domänennamen fest, den View Client für alle Verbindungen verwendet, und fügt den Domänennamen hinzu, den Sie im Feld [Domänenname] im View Client-Authentifizierungsdialogfeld angeben.

Tabelle 3-3. View Client-Befehlszeilenoptionen und -Konfigurationsdateischlüssel (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung
view.defaultPassword	-p "-", --password="-"	<p>Geben Sie immer "-" an, um das Kennwort aus stdin zu lesen.</p> <p>Legt das Kennwort fest, das View Client für alle Verbindungen verwendet, und fügt das Kennwort zum Feld [Kennwort] im View Client-Authentifizierungsdialogfeld hinzu, wenn der View-Verbindungs-server die Kennwortauthentifizierung akzeptiert.</p> <p>HINWEIS Ein leeres Kennwort kann nicht verwendet werden. Folgendes können Sie also nicht festlegen: --password=""</p>
view.defaultProtocol	--protocol=	<p>Gibt an, welches Anzeigeprotokoll verwendet werden soll. Geben Sie „PCOIP“ oder „RDP“ an. Bei diesen Werten wird zwischen Groß- und Kleinschreibung unterschieden. Wenn Sie beispielsweise rdp eingeben, wird der Standard als Protokoll verwendet. Bei dem Standard handelt es sich um die in View Administrator unter den Pool-Einstellungen für den Pool angegebene Einstellung.</p>
view.defaultUser	-u, --userName=	<p>Legt den Benutzernamen fest, den View Client für alle Verbindungen verwendet, und fügt den Benutzernamen hinzu, den Sie im Feld [Benutzername] im View Client-Authentifizierungsdialogfeld angeben.</p> <p>Im Kioskmodus kann der Kontoname auf der MAC-Adresse des Clients basieren oder mit einer anerkannten Präfixzeichenfolge beginnen, so z. B. custom-.</p>
view.fullScreen	--fullscreen	<p>Blendet das Betriebssystem des Hosts aus und öffnet die View Client-Benutzeroberfläche auf einem Monitor im Vollbildmodus. Diese Option hat keine Auswirkungen auf den Bildschirmmodus der Desktopsitzung.</p> <p>Geben Sie beim Festlegen des Konfigurationsschlüssels „TRUE“ oder „FALSE“ an. Die Standardeinstellung ist „FALSE“.</p>
view.kbdLayout	-k, --kbdLayout= Beispiele: --kbdLayout="en-us" -k "fr"	<p>Gibt über einen Sprachencode an, welches Gebietsschema für die Tastaturbelegung verwendet werden soll.</p>
view.kioskLogin	--kioskLogin Beispiel: Siehe „ Beispiel: Beispiel für Kioskmodus “, auf Seite 21.	<p>Gibt an, dass View Client die Authentifizierung über ein Kioskmodus-Konto durchführt.</p> <p>Geben Sie beim Festlegen des Konfigurationsschlüssels „TRUE“ oder „FALSE“ an. Die Standardeinstellung ist „FALSE“.</p>
view.mmrPath	-m, --mmrPath= Beispiel: --mmrPath="/usr/lib/altmmr"	<p>(Nur für von anderen Anbietern verteilte Versionen verfügbar) Gibt den Pfad zu dem Verzeichnis an, das die Wyse MMR-Bibliotheken (Wyse Multimedia-Umleitung-Bibliotheken) enthält.</p>

Tabelle 3-3. View Client-Befehlszeilenoptionen und -Konfigurationsdateischlüssel (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung
view.nomenubar	--nomenubar	Unterdrückt die View Client-Menüleiste bei einer View Client-Anzeige im Vollbildmodus, sodass die Benutzer keinen Zugriff auf die Menüoptionen zum Abmelden von einem View-Desktop, Zurücksetzen eines View-Desktops oder Trennen der Verbindung mit einem View-Desktop haben. Verwenden Sie diese Option bei der Konfiguration des Kioskmodus. Geben Sie beim Festlegen des Konfigurationsschlüssels „TRUE“ oder „FALSE“ an. Die Standardeinstellung ist „FALSE“.
view.nonInteractive	-q, --nonInteractive Beispiel: --nonInteractive --serverURL="https://view.company.com" --userName="user1" --password="-" --domainName="xyz" --desktopName="Windows 7"	Blendet für die Endbenutzer unnötige UI-Schritte durch Überspringen der Bildschirme aus, die in der Befehlszeile oder den Konfigurationseigenschaften angegeben werden. Geben Sie beim Festlegen des Konfigurationsschlüssels „TRUE“ oder „FALSE“ an. Die Standardeinstellung ist „FALSE“. Das Festlegen dieser Eigenschaft auf „TRUE“ ist gleichbedeutend mit dem Festlegen der Eigenschaften view.autoConnectBroker und view.autoConnectDesktop auf „TRUE“.
view.once	--once	Gibt an, dass View Client bei einem Fehler nicht erneut versuchen soll, eine Verbindung herzustellen. Verwenden Sie --once, wenn Sie einen ähnlichen Workflow wie beim View 4.6-Client erhalten möchten. Diese Option erzwingt das Beenden von View Client, nachdem der Benutzer die Verbindung getrennt oder sich am Desktop abgemeldet hat. Sie sollten diese Option normalerweise angeben, wenn Sie den Kioskmodus verwenden, und den Fehler mithilfe des Exitcodes behandeln. Anderenfalls kann es schwierig sein, den vmware-view-Prozess remote zu beenden. Geben Sie beim Festlegen des Konfigurationsschlüssels „TRUE“ oder „FALSE“ an. Die Standardeinstellung ist „FALSE“.
view.rdesktopOptions	--rdesktopOptions= Beispiel: --rdesktopOptions="-f -m"	(Verfügbar bei Verwendung des Microsoft RDP-Anzeigeprotokolls) Gibt die Befehlszeilenoptionen zur Weiterleitung an die rdesktop-Anwendung an. Informationen über die rdesktop-Optionen finden Sie in der rdesktop-Dokumentation.

Tabelle 3-3. View Client-Befehlszeilenoptionen und -Konfigurationsdateischlüssel (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung
Keine	<code>-r, --redirect=</code> Beispiel: <code>--redirect="sound:off"</code>	(Verfügbar bei Verwendung des Microsoft RDP-Anzeigeprotokolls) Gibt ein lokales Gerät an, das Sie über rdesktop an den View-Desktop umleiten möchten. Geben Sie die Geräteinformationen an, die Sie an die <code>-r</code> -Option von rdesktop übergeben möchten. Sie können mehrere Geräteoptionen in einem einzelnen Befehl festlegen.
<code>view.sslVerificationMode</code>	Keine	Legt den Überprüfungsmodus für das Serverzertifikat fest. Geben Sie „1“ an, wenn Sie Verbindungen bei Fehlern in der Zertifikatsprüfung ablehnen möchten. Geben Sie „2“ an, wenn Sie die Benutzer zwar warnen, aber Verbindungen mit einem selbstsignierten Zertifikat doch zulassen möchten. Geben Sie „3“ an, wenn Sie nicht überprüfbare Verbindungen zulassen möchten. Wenn Sie „3“ angeben, werden keine Überprüfungen durchgeführt. Die Standardeinstellung ist „2“.
Keine	<code>--printEnvironmentInfo</code> Beispiel: <code>--printEnvironmentInfo</code> <code>-s view.company.com</code>	Zeigt Informationen über die Umgebung eines Clientgerätes an, so z. B. dessen IP-Adresse, MAC-Adresse, Computername und Domänenname. Im Kioskmodus können Sie ein auf der MAC-Adresse basierendes Konto für den Client erstellen. Zur Anzeige der MAC-Adresse müssen Sie diese Option mit der Option <code>-s</code> verwenden.
Keine	<code>--usb=</code>	(Nur für von anderen Anbietern verteilte Versionen und für View Client 1.5 verfügbar) Legt fest, welche Optionen für die USB-Umleitung verwendet werden sollen. Siehe „Verwenden der Befehlszeilenoption aus View Client 1.5 zur Umleitung von USB-Geräten“ , auf Seite 43. Informationen zur Konfiguration der USB-Optionen mit View Client 1.6 und höher finden Sie unter Kapitel 7, „Konfigurieren der USB-Umleitung auf dem Client“ , auf Seite 39.
Keine	<code>--version</code>	Zeigt Versionsinformationen über View Client an.

Beispiel: Beispiel für Kioskmodus

Zu Kioskbenutzern gehören zum Beispiel Kunden an Checkin-Schaltern von Fluggesellschaften, Schüler in Klassenräumen oder Bibliotheken, medizinisches Personal an Eingabestationen für medizinische Daten oder Kunden an öffentlichen Zugangspunkten. Die Konten sind nicht mit Benutzern, sondern mit Clientgeräten verknüpft, da Benutzer sich nicht anmelden müssen, um das Clientgerät oder den View-Desktop zu nutzen. Dennoch müssen Benutzer für manche Anwendungen Anmeldeinformationen zur Authentifizierung bereitstellen.

Zum Einrichten des Kioskmodus müssen Sie die Befehlszeilenschnittstelle `vdmadmin` auf der View-Verbindungsserver-Instanz verwenden und mehrere Verfahren durchführen, die im Dokument *Verwaltung von VMware View* im Kapitel zum Thema Kioskmodus dokumentiert sind. Nach der Einrichtung des Kioskmodus können Sie den Befehl `vmware-view` auf einem Linux-Client zur Verbindungsherstellung mit einem View-Desktop im Kioskmodus verwenden.

Um von Linux-Clients im Kioskmodus eine Verbindung mit View-Desktops herstellen zu können, müssen Sie mindestens die folgenden Konfigurationsschlüssel oder Befehlszeilenooptionen angeben.

Konfigurationsschlüssel	Entsprechende Befehlszeilenooptionen
<code>view.kioskLogin</code>	<code>--kioskLogin</code>
<code>view.nonInteractive</code>	<code>-q, --nonInteractive</code>
<code>view.fullScreen</code>	<code>--fullScreen</code>
<code>view.noMenuBar</code>	<code>--noMenuBar</code>
<code>view.defaultBroker</code>	<code>-s, --serverURL=</code>

Das Auslassen einer dieser Konfigurationseinstellungen wird für den Kioskmodus nicht unterstützt. Wenn der View-Verbindungsserver so eingerichtet wurde, dass ein nicht standardmäßiger Kiosk-Benutzername erforderlich ist, müssen Sie zudem auch die Eigenschaft `view.defaultUser` festlegen oder die Befehlszeilenooption `-u` oder `--userName=` verwenden. Wenn kein nicht standardmäßiger Benutzername erforderlich ist und Sie keinen Benutzernamen angeben, kann View Client den standardmäßigen Kiosk-Benutzernamen ableiten und verwenden.

HINWEIS Stellen Sie sicher, dass der Konfigurationsschlüssel `view.sslVerificationMode` unbedingt in der Datei `/etc/vmware/view-mandatory-config` festgelegt wird. Wenn der Client im Kioskmodus ausgeführt wird, schaut er nicht in der Datei `view-preferences` nach.

Der in diesem Beispiel gezeigte Befehl führt View Client auf einem Linux-Clientsystem aus und verfügt über die folgenden Merkmale:

- Der Benutzerkontenname basiert auf der MAC-Adresse des Clients.
- View Client wird im Vollbildmodus ohne eine View Client-Menüleiste ausgeführt.
- Die Benutzer werden automatisch mit der angegebenen View-Verbindungsserver-Instanz und dem angegebenen View-Desktop verbunden und nicht zur Eingabe von Anmeldeinformationen aufgefordert.
- Beim Auftreten eines Verbindungsfehlers wird je nach zurückgegebenem Fehlercode ein Skript ausgeführt oder ein Kiosk-Überwachungsprogramm behandelt den Fehler. Demzufolge kann das Clientsystem beispielsweise ein Störungsanzeigebild einblenden oder eine gewisse Zeit warten, bevor es erneut versucht, eine Verbindung mit dem View-Verbindungsserver herzustellen.

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

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 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 „[Zertifikatprüfungsmodi für View Client](#)“, auf Seite 29.

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 17.

Aktivieren des FIPS-Modus auf dem Client

Sie können die Konfigurationseigenschaft so einstellen, dass der Client zur Herstellung einer Remote-PcoIP-Verbindung nur FIPS (Federal Information Processing Standard) 140-2-validierte kryptografische Algorithmen und Protokolle verwendet.

Diese Einstellung gilt sowohl für den Server als auch für den Client. Sie können entweder einen oder beide Endpunkte zum Betrieb im FIPS-Modus konfigurieren. Das Konfigurieren eines einzigen Endpunkts im FIPS-Modus begrenzt die bei der Sitzungsaushandlung verfügbaren Verschlüsselungsalgorithmen.

WICHTIG Wenn der FIPS-Modus auf einem Endpunkt aktiviert wird, der andere Endpunkt jedoch keine FIPS 140-2-validierten kryptografischen Algorithmen unterstützt, schlägt die Verbindung fehl.

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

Einstellen der Konfigurationseigenschaft

Zum Aktivieren oder Deaktivieren des FIPS-Modus können Sie die Eigenschaft `pcoip.enable_fips_mode` festlegen. Durch Einstellen der Eigenschaft auf den Wert `1` wird der FIPS-Modus aktiviert; mit dem Wert `0` wird der FIPS-Modus deaktiviert. Mit der folgenden Einstellung wird z. B. der FIPS-Modus aktiviert:

```
pcoip.enable_fips_mode = 1
```

Setzen Sie ein Leerzeichen vor und hinter das Gleichheitszeichen (=).

Diese Eigenschaft kann in verschiedenen Dateien festgelegt werden. 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.

Konfigurieren des PCoIP-Client-Bildcache

Bei der PCoIP-Client-Bildzwischen­speicherung wird Bildinhalt auf dem Client gespeichert, um erneute Übertragungen zu vermeiden. Diese Funktion ist standardmäßig aktiviert, um die Bandbreitenverwendung zu reduzieren.

WICHTIG Diese Funktion ist nur verfügbar, wenn View Agent und 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 Anzeigeeinfor­mationen 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 ohne clientseitige Zwischen­speicherung häufig ab. In einer solchen Situation ist es möglich, durch die clientseitige Zwischen­speicherung Bandbreite einzusparen und einen reibungslosen, äußerst schnellen Bildlauf sicherzustellen.

Standardmäßig ist die Funktion aktiviert, sodass der Client Teile der zuvor übermittelten Anzeige speichert. Die standardmäßige Cachegröße beträgt 250 MB. Bei Aktivierung dieser Einstellung können Sie die Client-Bildcachegröße von mindestens 50 MB auf 300 MB konfigurieren. Bei einer größeren Cachegröße wird zwar die Bandbreitenverwendung reduziert, jedoch wird mehr Speicher auf dem Client benötigt. Eine kleinere Cachegröße bedeutet eine größere Bandbreitenbelastung. Für einen Thin Client mit wenig Speicher ist beispielsweise eine kleinere Cachegröße erforderlich.

Einstellen der Konfigurationseigenschaft

Zum Konfigurieren der Cachegröße können Sie die Eigenschaft `pcoip.image_cache_size_mb` einstellen. Zum Beispiel wird durch die folgende Einstellung die Cachegröße auf 50 MB konfiguriert:

```
pcoip.image_cache_size_mb = 50
```

Setzen Sie ein Leerzeichen vor und hinter das Gleichheitszeichen (=). Wenn Sie einen Wert von unter 50 angeben, wird dieser in 50 umgewandelt. Wenn Sie einen Wert von über 300 eingeben, wird dieser in 300 umgewandelt.

Diese Eigenschaft kann in verschiedenen Dateien festgelegt werden. 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 festlegen, um die ordnungsgemäße Funktionsweise des Bildcaches visuell bestätigt zu bekommen:

```
pcoip.show_image_cache_hits = 1
```

Bei dieser Konfiguration wird um jede Kachel (32 x 32 Pixel) in einem aus dem Bildcache stammenden Bild ein Rechteck angezeigt.

Verwaltung der Serververbindungen und Desktops

4

Verwenden Sie View Client, um eine Verbindung zu View-Verbindungsserver oder einem Sicherheitsserver herzustellen und sich an einem View-Desktop an- bzw. von diesem abzumelden. Für die Problembehebung können Sie den Ihnen zugewiesenen View-Desktop zurücksetzen und für einen ausgecheckten Desktop ein Rollback durchführen.

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

- [Erstmalige Anmeldung an einem View-Desktop](#) auf Seite 27
Bevor Endbenutzer auf ihre virtuellen Desktops zugreifen, sollten Sie testen, ob Sie sich über ein Client-system an einem virtuellen Desktop anmelden können.
- [Zertifikatsprüfungsmodi für View Client](#) auf Seite 29
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 30
Wenn Sie mit einem Desktop verbunden sind, können Sie zu einem anderen Desktop wechseln.
- [Abmelden oder Trennen von Desktops](#) auf Seite 30
Wenn Sie die Verbindung zu einem View-Desktop trennen, ohne sich abzumelden, bleiben die Anwendungen geöffnet.
- [Rollback eines Desktops](#) auf Seite 31
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.

Erstmalige Anmeldung an einem View-Desktop

Bevor Endbenutzer auf ihre virtuellen Desktops zugreifen, sollten Sie testen, ob Sie sich über ein Clientsystem an einem virtuellen 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 Domännennamen für die Anmeldung.
- Durchführen der unter „[Vorbereitung des View-Verbindungservers für View Client](#)“, auf Seite 8.

- Wenn Sie sich außerhalb des Firmennetzwerks befinden und für den Zugriff auf den virtuellen 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 virtuellen 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 View-Desktop zu verwenden, müssen Sie sicherstellen, dass die View Agent-Gruppenrichtlinieneinstellung Allow-DirectRDP aktiviert ist.
- Wenn Ihr Administrator dies zulässt, können Sie den Zertifikatsprüfungsmodus für das von View Server vorgelegte SSL-Zertifikat konfigurieren. Siehe „Zertifikatsprüfungsmodi für View Client“, auf Seite 29.

Vorgehensweise

- 1 Öffnen Sie entweder ein Terminalfenster und geben Sie `vmware-view` ein oder wählen Sie **[Anwendungen]** > **[Internet]** > **[VMware View Client]** aus 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 View-Desktopverknüpfung, um die Verbindung herzustellen.

Nachdem die Verbindung hergestellt wurde, wird das Clientfenster angezeigt. Wenn 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. 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 den 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 View*.
- Stellen Sie sicher, dass der Benutzer zum Zugriff auf diesen Desktop berechtigt ist. Weitere Informationen finden Sie im Dokument *Verwaltung von VMware View*.
- Wenn Sie das RDP-Anzeigeprotokoll zur Verbindungsherstellung mit einem View-Desktop verwenden, müssen Sie bestätigen, dass der Clientcomputer Remote-Desktop-Verbindungen zulässt.

Zertifikatsprüfungsmodi für 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 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 View Client auf einen Server mit einem Zertifikat umleitet, das nicht mit dem in 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 unbekanntenen 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 die Vertrauenskette des Zertifikats bis in den Zertifikatspeicher des Geräts zurückverfolgt werden können.

HINWEIS Anweisungen zur Verteilung eines selbstsignierten Stammzertifikats, das die Benutzer auf ihren Linux-Clientsystemen installieren können, finden Sie in der Ubuntu-Dokumentation.

View Client verwendet die PEM-formatierten Zertifikate, die im Verzeichnis `/etc/ssl/certs` auf dem Client-System 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 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]** aus der VMware View Client-Menüleiste oder 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-Verbindungservers übereinstimmen, den Sie in 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 View-Desktop auf demselben oder einem anderen Server aus.

Option	Aktion
Einen anderen View-Desktop auf demselben Server auswählen	Wählen Sie [Desktop] > [Trennen] aus der Menüleiste.
Einen View-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 View-Desktop trennen, ohne sich abzumelden, bleiben die Anwendungen geöffnet.

Wenn Sie nicht mit einem View-Desktop verbunden sind, können Sie sich abmelden, ohne vorher die Verbindung herstellen zu müssen. Die Verwendung dieser Option hat dieselbe Funktion, wie wenn Sie die Tastenkombination Strg+Alt+Entf drücken und anschließend auf **[Abmelden]** klicken.

HINWEIS Die Windows-Tastenkombination Strg+Alt+Entf wird auf View-Desktops nur unterstützt, wenn Sie das RDP-Anzeigeprotokoll verwenden. Wählen Sie, um bei einer Verwendung des PCoIP-Anzeigeprotokolls dieselben Resultate wie bei einer Betätigung von Strg+Alt+Entf zu erzielen, die Optionen **[Desktop]** > **[Strg+Alt+Entf senden]** aus der Menüleiste.

Alternativ können Sie auch die Tastenkombination Strg+Alt+Eingf betätigen.

Vorgehensweise

- Trennen Sie die Verbindung, ohne sich abzumelden.

Option	Aktion
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 View-Desktop auf demselben Server auswählen	Wählen Sie [Desktop] > [Trennen] aus der Menüleiste.
Einen View-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 gehalten.

- Melden Sie sich ab und trennen Sie die Verbindung.

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 View-Desktop geöffnet sind, ohne vorheriges Speichern geschlossen.

- Melden Sie sich ab, wenn Sie nicht mit einem View-Desktop verbunden sind.
 - Wählen Sie auf der Startseite mit den Desktop-Verknüpfungen den entsprechenden Desktop und anschließend **[Desktop] > [Abmelden]** in der Menüleiste.
 - Geben Sie bei Aufforderung die Anmeldeinformationen für den Zugriff auf den View-Desktop an.
Bei Verwendung dieser Option werden alle Dateien, die auf dem View-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 View-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 Geben Sie, wenn auf der View Client-Startseite die **[View-Verbindungsserver]**-Aufforderung angezeigt wird, den Servernamen an und klicken Sie auf **[Weiter.]**
 - 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 View Client-Startseite, auf der View-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 View-Desktop können Sie sich vom Linux-Client an diesem anmelden.

Verwendung eines Microsoft Windows-Desktops auf einem Linux-System

5

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

Dieses Kapitel behandelt die folgenden Themen:

- „[Funktionsunterstützungs-Matrix](#)“, auf Seite 33
- „[Internationalisierung](#)“, auf Seite 34
- „[Tastaturen und Monitore](#)“, auf Seite 34
- „[Kopieren und Einfügen von Text](#)“, auf Seite 35

Funktionsunterstützungs-Matrix

View Client für Linux unterstützt einige der auf anderen Clients verfügbaren Funktionen, so z. B. View Client für Windows-Desktops und Laptops.

Tabelle 5-1. Auf Windows-Desktops für Linux-Clients unterstützte Funktionen

Funktion	Windows 7 View Desktop	Windows Vista View Desktop	Windows XP View Desktop
RSA SecurID oder RADIUS	X	X	X
Einmaliges Anmelden	X	X	X
RDP-Anzeigeprotokoll	X	X	X
PCoIP-Anzeigeprotokoll	X	X	X
USB-Zugriff			
Wyse MMR			
Virtuelles Drucken			
Standortbasiertes Drucken	X	X	X
Smartcards			
Mehrere Monitore	X	X	X
Lokaler Modus			

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

HINWEIS Diese Funktionsunterstützungs-Matrix gilt für die View Client für Linux-Instanz, die VMware auf Ubuntu zur Verfügung stellt. Darüber hinaus bieten verschiedene VMware-Partner Thin Client-Geräte für VMware View-Bereitstellungen. 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](#), das auf der VMware-Website zur Verfügung steht.

Internationalisierung

Sowohl die Benutzeroberfläche als auch die Dokumentation für View Client sind auf Englisch, Japanisch, Französisch, Deutsch, Chinesisch (vereinfacht) 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 View-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 View-Desktop:

- Sie können bis zu vier Monitore verwenden, sofern Sie über ausreichend Video-RAM verfügen.

Um mehr als zwei Monitore zum Anzeigen Ihres View-Desktops auf einem Ubuntu-Clientsystem zu verwenden, müssen Sie die Einstellung `kernel.xhmmx` 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.

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

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 View-Desktop auf einem sekundären Monitor öffnen und dann die Bildschirmauflösung auf diesem Monitor ändern, geht der View-Desktop zum primären Monitor über.
- Mit PCoIP können Sie bei der Verwendung von zwei Monitoren die Auflösung für jeden Monitor separat festlegen und eine Auflösung von bis zu 2560 × 1600 pro Anzeige einstellen. 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 View-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:

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

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

Kopieren und Einfügen von Text

Sie können Text aus Ihrem Clientsystem kopieren und auf einen Remote-View-Desktop einfügen. Sofern Ihr Administrator diese Funktion aktiviert hat, können Sie zudem auch Text von einem View-Desktop kopieren und auf Ihr Clientsystem einfügen oder Text 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 im Hilfetema zu den allgemeinen View PCoIP-Sitzungsvariablen im Dokument *Verwaltung von VMware View* (Kapitel über die Konfiguration von Richtlinien).

Sie können einfachen Text oder formatierten Text von View Client auf einen View-Desktop oder umgekehrt kopieren. Der Text wird jedoch als einfacher Text eingefügt.

Grafiken können nicht kopiert und eingefügt werden. Sie können zudem auch keine Dateien zwischen einem View-Desktop und dem Dateisystem auf Ihrem Clientcomputer kopieren und einfügen.

Fehlerbehebung für View Client

Die meisten Probleme mit View Client können durch ein Zurücksetzen des Desktops oder eine Neuinstallation von VMware View Client behoben werden.

Dieses Kapitel behandelt die folgenden Themen:

- „Zurücksetzen eines Desktops“, auf Seite 37
- „Deinstallation von View Client“, auf Seite 38

Zurücksetzen eines Desktops

Beim Zurücksetzen wird der Desktop heruntergefahren und neu gestartet. Nicht gespeicherte Daten gehen verloren.

Eventuell muss der Desktop zurückgesetzt werden, wenn das Desktop-Betriebssystem nicht mehr reagiert.

Das Zurücksetzen eines Desktops entspricht dem Betätigen der Taste „Zurücksetzen“ auf einem physischen Computer, mit der der Neustart des Computers erzwungen wird. Alle Dateien, die auf dem View-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 Befehl **[Desktop zurücksetzen]** .

Option	Aufgabe
Aus dem Desktop-Betriebssystem heraus	Wählen Sie [Desktop] > [Desktop zurücksetzen] aus der Menüleiste aus.
Vom Startbildschirm aus (mit Desktop-Verknüpfungen)	Wählen Sie zuerst den Desktop und anschließend [Desktop] > [Desktop zurücksetzen] aus der Menüleiste aus.

Das Betriebssystem des View-Desktops wird neu gestartet. View Client trennt die Verbindung zum Desktop.

Weiter

Warten Sie eine gewisse Weile, bis der Systemneustart ausgeführt wurde, bevor Sie versuchen, eine Verbindung mit dem View-Desktop herzustellen.

Deinstallation von View Client

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

View Client kann mit der gleichen Methode deinstalliert werden, mit der Sie auch alle anderen Anwendungen deinstallieren.

Navigieren Sie zum Beispiel zu **[Anwendungen] > [Ubuntu Software Center]**, wählen Sie im Abschnitt **[Installierte Software]** die Option **[vmware-view-client]** und klicken Sie dann auf **[Entfernen.]**

Nach Abschluss der Deinstallation können Sie die Anwendung neu installieren.

Siehe „[Installation von View Client für Linux](#)“, auf Seite 9.

Konfigurieren der USB-Umleitung auf dem Client

7

Mit View Client 1.6 können Sie über eine Konfigurationsdatei auf dem Clientsystem angeben, welche USB-Geräte an einen View-Desktop umgeleitet werden können. Die USB-Komponente ist nur für die von anderen Anbietern bereitgestellte Version von View Client für Linux verfügbar.

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.

WICHTIG Die Funktion zur USB-Umleitung ist nur verfügbar, wenn es sich bei der Version von View Agent und des View-Verbindungsservers um View 4.6.1 oder höher und um die Drittanbieter-Version von View Client handelt. Die in diesen Hilfethemen beschriebenen USB-Filterfunktionen sind ab dem View-Verbindungsserver 5.1 und höher verfügbar. Weitere Informationen über die Thin Client- und Zero Client-Partner von VMware finden Sie im [VMware-Kompatibilitätshandbuch](#).

Um die für Drittanbieter von View Client 1.6 und höher verfügbaren USB-Komponenten verwenden zu können, müssen bestimmte Dateien an bestimmten Speicherorten installiert und bestimmte Prozesse dahingehend konfiguriert werden, dass sie vor dem Start von View Client gestartet werden. Eine detaillierte Beschreibung dieser Vorgänge ist in diesem Dokument nicht vorgesehen.

Dieses Kapitel behandelt die folgenden Themen:

- [„Festlegen der USB-Konfigurationseigenschaften“](#), auf Seite 39
- [„USB-Gerätefamilien“](#), auf Seite 42
- [„Verwenden der Befehlszeilenooption aus View Client 1.5 zur Umleitung von USB-Geräten“](#), auf Seite 43

Festlegen der USB-Konfigurationseigenschaften

Sie können die USB-Eigenschaften in jeder der Konfigurationsdateien festlegen.

- 1 `/etc/vmware/config`. Der Dienst `vmware-view-usbd` untersucht diese Datei zuerst. Wenn bestimmte USB-Konfigurationseigenschaften in dieser Datei festgelegt sind, werden diese verwendet.
- 2 `/usr/lib/vmware/config`. Wenn die USB-Eigenschaften unter `/etc/vmware/config` nicht gefunden werden, wird die Datei `/usr/lib/vmware/config` überprüft.
- 3 `~/.vmware/config`. Wenn die USB-Eigenschaften in den anderen Dateien nicht gefunden werden, wird die Datei `~/.vmware/config` überprüft.

Verwenden Sie zum Festlegen dieser Eigenschaften in der Konfigurationsdatei die folgende Syntax.

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

HINWEIS Über diese Eigenschaften können Sie steuern, ob bestimmte Gerätetypen weitergeleitet werden. Es sind zudem auch Filtereigenschaften verfügbar, über die Sie bestimmte Gerätetypen ausschließen und andere einschließen können. Für Windows-Clients sind außerdem Eigenschaften zur Aufschlüsselung von Verbundgeräten verfügbar. Auf Linux-Clients sind diese Aufschlüsselungseigenschaften dagegen aktuell nicht verfügbar.

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 nach Anschluss des USB-Geräts an das lokale System bei Ausführung von View Client auch in der Datei `/tmp/vmware-root/vmware-view-usb-*.log` nachsehen. Den Speicherort dieser Datei können Sie beispielsweise über die Eigenschaft `view-usb.log.fileName` in der Datei `/etc/vmware/config` angeben:

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

WICHTIG Hinsichtlich der Umleitung von Audiogeräten sollten Sie sicherstellen, dass es sich bei der Kernel-Version Ihres Ubuntu-Systems um 3.2.0-27.43 oder höher handelt. Ubuntu 12.04 umfasst die Kernel-Version 3.2.0-27.43. Wenn Sie kein Upgrade auf diese Kernel-Version durchführen können, können Sie alternativ auch den Host-Zugriff auf das Audiogerät deaktivieren. So können Sie beispielsweise die Zeile `blacklist snd-usb-audio` an das Ende der Datei `/etc/modprobe.d/blacklist.conf` anhängen. Erfüllt Ihr System keine dieser Voraussetzungen, kann es zu einem Absturz des Clientsystems kommen, wenn View Client die Umleitung des Audiogeräts startet. Audiogeräte werden standardmäßig umgeleitet.

Tabelle 7-1. Konfigurationseigenschaften für die USB-Umleitung

Name und Eigenschaft der Richtlinie	Beschreibung
Audioeingabegeräte zulassen Eigenschaft: <code>viewusb.AllowAudioIn</code>	Ermöglicht die Umleitung von Audioeingabegeräten. Der Standardwert ist nicht definiert; dies entspricht true .
Audioausgabegeräte zulassen Eigenschaft: <code>viewusb.AllowAudioOut</code>	Ermöglicht die Umleitung von Audioausgabegeräten. Der Standardwert ist nicht definiert; dies entspricht false .
HID zulassen Eigenschaft: <code>viewusb.AllowHID</code>	Ermöglicht die Umleitung anderer Eingabegeräte neben Tastaturen und Mäusen. Der Standardwert ist nicht definiert; dies entspricht true .
HIDBootable zulassen Eigenschaft: <code>viewusb.AllowHIDBootable</code>	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: <code>viewusb.AllowDevDescFailsafe</code>	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 <code>IncludeVidPid</code> oder <code>IncludePath</code> . Der Standardwert ist nicht definiert; dies entspricht false .
Tastatur- und Mausgeräte zulassen Eigenschaft: <code>viewusb.AllowKeyboardMouse</code>	Ermöglicht die Umleitung von Tastaturen mit integrierten Zeigegegeräten (zum Beispiel Maus, Trackball, Touchpad). Der Standardwert ist nicht definiert; dies entspricht false .
Smartcards zulassen Eigenschaft: <code>viewusb.AllowSmartcard</code>	Ermöglicht die Umleitung von Smartcard-Geräten. Der Standardwert ist nicht definiert; dies entspricht false .

Tabelle 7-1. Konfigurationseigenschaften für die USB-Umleitung (Fortsetzung)

Name und Eigenschaft der Richtlinie	Beschreibung
Videogeräte zulassen Eigenschaft: viewusb.AllowVideo	Ermöglicht die Umleitung von Videogeräten. Der Standardwert ist nicht definiert; dies entspricht true .
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 <code>Exclude All Devices</code> 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 <code>family_name_1[;family_name_2]...</code> Beispiel: bluetooth;smart-card 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 <code>vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]...</code> 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 <code>bus-x1[/y1]..._port-z1[;bus-x2[/y2]..._port-z2]...</code> 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 <code>family_name_1[;family_name_2]...</code> 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 <code>bus-x1[/y1]..._port-z1[;bus-x2[/y2]..._port-z2]...</code> 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 <code>vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]...</code> 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.

USB-Gerätefamilien

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

Tabelle 7-2. USB-Gerätefamilien

Name Gerätefamilie	Beschreibung
audio (Audio)	Alle Audioeingabe- oder Audioausgabegeräte.
audio-in (Audioeingabe)	Audioeingabegeräte, zum Beispiel Mikrofone.
audio-out (Audioausgabe)	Audioausgabegeräte, zum Beispiel Lautsprecher und Kopfhörer.
bluetooth (Bluetooth)	Über Bluetooth verbundene Geräte.
comm (Komm)	Kommunikationsgeräte, zum Beispiel Modems und kabelgebundene Netzwerkadapter.
hid (Eingabegeräte (Human Interface Devices))	Eingabegeräte (Human Interface Devices), mit Ausnahme von Tastaturen und Zeigegegeräten.
hid-bootable (Eingabegeräte startfähig)	Eingabegeräte (Human Interface Devices), die zur Startzeit verfügbar sind, mit Ausnahme von Tastaturen und Zeigegegeräten.
imaging (Bildverarbeitung)	Bildverarbeitungsgeräte, zum Beispiel Scanner.
keyboard (Tastatur)	Tastaturgeräte.
mouse (Maus)	Zeigegegeräte, zum Beispiel eine Maus.
other (andere)	Familie nicht angegeben.
pda (PDA)	PDAs (Personal Digital Assistants).
physical (physisch)	Force Feedback-Geräte, zum Beispiel Force Feedback-Joysticks.
printer (Drucker)	Druckgeräte.
security (Sicherheit)	Sicherheitsgeräte, zum Beispiel Fingerabdruckleser.
smart-card (Smartcard)	Smartcard-Geräte.
storage (Speicher)	Massenspeichergeräte, zum Beispiel Flashlaufwerke 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 nicht vom Gerätetreiber, sondern vom Gerät selbst aus. Die Firmware auf einem USB-Gerät definiert üblicherweise die Familie des Geräts, die dessen bestimmungsgemäße Funktionalität beschreibt. Nicht alle Geräte geben jedoch den korrekten 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 7, „Konfigurieren der USB-Umleitung auf dem Client“](#), auf Seite 39.

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

Mit dem folgenden Beispiel wird die Protokollierung auf Ablafebene 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 7-3. USB-Umleitungsoptionen

Option	Beschreibung
<code>disable-boot-fw</code>	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.
<code>ex:Gerät1[,Gerät2]...</code>	Schließt eine Liste benannter Geräte von der Weiterleitung ein. Beispiel: <pre>vmware-view --usb=ex:"flash 1"</pre>
<code>exfa:Gerätefamilie1[,Gerätefamilie2]...</code>	Schließt eine Liste benannter Gerätefamilien von der Weiterleitung aus. Beispiel: <pre>vmware-view --usb=exfa:storage</pre>
<code>exid:Geräte-ID1[,Geräte-ID2]...</code>	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 <code>vidxxxxpidxxxx</code> . Zum Beispiel: <pre>vmware-view --usb=exid:vid1e2fpid5a1e</pre>
<code>expt:Gerätepfad1[,Gerätepfad2]...</code>	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 <code>bus#port#</code> . Zum Beispiel: <pre>vmware-view --usb=expt:bus1port4,bus5port3</pre>

Tabelle 7-3. USB-Umleitungsoptionen (Fortsetzung)

Option	Beschreibung
<code>in:Gerät1[,Gerät2]...</code>	Schließt eine Liste benannter Geräte in die Weiterleitung ein. Beispiel: <code>vmware-view</code> <code>--usb=in:"flash 1"</code>
<code>infa:Gerätefamilie1[,Gerätefamilie2]...</code>	Schließt eine Liste benannter Gerätefamilien in die Weiterleitung ein. Beispiel: <code>vmware-view</code> <code>--usb=infa:storage</code>
<code>inid:Geräte-ID1[,Geräte-ID2]...</code>	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 <code>vidxxxxpidxxxx</code> . Beispiel: <code>vmware-view</code> <code>--usb=inid:vid27f8pid2a1b</code>
<code>inpt:Gerätppfad1[,Gerätppfad2]...</code>	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 <code>busnportn</code> . Zum Beispiel: <code>vmware-view</code> <code>--usb=inpt:bus3port1,bus4port2</code>
<code>log:{debug error info trace}</code>	Legt die Protokollierungsebene für <code>vmware-view-usb</code> fest: <code>trace</code> , <code>debug</code> , <code>info</code> (Standardeinstellung) oder <code>error</code> nach abnehmender Detailtiefe fest. Die Protokolldatei (<code>backendLog.txt</code>) wird in <code>/tmp/vmware-username/vmware-view-usb-pid.log</code> geschrieben. Beispiel: <code>vmware-view</code> <code>--usb=log:error</code>

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

A

- Abmeldung **30**
- Anmelden an einem View-Desktop **27**

B

- Befehlszeilenschnittstelle **17**
- Befehlszeilenschnittstelle VMware View **15, 17**
- Betriebssysteme, Unterstützung auf View Agent **8**
- Bildcache, Client **24**
- Bildschirmauflösung **34**

C

- Client-Bildcache **24**

D

- Deinstallation von View Client **38**
- Desktop
 - Abmelden **30**
 - Rollback **31**
 - wechseln **30**
 - zurücksetzen **37**

E

- Einfügen von Text **35**

F

- FIPS-Modus **23**
- Funktionsunterstützungs-Matrix, für Linux **33**

G

- Geräte, USB **39, 43**
- Gerätefamilien **42**

H

- Hardwareanforderungen, für Linux-Systeme **7**

I

- Installationsanweisungen **9**

K

- Kanonisch **9**
- Konfigurationseigenschaften **15, 17**
- Kopieren von Text **35**

L

- Linux, Installation von View Client auf **7**

M

- Menübefehl Strg+Alt+Entf senden **30**
- Monitore **34**

P

- PCoIP-Client-Bildcache **24**
- Protokollieren, für USB-Geräte **39, 43**
- Proxysteinstellungen **17**

R

- Rollback eines View-Desktops **31**

S

- Serververbindungen **27**
- Sicherheitsserver **8**
- SSL-Zertifikate, Überprüfen **22**
- Strg+Alt+Entf **30**
- Systemanforderungen, für Linux **7**

T

- Tastaturen **34**
- Text, kopieren **35**
- Trennen der Verbindung mit einem View-Desktop **30**

U

- Überprüfung des Serverzertifikats **22**
- Überprüfungsmodi für die Zertifikatsprüfung **22**
- Ubuntu **9**
- Umleitung, USB **39, 43**
- UPNs, View Client **27**
- URI-Beispiele **14**
- URI-Syntax für View Clients **12**
- URIs (Uniform Resource Identifier) **11**
- USB-Gerätefamilien **42**
- USB-Umleitung **39, 43**

V

- View Agent, Installationsanforderungen **8**
- View Client
 - Fehlerbehebung **37**
 - Installation **7**
 - Konfiguration von **11**

starten **27**

Systemanforderungen **7**

Systemanforderungen für Linux **7**

Trennen der Verbindung mit einem Desktop **30**

View Client für Linux, installieren **9**

View-Desktop, Rollback **31**

View-Verbindungsserver **8**

Voraussetzungen für Clientgeräte **8**

W

Wechseln zwischen Desktops **30**

Weiterleiten von USB-Geräten **39, 43**

Z

Zertifikate, Ignorieren von Problemen **22, 29**

Zurücksetzen eines Desktops **37**

Zwischenspeicherung, Clientseitiges Bild **24**