Verwendung von VMware View Client für Linux

Mai 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-000780-01

vmware®

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

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

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

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

docfeedback@vmware.com

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

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

Inhalt

Verwendung von VMware 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.

Installation und Konfiguration

Zur Konfiguration einer View-Bereitstellung für Linux-Clients gehören die Erfüllung der Systemanforderungen für Linux-Clients, das Herunterladen und Installieren von View Client für Linux sowie das Konfigurieren der Sicherheits- und Leistungseinstellungen auf den Linux-Clientsystemen.

Systemanforderungen für Linux-Clients

Sie können View Client für Linux auf PCs installieren, die das Betriebssystem Ubuntu Linux 10.04 oder 10.10 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 2GB Arbeitsspeicher (RAM)
Betriebssysteme	Ubuntu Linux 10.04 oder 10.10 mit 32 Bit
View-Verbindungsserver , 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 MB + (24 * (Anzahl der Monitore) * (Breite des Monitors) * (Höhe des Monitors))`
	Als grobes Maß können Sie die folgenden Berechnungen verwenden:
	`1 Monitor: 1600 x 1200: 64MB`
	`2 Monitore: 1600 x 1200: 128MB`
	`3 Monitore: 1600 x 1200: 256MB`

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

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 Verbindung 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 10.10-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 6.
- 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 6.

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 11.

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 „Zertifikatsprüfungsmodi für View Client“, auf Seite 13.

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-Befehlssyntax und -Konfigurationseinstellungen“, auf Seite 19.

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 Anzeigeinformationen in erster Linie um eine Abfolge von Cache-Indizes handelt, lassen sich durch die Verwendung eines Bildcaches deutliche Bandbreiteneinsparungen erzielen. Dieser effiziente Bildlauf hat sowohl bei LAN- als auch WAN-Verbindungen Vorteile.

- Bei LAN-Verbindungen mit relativ uneingeschränkter Bandbreite führt die clientseitige Bildzwischenspeicherung zu deutlichen Bandbreiteneinsparungen.
- Um bei WAN-Verbindungen innerhalb der Bandbreiteneinschränkungen zu bleiben, nimmt die Bildlaufleistung 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

Verwenden Sie View Client, um eine Verbindung zu View Connection Server 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 11

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

- Zertifikatsprüfungsmodi für View Client auf Seite 13

  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 14

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

- Abmelden oder Trennen von Desktops auf Seite 14

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

- Rollback eines Desktops auf Seite 15

  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 Domänennamen für die Anmeldung.
- Durchführen der unter „Vorbereitung des View-Verbindungsservers für View Client“, auf Seite 7.

- 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 AllowDirectRDP 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 13.

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 **[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 unbekannten oder nicht als vertrauenswürdig eingestuften Zertifizierungsstelle (CA) signiert worden? Selbstsignierte Zertifikate sind ein Typ der nicht als vertrauenswürdig eingestuften CA.

  Um diese Prüfung zu bestehen, muss 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 Clientsystem gespeichert sind. Anweisungen zum Import eines Stammzertifikats, das an diesem Speicherort gespeichert ist, finden Sie im Abschnitt „Import eines Zertifikats in die systemweite Zertifikatsautorität-Datenbank“ des Dokuments unter https://help.ubuntu.com/community/OpenSSL.

Neben der Bereitstellung eines Serverzertifikats sendet der View-Verbindungsserver der Version 4.6.1, 5.0.1 und höher ebenfalls einen Zertifikat-Fingerabdruck an 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 **[Fortfahren]** klicken, um die Warnung zu ignorieren. Bei selbstsignierten Zertifikaten muss der Zertifikatsname nicht mit dem Namen des View-Verbindungsservers 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] > [Anderen Server auswählen]** 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 Eingabe der Windows-Tastenkombination Strg+Alt+Entf wird für View-Desktops nicht unterstützt. Wählen Sie, um 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+Einfg 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] > [Anderen Server auswählen]** aus der Menüleiste aus.

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

- Melden Sie sich ab und trennen Sie die Verbindung.

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.

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

  b Geben Sie bei Aufforderung die Anmeldeinformationen für den Zugriff auf den 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

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

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 1-1. 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:

- Bei PCoIP können Sie 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.xhmmax` 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.

- Mit RDP kann die Anzeige lediglich im Erweiterungsmodus dargestellt werden. Um den Erweiterungsmodus zum korrekten Ausdehnen der Anzeige auf mehrere Monitore zu verwenden, müssen die Monitore gleich hoch sein.

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.
- Bei PCoIP und mehreren Monitoren können Sie die Auflösung für jeden Monitor einzeln festlegen, wobei eine Einstellung auf bis zu 2560 x 1600 pro Anzeigegerät möglich ist.
- Bei RDP und mehreren Monitoren können Sie die Auflösung für jeden Monitor einzeln festlegen. Die Anzeige wird dann auf die Monitore ausgedehnt, sofern alle Monitore gleich hoch sind.

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 Hilfethema 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.

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 8.

View Client-Befehlssyntax und -Konfigurationseinstellungen

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

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 1-2. View Client-Befehlszeilenoptionen und -Konfigurationsdateischlüssel

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung

`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 `view.defaultBroker` festgelegt ist oder die Befehlszeilenoption `--serverURL=` verwendet wird. Geben Sie **„TRUE“** oder **„FALSE“** an. Die Standardeinstellung ist „FALSE“. Das Festlegen dieser Eigenschaft und der Eigenschaft `view.autoConnectDesktop` auf „TRUE“ ist gleichbedeutend mit dem Festlegen der Eigenschaft `view.nonInteractive` auf „TRUE“.

Tabelle 1-2. View Client-Befehlszeilenoptionen und -Konfigurationsdateischlüssel (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung
`view.autoConnectDesktop`	Keine	Stellt automatisch eine Verbindung mit dem zuletzt verwendeten View-Desktop her, außer wenn die Konfigurationseigenschaft `view.defaultDesktop` festgelegt ist oder die Befehlszeilenoption `--desktopName=` verwendet wird. Geben Sie **„TRUE“** oder **„FALSE“** an. Die Standardeinstellung ist „FALSE“. Das Festlegen dieser Eigenschaft und der Eigenschaft `view.autoConnectBroker` auf „TRUE“ ist gleichbedeutend mit dem Festlegen der Eigenschaft `view.nonInteractive` auf „TRUE“.

`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 `autoConnectDesktop` 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.

Tabelle 1-2. View Client-Befehlszeilenoptionen und -Konfigurationsdateischlüssel (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung

`view.defaultDesktopSize`	`--desktopSize=`
	Beispiele:
	`--desktopSize="1280x800"`
	`--desktopSize="all"`
		Legt die Standardgröße des Fensters für den View-Desktop fest:
		■ 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 `view.defaultDesktopWidth` und `view.defaultDesktopHeight` 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.
`view.defaultPassword`	`-p "-", --password="-"`	Geben Sie immer **`"-"`** an, um das Kennwort aus `stdin` zu lesen. 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-Verbindungsserver die Kennwortauthentifizierung akzeptiert. **Hinweis** Ein leeres Kennwort kann nicht verwendet werden. Folgendes können Sie also nicht festlegen: --password=""

Tabelle 1-2. View Client-Befehlszeilenoptionen und -Konfigurationsdateischlüssel (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung
`view.defaultProtocol`	`--protocol=`	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.
`view.defaultUser`	`-u, --userName=`	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. Im Kioskmodus kann der Kontoname auf der MAC-Adresse des Clients basieren oder mit einer anerkannten Präfixzeichenfolge beginnen, so z. B. **`custom-`**.
`view.fullScreen`	`--fullscreen`	Blendet das Betriebssystem des Hosts aus und öffnet die View Client-Benutzeroberfläche im Vollbildmodus. Diese Option hat keine Auswirkungen auf den Bildschirmmodus der Desktopsitzung. Geben Sie beim Festlegen des Konfigurationsschlüssels **„TRUE“** oder **„FALSE“** an. Die Standardeinstellung ist „FALSE“.

`view.kbdLayout`	`-k, --kbdLayout=`
	Beispiele:
	`--kbdLayout="en-us"`
	`-k "fr"`
		Gibt über einen Sprachencode an, welches Gebietsschema für die Tastaturbelegung verwendet werden soll.

`view.kioskLogin`	`--kioskLogin` Beispiel: Siehe „Beispiel: Beispiel für Kioskmodus“, auf Seite 25.	Gibt an, dass View Client die Authentifizierung über ein Kioskmodus-Konto durchführt. Geben Sie beim Festlegen des Konfigurationsschlüssels **„TRUE“** oder **„FALSE“** an. Die Standardeinstellung ist „FALSE“.

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

`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“.

Tabelle 1-2. View Client-Befehlszeilenoptionen und -Konfigurationsdateischlüssel (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung

`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.

Keine	`-r`, `--redirect=`
	Beispiel:
	`--redirect="sound:off"`
		(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 `-r`-Option von rdesktop übergeben möchten. Sie können mehrere Geräteoptionen in einem einzelnen Befehl festlegen.

Tabelle 1-2. View Client-Befehlszeilenoptionen und -Konfigurationsdateischlüssel (Fortsetzung)

Konfigurationsschlüssel	Befehlszeilenoption	Beschreibung
`view.sslVerificationMode`	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	`--printEnvironmentInfo`
	Beispiel:
	`--printEnvironmentInfo -s view.company.com`
		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 `-s` verwenden.

Keine	`--usb=`	(Nur für von anderen Anbietern verteilte Versionen verfügbar) Legt fest, welche Optionen für die USB-Umleitung verwendet werden sollen. Siehe „Umleiten eines USB-Geräts auf einen Remotedesktop“, auf Seite 27.
Keine	`--version`	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 Befehlszeilenoptionen angeben.

Konfigurationsschlüssel	Entsprechende Befehlszeilenoptionen
`view.kioskLogin`	`--kioskLogin`
`view.nonInteractive`	`-q`, `--nonInteractive`
`view.fullScreen`	`--fullscreen`
`view.nomenubar`	`--nomenubar`

Konfigurationsschlüssel	Entsprechende Befehlszeilenoptionen
`view.defaultBroker`	`-s, --serverURL=`

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 Befehlszeilenoption `-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.mycomany.com" --userName="CM-00:11:22:33:44:55:66:77" --password="mypassword"
```

View Client-Exitcodes

Die Befehlszeilenschnittstelle für View Client kann Exitcodes mit Informationen zu Fehlern zurückgeben, die von View Client ermittelt werden.

Tabelle 1-3 zeigt die Exitcodes, die vom Befehl `vmware-view` zurückgegeben werden können. Manche Codes betreffen ausschließlich View Client für Windows.

Tabelle 1-3. View Client-Exitcodes

Exitcode	Beschreibung
-1	Schwerwiegender Fehler im Kiosk-Modus.
0	Vorgang erfolgreich.
1	Verbindung fehlgeschlagen.
2	Anmeldung fehlgeschlagen.
3	Desktop konnte nicht gestartet werden.
4	RDP konnte nicht gestartet werden.
5	RDP-Vorgang fehlgeschlagen.
6	Tunnelverbindung unterbrochen.
7	Fehler beim Übertragen des lokalen Desktops.
8	Fehler beim Einchecken des lokalen Desktops.
9	Fehler beim Auschecken des lokalen Desktops.

Tabelle 1-3. View Client-Exitcodes (Fortsetzung)

Exitcode	Beschreibung
10	Fehler beim Rollback des lokalen Desktops.
11	Unbekanntes Ergebnis während der Authentifizierung.
12	Authentifizierungsfehler.
13	Anforderung zur Verwendung einer unbekannten Authentifizierungsmethode empfangen.
14	Ungültige Serverantwort.
15	Desktop wurde getrennt.
16	Tunnel wurde getrennt.
17	Für zukünftige Entwicklung reserviert.
18	Für zukünftige Entwicklung reserviert.
19	Nicht unterstützter Kiosk-Vorgang.
20	RMKS-Verbindungsfehler (Remote Mouse, Keyboard, or Screen).
21	PIN-Fehler.
22	Keine Übereinstimmung für PIN.
23	Keine Übereinstimmung für Kennwort.
24	View Connection Server-Fehler.
25	Desktop war nicht verfügbar.

Umleiten eines USB-Geräts auf einen Remotedesktop

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

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

Mit dem folgenden Beispiel wird die Protokollierung auf Ablaufebene aktiviert:

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

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

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

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

Tabelle 1-4. USB-Umleitungsoptionen

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

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

Tabelle 1-4. USB-Umleitungsoptionen (Fortsetzung)

Option	Beschreibung

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Mit dem folgenden Beispiel werden bis auf ein durch seine ID angegebenes Gerät alle Storage-Gerätefamilien ausgeschlossen:

```
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

W

Z