

# Einrichten von Horizon 7 for Linux-Desktops

DEZ 2019

VMware Horizon 7 7.11



vmware®

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

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

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese an:

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**VMware Global, Inc.**  
Zweigniederlassung Deutschland  
Willy-Brandt-Platz 2  
81829 München  
Germany  
Tel.: +49 (0) 89 3706 17 000  
Fax: +49 (0) 89 3706 17 333  
[www.vmware.com/de](http://www.vmware.com/de)

Copyright © 2016–2019 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

# Inhalt

Einrichten von Horizon 7 für Linux-Desktops	6
<b>1 Funktionen und Systemanforderungen</b>	<b>7</b>
Funktionen von Horizon Linux-Desktops	7
Übersicht über die Konfigurationsschritte für Horizon 7 for Linux-Desktops	13
Systemanforderungen für Horizon 7 for Linux	15
Einstellungen der virtuellen Maschine für 2D-Grafiken	24
Funktion „Session Collaboration“ auf Linux-Desktops konfigurieren	25
<b>2 Vorbereiten einer virtuellen Linux-Maschine für die Desktop-Bereitstellung</b>	<b>28</b>
Erstellen einer virtuellen Maschine und Installieren von Linux	28
Vorbereiten einer Linux-Maschine für die Remote-Desktop-Bereitstellung	29
Installieren von Abhängigkeitspaketen für Horizon Agent	32
<b>3 Einrichten der Active Directory-Integration für Linux-Desktops</b>	<b>33</b>
Integrieren von Linux mit Active Directory	33
Verwenden der OpenLDAP-Server-Pass-Through-Authentifizierung	34
SSSD-LDAP-Authentifizierung bei Microsoft Active Directory einrichten	34
Verwenden der Winbind-Domänenbeitrittslösung	34
PowerBroker Identity Services Open(PBISO)-Authentifizierung konfigurieren	35
Konfigurieren des Samba-Offline-Domänenbeitritts	36
Verwenden der Realmd-Beitrittslösung für RHEL/CentOS 8.0	38
Einrichten von Single Sign-On	39
Einrichten der Smartcard-Umleitung	41
Konfigurieren der Smartcard-Umleitung für RHEL 8.0-Desktops	42
Konfigurieren der Smartcard-Umleitung für RHEL 7.x/6.x-Desktops	47
Konfigurieren der Smartcard-Umleitung für Ubuntu-Desktops	53
Konfigurieren der Smartcard-Umleitung für SLED/SLES-Desktops	63
Einrichten von True SSO für Linux-Desktops	70
Konfigurieren von True SSO auf RHEL/CentOS 8.0-Desktops	70
Konfigurieren von True SSO für RHEL/CentOS 7.x-Desktops	72
Konfigurieren von True SSO für Ubuntu-Desktops	76
Konfigurieren von True SSO für SLED/SLES-Desktops	82
<b>4 Einrichten von Grafiken für Linux-Desktops</b>	<b>87</b>
Konfigurieren unterstützter Linux-Distributionen für vGPU	87
Installieren des VIB für die NVIDIA GRID vGPU-Grafikkarte auf dem ESXi-Host	88

Konfigurieren eines gemeinsam genutzten PCI-Geräts für vGPU auf der virtuellen Linux-Maschine	89
Installieren des NVIDIA GRID vGPU-Anzeigetreibers	90
Überprüfen, ob der NVIDIA-Anzeigetreiber installiert ist	91
Konfigurieren von RHEL 6.x für vDGA	92
Aktivieren von DirectPath I/O für NVIDIA GRID auf einem Host	92
Hinzufügen eines vDGA-Passthrough-Geräts zu einer virtuellen RHEL 6.x-Maschine	93
Installieren des NVIDIA-Anzeigetreibers für vDGA	94
Überprüfen, ob der NVIDIA-Anzeigetreiber installiert ist	95
<b>5 Installieren von Horizon Agent</b>	<b>97</b>
Installieren von Horizon Agent auf einer virtuellen Linux-Maschine	97
Befehlszeilenoptionen für install_viewagent.sh	98
Konfigurieren des Zertifikats für den Linux Agent	100
Durchführen eines Upgrades von Horizon Agent auf einer virtuellen Linux-Maschine	101
Durchführen eines Upgrades von Horizon Agent auf einer virtuellen Linux-Maschine	102
Deinstallieren von Horizon 7 für Linux-Maschinen	103
<b>6 Konfigurationsoptionen für Linux-Desktops</b>	<b>105</b>
Einstellen der Optionen in Konfigurationsdateien auf einem Linux-Desktop	105
Verwenden von Intelligente Richtlinien	117
Anforderungen für Intelligente Richtlinien	118
Installieren von Dynamic Environment Manager	118
Konfigurieren von Dynamic Environment Manager	118
Einstellungen für intelligente Horizon-Richtlinien	119
Hinzufügen von Bedingungen zu intelligenten Horizon-Richtliniendefinitionen	119
Erstellen einer intelligenten Horizon-Richtlinie in Dynamic Environment Manager	120
Beispiel für Blast-Einstellungen für Linux-Desktops	122
Beispiel für Optionen der Clientlaufwerksumleitung für Linux-Desktops	123
<b>7 Erstellen und Verwalten von Linux-Desktop-Pools</b>	<b>124</b>
Erstellen eines manuellen Desktop-Pools für Linux	125
Verwalten von Linux-Desktop-Pools	126
Erstellen eines automatisierten Full-Clone-Desktop-Pools für Linux	127
Erstellen eines dynamischen Instant-Clone-Desktop-Pools für Linux	129
Broker-PowerCLI-Befehle	133
<b>8 Massenbereitstellung von Horizon 7 für manuelle Desktop-Pools</b>	<b>137</b>
Überblick über die Massenbereitstellung von Linux-Desktops	138
Überblick über die Massenaktualisierung von Linux-Desktops	139
Erstellen einer Vorlage für virtuelle Maschinen zum Klonen von Linux-Desktop-Maschinen	140
Eingabedatei für die PowerCLI-Beispielskripts zur Bereitstellung von Linux-Desktops	142

Beispielskript zum Klonen von virtuellen Linux-Maschinen	143
Beispielskript zum Hinzufügen geklonter virtueller Maschinen zu einer AD-Domäne	147
Beispielskript zum Hinzufügen geklonter virtueller Maschinen zu einer AD-Domäne mithilfe von SSH	150
Beispielskript zum Hochladen von Konfigurationsdateien zu virtuellen Linux-Maschinen	154
Beispielskript zum Hochladen von Konfigurationsdateien zu virtuellen Linux-Maschinen mithilfe von SSH	157
Beispiel-PowerCLI-Skript zum Upgrade von Horizon Agent auf Linux-Desktop-Maschinen	161
Beispielskript zur Durchführung eines Upgrades von Horizon Agent auf virtuellen Linux-Maschinen mithilfe von SSH	166
Beispielskript zum Ausführen von Vorgängen auf virtuellen Linux-Maschinen	172

## 9 Fehlerbehebung bei Linux-Desktops 176

Verwenden des Horizon Help Desk Tool in Horizon Console	176
Starten des Horizon Help Desk Tool an der Horizon Console	177
Fehlerbehebung bei Benutzern in Horizon Help Desk Tool	177
Sitzungsdetails für das Horizon Help Desk Tool	180
Sitzungsprozesse für das Horizon Help Desk Tool	184
Fehlerbehebung bei Linux-Desktop-Sitzungen in Horizon Help Desk Tool	185
Ermitteln von Diagnoseinformationen für eine Horizon 7 for Linux-Maschine	186
Fehler beim Trennen der Verbindung auf dem Horizon Client für ein iPad Pro durch Horizon Agent	187
SLES 12 SP1-Desktop wird nicht automatisch aktualisiert	187
Fehlerhafte SSO-Verbindung zu einem PowerOff-Agenten	188
Nicht erreichbare VM nach dem Erstellen eines manuellen Desktop-Pools für Linux	188

# Einrichten von Horizon 7 für Linux-Desktops

Im Dokument *Einrichten von Horizon 7 for Linux-Desktops* finden Sie Informationen zum Einrichten einer virtuellen Linux-Maschine für die Verwendung als VMware Horizon® 7 für Linux-Desktop. Die Informationen beziehen sich auf die Vorbereitung des Linux-Gastbetriebssystems, die Installation von Horizon Agent auf der virtuellen Maschine und die Konfiguration der Maschine in Horizon Console für die Verwendung in einer Horizon 7-Bereitstellung.

## Zielgruppe

Diese Informationen richten sich an alle, die Remote-Desktops konfigurieren und verwenden möchten, die auf Linux-Gastbetriebssystemen ausgeführt werden. Diese Informationen sind für erfahrene Linux-Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und Vorgängen in Datacentern vertraut sind.

# Funktionen und Systemanforderungen

# 1

Mit Horizon 6.2.x oder höher können Benutzer eine Verbindung zu Remote-Desktops herstellen, auf denen das Linux-Betriebssystem ausgeführt wird.

Dieses Kapitel enthält die folgenden Themen:

- [Funktionen von Horizon Linux-Desktops](#)
- [Übersicht über die Konfigurationsschritte für Horizon 7 for Linux-Desktops](#)
- [Systemanforderungen für Horizon 7 for Linux](#)

## Funktionen von Horizon Linux-Desktops

Die folgende Liste enthält die wichtigsten Funktionen, die für Horizon-Linux-Desktops unterstützt werden.

### Auf Linux-Desktops unterstützte Funktionen

#### Active Directory-Integration

Instant-Clone-Desktops, auf denen die folgenden Linux-Distributionen ausgeführt werden, können einen Offline-Domänenbeitritt mit Active Directory mithilfe von PowerBroker Identity Services Open (PBISO) durchführen.

- Ubuntu 16.04 und 18.04
- SLED/SLES 12.x

Weitere Informationen finden Sie im Abschnitt „PBISO-Authentifizierung (PowerBroker Identity Services Open)“ in [Integrieren von Linux mit Active Directory](#).

Instant-Clone-Desktops, auf denen die folgenden Linux-Distributionen ausgeführt werden, können einen Offline-Domänenbeitritt mit Active Directory mithilfe von Samba durchführen.

- Ubuntu 16.04 und 18.04

- RHEL 7.3 und 8.0

## Audio-Eingang

Die Umleitung des Audio-Eingangs von einem Clienthost zu einem Linux-Remote-Desktop wird unterstützt. Diese Funktion basiert nicht auf der Funktion der USB-Umleitung. Wenn diese Funktion aktiviert werden soll, müssen Sie diese bei der Installation auswählen. Gleichzeitig müssen Sie das standardmäßige System-Audio im Gerät „PulseAudio Server (lokal)“ in Ihrer Anwendung für den Audio-Eingang auswählen. Diese Funktion wird auf den im Folgenden aufgeführten Linux-Distributionen unterstützt.

- Ubuntu 16.04 x64 mit MATE- oder Gnome Flashback (Metacity)-Desktop-Umgebung
- Ubuntu 18.04 x64 mit MATE- oder Gnome Ubuntu-Desktop-Umgebung
- RHEL 7.x Workstation x64 mit KDE- oder Gnome-Desktop-Umgebung
- RHEL 8.0 Workstation x64 mit Gnome-Desktop-Umgebung
- SLED/SLES 12.x SP3 x64

## Audio-Ausgabe

Die Umleitung der Audioausgabe wird unterstützt. Diese Funktion ist standardmäßig aktiviert. Um diese Funktion zu deaktivieren, müssen Sie für die Option `RemoteDisplay.allowAudio` **false** festlegen. Bei Verwendung von Chrome oder Firefox realisiert VMware Horizon HTML Access die Unterstützung der Audio-Ausgabe für Linux-Desktops.

## Automatisierter Full-Clone-Desktop-Pool

Sie können automatisierte Full-Clone-Desktop-Pools für Linux-Desktops erstellen.

## Clientlaufwerksumleitung

Wenn Sie die CDR-Funktion (Client Drive Redirection) aktivieren, können Sie auf die freigegebenen Ordner und Laufwerke Ihres lokalen Systems zugreifen. Sie verwenden dazu den `tsclient`-Ordner in Ihrem Stammverzeichnis auf dem Remote-Linux-Desktop. Um diese Funktion verwenden zu können, müssen Sie die CDR-Komponenten installieren.

## Zwischenablagenumleitung

Mit der Zwischenablagenumleitung können Sie RTF- oder reinen Text zwischen einem Clienthost und einem Linux-Remote-Desktop kopieren und einfügen. Sie können mithilfe der Optionen von Horizon Agent die Richtung und die maximale Textgröße für das Kopieren/Einfügen festlegen. Diese Funktion ist standardmäßig aktiviert. Sie können die Funktion bei der Installation deaktivieren.

## FIPS 140-2-Modus

Die Unterstützung des FIPS 140-2-Modus (Federal Information Processing Standard) ist zwar noch nicht NIST CMVP-validiert (Cryptographic Module Validation Program), ist aber für Linux-Desktops verfügbar.



Horizon 7 Agent für Linux implementiert kryptografische Module, die auf FIPS 140-2-Kompatibilität ausgelegt sind. Diese Module wurden in im CMVP-Zertifikat 2839 und 2866 aufgelisteten Betriebsumgebungen überprüft und auf diese Plattform portiert. Allerdings muss die CAVP- und CMVP-Testanforderung, die neuen Betriebsumgebungen in den NIST CAVP- und CMVP-Zertifikaten von VMware aufzuführen, im Rahmen der Produkt-Roadmap noch erfüllt werden.

---

**Hinweis** Für die Unterstützung des FIPS 140-2-Modus ist das TLS-Protokoll (Transport Layer Security-Protokoll) Version 1.2 erforderlich.

---

### Helpdesk-Tool

Horizon Help Desk Tool ist eine Webanwendung, mit der Sie Fehler in Linux-Desktop-Sitzungen beheben können. Mithilfe des Horizon Help Desk Tool können Sie den Status von Horizon 7-Benutzersitzungen abrufen und eine Fehlerbehebung sowie Wartungsvorgänge durchführen. Siehe [Verwenden des Horizon Help Desk Tool in Horizon Console](#).

### Intelligente Horizon-Richtlinien

Mithilfe von VMware Dynamic Environment Manager™ 9.4 oder höher können Sie Horizon Intelligente Richtlinien erstellen, die das Verhalten der Funktionen für die USB-Umleitung, Umleitung der Zwischenablage und Clientlaufwerksumleitung auf bestimmten Remote-Linux-Desktops steuern. Siehe [Verwenden von Intelligente Richtlinien](#).

### H.264-Encoder

Die H.264-Decodierung kann die Blast Extreme-Leistung für Horizon Desktop verbessern, insbesondere bei Netzwerken mit niedriger Bandbreite. Wenn für das Clientsystem H.264 deaktiviert ist, wird Blast Extreme automatisch auf die Verwendung der JPEG-/PNG-Codierung zurückgesetzt.

Der H.264-Encoder unterstützt sowohl H.264-Hardware- als auch Software-Encoder. Für die Hardware-H.264-Codierung gelten die folgenden Anforderungen.

- Die vGPU ist mit einer NVIDIA-Grafikkarte konfiguriert.
- Ein NVIDIA-Treiber der Serie 384 oder höher ist in der NVIDIA-Grafikkarte installiert.

Wenn das System die vorherigen Anforderungen erfüllt, nutzt Horizon 7 for Linux den Hardware-H.264-Encoder. Anderenfalls wird der Software-H.264-Encoder verwendet.

### Dynamischer Instant-Clone-Desktop-Pool

Sie können dynamische Instant-Clone-Desktop-Pools für Linux-Desktops erstellen. Diese Funktion wird nur auf Systemen mit den folgenden Linux-Distributionen unterstützt.

- Ubuntu 16.04 und 18.04

- RHEL 7.1 oder höher
- RHEL 8.0
- SLED/SLES 12.x

Weitere Informationen finden Sie unter [Erstellen eines dynamischen Instant-Clone-Desktop-Pools für Linux](#).

## K Desktop Environment

KDE (K Desktop Environment) wird von den folgenden Linux-Distributionen unterstützt.

- CentOS 6.x und 7.x
- RHEL 6.x und 7.x
- Ubuntu 16.04 und 18.04

## Synchronisierung von Tastaturlayout und Gebietsschema

Diese Funktion legt fest, ob das Systemgebietsschema und das aktuelle Tastaturlayout eines Clients mit den Horizon Linux Agent-Desktops synchronisiert werden sollen. Wenn diese Einstellung aktiviert wurde oder nicht konfiguriert ist, ist eine Synchronisierung zugelassen. Wenn diese Einstellung deaktiviert ist, ist eine Synchronisierung nicht erlaubt.

Diese Funktion wird nur für VMware Horizon for Windows und nur für die Gebietsschemas Englisch, Französisch, Deutsch, Japanisch, Koreanisch, Spanisch, Chinesisch (vereinfacht) und Chinesisch (traditionell) unterstützt.

## Verlustfreier PNG-Modus

Bilder und Videos, die auf einem Desktop erzeugt werden, werden auf dem Clientgerät pixelgenau gerendert.

## Manueller Desktop-Pool

Computerquelle.

- **Verwaltete virtuelle Maschine:** Computerquelle der virtuellen vCenter-Maschine. Eine verwaltete virtuelle Maschine wird für eine neue und eine Upgrade-Bereitstellung unterstützt.
- **Verwaltung der virtuellen Maschine aufheben:** Computerquelle anderer Quellen. Eine nicht verwaltete virtuelle Maschine wird nur beim Upgrade von einer Bereitstellung mit aufgehobener Verwaltung der virtuellen Maschine unterstützt.

---

**Hinweis** Um die bestmögliche Leistung zu gewährleisten, sollten Sie keine nicht verwaltete virtuelle Maschine verwenden.

---

## MATE-Desktop-Umgebung

Die MATE-Desktop-Umgebung wird von den folgenden Linux-Distributionen unterstützt.

- Ubuntu 16.04
- Ubuntu 18.04

## Mehrere Monitore

- vDGA/vGPU-Desktop unterstützt eine maximale Auflösung von 2560x1600 auf vier Monitoren.
- 2D-Desktop auf VMware vSphere® 6.0 oder höher unterstützt eine maximale Auflösung von 2048 x 1536 auf vier Monitoren oder eine maximale Auflösung von 2560 x 1600 auf drei Monitoren.

Für Ubuntu 16.04 und 18.04 müssen Sie Gnome, KDE oder die MATE-Desktop-Umgebung verwenden, um die Funktion für mehrere Monitore zu verwenden. Weitere Informationen finden Sie unter <http://kb.vmware.com/kb/2151294>.

Für SLES 12 SP1 müssen Sie das Standardpaket mit der Kernelebene kernel-default-3.12.49-11.1 verwenden. Wenn Sie ein Upgrade für das Paket durchgeführt haben, kann die Funktion für mehrere Monitore nicht benutzt werden. Der Desktop wird nur in einem Monitor angezeigt.

Ab VMware Horizon HTML Access™ Version 5.0 wird die Funktion für mehrere Monitore in Horizon 7 für Linux-Desktops unterstützt.

## Unterstützung für intelligente Netzwerke für VMware Blast

Der intelligente Netzwerktransport wird für VMware Blast unterstützt. Diese Funktion ist standardmäßig aktiviert.

Wenn das User Datagram Protocol (UDP) aktiviert ist, stellt Blast sowohl Verbindungen über das Transmission Control Protocol (TCP) als auch über das UDP her. Basierend auf den aktuellen Netzwerkbedingungen wählt Blast dynamisch eine der Transportoptionen für die Übertragung von Daten aus, um die bestmögliche Benutzererfahrung bereitzustellen. Für ein lokales Netzwerk (Local Area Network, LAN) eignet sich TCP beispielsweise besser als UDP, weshalb Blast für den Datentransport TCP auswählt. Gleichermaßen ist die Leistung von UDP in einem Fernnetz (Wide Area Network, WAN) höher als die von TCP, weshalb Blast in dieser Umgebung den UDP-Transport auswählt.

Wenn eine der verwendeten Inline-Komponenten UDP nicht unterstützt, stellt Blast nur eine TCP-Verbindung her. Wenn für Ihre Verbindung beispielsweise die Blast Security Gateway-Komponente des Horizon-Verbindungsservers oder des Sicherheitsservers genutzt wird, wird nur eine TCP-Verbindung hergestellt. Auch wenn UDP sowohl für Client wie auch für Agent aktiviert ist, wird für die Verbindung TCP verwendet, da Blast Security Gateway UDP nicht unterstützt. Wenn der Benutzer eine Verbindung von außerhalb des Unternehmensnetzwerks herstellt, erfordert die UDP-Komponente das VMware Unified Access Gateway (früher: Access Point), das UDP unterstützt.

Verwenden Sie die folgenden Informationen zum Herstellen einer UDP-basierten Blast-Verbindung.

- Falls der Client direkt mit einem Linux-Desktop verbunden wird, aktivieren Sie die UDP-Funktion auf dem Client und dem Agent. UDP ist standardmäßig auf dem Client und dem Agent aktiviert.
- Falls der Client über das Unified Access Gateway mit einem Linux-Desktop verbunden wird, aktivieren Sie die UDP-Funktion auf dem Client, dem Agent und im Unified Access Gateway.

### **Session Collaboration**

Mit der Funktion „Session Collaboration“ können Benutzer andere Benutzer zur Teilnahme an einer vorhandenen Linux-Desktop-Sitzung einladen. Oder Sie können an einer gemeinsamen Sitzung teilnehmen, wenn Sie eine Einladung von einem anderen Benutzer erhalten. Diese Funktion wird nur auf Linux-Remote-Desktops mit den folgenden Linux-Distributionen unterstützt.

- Ubuntu 18.04 mit Gnome-Desktop-Umgebung
- RHEL 7.5 oder höher mit klassischer Gnome-Desktop-Umgebung
- RHEL 8.0 mit klassischer Gnome-Desktop-Umgebung

### **Single Sign-On**

Single Sign-On (SSO) wird von den folgenden Linux-Distributionen unterstützt.

- RHEL 8.0/7.x/6.x Workstation x64
- CentOS 8.0/7.x/6.x x64
- SLED/SLES 12.x SP3/SP2/SP1
- Ubuntu 18.04/16.04 x64

### **Smartcard-Umleitung**

Die Smartcard-Umleitung wird von den folgenden Linux-Distributionen unterstützt.

- RHEL 8.0
- RHEL 7.1 und höher
- RHEL 6.6 und höher
- Ubuntu 18.04/16.04
- SLED/SLES 12.x SP3

Diese Funktion unterstützt PIV(Personal Identity Verification)- und CAC-Karten (Common Access Cards). Weitere Informationen finden Sie unter [Einrichten der Smartcard-Umleitung](#).

### **True SSO-Unterstützung**

True SSO wird von den folgenden Linux-Distributionen unterstützt.

- RHEL 7.x/8.0

- CentOS 7.x/8.0
- SLED/SLES 12.x SP3
- Ubuntu 18.04/16.04

Weitere Informationen finden Sie unter [Einrichten von True SSO für Linux-Desktops](#).

### USB-Umleitung

Mit der Funktion für die USB-Umleitung haben Sie von Linux-Remote-Desktops aus Zugriff auf lokal angeschlossene USB-Geräte. Sie müssen die Komponenten der USB-Umleitung und das USB-VHCI-Treiber-Kernelmodul installieren, um die USB-Funktion verwenden zu können. Stellen Sie sicher, dass Sie über ausreichend Rechte für die Verwendung des USB-Geräts verfügen, das Sie umleiten möchten.

### 3Dconnexion-Maus

Um die 3Dconnexion-Maus verwenden zu können, müssen Sie den entsprechenden Gerätetreiber installieren und die Maus mithilfe des Menüs „USB-Gerät verbinden“ auf Ihrem Linux-Desktop verbinden.

### 3D-Grafiken

Die 3D-Grafikfunktion unterstützt die folgenden Kombinationen von Linux-Versionen und Grafikkarten:

- vDGA wird von RHEL 6.x Workstation x64 mit NVIDIA GRID K1- oder K2-Grafikkarten unterstützt.
- vGPU wird von den Linux-Distributionen und NVIDIA-Grafikkarten unterstützt, die auf <https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html> aufgeführt sind.

## Einschränkungen für Linux-Desktops und Desktop-Pools

Für Linux-Desktops und Desktop-Pools gelten die folgenden Einschränkungen:

- Virtueller Druck, standortbasiertes Drucken und Echtzeit-Video werden nicht unterstützt.
- Die Funktion zur Dateiübertragung von VMware HTML Access wird nicht unterstützt.

---

**Hinweis** Wird ein Sicherheitsserver verwendet, muss der Port 22443 in der internen Firewall geöffnet sein, damit ein Datenverkehr zwischen dem Sicherheitsserver und dem Linux-Desktop möglich ist.

---

## Übersicht über die Konfigurationsschritte für Horizon 7 for Linux-Desktops

Wenn Sie Horizon 7 for Linux-Desktops installieren und konfigurieren, müssen Sie unterschiedliche Schritte durchführen, je nachdem, ob Sie 2D-Grafiken oder 3D-Grafiken auf den virtuellen Maschinen installieren.

## 2D-Grafiken – Überblick über die Konfigurationsschritte

Für 2D-Grafiken führen Sie die folgenden Schritte durch:

- 1 Überprüfen Sie die Systemanforderungen für die Einrichtung einer Horizon 7 for Linux-Bereitstellung. Siehe [Systemanforderungen für Horizon 7 for Linux](#).
- 2 Erstellen Sie in vSphere eine virtuelle Maschine und installieren Sie das Linux-Betriebssystem. Siehe [Erstellen einer virtuellen Maschine und Installieren von Linux](#).
- 3 Bereiten Sie das Gastbetriebssystem für eine Bereitstellung als Desktop in einer Horizon 7-Umgebung vor. Siehe [Vorbereiten einer Linux-Maschine für die Remote-Desktop-Bereitstellung](#).
- 4 Konfigurieren Sie das Linux-Gastbetriebssystem zur Authentifizierung mit Active Directory. Dieser Schritt wird mit einer Drittanbietersoftware basierend auf den Anforderungen in Ihrer Umgebung implementiert. Weitere Informationen finden Sie unter [Integrieren von Linux mit Active Directory](#).
- 5 Installieren Sie Horizon Agent auf der virtuellen Linux-Maschine. Siehe [Installieren von Horizon Agent auf einer virtuellen Linux-Maschine](#).
- 6 Erstellen Sie einen Desktop-Pool mit den konfigurierten virtuellen Linux-Maschinen. Siehe [Erstellen eines manuellen Desktop-Pools für Linux](#).

## 3D-Grafiken – Überblick über die Konfigurationsschritte

Sie müssen die Konfiguration von NVIDIA GRID vGPU oder vDGA auf den virtuellen Linux-Maschinen abschließen, bevor Sie Horizon Agent auf den Maschinen installieren und einen Desktop-Pool in Horizon Console bereitstellen.

- 1 Überprüfen Sie die Systemanforderungen für die Einrichtung einer Horizon 7 for Linux-Bereitstellung. Siehe [Systemanforderungen für Horizon 7 for Linux](#).
- 2 Erstellen Sie in vSphere eine virtuelle Maschine und installieren Sie das Linux-Betriebssystem. Siehe [Erstellen einer virtuellen Maschine und Installieren von Linux](#).
- 3 Bereiten Sie das Gastbetriebssystem für eine Bereitstellung als Desktop in einer Horizon 7-Umgebung vor. Siehe [Vorbereiten einer Linux-Maschine für die Remote-Desktop-Bereitstellung](#).
- 4 Konfigurieren Sie das Linux-Gastbetriebssystem zur Authentifizierung mit Active Directory. Dieser Schritt wird mit einer Drittanbietersoftware basierend auf den Anforderungen in Ihrer Umgebung implementiert. Weitere Informationen finden Sie unter [Integrieren von Linux mit Active Directory](#).
- 5 Konfigurieren Sie 3D-Funktionen auf Ihren ESXi-Hosts und der virtuellen Linux-Maschine. Folgen Sie den Vorgehensweisen für die 3D-Funktion, die Sie installieren möchten.
  - Siehe [Konfigurieren unterstützter Linux-Distributionen für vGPU](#).
  - Siehe [Konfigurieren von RHEL 6.x für vDGA](#).
- 6 Installieren Sie Horizon Agent auf der virtuellen Linux-Maschine. Siehe [Installieren von Horizon Agent auf einer virtuellen Linux-Maschine](#).
- 7 Erstellen Sie einen Desktop-Pool mit den konfigurierten virtuellen Linux-Maschinen. Siehe [Erstellen eines manuellen Desktop-Pools für Linux](#).

## Massenbereitstellung

Mit Horizon Console können Sie nur virtuelle Linux-Maschinen in einem manuellen Desktop-Pool bereitstellen. vSphere PowerCLI bietet dagegen die Möglichkeit zur Entwicklung von Skripts, die die Bereitstellung eines Pools von Linux-Desktop-Maschinen automatisieren. Siehe [Kapitel 8 Massenbereitstellung von Horizon 7 für manuelle Desktop-Pools](#).

## Systemanforderungen für Horizon 7 for Linux

Für die Installation von Horizon 7 for Linux muss Ihr Linux-System bestimmte Anforderungen in Bezug auf das Betriebssystem, Horizon 7 und die vSphere-Plattform erfüllen.

### Unterstützte Linux-Versionen für Horizon Agent

In der folgenden Tabelle sind die Linux-Betriebssysteme aufgeführt, die für Horizon Agent unterstützt werden.

**Tabelle 1-1. Unterstützte Linux-Betriebssysteme für Horizon Agent**

Linux-Distribution	Architektur
Ubuntu 16.04 und 18.04	x64
<b>Hinweis</b> Sie müssen eine der im VMware-KB-Artikel <a href="http://kb.vmware.com/kb/2151294">http://kb.vmware.com/kb/2151294</a> beschriebenen Lösungen anwenden.	
RHEL 6.6, 6.7, 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7 und 8.0	x64
CentOS 6.6, 6.7, 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7 und 8.0	x64
NeoKylin 6 Update 1	x64
SLED 12.x SP1/SP2/SP3	x64
SLES 12.x SP1/SP2/SP3	x64

**Hinweis** Der Linux Agent verfügt bei einigen Linux-Distributionen über Abhängigkeitspakete. Weitere Informationen finden Sie unter [Installieren von Abhängigkeitspaketen für Horizon Agent](#).

**Hinweis** Auf RHEL/CentOS 8.0-Systemen unterstützt Horizon Agent nur das X11-Anzeigeserverprotokoll. Das Wayland-Protokoll wird nicht unterstützt.

### Erforderliche Plattform- und Horizon 7-Softwareversionen

Um Horizon 7 for Linux installieren und anwenden zu können, muss Ihre Bereitstellung bestimmte Anforderungen für die vSphere-Plattform, Horizon 7 und die Horizon Client-Software erfüllen.

**Tabelle 1-2. Erforderliche Plattform- und Horizon 7-Softwareversionen**

Plattform und Software	Unterstützte Versionen
vSphere-Plattformversion	<ul style="list-style-type: none"> <li>■ vSphere 6.0 U2 oder eine höhere Version</li> <li>■ vSphere 6.5 U1 oder eine höhere Version</li> <li>■ vSphere 6.7 oder eine höhere Version</li> </ul>
Horizon-Umgebung	<ul style="list-style-type: none"> <li>■ Horizon-Verbindungsserver 7.11</li> </ul>
Horizon Client-Software	<ul style="list-style-type: none"> <li>■ Horizon Client 5.3.0 für Android</li> <li>■ Horizon Client 5.3.0 für Windows</li> <li>■ Horizon Client 5.3.0 für Linux</li> <li>■ Horizon Client 5.3.0 für Mac OS X</li> <li>■ Horizon Client 5.3.0 für iOS (iPad Pro)</li> <li>■ HTML Access 5.3.0 für Chrome, Firefox und Internet Explorer</li> <li>■ Zero Clients werden nicht unterstützt.</li> </ul>

## Von virtuellen Linux-Maschinen verwendete TCP/UDP-Ports

Horizon Agent und Horizon Clients verwenden TCP- bzw. UDP-Ports für den Netzwerkzugriff untereinander und zwischen den verschiedenen Horizon Server-Komponenten.

**Tabelle 1-3. Von virtuellen Linux-Maschinen verwendete TCP/UDP-Ports**

Quelle	Port	Ziel	Port	Protokoll	Beschreibung
Horizon Client	*	Linux Agent	22443	TCP/UDP	Blast, wenn Blast Security Gateway nicht verwendet wird
Sicherheitsserver, Horizon-Verbindungsserver oder Access Point-Appliance	*	Linux Agent	22443	TCP/UDP	Blast, wenn Blast Security Gateway verwendet wird
Horizon-Agent	*	Horizon-Verbindungsserver	4001, 4002	TCP	JMS-SSL-Datenverkehr.

**Hinweis** Weitere Informationen zu von Clients verwendeten TCP- und UDP-Ports finden Sie im Dokument *Horizon Client und Agent-Sicherheit* und im Leitfaden [Netzwerkports in VMware Horizon 7](#).

Damit Benutzer sich mit ihren Linux-Desktops verbinden können, müssen die Desktops eingehende TCP-Verbindungen von Horizon Client-Geräten, vom Sicherheitsserver und von Horizon Connection Server akzeptieren.

Bei Ubuntu- und Kylin-Distributionen wird standardmäßig die iptables-Firewall mit einer Eingaberichtlinie von ACCEPT konfiguriert.

Bei RHEL- und CentOS-Distributionen konfiguriert, wenn möglich, das Horizon Agent-Installationsskript die iptables-Firewall mit einer Eingaberichtlinie von ACCEPT.



Stellen Sie sicher, dass `iptables` auf einem RHEL- oder CentOS-Gastbetriebssystem über eine Eingaberichtlinie von ACCEPT für neue Verbindungen vom Blast-Port 22443 verfügt.

Wenn der BSG (Blast Secure Gateway) aktiviert ist, werden die Clientverbindungen von einem Horizon Client-Gerät über den BSG auf einem Sicherheitsserver oder Horizon Connection Server zum Linux-Desktop hergestellt. Ist der BSG nicht aktiviert, werden die Verbindungen zum Linux-Desktop direkt vom Horizon Client-Gerät hergestellt.

## Überprüfen des von virtuellen Linux-Maschinen verwendeten Linux-Kontos

**Tabelle 1-4. Kontoname und Kontotyp** enthält den Kontonamen und den Kontotyp, die von Linux-Maschinen verwendet werden.

**Tabelle 1-4. Kontoname und Kontotyp**

Kontoname	Kontotyp	Verwendet von
Stammordner	Integriertes Linux-Betriebssystem	Java Standalone Agent, mksvchanserver, Shell-Skripts
vmwblast	Erstellt durch das Linux Agent-Installationsprogramm	VMwareBlastServer
<Aktuell angemeldeter Benutzer>	Integriertes Linux-Betriebssystem oder AD-Benutzer oder LDAP-Benutzer	Python-Skript

## Desktop-Umgebung

Horizon 7 for Linux unterstützt mehrere Desktop-Umgebungen auf unterschiedlichen Linux-Distributionen.

**Tabelle 1-5. Unterstützte Desktop-Umgebungen** enthält die Standard-Desktop-Umgebungen für jede Linux-Distribution und die zusätzlichen Desktop-Umgebungen, die von Horizon 7 for Linux unterstützt werden.

**Tabelle 1-5. Unterstützte Desktop-Umgebungen**

Linux-Distribution	Standard-Desktop-Umgebung	Von Horizon 7 for Linux-Desktops unterstützte Desktop-Umgebungen
Ubuntu 18.04	Gnome	Gnome Ubuntu, K Desktop Environment (KDE), MATE
Ubuntu 16.04	Unity	Gnome Flashback (Metacity), KDE, MATE
RHEL/CentOS 6.x	Gnome	Gnome, KDE
RHEL/CentOS 7.x	Gnome	Gnome, KDE
RHEL/CentOS 8.0	Gnome	Gnome
SLED 12 SP1/SP2/SP3	Gnome	Gnome
SLES 12 SP1/SP2/SP3	Gnome	Gnome
NeoKylin 6 Update 1	Mate	Mate

Um die Standard-Desktop-Umgebung zu ändern, die auf einem der unterstützten Linux-Distributionen verwendet wird, müssen Sie die folgenden für Ihren Linux-Desktop geeigneten Schritte und Befehle ausführen.

**Hinweis** Die einmalige Anmeldung (Single Sign-on, SSO) für KDE und die MATE-Desktop-Umgebung funktionieren nur, wenn Ihr Linux-Desktop den standardmäßigen Greeter (Anmeldebildschirm) verwendet. Sie müssen KDE und MATE mit den unter [Tabelle 1-6. Befehle zum Installieren von Desktop-Umgebungen](#) beschriebenen Befehlen installieren.

Wenn Sie RHEL/CentOS 7.x- und Ubuntu 18.04/16.04-Distributionen verwenden, kann eine gesperrte KDE-Sitzung nicht durch SSO entsperrt werden. Sie müssen Ihr Kennwort manuell eingeben, um die gesperrte Sitzung zu entsperren.

- 1 Installieren Sie das unterstützte Betriebssystem der Linux-Distribution mit der Einstellung für die Standard-Desktop-Umgebung.
- 2 Führen Sie die unter [Tabelle 1-6. Befehle zum Installieren von Desktop-Umgebungen](#) aufgeführten entsprechenden Befehle für Ihre spezifische Linux-Distribution aus.

**Tabelle 1-6. Befehle zum Installieren von Desktop-Umgebungen**

Linux-Distribution	Neue Standard-Desktop-Umgebung	Befehle zum Ändern der Standard-Desktop-Umgebung
RHEL/CentOS 6.x	KDE	<code># yum groupinstall "X Window System" "KDE Desktop"</code>
RHEL/CentOS 7.x	KDE	<code># yum groupinstall "KDE Plasma Workspaces"</code>
Ubuntu 18.04/16.04	KDE	<code># apt install plasma-desktop</code>
Ubuntu 18.04	MATE 1.225	<code># apt install ubuntu-mate-desktop</code>
Ubuntu 16.04	MATE 1.16	<code># apt-add-repository ppa:ubuntu-mate-dev/xenial-mate</code> <code># apt update</code> <code># apt upgrade</code> <code># apt install mate</code> <code># apt install ubuntu-mate-themes</code>
Ubuntu 16.04	Gnome Flashback (Metacity)	<code># apt install gnome-session-flashback</code>

- 3 Um die neue Standard-Desktop-Umgebung zu verwenden, starten Sie den Desktop neu.

Wenn Sie die SSO-Funktion auf einem Linux-Desktop aktivieren, auf der mehrere Desktop-Umgebungen installiert sind, beachten Sie die nachfolgend aufgeführten Hinweise zur Auswahl der Desktop-Umgebung.

- Verwenden Sie für Ubuntu 18.04/16.04 und RHEL/CentOS 7.x die Informationen im Abschnitt [Tabelle 1-7. Option SSODesktopType](#) zum Konfigurieren der Option `SSODesktopType` in der Datei `/etc/vmware/viewagent-custom.conf`, um die Desktop-Umgebung festzulegen, für die die SSO-Funktion verwendet werden soll.

**Tabelle 1-7. Option SSODesktopType**

Desktop-Typ	Einstellung der Option SSODesktopType
MATE	<code>SSODesktopType=UseMATE</code>
GnomeUbuntu	<code>SSODesktopType=UseGnomeUbuntu</code>
GnomeFlashback	<code>SSODesktopType=UseGnomeFlashback</code>
KDE	<code>SSODesktopType=UseKdePlasma</code>
GnomeClassic	<code>SSODesktopType=UseGnomeClassic</code>

- Um für RHEL/CentOS 6.x KDE für die SSO-Anmeldesitzung zu verwenden, entfernen Sie alle Desktop-Startdateien mit Ausnahme der KDE-Startdatei aus dem Verzeichnis `/usr/share/xsession`. Verwenden Sie den folgenden Satz an Befehlen als Beispiel.

```
# cd /usr/share/xsessions
# mkdir backup
# mv *.desktop backup
# mv backup/kde*.desktop ./
```

Nach der ersten Einrichtung muss sich der Endbenutzer abmelden oder den Linux-Desktop neu starten, damit KDE in der nächsten SSO-Sitzung als Standard-Desktop verwendet wird.

- Um mit RHEL/CentOS 8.0 für die SSO-Anmeldesitzung Gnome Classic zu verwenden, entfernen Sie alle Desktop-Startdateien mit Ausnahme der Gnome Classic-Startdatei aus dem Verzeichnis `/usr/share/xsession`. Verwenden Sie den folgenden Satz an Befehlen als Beispiel.

```
# cd /usr/share/xsessions
# mkdir backup
# mv *.desktop backup
# mv backup/gnome-classic.desktop ./
```

Nach der ersten Einrichtung muss sich der Endbenutzer abmelden oder den Linux-Desktop neu starten, damit Gnome Classic in der nächsten SSO-Sitzung als Standard-Desktop verwendet wird.

Wenn Sie die SSO-Funktion auf einem Linux-Desktop deaktivieren, auf dem mehrere Desktop-Umgebungen installiert sind, müssen Sie keinen der zuvor beschriebenen Schritte ausführen. Die Endbenutzer müssen ihre gewünschte Desktop-Umgebung auswählen, wenn sie sich mit diesem Linux-Desktop anmelden.

## Netzwerkanforderungen

VMware Blast Extreme unterstützt sowohl das User Datagram Protocol (UDP) als auch das Transmission Control Protocol (TCP). Die Netzwerkbedingungen wirken sich auf die Leistungsfähigkeit von UDP und TCP aus. Wählen Sie für eine bestmögliche Benutzererfahrung UDP oder TCP basierend auf der Netzwerkverbindung aus.

- Wählen Sie TCP aus, wenn die Netzwerkverbindung gut ist, wie z. B. in einer Umgebung mit lokalem Netzwerk (LAN).
- Wählen Sie UDP aus, wenn die Netzwerkverbindung schlecht ist, wie z. B. in einer WAN (Wide Area Network)-Umgebung, in der es zu Paketverlusten und einer zeitlichen Verzögerung kommt.

Ermitteln Sie mit einem Netzwerkanalysetool wie Wireshark, ob VMware Blast Extreme TCP oder UDP verwendet wird. Die im Folgenden aufgeführten Schritte mit Wireshark zeigen eine beispielhafte Verwendung.

- 1 Laden Sie Wireshark herunter und installieren Sie es auf Ihrer Linux-VM.

Für RHEL/CentOS 6:

```
sudo yum install wireshark
```

Für Ubuntu 18.04/16.04:

```
sudo apt install tshark
```

Für SLED/SLES 12:

```
sudo zypper install wireshark
```

- 2 Stellen Sie mithilfe von VMware Horizon Client eine Verbindung mit dem Linux-Desktop her.
- 3 Öffnen Sie ein Terminal-Fenster und führen Sie den im Folgenden aufgeführten Befehl aus. Dieser zeigt das TCP- oder UDP-Paket an, das von VMware Blast Extreme verwendet wird.

```
sudo tshark -i any | grep 22443
```

Die Funktionen USB-Umleitung und Clientlaufwerkumleitung hängen von der Netzwerkverbindung ab. Wenn die Netzwerkverbindung schlecht ist, d. h. nur eine begrenzte Bandbreite mit Zeitverzögerung und Paketverlusten zur Verfügung steht, beeinträchtigt dies die Benutzererfahrung. In diesem Fall kann der Endbenutzer möglicherweise Folgendes feststellen:

- Das Kopieren der Remote-Dateien kann lange dauern. Ist dies der Fall, übertragen Sie stattdessen kleinere Dateien.
- Das USB-Gerät wird nicht auf dem Linux-Remote-Desktop angezeigt.
- Die USB-Daten werden nicht vollständig übertragen. Wenn Sie beispielsweise eine große Datei kopieren, erhalten Sie möglicherweise eine Datei, die kleiner als die Originaldatei ist.

## VHCI-Treiber für die USB-Umleitung

Die USB-Weiterleitungsfunktion verfügt über eine Abhängigkeit vom Kernaltreiber des USB Virtual Host Controller Interface (VHCI). Um USB 3.0 und die USB-Umleitungsfunktion zu unterstützen, müssen Sie die folgenden Schritte ausführen:

- 1 Laden Sie den USB-VHCI-Quellcode von <https://sourceforge.net/projects/usb-vhci/files/linux%20kernel%20module/> herunter.
- 2 Verwenden Sie zum Kompilieren des Quellcodes des VHCI-Treibers und zum Installieren der resultierenden Binärdatei auf Ihrem Linux-System die Befehle in [Tabelle 1-8. Kompilieren und Installieren der VHCI-USB-Treiber](#).

Wenn Sie beispielsweise die Installationsdatei `VMware-horizonagent-linux-x86_64-<version>-<build-number>.tar.gz` entpacken, ist im Verzeichnis `/install_tmp/` die *full-path-to-patch-file* `/install_tmp/VMware-horizonagent-linux-x86_64-<version>-<buildnumber>/resources/vhci/patch/vhci.patch`, und der zu verwendende patch-Befehl lautet

```
# patch -p1 < /install_tmp/VMware-horizonagent-linux-x86_64-<Version>-<Build-Nummer>/resources/
vhci/patch/vhci.patch
```

**Hinweis** Der VHCI-Treiber muss vor der Installation von Horizon for Linux installiert werden.

**Tabelle 1-8. Kompilieren und Installieren der VHCI-USB-Treiber**

Linux-Distribution	Schritte zum Kompilieren und Installieren der VHCI-USB-Treiber
Ubuntu 18.04	<ol style="list-style-type: none"> <li>1 Installieren Sie die Abhängigkeitspakete. <pre># apt-get install make # apt-get install gcc # apt-get install libelf-dev</pre> </li> <li>2 Kompilieren und installieren Sie die VHCI-Treiber. <pre># tar -xzf vhci-hcd-1.15.tar.gz # cd vhci-hcd-1.15 # patch -p1 &lt; full-path-to-patch-file # make clean &amp;&amp; make &amp;&amp; make install</pre> </li> </ol>
Ubuntu 16.04	<p>Kompilieren und installieren Sie die VHCI-Treiber.</p> <pre># tar -xzf vhci-hcd-1.15.tar.gz # cd vhci-hcd-1.15 # patch -p1 &lt; full-path-to-patch-file # make clean &amp;&amp; make &amp;&amp; make install</pre>

**Tabelle 1-8. Kompilieren und Installieren der VHCI-USB-Treiber (Fortsetzung)**

Linux-Distribution	Schritte zum Kompilieren und Installieren der VHCI-USB-Treiber
RHEL/ CentOS 6.9/6.10  RHEL/CentOS 7.x  RHEL/ CentOS 8.0	<p>1 Installieren Sie die Abhängigkeitspakete.</p> <pre># yum install gcc-c++ # yum install kernel-devel-\$(uname -r) # yum install kernel-headers-\$(uname -r) # yum install patch # yum install elfutils-libelf-devel</pre> <p>2 Kompilieren und installieren Sie die VHCI-Treiber.</p> <pre># tar -xvzf vhci-hcd-1.15.tar.gz # cd vhci-hcd-1.15 # patch -p1 &lt; full-path-to-patch-file # make clean &amp;&amp; make &amp;&amp; make install</pre> <p>3 (RHEL/CentOS 8.0) Um sicherzustellen, dass die VHCI-Treiber mit der USB-Umleitung ordnungsgemäß funktionieren, konfigurieren Sie die Signatureinstellungen für den USB-Treiber.</p> <p>a Erstellen Sie ein SSL-Schlüsselpaar für den USB-Treiber.</p> <pre>openssl req -new -x509 -newkey rsa:2048 -keyout MOK.priv -outform DER -out MOK.der -nodes -days 36500 -subj "/CN=Descriptive name/"</pre> <p>b Erstellen Sie eine Signatur für den USB-Treiber.</p> <pre>sudo /usr/src/kernels/\$(uname -r)/scripts/sign-file sha256 ./MOK.priv ./MOK.der /lib/modules/\$(uname -r)/kernel/drivers/usb/host/usb-vhci-iocifc.ko sudo /usr/src/kernels/\$(uname -r)/scripts/sign-file sha256 ./MOK.priv ./MOK.der /lib/modules/\$(uname -r)/kernel/drivers/usb/host/usb-vhci-hcd.ko</pre> <p>c Registrieren Sie den Schlüssel für den sicheren UEFI-Startvorgang.</p> <pre>sudo mokutil --import MOK.der</pre> <p><b>Hinweis</b> Dieser Befehl gibt eine Anforderung zum Festlegen eines Kennworts für den Machine Owner Key (MOK) für den sicheren UEFI-Start aus.</p> <p>d Um einen sicheren UEFI-Start in der vSphere-Konsole einzurichten, starten Sie das System neu. Weitere Informationen finden Sie unter <a href="https://sourceware.org/systemtap/wiki/SecureBoot">https://sourceware.org/systemtap/wiki/SecureBoot</a>.</p>
SLED/SLES 12 SP2	<p>1 Ermitteln Sie die Version des aktuellen Kernelpakets.</p> <pre># rpm -qa   grep kernel-default-\$(echo \$(uname -r)   cut -d '-' -f 1,2)</pre> <p>Die Ausgabe besteht aus dem Namen des aktuell installierten Kernelpakets. Wenn der Name des Pakets z. B. kernel-default-3.0.101-63.1 lautet, ist die aktuelle Version des Kernelpakets 3.0.101-63.1.</p> <p>2 Installieren Sie die Pakete kernel-devel, kernel-default-devel, kernel-macros und patch.</p> <pre># zypper install --oldpackage kernel-devel-&lt;Kernelpaketversion&gt; \ kernel-default-devel-&lt;Kernelpaketversion&gt; kernel-macros-&lt;Kernelpaketversion&gt; patch</pre> <p>Beispiel:</p> <pre># zypper install --oldpackage kernel-devel-4.4.21-90.1 kernel-default-devel-4.4.21-90.1 kernel-macros-4.4.21-90.1 patch</pre>

**Tabelle 1-8. Kompilieren und Installieren der VHCI-USB-Treiber (Fortsetzung)**

Linux-Distribution	Schritte zum Kompilieren und Installieren der VHCI-USB-Treiber
	<p>3 Kompilieren und installieren Sie die VHCI-Treiber.</p> <pre># tar -xzf vhci-hcd-1.15.tar.gz # cd vhci-hcd-1.15 # patch -p1 &lt; full-path-to-patch-file # mkdir -p linux/\$(echo \$(uname -r)   cut -d '-' -f 1)/drivers/usb/core # cp /lib/modules/\$(uname -r)/source/include/linux/usb/hcd.h linux/\$(echo \$(uname -r)   cut -d '-' -f 1)/drivers/usb/core # make clean &amp;&amp; make &amp;&amp; make install</pre>

Beachten Sie außerdem die folgenden Richtlinien:

- Wenn sich Ihre Linux-Kernelversion zu einer neuen Version ändert, müssen Sie den VHCI-Treiber erneut kompilieren und installieren. Horizon for Linux muss aber nicht erneut installiert werden.
- Sie können auch DKMS (Dynamic Kernel Module Support) zum VHCI-Treiber hinzufügen. Gehen Sie dazu wie im folgenden Beispiel für ein Ubuntu 18.04/16.04-System vor.
  - a Installieren Sie die Kernel-Header.

```
# apt install linux-headers-`uname -r`
```

- b Installieren Sie dkms mit dem folgenden Befehl.

```
# apt install dkms
```

- c Extrahieren und patchen Sie die VHCI-TAR-Datei.

```
# tar xzvf vhci-hcd-1.15.tar.gz
# cd vhci-hcd-1.15
# patch -p1 <full-path-to-patch-file>
# cd ..
```

- d Kopieren Sie die extrahierten VHCI-Quelldateien in das Verzeichnis /usr/src.

```
# cp -r vhci-hcd-1.15 /usr/src/usb-vhci-hcd-1.15
```

- e Erstellen Sie eine Datei mit dem Namen dkms.conf und speichern Sie diese im Verzeichnis /usr/src/usb-vhci-hcd-1.15.

```
# touch /usr/src/usb-vhci-hcd-1.15/dkms.conf
```

- f Fügen Sie die folgenden Inhalte zur Datei dkms.conf hinzu.

```
PACKAGE_NAME="usb-vhci-hcd"
PACKAGE_VERSION=1.15
MAKE_CMD_TMPL="make KVERSION=$kernelver"

CLEAN="$MAKE_CMD_TMPL clean"
```

```
BUILT_MODULE_NAME[0]="usb-vhci-iocifc"
DEST_MODULE_LOCATION[0]="/kernel/drivers/usb/host"
MAKE[0]="$MAKE_CMD_TMPL"

BUILT_MODULE_NAME[1]="usb-vhci-hcd"
DEST_MODULE_LOCATION[1]="/kernel/drivers/usb/host"
MAKE[1]="$MAKE_CMD_TMPL"

AUTOINSTALL="YES"
```

- g Fügen Sie diesen VHCI-Treiber zur Datei dkms hinzu.

```
# dkms add usb-vhci-hcd/1.15
```

- h Erstellen Sie den VHCI-Treiber.

```
# dkms build usb-vhci-hcd/1.15
```

- i Installieren Sie den VHCI-Treiber.

```
# dkms install usb-vhci-hcd/1.15
```

## Einstellungen der virtuellen Maschine für 2D-Grafiken

Wenn Sie bestimmte virtuelle Horizon 7 für Linux-Maschinen erstellen, müssen Sie die Einstellungen für vCPU und virtuellen Arbeitsspeicher für die Leistungsanforderungen ändern.

Virtuelle Maschinen, die für die Verwendung von NVIDIA vDGA konfiguriert sind, benutzen die physische NVIDIA-Grafikkarte. Virtuelle Maschinen, die für die Verwendung von NVIDIA GRID vGPU konfiguriert sind, benutzen die virtuelle NVIDIA-Grafikkarte, die auf der Beschleunigung der physischen NVIDIA-Grafikkarte basiert. Sie müssen die Einstellungen für vCPU und virtuellen Arbeitsspeicher für diese virtuellen Maschinen nicht ändern.

Virtuelle Maschinen, die für die Verwendung von 2D-Grafiken konfiguriert sind, verwenden die virtuelle VMware-Grafikkarte, und Sie müssen die Einstellungen für vCPU und virtuellen Arbeitsspeicher ändern, um die Desktop-Leistung zu verbessern. Verwenden Sie die folgenden Richtlinien:

- Wenn Sie die Leistung eines 2D-Desktops verbessern möchten, legen Sie mehr vCPUs und einen größeren virtuellen Arbeitsspeicher für die virtuelle Linux-Maschine fest. So können Sie z. B. zwei vCPUs und zwei GB virtuellen Arbeitsspeicher verwenden.
- Für eine große Bildschirmanzeige mit mehreren Monitoren (z. B. vier Monitore) legen Sie 4 vCPUs und 4 GB virtuellen Arbeitsspeicher für die virtuelle Maschine fest.
- Für die verbesserte Videowiedergabe in einem 2D-Desktop legen Sie 4 vCPUs und 4 GB virtuellen Arbeitsspeicher für die virtuelle Maschine fest.



## Funktion „Session Collaboration“ auf Linux-Desktops konfigurieren

Mit der Funktion „Session Collaboration“ können Benutzer andere Benutzer zur Teilnahme an einer vorhandenen Linux-Remote-Desktop-Sitzung einladen.

### Systemanforderungen für die Funktion „Session Collaboration“

Um die Funktion „Session Collaboration“ zu unterstützen, muss Ihre Horizon-Bereitstellung bestimmte Anforderungen erfüllen.

**Tabelle 1-9. Systemanforderungen für die Funktion „Session Collaboration“**

Komponente	Anforderungen
Clientsystem	Für Sitzungsbesitzer und Sitzungsteilnehmer muss Horizon Client 4.10 oder höher für Windows, Mac oder Linux auf dem Clientsystem installiert sein oder HTML Access 4.10 oder höher verwendet werden.
Linux-Remote-Desktops	Horizon Agent 7.7 oder höher muss auf dem virtuellen Linux-Desktop installiert sein. Die Funktion „Session Collaboration“ muss auf Desktop-Pool- und VDI-Ebene aktiviert sein.
Verbindungsserver	Die Verbindungsserver-Instanz verwendet eine Enterprise-Lizenz.
Anzeigeprotokoll	VMware Blast

**Hinweis** RHEL 8.0-Desktops erfordern eine zusätzliche Systemkonfiguration zur Unterstützung von Session Collaboration. Siehe [Konfigurieren eines RHEL 8.0-Desktops für „Session Collaboration“](#).

Informationen zur Verwendung der „Session Collaboration“-Funktion finden Sie in der Dokumentation zu Horizon Client.

### Optionen der Funktion „Session Collaboration“ in Konfigurationsdateien einstellen

Legen Sie die folgende Option in der Datei `/etc/vmware/viewagent-custom.conf` fest, um die Funktion „Session Collaboration“ zu aktivieren oder deaktivieren.

- `CollaborationEnable`

Legen Sie die folgenden Optionen in der Datei `/etc/vmware/config` fest, um die Einstellungen während einer Zusammenarbeitssitzung zu konfigurieren.

- `collaboration.logLevel`
- `collaboration.maxCollabors`
- `collaboration.enableEmail`
- `collaboration.serverUrl`
- `collaboration.enableControlPassing`

Weitere Informationen finden Sie unter [Einstellen der Optionen in Konfigurationsdateien auf einem Linux-Desktop](#).

## Einschränkungen der Funktion „Session Collaboration“

Benutzern stehen die folgenden Remote-Desktop-Funktionen in einer Zusammenarbeitssitzung nicht zur Verfügung.

- USB-Umleitung
- Audio-Eingabe-Umleitung
- Clientlaufwerkumleitung
- Smartcard-Umleitung
- Zwischenablagenumleitung

Benutzer können die Auflösung des Remote-Desktops in einer gemeinsamen Sitzung nicht ändern.

Benutzer dürfen nicht mehrere Collaboration-Sitzungen auf einem Client Computer ausführen.

---

**Hinweis** Wenn das Symbol „Session Collaboration“ in der Taskleiste nicht mehr reagiert, nachdem sich ein Benutzer zum ersten Mal beim Remote-Desktop angemeldet hat, weisen Sie den Benutzer an, die Größe des Remote-Desktop-Fensters zu ändern. Das Symbol „Session Collaboration“ reagiert wieder, nachdem die Größe des Desktop-Fensters geändert wurde.

---

## Konfigurieren eines RHEL 8.0-Desktops für „Session Collaboration“

Um die Funktion „Session Collaboration“ auf einem RHEL 8.0-Desktop verwenden zu können, müssen Sie zuerst die Shell-Erweiterung GNOME 3.28.26 herunterladen und installieren.

### Verfahren

- 1 Laden Sie die erforderliche GNOME-Shell-Erweiterung von <https://extensions.gnome.org/extension/615/appindicator-support/> für das RHEL 8.0-System herunter. Wählen Sie als Shell-Version **3.28** aus. Wählen Sie als Erweiterungsversion **26** aus.
- 2 Entpacken Sie das heruntergeladene Paket und benennen Sie das Verzeichnis in `appindicator-support@rgcjonas.gmail.com` (der Wert "uuid" in der Datei `metadata.json` im Paket) um.
- 3 Verwenden Sie den Befehl `mv`, um das Verzeichnis `appindicator-support@rgcjonas.gmail.com` an diesen Speicherort zu verschieben: `/usr/share/gnome-shell/extensions`.

Standardmäßig ist die Datei `metadata.json` im Verzeichnis `appindicator-support@rgcjonas.gmail.com` nur für den Root-Benutzer lesbar. Um die Funktion „Session Collaboration“ zu unterstützen, müssen Sie diese Datei auch für andere Benutzer lesbar machen.

- 4 Führen Sie den Befehl aus, um `metadata.json` für andere Benutzer lesbar zu machen, wie im folgenden Beispiel gezeigt.

```
chmod a+r metadata.json
```

- 5 Installieren Sie `gnome-tweaks`.

- 6 Starten Sie GNOME-Shell in der Desktop-Umgebung neu, indem Sie die folgende Tastenkombination auf der Tastatur drücken.

```
Alt+F2  
r  
Enter
```

- 7 Führen Sie `gnome-tweaks` in der Desktop-Umgebung aus und aktivieren Sie dann **KStatusNotifierItem/AppIndicator Support**.

# Vorbereiten einer virtuellen Linux-Maschine für die Desktop-Bereitstellung

## 2

Das Einrichten eines Linux-Desktops umfasst das Erstellen einer virtuellen Linux-Maschine und das Vorbereiten des Betriebssystems auf die Remote-Desktop-Bereitstellung.

Dieses Kapitel enthält die folgenden Themen:

- [Erstellen einer virtuellen Maschine und Installieren von Linux](#)
- [Vorbereiten einer Linux-Maschine für die Remote-Desktop-Bereitstellung](#)
- [Installieren von Abhängigkeitspaketen für Horizon Agent](#)

## Erstellen einer virtuellen Maschine und Installieren von Linux

Sie erstellen eine neue virtuelle Maschine für jeden in Horizon 7 bereitgestellten Remote-Desktop in vCenter Server. Dazu müssen Sie Ihre Linux-Distribution auf der virtuellen Maschine installieren.

### Voraussetzungen

- Stellen Sie sicher, dass Ihre Bereitstellung den Anforderungen für die Unterstützung von Linux-Desktops entspricht. Siehe [Systemanforderungen für Horizon 7 for Linux](#).
- Machen Sie sich mit den Schritten für das Erstellen virtueller Maschinen in vCenter Server und mit der Installation von Gastbetriebssystemen vertraut. Unter „Erstellen und Vorbereiten virtueller Maschinen“ im *Einrichten von virtuellen Desktops in Horizon 7*-Dokument finden Sie dazu Erläuterungen.
- Informieren Sie sich über die erforderlichen Videospeichereinstellungen (vRAM) für die Monitore, die Sie mit der virtuellen Maschine verwenden möchten. Siehe [Systemanforderungen für Horizon 7 for Linux](#).

### Verfahren

- 1 Erstellen Sie im vSphere Web Client oder vSphere Client eine neue virtuelle Maschine.

## 2 Konfigurieren Sie die benutzerdefinierten Konfigurationsoptionen.

- a Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie auf **Einstellungen bearbeiten**.
- b Geben Sie die Anzahl der vCPUs und die Größe des vMemory-Arbeitsspeichers an.  
Die erforderlichen Einstellungen finden Sie im Installationshandbuch Ihrer Linux-Distribution. Ubuntu 18.04 erfordert beispielsweise die Konfiguration von 2.048 MB für den vMemory-Arbeitsspeicher und zwei vCPUs.
- c Wählen Sie **Grafikkarte** aus und geben Sie die Anzahl der Anzeigegeräte sowie den gesamten Videospeicher (vRAM) ein.

Legen Sie im vSphere Web Client die vRAM-Größe für virtuelle Maschinen mit 2D-Grafik fest. Diese verwenden den VMware-Treiber. Die vRAM-Größe hat keinen Einfluss auf vDGA- oder NVIDIA GRID vGPU-Maschinen. Diese verwenden NVIDIA-Treiber.

Die erforderlichen Einstellungen finden Sie in den Anweisungen in [Einstellungen der virtuellen Maschine für 2D-Grafiken](#). Verwenden Sie nicht die Videospeicherberechnung.

- 3 Schalten Sie die virtuelle Maschine ein und installieren Sie die Linux-Distribution.
- 4 Konfigurieren Sie die Desktop-Umgebung für die Verwendung der jeweiligen Linux-Distribution.

Weitere Informationen finden Sie im Abschnitt „Desktop-Umgebung“ in [Systemanforderungen für Horizon 7 for Linux](#).

- 5 Stellen Sie sicher, dass der Hostname des Systems als 127.0.0.1 aufgelöst werden kann.

## Vorbereiten einer Linux-Maschine für die Remote-Desktop-Bereitstellung

Zur Vorbereitung einer Linux-Maschine für die Verwendung als Desktop in einer Horizon 7-Bereitstellung müssen Sie bestimmte Aufgaben durchführen.

Um eine Linux-Maschine für die Verwaltung durch Horizon 7 vorzubereiten, müssen Sie die Kommunikation zwischen der Maschine und dem Verbindungsserver aktivieren. Sie müssen die Netzwerkeinstellungen auf der Linux-Maschine konfigurieren, damit diese unter Verwendung des vollqualifizierten Domänennamens (FQDN) die Verbindungsserver-Instanz pingen kann.

Open VMware Tools (OVT) sind auf Maschinen mit RHEL 8.0/7x, CentOS 8.0/7x und SLED/SLES 12.x vorinstalliert. Wenn Sie eine dieser Maschinen für die Verwendung als Remote-Desktop vorbereiten, können Sie bei manueller Ausführung des Installationsprogramms in der nachfolgend beschriebenen Installation der VMware Tools die Schritte 1 bis 5 überspringen.

Wenn Sie eine Ubuntu 16.04/18.04-Maschine verwenden, installieren Sie darauf OVT. Wenn Sie diese Maschine für eine Verwendung als Remote-Desktop vorbereiten, können Sie die Schritte 1 bis 5 im nachfolgend dargestellten Vorgang überspringen und OVT manuell auf Ihrer Ubuntu 16.04/18.04-Maschine mithilfe des folgenden Befehls installieren:

```
apt-get install open-vm-tools-desktop
```

### Voraussetzungen

- Stellen Sie sicher, dass eine neue virtuelle Maschine (VM) in vCenter Server erstellt und Ihre Linux-Distribution auf der Maschine installiert wurde.
- Machen Sie sich mit den Schritten zum Mounten und Installieren von VMware Tools auf einer Linux-VM vertraut. Erläuterungen dazu finden Sie unter „Manuelles Installieren oder Durchführen eines Upgrades der VMware Tools in einer virtuellen Linux-Maschine“ im Dokument *Verwaltung virtueller vSphere-Maschinen*.
- Machen Sie sich mit den Schritten zur Konfiguration Ihrer Linux-Maschine für deren Auflösung über das DNS vertraut. Die Schritte sind im Einzelnen von den jeweiligen Linux-Distributionen und -Versionen abhängig. Anleitungen dazu finden Sie in der Dokumentation Ihrer Linux-Distributionen und -Versionen.

### Verfahren

- 1 Im vSphere Web Client oder vSphere Client mounten Sie die virtuelle Festplatte von VMware Tools auf der VM.
- 2 Klicken Sie mit der rechten Maustaste auf die Installationsdatei `VMwareTools.x.x.x-xxxx.tar.gz` von VMware Tools, klicken Sie im eingblendeten Kontextmenü auf **Extrahieren nach** und wählen Sie den Desktop für Ihre Linux-Distribution aus.

Der Ordner `vmware-tools-distrib` wird für den Desktop extrahiert.

- 3 Melden Sie sich auf der VM als Root an und öffnen Sie ein Terminalfenster.
- 4 Dekomprimieren Sie die TAR-Installationsdatei von VMware Tools.

Beispiel:

```
tar xzpf /mnt/cdrom/VMwareTools-x.x.x-yyyy.tar.gz
```

- 5 Führen Sie das Installationsprogramm aus und konfigurieren Sie VMware Tools.

Der exakte Befehl ist von den jeweiligen Linux-Distributionen abhängig. Beispiel:

```
cd vmware-tools-distrib
sudo ./vmware-install.pl -d
```

In der Regel wird die Konfigurationsdatei `vmware-config-tools.pl` nach Ausführung der Installationsprogrammdatei ausgeführt.

- 6 Ordnen Sie den Hostnamen der Linux-Maschine zu 127.0.0.1 in der Datei `/etc/hosts` zu.

Für RHEL, CentOS, SLES und SLED müssen Sie den Hostnamen manuell zu 127.0.0.1 zuordnen, da dies nicht automatisch erfolgt. Für Ubuntu ist dieser Schritt nicht erforderlich, da die Zuordnung hier automatisch erfolgt. Dieser Schritt ist auch nicht erforderlich, wenn Sie die Massenbereitstellung von Desktops verwenden, weil der Klonvorgang diese Zuordnung hinzufügt.

---

**Hinweis** Wenn Sie den Hostnamen der Linux-Maschine nach der Installation von Horizon Agent ändern, müssen Sie den neuen Hostnamen zu 127.0.0.1 in der Datei `/etc/hosts` zuordnen. Andernfalls wird der alte Hostname weiterhin verwendet.

---

- 7 Für RHEL und CentOS müssen Sie sicherstellen, dass `virbr0` deaktiviert ist.

```
virsh net-destroy default
virsh net-undefine default
service libvirtd restart
```

- 8 Stellen Sie sicher, dass die Horizon Connection Server-Verbindungsserver-Instanzen im Pod über das DNS aufgelöst werden können.

- 9 Konfigurieren Sie die Linux-Maschine für Runlevel 5 als Standard.

Für Linux-Desktops muss das Runlevel 5 zur ordnungsgemäßen Ausführung gültig sein.

- 10 Auf einer Ubuntu-Maschine, die für die Authentifizierung mit einem OpenLDAP-Server konfiguriert wurde, geben Sie den vollqualifizierten Domännennamen auf der Maschine an.

Dieser Schritt stellt sicher, dass die Informationen im Benutzerfeld auf der Seite „Sitzungen“ in Horizon Console korrekt dargestellt werden. Bearbeiten Sie die Datei `/etc/hosts` wie folgt:

- a `# nano /etc/hosts`
- b Fügen Sie den vollqualifizierten Domännennamen hinzu. Beispiel: `127.0.0.1  
hostname.domainname hostname.`
- c Beenden Sie und speichern Sie die Datei.

- 11 Für SUSE deaktivieren Sie „Hostnamen über DHCP ändern“. Legen Sie den Hostnamen oder den Domännennamen fest.

- a Klicken Sie in Yast auf **Netzwerkeinstellungen**.
- b Klicken Sie auf die Registerkarte **Hostname/DNS**.
- c Deaktivieren Sie **Hostnamen über DHCP ändern**
- d Geben Sie den Hostnamen und den Domännennamen ein.
- e Klicken Sie auf **OK**.

Wenn Sie nach der Installation von VMware Tools ein Upgrade für den Linux-Kernel durchführen, wird VMware Tools eventuell nicht mehr ausgeführt. Zur Lösung dieses Problems finden Sie Erläuterungen unter <http://kb.vmware.com/kb/2050592>.

# Installieren von Abhängigkeitspaketen für Horizon Agent

Horizon Agent for Linux verfügt für jede Linux-Distribution über spezifische Abhängigkeitspakete. Sie müssen diese Pakete vor der Installation von Horizon Agent for Linux installieren.

## Voraussetzungen

Stellen Sie sicher, dass eine neue virtuelle Maschine (VM) in vCenter Server erstellt und Ihre Linux-Distribution auf der Maschine installiert wurde.

## Verfahren

- 1 Installieren Sie die obligatorischen Pakete, wenn diese noch nicht installiert oder nicht standardmäßig aktualisiert wurden. Wenn ein Paket nicht den Anforderungen entspricht, wird die Installation vom Installationsprogramm abgebrochen.

**Tabelle 2-1. Obligatorische Abhängigkeitspakete**

Linux-Distribution	Pakete
RHEL 7.5	<code>yum install libappindicator-gtk3</code>
SLES 12.x SP1/SLED 12.x SP1 Führen Sie ein Upgrade von xf86-video-vmware auf eine höhere Version als 13.0.2-3.2 vom SUSE-Repository durch.	<ol style="list-style-type: none"> <li>1 Registrieren Sie SUSE 12.x, um die SUSE-Repositorys zu aktivieren. <code>SUSEConnect -r <i>Registrierungscode</i> -e <i>E-Mail</i></code></li> <li>2 Aktualisieren Sie die Version xf86-video-vmware. <code>zypper update xf86-video-vmware</code></li> </ol>
SLES 12.x	<p>Eine python-gobject2-Installation ist für SLES 12.x Linux-Desktops erforderlich, wenn Sie Horizon Agent installieren möchten.</p> <ol style="list-style-type: none"> <li>1 Registrieren Sie SUSE 12.x, um die SUSE-Repositorys zu aktivieren. <code>SUSEConnect -r <i>Registrierungscode</i> -e <i>E-Mail</i></code></li> <li>2 Installieren Sie python-gobject2. <code>zypper install python-gobject2</code></li> </ol>
Ubuntu 16.04	<code>apt-get install python-dbus python-gobject</code>
Ubuntu 18.04	<code>apt-get install python python-dbus python-gobject</code>

- 2 Installieren Sie das optionale Paket für Horizon Agent.

- In RHEL oder CentOS 6.7 ist standardmäßig glibc-2.12-1.166.el6.x86\_64 installiert, was zu einem Stillstand führen kann. Daraufhin hängt die Desktopverbindung. Zur Beseitigung dieses Problems müssen Sie glibc auf die neueste Version aus einem Online-Repository aktualisieren.

```
sudo yum install glibc
```



# Einrichten der Active Directory-Integration für Linux-Desktops

# 3

Horizon 7 nutzt die vorhandene Microsoft Active Directory (AD)-Infrastruktur für die Benutzerauthentifizierung und -verwaltung. Sie können die Linux-Desktops mit Active Directory integrieren, sodass sich Benutzer mit ihrem Active Directory-Benutzerkonto bei einem Linux-Desktop anmelden können.

---

**Hinweis** Horizon Agent erwartet, dass sich der Linux-Desktop und der Clientbenutzer in derselben Active Directory-Domäne befinden. Wenn sich der Desktop und der Benutzer in unterschiedlichen Domänen befinden, wird die Desktop-Domäne von Horizon Agent möglicherweise als Benutzerdomäne identifiziert.

---

Dieses Kapitel enthält die folgenden Themen:

- [Integrieren von Linux mit Active Directory](#)
- [Einrichten von Single Sign-On](#)
- [Einrichten der Smartcard-Umleitung](#)
- [Einrichten von True SSO für Linux-Desktops](#)

## Integrieren von Linux mit Active Directory

Für die Integration von Linux in Microsoft Active Directory (AD) sind mehrere Lösungen verfügbar. Für Horizon 7 for Linux Desktop sind alle Lösungen anwendbar.

Die folgenden Lösungen können in einer Horizon 7 for Linux-Desktop-Umgebung verwendet werden:

- OpenLDAP-Server-Pass-Through-Authentifizierung
- System Security Services Daemon (SSSD) LDAP-Authentifizierung bei Microsoft Active Directory
- Winbind-Domänenbeitritt
- PowerBroker Identity Services Open(PBISO)-Authentifizierung
- Samba-Offline-Domänenbeitritt

Wenn Sie die LDAP-basierten Lösungen verwenden, müssen Sie die Konfiguration in einer Vorlagen-VM durchführen. In den geklonten virtuellen Maschinen sind keine zusätzlichen Schritte erforderlich.

---

**Hinweis** Verwenden Sie zur Vereinfachung der Bereitstellung die Lösung mit SSSD-LDAP-Authentifizierung bei Microsoft Active Directory.

---

## Verwenden der OpenLDAP-Server-Pass-Through-Authentifizierung

Sie können einen OpenLDAP-Server einrichten und den Mechanismus für die Pass-Through-Authentifizierung (PTA) verwenden, um die Anmeldedaten für Active Directory zu verifizieren.

Auf einer höheren Ebene umfasst die Lösung mit der OpenLDAP-Pass-Through-Authentifizierung die folgenden Schritte.

### Verfahren

- 1 Um LDAPS (Lightweight Directory Access Protocol over SSL) zu aktivieren, installieren Sie Zertifikatdienste in Active Directory.
- 2 Richten Sie einen OpenLDAP-Server ein.
- 3 Synchronisieren Sie die Benutzerinformationen (außer Kennwort) von Active Directory mit dem OpenLDAP-Server.
- 4 Konfigurieren Sie den OpenLDAP-Server, um die Kennwortüberprüfung an einen separaten Prozess zu delegieren, z. B. an `saslauthd`, der die Kennwortüberprüfung bei Active Directory durchführen kann.
- 5 Konfigurieren Sie die Linux-Desktops für die Verwendung eines LDAP-Clients zur Authentifizierung von Benutzern mit dem OpenLDAP-Server.

## SSSD-LDAP-Authentifizierung bei Microsoft Active Directory einrichten

Sie können LDAP-Authentifizierung bei Windows Active Directory verwenden, indem Sie ein System Security Services Daemon (SSSD) auf dem Linux-Desktop konfigurieren.

Verwenden Sie die folgenden hochrangigen Schritte zur SSSD-LDAP-Authentifizierung-Lösung.

### Verfahren

- 1 Um LDAPS (Lightweight Directory Access Protocol Over Secure Socket Layer) zu aktivieren, installieren Sie die Zertifikatdienste auf dem Active Directory-Server.
- 2 Um die LDAP-Authentifizierung direkt für Microsoft Active Directory zu verwenden, konfigurieren Sie SSSD auf dem Linux-Desktop.

## Verwenden der Winbind-Domänenbeitrittslösung

Die Winbind-Domänenbeitrittslösung, eine Kerberos-basierte Authentifizierungslösung, ist eine andere Methode zur Authentifizierung bei Active Directory.

Verwenden Sie die folgenden allgemeinen Schritte zum Einrichten der Winbind-Domänenbeitrittslösung.

### Verfahren

- 1 Installieren Sie die winbind-, samba- und Kerberos-Pakete auf dem Linux-Desktop.
- 2 Fügen Sie den Linux-Desktop zu Microsoft Active Directory hinzu.

### Nächste Schritte

Bei Verwendung der Winbind-Domänenbeitrittslösung oder anderer Kerberos-basierter Authentifizierungslösungen fügen Sie die Vorlagen-VM zu Active Directory und die geklonte virtuelle Maschine erneut zu Active Directory hinzu. Verwenden Sie dazu beispielsweise den folgenden Befehl:

```
sudo /usr/bin/net ads join -U <Domänenbenutzer>%<Domänenkennwort>
```

Verwenden Sie die folgenden Optionen, um den Befehl für den erneuten Beitritt zur Domäne auf einer geklonten virtuellen Maschine für die Winbind-Lösung auszuführen:

- Stellen Sie eine Remote-Verbindung wie SSH oder vSphere PowerCLI zu jeder virtuellen Maschine her und führen Sie den Befehl aus. Weitere Informationen zu Skripts finden Sie unter [Kapitel 8 Massenbereitstellung von Horizon 7 für manuelle Desktop-Pools](#).
- Fügen Sie den Befehl einem Shell-Skript hinzu und geben Sie den Skriptpfad zur Horizon Agent-Option RunOnceScript in der Datei /etc/vmware/viewagent-custom.conf an. Weitere Informationen finden Sie unter [Einstellen der Optionen in Konfigurationsdateien auf einem Linux-Desktop](#).

## PowerBroker Identity Services Open(PBISO)-Authentifizierung konfigurieren

Die Authentifizierungsmethode PowerBroker Identity Services Open (PBISO) ist eine der unterstützten Lösungen zur Durchführung eines Offline-Domänenbeitritts.

Fügen Sie einen Linux-Desktop zu Active Directory mit PBISO anhand folgender Schritte hinzu.

### Verfahren

- 1 Laden Sie PBISO 8.5.6 oder höher von <https://www.beyondtrust.com/products/powerbroker-identity-services-open/> herunter.
- 2 Installieren Sie PBISO auf Ihrer Linux-VM.

```
sudo ./pbis-open-8.5.6.2029.linux.x86_64.deb.sh
```

- 3 Installieren Sie Horizon 7 Agent for Linux.
- 4 Verwenden Sie PBISO, um den Linux-Desktop zur AD-Domäne hinzuzufügen.

Im folgenden Beispiel steht **lxdm.vdi** für den Domännennamen und **administrator** für den Domänenbenutzernamen.

```
sudo domainjoin-cli join lxdm.vdi administrator
```

## 5 Richten Sie die Standardkonfiguration für Domänenbenutzer ein.

```
sudo /opt/pbis/bin/config UserDomainPrefix lxdc
sudo /opt/pbis/bin/config AssumeDefaultDomain true
sudo /opt/pbis/bin/config LoginShellTemplate /bin/bash
sudo /opt/pbis/bin/config HomeDirTemplate %H/%U
```

## 6 Bearbeiten Sie die Datei /etc/pam.d/common-session.

- a Suchen Sie die Zeile **session sufficient pam\_lsass.so**.
- b Ersetzen Sie diese Zeile mit **session [success=ok default=ignore] pam\_lsass.so**.

**Hinweis** Dieser Schritt muss erneut durchgeführt werden, wenn Sie Horizon Agent for Linux neu installieren oder aktualisieren.

## 7 Fügen Sie für Ubuntu 16.04 die folgenden Zeilen an die Konfigurationsdatei /usr/share/lightdm/lightdm.conf.d/50-unity-greeter.conf an.

```
allow-guest=false
greeter-show-manual-login=true
```

**Hinweis** Wenn Sie Ubuntu 18.04 verwenden, ist keine Änderung an der Konfigurationsdatei lightdm erforderlich.

## 8 Starten Sie Ihr System neu und melden Sie sich an.

### Nächste Schritte

#### Hinweis

- Wenn die Option /opt/pbis/bin/config AssumeDefaultDomain auf **false** festgelegt ist, müssen Sie die Einstellung SSOUserFormat=<username>@<domain> in der Datei /etc/vmware/viewagent-custom.conf aktualisieren.
- Wenn Sie die dynamische Horizon-Instant-Clone-Desktop-Pool-Funktion verwenden, müssen Sie die Datei resolv.conf für Ihr Linux-System ändern, damit die DNS-Server-Einstellung nicht verloren geht, wenn Sie der geklonten VM den neuen Netzwerkadapter hinzufügen. Verwenden Sie das folgende Beispiel für ein Ubuntu 16.04-System als Vorlage für die Zeilen, die Sie der Datei /etc/resolvconf/resolv.conf.d/head hinzufügen müssen.

```
nameserver 10.10.10.10
search mydomain.org
```

## Konfigurieren des Samba-Offline-Domänenbeitritts

Konfigurieren Sie zur Unterstützung von SSO auf einer Instant-Clone-VM in einer Horizon 7-Linux-Desktopumgebung Samba auf der Master-Linux-VM.

Verwenden Sie das folgende Verfahren als Beispiel für die Verwendung von Samba für den Offline-Domänenbeitritt eines Instant-Clone-Linux-Desktops zu Active Directory. Dieses Verfahren enthält die Schritte für ein Ubuntu-System.

### Verfahren

- 1 Installieren Sie auf Ihrer Master-Linux-VM die winbind- und samba-Pakete, einschließlich anderer abhängiger Bibliotheken wie smbfs und smbclient.
- 2 Installieren Sie das Samba-tdb-tools-Paket mithilfe des folgenden Befehls.

```
sudo apt-get install tdb-tools
```

- 3 Installieren Sie Horizon 7 Agent for Linux.
- 4 Bearbeiten Sie die Konfigurationsdatei `/etc/samba/smb.conf`, sodass sie über Inhalte ähnlich dem folgenden Beispiel verfügt.

```
[global]
security = ads
realm = LAB.EXAMPLE.COM
workgroup = LAB
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum group = yes
template homedir = /home/%D/%U
template shell = /bin/bash
client use spnego = yes
client ntlmv2 auth = yes
encrypt passwords = yes
winbind use default domain = yes
restrict anonymous = 2
```

- 5 Bearbeiten Sie die Konfigurationsdatei `/etc/krb5.conf`, sodass sie über Inhalte ähnlich dem folgenden Beispiel verfügt ...

```
[libdefaults]
default_realm = EXAMPLE.COM

krb4_config = /etc/krb.conf
krb4_realms = /etc/krb.realms

kdc_timesync = 1
ccache_type = 4
forwardable = true
proxiable = true

[realms]
YOUR-DOMAIN = {
kdc = 10.111.222.33
}
```

```
[domain_realm]
your-domain = EXAMPLE.COM
.your-domain = EXAMPLE.COM
```

- 6 Bearbeiten Sie die Konfigurationsdatei `/etc/nsswitch.conf`, wie im folgenden Beispiel gezeigt.

```
passwd: files winbind
group: files winbind
shadow: files winbind
gshadow: files
```

- 7 Stellen Sie sicher, dass der Hostname korrekt ist und Systemdatum sowie -uhrzeit mit Ihrem DNS synchronisiert sind.
- 8 Um Horizon Agent darüber zu informieren, dass die Linux-VM mit der Samba-Methode der Domäne beigetreten ist, legen Sie die folgende Option in der Datei `/etc/vmware/viewagent-custom.conf` fest.

```
OfflineJoinDomain=samba
```

- 9 Starten Sie Ihr System neu und melden Sie sich an.

## Verwenden der Realmd-Beitrittslösung für RHEL/CentOS 8.0

Um sicherzustellen, dass Funktionen wie Single Sign-On auf einem RHEL/CentOS 8.0-Desktop verwendet werden können, verbinden Sie den Desktop mit Ihrer Active Directory(AD)Domäne mithilfe der realmd-Lösung.

### Verfahren

- 1 Konfigurieren Sie einen vollqualifizierten Hostnamen für das RHEL/CentOS 8.0-System.

Beispiel: Wenn **rhel8** der nicht qualifizierte Hostname des Systems und **LXD.VDI** die AD-Domäne ist, führen Sie den folgenden Befehl aus.

```
# hostnamectl set-hostname rhel8.lxd.vdi
```

- 2 Überprüfen Sie die Netzwerkverbindung mit der AD-Domäne, wie im folgenden Beispiel gezeigt.

```
# realm discover -vvv LXD.VDI
```

- 3 Installieren Sie die erforderlichen Abhängigkeitspakete, wie im folgenden Beispiel gezeigt.

```
# dnf install -y sssd adcli samba-common-tools oddjob oddjob-mkhomedir
```

- 4 Treten Sie der AD-Domäne bei, wie im folgenden Beispiel gezeigt.

```
# realm join -U Administrator LXD.VDI
```

- 5 Bearbeiten Sie die Datei `/etc/sss/sss.conf`, sodass sie dem folgenden Beispiel ähnelt. Fügen Sie `ad_gpo_map_interactive = +gdm-vmwcred` unter dem Abschnitt `[domain/domain name]` hinzu.

```
[sss]
domains = LXD.VDI
config_file_version = 2
services = nss, pam

[domain/LXD.VDI]
ad_domain = LXD.VDI
krb5_realm = LXD.VDI
realmd_tags = manages-system joined-with-adcli
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = False
fallback_homedir = /home/%u
access_provider = ad
ad_gpo_map_interactive = +gdm-vmwcred
```

- 6 Um sicherzustellen, dass der Domänenbeitritt wirksam wird, starten Sie Ihr System neu und melden Sie sich erneut an.
- 7 Stellen Sie sicher, dass die Domänenbenutzer ordnungsgemäß konfiguriert sind. Das folgende Beispiel zeigt, wie Sie mit dem Befehl `id` die Konfigurationsausgabe von Domänenbenutzer **zyc1** zurückgeben.

```
# id zyc1

uid=1084401403(zyc1) gid=1084400513(domain users) groups=1084400513(domain users)
```

- 8 Überprüfen Sie mithilfe der Anmeldedaten eines Domänenbenutzers, ob Sie sich erfolgreich beim Desktop anmelden können.

---

**Hinweis** Horizon Agent unterstützt nur das X11-Anzeigeserverprotokoll für RHEL/CentOS 8.0-Desktops. Um X11 als standardmäßiges Anzeigeserverprotokoll für Ihr System zu konfigurieren, klicken Sie im Anmeldebildschirm auf das Symbol „Einstellungen“ und wählen Sie **Classic (X11 display server)** aus dem Dropdown-Menü aus.

---

## Einrichten von Single Sign-On

Um Single Sign-On (SSO) einzurichten, müssen Sie verschiedene Konfigurationsschritte durchführen.

Das Single-Sign-On-Modul von Horizon kommuniziert mit PAMs (Pluggable Authentication Modules) in Linux und ist nicht von der Methode abhängig, die Sie zur Integration von Linux in Active Directory (AD) verwenden. Das Horizon-SSO funktioniert bekanntermaßen mit den OpenLDAP- und Winbind-Lösungen, die Linux in AD integrieren.

Standardmäßig nimmt SSO an, dass das `sAMAccountName`-Attribut von AD die Anmelde-ID ist. Um sicherzustellen, dass die korrekte Anmelde-ID für SSO verwendet wird, müssen Sie die nachfolgend aufgeführten Konfigurationsschritte durchführen, wenn Sie die OpenLDAP- oder Winbind-Lösung verwenden.

- Für OpenLDAP setzen Sie `sAMAccountName` auf `uid`.
- Für Winbind fügen Sie die folgende Anweisung zur Konfigurationsdatei `/etc/samba/smb.conf` hinzu.

```
winbind use default domain = true
```

Wenn Benutzer den Domännennamen angeben müssen, um sich anzumelden, müssen Sie die `SSOUserFormat`-Option auf dem Linux-Desktop angeben. Weitere Informationen finden Sie unter [Einstellen der Optionen in Konfigurationsdateien auf einem Linux-Desktop](#). SSO verwendet immer die Kurzform des Domännennamens in Großbuchstaben. Wenn zum Beispiel die Domäne `mydomain.com` ist, wird `MYDOMAIN` von SSO als Domänenname verwendet. Aus diesem Grund müssen Sie `MYDOMAIN` angeben, wenn Sie `SSOUserFormat` festlegen. In Bezug auf die Kurz- und Langformen von Domännennamen gelten die folgenden Regeln:

- Für OpenLDAP müssen Sie die Kurzform der Domännennamen in Großbuchstaben verwenden.
- Winbind unterstützt sowohl die Langform als auch die Kurzform der Domännennamen.

AD unterstützt Sonderzeichen in Anmeldenamen, Linux jedoch nicht. Deshalb dürfen Sie keine Sonderzeichen in Anmeldenamen verwenden, wenn Sie SSO einrichten.

Wenn in AD das `UserPrincipalName`-Attribut (UPN) und das `sAMAccount`-Attribut eines Benutzers nicht übereinstimmen und der Benutzer sich mit dem UPN anmeldet, schlägt SSO fehl. Wenn Sie beispielsweise einen Benutzer (`juser` in AD `mycompany.com`) haben, die Benutzer-UPN jedoch auf `juser123@mycompany.com` anstelle von `juser@mycompany.com` festgelegt ist, schlägt SSO fehl. Zur Umgehung des Problems kann sich der Benutzer mit dem Namen anmelden, der in `sAMAccount` gespeichert ist. Beispiel: `juser`.

Horizon 7 erfordert nicht, dass beim Benutzernamen zwischen Groß- und Kleinschreibung unterschieden wird. Sie müssen sicherstellen, dass das Linux-Betriebssystem Benutzernamen verarbeiten kann, bei denen zwischen Groß- und Kleinschreibung unterschieden wird.

- Für Winbind wird beim Benutzernamen standardmäßig zwischen Groß- und Kleinschreibung unterschieden.
- Für OpenLDAP verwendet Ubuntu NSCD zur Authentifizierung von Benutzern, und es wird standardmäßig zwischen Groß- und Kleinschreibung unterschieden. RHEL und CentOS verwenden SSSD zur Authentifizierung von Benutzern, und es wird standardmäßig zwischen Groß- und Kleinschreibung unterschieden. Zum Ändern der Einstellung bearbeiten Sie die Datei `/etc/sss/sss.conf` und fügen Sie dem Abschnitt `[domain/default]` die folgende Zeile hinzu:

```
case_sensitive = false
```



Verfügt der Linux-Desktop über mehrere auf ihm installierte Desktop-Umgebungen, finden Sie Informationen zur Auswahl der bei aktivierter SSO-Funktion zu verwendenden Desktop-Umgebung im Abschnitt [Desktop-Umgebung](#).

## Einrichten der Smartcard-Umleitung

Für das Einrichten der Smartcard-Umleitung müssen Sie einige Konfigurationsschritte ausführen.

### Überblick über die Smartcard-Umleitung

Die Smartcard-Umleitung wird auf Desktops unterstützt, auf denen die folgenden Linux-Distributionen mit den angegebenen Versionen von Horizon Agent installiert sind.

**Tabelle 3-1. Systemanforderungen für die Smartcard-Umleitung**

Linux-Distribution	Horizon Agent
RHEL 8.0	Horizon Agent 7.10 oder höher
RHEL 7.1 oder höher	Horizon Agent 7.8 oder höher
RHEL 6.6 oder höher	Horizon Agent 6.2.1 oder höher
Ubuntu 18.04/16.04	Horizon Agent 7.9 oder höher
SLED/SLES 12.x SP3	Horizon Agent 7.9 oder höher

Wenn Sie Horizon Agent installieren, müssen Sie zuerst SELinux deaktivieren. Sie müssen auch die Smartcard-Umleitungskomponente speziell auswählen, weil die Komponente nicht standardmäßig ausgewählt wird. Weitere Informationen finden Sie unter [Befehlszeilenoptionen für install\\_viewagent.sh](#).

Wenn die Funktion der Smartcard-Umleitung in einer virtuellen Maschine aktiviert ist, funktioniert die USB-Umleitung des vSphere-Clients mit der Smartcard nicht.

Die Smartcard-Umleitung unterstützt jeweils nur einen Smartcard-Leser. Diese Funktion ist nicht funktionsfähig, wenn zwei oder mehr Lesegeräte an das Client-System angeschlossen sind.

Die Smartcard-Umleitung unterstützt nur ein Zertifikat auf der Smartcard. Wenn sich auf der Smartcard mehrere Zertifikate befinden, wird das im ersten Slot befindliche Zertifikat verwendet; die anderen werden ignoriert. Dieses Verhalten ist eine Einschränkung durch Linux.

**Hinweis** Die Smartcard-Umleitung unterstützt PIV-Karten auf Linux-Desktops. Wenn Horizon Client für Linux zur Authentifizierung des Broker mit einer PIV-Karte verwendet wird, müssen Sie die PIV-Smartcard mit TLSv1.2-Unterstützung konfigurieren, um einen SSL-Fehler zu vermeiden. Verwenden Sie dazu die im VMware Knowledgebase-Artikel <http://kb.vmware.com/kb/2150470> beschriebene Lösung.

**Hinweis** Smartcard-SSO ist in Horizon 7 Version 7.0.1 oder höher aktiviert. RHEL 6.x-Desktops unterstützen Smartcard-SSO. RHEL 7.x- und RHEL 8.0-Desktops unterstützen diese Funktion jedoch nicht.

## Konfigurieren der Smartcard-Umleitung

Führen Sie die folgenden Aufgaben aus, um die Smartcard-Umleitung zu konfigurieren.

- 1 Richten Sie die Smartcard für Ihren Desktop gemäß den Anweisungen des Linux-Distributors und des Smartcard-Anbieters ein.
- 2 Integrieren Sie Ihren Desktop in eine Active Directory-Domäne, indem Sie die für Ihre Linux-Distribution erforderlichen Schritte ausführen.
- 3 Konfigurieren Sie eine Smartcard-Umleitung auf Ihrem Desktop, indem Sie die für Ihre Linux-Distribution erforderlichen Schritte ausführen.

## Konfigurieren der Smartcard-Umleitung für RHEL 8.0-Desktops

Um die Smartcard-Umleitung für einen RHEL 8.0-Desktop einzurichten, müssen Sie zuerst den Desktop in eine Active Directory-Domäne integrieren. Installieren Sie dann die erforderlichen Bibliotheken und das Root-CA-Zertifikat, bevor Sie Horizon Agent installieren.

### Integrieren eines RHEL 8.0-Desktops in Active Directory für die Smartcard-Umleitung

Wenden Sie das folgende Verfahren an, um einen RHEL 8.0-Desktop für die Smartcard-Umleitung in eine Active Directory-(AD-)Domäne zu integrieren.

In einigen der Beispiele im Verfahren werden Platzhalterwerte verwendet, um Entitäten in Ihrer Netzwerkkonfiguration darzustellen, z. B. den DNS-Namen Ihrer Active Directory-Domäne. Ersetzen Sie die Platzhalterwerte durch spezifische Informationen für Ihre Konfiguration, wie in der folgenden Tabelle gezeigt.

Platzhalterwert	Beschreibung
dns_IP_ADDRESS	IP-Adresse Ihres DNS-Namensservers
rhel8sc.rzview2.com	Vollqualifizierter Hostname Ihres RHEL 8.0-Systems
rhel8sc	Nicht qualifizierter Hostname Ihres RHEL 8.0-Systems
rzview2.com	DNS-Name Ihrer Active Directory-Domäne
RZVIEW2.COM	DNS-Name Ihrer Active Directory-Domäne in Großbuchstaben
RZVIEW2	DNS-Name der Arbeitsgruppe oder NT-Domäne, in der sich Ihr Samba-Server befindet, in Großbuchstaben
rzviewdns.rzview2.com	Hostname Ihres AD-Servers

### Verfahren

- 1 Führen Sie auf Ihrem RHEL 8.0-System die folgenden Schritte aus.
  - a Konfigurieren Sie die Netzwerk- und DNS-Einstellungen gemäß den Anforderungen Ihrer Organisation.
  - b Deaktivieren Sie **IPv6**.
  - c Deaktivieren Sie **Automatisches DNS**.

- 2 Konfigurieren Sie die Konfigurationsdatei `–/etc/hosts`, sodass Sie dem folgenden Beispiel ähnelt.

```
127.0.0.1      rhel8sc.rzview2.com rhel8sc localhost localhost.localdomain localhost4
localhost4.localhost4
::1          localhost localhost.localdomain localhost6 localhost6.localhost6

dns_IP_ADDRESS  rzviewdns.rzview2.com
```

- 3 Konfigurieren Sie die Konfigurationsdatei `–/etc/resolv.conf`, sodass Sie dem folgenden Beispiel ähnelt.

```
# Generated by NetworkManager
search rzview2.com
nameserver dns_IP_ADDRESS
```

- 4 Installieren Sie die Pakete, die für die AD-Integration erforderlich sind.

```
# yum install -y samba-common-tools oddjob-mkhomedir
```

- 5 Aktivieren Sie den `oddjobd`-Dienst.

```
# systemctl enable oddjobd.service
# systemctl start oddjobd.service
```

- 6 Geben Sie die Systemidentität und die Authentifizierungsquellen an.

```
# authselect select sssd with-smartcard with-mkhomedir
```

- 7 Starten Sie den `oddjobd`-Dienst.

```
# systemctl enable oddjobd.service
# systemctl start oddjobd.service
```

- 8 Um die Smartcard-Authentifizierung zu unterstützen, erstellen Sie die Datei `/etc/sss/sss.conf`.

```
# touch /etc/sss/sss.conf
# chmod 600 touch /etc/sss/sss.conf
# chown root:root /etc/sss/sss.conf
```

- 9 Fügen Sie den erforderlichen Content zu `/etc/sss/sss.conf` wie im folgenden Beispiel gezeigt hinzu. Geben Sie im Abschnitt **[pam]** `pam_cert_auth = True` an.

```
[sss]
config_file_version = 2
domains = rzview2.com
services = nss, pam, pac

[domain/RZVIEW2.COM]
id_provider = ad
auth_provider = ad
chpass_provider = ad
```

```
access_provider = ad
cache_credentials = true

[pam]
pam_cert_auth = True
```

## 10 Aktivieren Sie den sssd-Dienst.

```
# systemctl enable sssd.service
# systemctl start sssd.service
```

## 11 Bearbeiten Sie die Konfigurationsdatei /etc/krb5.conf, sodass Sie dem folgenden Beispiel ähnelt.

```
# To opt out of the system crypto-policies configuration of krb5, remove the
# symlink at /etc/krb5.conf.d/crypto-policies which will not be recreated.
includedir /etc/krb5.conf.d/

[logging]
    default = FILE:/var/log/krb5libs.log
    kdc = FILE:/var/log/krb5kdc.log
    admin_server = FILE:/var/log/kadmind.log

[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    pkinit_anchors = /etc/pki/tls/certs/ca-bundle.crt
    spake_preauth_groups = edwards25519
    default_realm = RZVIEW2.COM
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
    RZVIEW2.COM = {
        kdc = rzviewdns.rzview2.com
        admin_server = rzviewdns.rzview2.com
        default_domain = rzviewdns.rzview2.com
        pkinit_anchors = FILE:/etc/pki/nssdb/certificate.pem
        pkinit_cert_match = <KU>digitalSignature
        pkinit_kdc_hostname = rzviewdns.rzview2.com
    }

[domain_realm]
    .rzview2.com = RZVIEW2.COM
    rzview2.com = RZVIEW2.COM
```

## 12 Bearbeiten Sie die Konfigurationsdatei /etc/samba/smb.conf, sodass Sie dem folgenden Beispiel ähnelt.

```
[global]
    workgroup = RZVIEW2
    security = ads
    passdb backend = tdbsam
```

```

printing = cups
printcap name = cups
load printers = yes
cups options = raw
password server = rzviewdns.rzview2.com
realm = RZVIEW2.COM
idmap config * : range = 16777216-33554431
template homedir = /home/RZVIEW2/%U
template shell = /bin/bash
kerberos method = secrets and keytab

[homes]
comment = Home Directories
valid users = %S, %D%w%S
browseable = No
read only = No
inherit acls = Yes

[printers]
comment = All Printers
path = /var/tmp
printable = Yes
create mask = 0600
browseable = No

[print$]
comment = Printer Drivers
path = /var/lib/samba/drivers
write list = @printadmin root
force group = @printadmin
create mask = 0664
directory mask = 0775

```

- 13** Treten Sie der AD-Domäne bei, wie im folgenden Beispiel gezeigt.

```
# net ads join -U AdminUser
```

Durch Ausführen des Befehls `join` wird Ausgabe ähnlich dem folgenden Beispiel zurückgegeben.

```

Enter AdminUser's password:
Using short domain name -- RZVIEW2
Joined 'RHEL8SC' to dns domain 'rzview2.com'

```

- 14** Stellen Sie sicher, dass der RHEL 8.0-Desktop erfolgreich der AD-Domäne beigetreten ist.

```

# net ads testjoin

Join is OK

```

## Nächste Schritte

### Konfigurieren der Smartcard-Umleitung für RHEL 8.0-Desktop

## Konfigurieren der Smartcard-Umleitung für RHEL 8.0-Desktop

Um die Smartcard-Umleitung auf einem RHEL 8.0-Desktop zu konfigurieren, müssen Sie die Bibliotheken, von denen die Funktion abhängt, das Stamm-CA-Zertifikat für die vertrauenswürdige Authentifizierung von Smartcards sowie die erforderliche PC/SC Lite-Bibliothek installieren.

### Voraussetzungen

[Integrieren eines RHEL 8.0-Desktops in Active Directory für die Smartcard-Umleitung](#)

### Verfahren

- 1 Installieren Sie die erforderlichen Bibliotheken.

```
# yum install -y opensc pcsc-lite pcsc-lite-libs pcsc-lite-ccid nss-tools
```

- 2 Aktivieren Sie den pcscd-Dienst.

```
# systemctl enable pcscd
# systemctl start pcscd
```

- 3 Stellen Sie sicher, dass die Konfigurationsdatei `/etc/sss/sss.conf` die folgenden Zeilen enthält, die die Smartcard-Authentifizierung aktivieren.

```
[pam]
pam_cert_auth = True
```

- 4 Kopieren Sie das erforderliche CA-Zertifikat in `/etc/sss/pki/sss_auth_ca_db.pem`.

```
# openssl x509 -inform der -in certificate.cer -out certificate.pem
# cp certificate.pem /etc/sss/pki/sss_auth_ca_db.pem
```

- 5 Um den Status der Smartcard zu überprüfen, führen Sie die folgenden `pkcs11-tool`-Befehle aus und bestätigen Sie, dass diese die korrekte Ausgabe zurückgeben.

```
# pkcs11-tool -L

# pkcs11-tool --login -0

# pkcs11-tool --test --login
```

- 6 Richten Sie das PKCS11-Modul ein.

```
cp libcmP11.so /usr/lib64/
```

- 7 Erstellen Sie die Datei `/usr/share/p11-kit/modules/libcmP11.module`. Fügen Sie der Datei den folgenden Inhalt hinzu.

```
# This file describes how to load the opensc module
# See: http://p11-glue.freedesktop.org/doc/p11-kit/config.html

# This is a relative path, which means it will be loaded from
# the p11-kit default path which is usually $(libdir)/pkcs11.
```

```
# Doing it this way allows for packagers to package opensc for
# 32-bit and 64-bit and make them parallel installable
module: /usr/lib64/libcmP11.so
priority: 99
```

## 8 Aktualisieren Sie PC/SC Lite auf Version 1.8.8.

```
# yum install -y git flex autoconf automake libtool libudev-devel flex
# git clone https://salsa.debian.org/rousseau/PCSC.git
# cd PCSC
# git checkout -b 1.8.8 pcsc-1.8.8
# ./bootstrap
# ./configure --build=x86_64-redhat-linux-gnu --host=x86_64-redhat-linux-gnu
--program-prefix= --disable-dependency-tracking --prefix=/usr --exec-prefix=/usr
--bindir=/usr/bin --sbindir=/usr/sbin --sysconfdir=/etc --datadir=/usr/share
--includedir=/usr/include --libdir=/usr/lib64 --libexecdir=/usr/libexec
--localstatedir=/var --sharedstatedir=/var/lib --mandir=/usr/share/man
--infodir=/usr/share/info --disable-static --enable-usbdropdir=/usr/lib64/pcsc/drivers
# make
# make install
```

## 9 Installieren Sie Horizon Agent 7.10 oder höher mit aktivierter Smartcard-Umleitung.

## 10 Starten Sie Ihr System neu und melden Sie sich an.

# Konfigurieren der Smartcard-Umleitung für RHEL 7.x/6.x-Desktops

Um die Smartcard-Umleitung für einen RHEL 7.x/6.x-Desktop einzurichten, müssen Sie zuerst den Desktop in eine Active Directory-Domäne integrieren. Installieren Sie dann die erforderlichen Bibliotheken und das Root-CA-Zertifikat, bevor Sie Horizon Agent installieren.

## Integrieren eines RHEL 7.x/6.x-Desktops in Active Directory für die Smartcard-Umleitung

Integrieren Sie den Desktop mithilfe von Samba und Winbind in eine Active Directory(AD)-Domäne, um die Smartcard-Umleitung auf einem RHEL 7.x/6.x-Desktop zu unterstützen.

Wenden Sie das folgende Verfahren an, um einen RHEL 7.x/6.x-Desktop für die Smartcard-Umleitung in eine AD-Domäne zu integrieren.

In einigen der Beispiele im Verfahren werden Platzhalterwerte verwendet, um Entitäten in Ihrer Netzwerkkonfiguration darzustellen, z. B. den DNS-Namen Ihrer Active Directory-Domäne. Ersetzen Sie die Platzhalterwerte durch spezifische Informationen für Ihre Konfiguration, wie in der folgenden Tabelle gezeigt.

Platzhalterwert	Beschreibung
dns_IP_ADDRESS	IP-Adresse Ihres DNS-Namenservers
mydomain.com	DNS-Name Ihrer Active Directory-Domäne
MYDOMAIN.COM	DNS-Name Ihrer Active Directory-Domäne in Großbuchstaben

Platzhalterwert	Beschreibung
MYDOMAIN	DNS-Name der Arbeitsgruppe oder NT-Domäne, in der sich Ihr Samba-Server befindet, in Großbuchstaben
ads-hostname	Hostname Ihres AD-Servers

**Hinweis** Die Smartcard-Umleitung wird für Desktops unterstützt, auf denen RHEL 6.0 oder höher oder RHEL 7.1 oder höher ausgeführt wird.

## Verfahren

- 1 Installieren Sie die erforderlichen Pakete auf Ihrem RHEL 7.x/6.x-Desktop.

```
# yum install nscd samba-winbind krb5-workstation pam_krb5 samba-winbind-clients authconfig-gtk
```

- 2 Bearbeiten Sie die Netzwerkeinstellungen für Ihre Systemverbindung. Öffnen Sie die Einstellungen von NetworkManager und navigieren Sie zu den **IPv4-Einstellungen** für Ihre Systemverbindung. Wählen Sie als IPv4-Methode **Automatisch (DHCP)** aus. Geben Sie im Textfeld **DNS** die IP-Adresse Ihres DNS-Namensservers ein. Klicken Sie anschließend auf **Anwenden**.
- 3 Führen Sie den folgenden Befehl aus und prüfen Sie, ob von Ihrem RHEL-Desktop der vollqualifizierte Domänenname (FQDN) zurückgegeben wird.

```
# hostname -f
```

- 4 Bearbeiten Sie die Konfigurationsdatei `/etc/resolve.conf`, wie im folgenden Beispiel.

```
search mydomain.com
nameserver dns_IP_ADDRESS
```

- 5 Deaktivieren Sie Security-Enhanced Linux (SELinux) in Ihrem RHEL-Desktop. Bearbeiten Sie die Konfigurationsdatei `/etc/selinux/config`, wie im folgenden Beispiel.

```
SELINUX=disabled
```

- 6 Bearbeiten Sie die Konfigurationsdatei `/etc/krb5.conf`, wie im folgenden Beispiel.

```
[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    default_realm = MYDOMAIN.COM
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
    MYDOMAIN.COM = {
        kdc = ads-hostname
        admin_server = ads-hostname
        default_domain = ads-hostname
```



```

    }

[domain_realm]
    .mydomain.com = MYDOMAIN.COM
    mydomain.com = MYDOMAIN.COM

```

- 7 Bearbeiten Sie die Konfigurationsdatei `/etc/samba/smb.conf`, wie im folgenden Beispiel.

```

[global]
    workgroup = MYDOMAIN
    password server = ads-hostname
    realm = MYDOMAIN.COM
    security = ads
    idmap config * : range = 16777216-33554431
    template homedir = /home/MYDOMAIN/%U
    template shell = /bin/bash
    kerberos method = secrets and keytab
    winbind use default domain = true
    winbind offline logon = false
    winbind refresh tickets = true

    passdb backend = tdbsam

```

- 8 Öffnen Sie das Tool `authconfig-gtk` und konfigurieren Sie Einstellungen wie folgt.
- Wechseln Sie zur Registerkarte für **Identität und Authentifizierung**. Wählen Sie für die Benutzerkontodatenbank **Winbind** aus.
  - Wechseln Sie zur Registerkarte für **Erweiterte Optionen** und aktivieren Sie das Kontrollkästchen für **Home-Verzeichnisse bei der ersten Anmeldung erstellen**.
  - Wechseln Sie zur Registerkarte für **Identität und Authentifizierung** und klicken Sie auf **Domäne beitreten**. Klicken Sie in der Warnung, die Sie zum Speichern auffordert, auf **Speichern**.
  - Geben Sie bei Aufforderung den Benutzernamen und das Kennwort des Domänenadministrators ein und klicken Sie auf **OK**.

Ihr RHEL-Desktop wird zur AD-Domäne hinzugefügt.

- 9 Richten Sie das Ticket-Caching in PAM Winbind ein. Bearbeiten Sie die Konfigurationsdatei `/etc/security/pam_winbind.conf`, damit sie die im folgenden Beispiel gezeigten Zeilen enthält.

```

[global]

# authenticate using kerberos
;krb5_auth = yes

# create homedirectory on the fly
;mkhomedir = yes

```

- 10 Starten Sie den Winbind-Dienst neu.

```

# sudo service winbind restart

```

11 Um den AD-Beitritt zu prüfen, führen Sie die folgenden Befehle aus und prüfen Sie, ob die richtige Ausgabe zurückgegeben wird.

- `net ads testjoin`
- `net ads info`

12 Starten Sie Ihr System neu und melden Sie sich an.

## Nächste Schritte

[Einrichten der Smartcard-Umleitung für einen RHEL 7.x/6.x-Desktop](#)

## Einrichten der Smartcard-Umleitung für einen RHEL 7.x/6.x-Desktop

Um die Smartcard-Umleitung auf einem RHEL 7.x/6.x-Desktop zu konfigurieren, müssen Sie die Bibliotheken, von denen die Funktion abhängt, das Stamm-CA-Zertifikat für die Authentifizierung sowie die erforderliche PC/SC Lite-Bibliothek installieren. Außerdem müssen Sie einige Konfigurationsdateien bearbeiten, um das Einrichten der Authentifizierung abzuschließen.

Wenden Sie das folgende Verfahren an, um die Smartcard-Umleitung für einen RHEL 7.x/6.x-Desktop einzurichten.

In einigen der Beispiele im Verfahren werden Platzhalterwerte verwendet, um Entitäten in Ihrer Netzwerkkonfiguration darzustellen, z. B. den DNS-Namen Ihrer Active Directory-Domäne. Ersetzen Sie die Platzhalterwerte durch spezifische Informationen für Ihre Konfiguration, wie in der folgenden Tabelle gezeigt.

Platzhalterwert	Beschreibung
<code>dns_IP_ADDRESS</code>	IP-Adresse Ihres DNS-Namensservers
<code>mydomain.com</code>	DNS-Name Ihrer Active Directory-Domäne
<code>MYDOMAIN.COM</code>	DNS-Name Ihrer Active Directory-Domäne in Großbuchstaben
<code>MYDOMAIN</code>	DNS-Name der Arbeitsgruppe oder NT-Domäne, in der sich Ihr Samba-Server befindet, in Großbuchstaben
<code>ads-hostname</code>	Hostname Ihres AD-Servers

Die Smartcard-Umleitung wird für Desktops unterstützt, auf denen RHEL 6.0 oder höher oder RHEL 7.1 oder höher ausgeführt wird.

**Hinweis** Wenn Sie die vSphere-Konsole verwenden, um sich bei einem RHEL 7.x.-System anzumelden, auf dem Horizon Agent installiert ist und die Smartcard-Umleitung aktiviert ist, kann eine verzögerte Abmeldezeit von zwei Minuten oder länger auftreten. Diese verzögerte Abmeldung tritt nur bei der vSphere-Konsole auf. Die RHEL 7.x-Abmeldeerfahrung von Horizon Client ist nicht betroffen.

## Voraussetzungen

[Integrieren eines RHEL 7.x/6.x-Desktops in Active Directory für die Smartcard-Umleitung](#)

## Verfahren

- 1 Installieren Sie die erforderlichen Bibliotheken.

```
yum install nss-tools nss-pam-ldapd esc pam_pkcs11 pam_krb5 opensc pcsc-lite-ccid authconfig
authconfig-gtk krb5-libs krb5-workstation krb5-pkinit pcsc-lite pcsc-lite-libs
```

- 2 Installieren Sie ein Stamm-CA-Zertifikat.

- a Laden Sie ein Stamm-CA-Zertifikat herunter und speichern Sie es in /tmp/certificate.cer auf Ihrem Desktop. Siehe [How to export Root Certification Authority Certificate](#).
- b Übertragen Sie das heruntergeladene Stamm-CA-Zertifikat in eine .pem-Datei.

```
openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

- c Verwenden Sie den Befehl certutil, um das Stamm-CA-Zertifikat in der Systemdatenbank /etc/pki/nssdb zu installieren.

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

- d Kopieren Sie das Stamm-CA-Zertifikat in das Verzeichnis /etc/pam\_pkcs11/cacerts.

```
mkdir -p /etc/pam_pkcs11/cacerts

cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
```

- 3 Navigieren Sie zu **Anwendungen > Verschiedene > Authentifizierung**, aktivieren Sie das Kontrollkästchen **Smartcard-Unterstützung aktivieren** und klicken Sie auf **Anwenden**.
- 4 Kopieren Sie die Smartcard-Treiber und die Treiberbibliothek in die Systemdatenbank /etc/pki/nssdb.

```
cp libcmP11.so /usr/lib64/
modutil -add "piv card 2.0" -libfile /usr/lib64/libcmP11.so -dbdir /etc/pki/nssdb/
```

- 5 Bearbeiten Sie die Einstellung module in der Konfigurationsdatei /etc/pam\_pkcs11/pam\_pkcs11.conf, wie im folgenden Beispiel.

```
pkcs11_module coolkey {
    module = libcmP11.so;
    description = "Cool Key";
    slot_num = 0;
    ca_dir = /etc/pam_pkcs11/cacerts;
    nss_dir = /etc/pki/nssdb;
    cert_policy = ca, signature;
}
```

- 6 Bearbeiten Sie die Datei `/etc/pam_pkcs11/cn_map`, damit sie die im folgenden Beispiel gezeigten Inhalte enthält. Welche konkreten Inhalte Sie einfügen müssen, entnehmen Sie den im Smartcard-Zertifikat aufgeführten Benutzerinformationen.

```
user sc -> user-sc
```

- 7 Bearbeiten Sie die Konfigurationsdatei `/etc/krb5.conf/`, wie im folgenden Beispiel.

```
[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    default_realm = MYDOMAIN.COM
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
    MYDOMAIN.COM = {
        kdc = ads-hostname
        admin_server = ads-hostname
        default_domain = ads-hostname
        pkinit_anchors = FILE:/etc/pki/nssdb/certificate.pem
        pkinit_cert_match = <KU>digitalSignature
        pkinit_kdc_hostname = ads-hostname
    }

[domain_realm]
    .mydomain.com = MYDOMAIN.COM
    mydomain.com = MYDOMAIN.COM
```

- 8 Bearbeiten Sie die Konfigurationsdatei `/etc/pam.d/system-auth`, damit sie die im folgenden Beispiel gezeigte Zeile enthält.

```
auth optional pam_krb5.so use_first_pass no_subsequent_prompt
    preauth_options=X509_user_identity=PKCS11:/usr/lib64/libcsp11.so
```

- 9 Starten Sie den PC/SC-Daemon neu.

```
chkconfig pcscd on
service pcscd start
```

- 10 Installieren Sie die erforderliche PC/SC-Lite-Version für Ihre RHEL-Distribution.

- Installieren Sie für RHEL 7.x PC/SC-Lite Version 1.8.8.

```
yum install git flex autoconf automake libtool libudev-devel flex
git clone https://salsa.debian.org/rousseau/PCSC.git
cd PCSC
git checkout -b 1.8.8 pcsc-1.8.8
./bootstrap
./configure --build=x86_64-redhat-linux-gnu --host=x86_64-redhat-linux-gnu --program-prefix=
--disable-dependency-tracking --prefix=/usr --exec-prefix=/usr --bindir=/usr/bin --
```

```

sbindir=/usr/sbin
--sysconfdir=/etc --datadir=/usr/share --includedir=/usr/include --libdir=/usr/lib64
--libexecdir=/usr/libexec --localstatedir=/var --sharedstatedir=/var/lib --mandir=/usr/
share/man
--infodir=/usr/share/info --disable-static --enable-usbdropdir=/usr/lib64/pcsc/drivers
make
make install

```

- Installieren Sie für RHEL 6.x PC/SC-Lite Version 1.7.4.

```

yum groupinstall "Development tools"
yum install libudev-devel
service pcscd stop
wget https://alioth.debian.org/frs/download.php/file/3598/pcsc-lite-1.7.4.tar.bz2
tar -xjvf pcsc-lite-1.7.4.tar.bz2
cd ./pcsc-lite-1.7.4
./configure --prefix=/usr/ --libdir=/usr/lib64/ --enable-usbdropdir=/usr/lib64/pcsc/drivers
--enable-confdir=/etc --enable-ipcdir=/var/run --disable-libusb --disable-serial --disable-
usb
--disable-libudev
make
make install
service pcscd start

```

- 11 Installieren Sie das Paket Horizon Agent mit aktivierter Smartcard-Umleitung.

```
sudo ./install_viewagent.sh -m yes
```

Installieren Sie das erforderliche Paket für Ihre RHEL-Distribution:

- Für RHEL 7.x müssen Sie Horizon Agent 7.8 oder höher installieren.
- Für RHEL 6.x installieren Sie View Agent 6.2.1 oder höher.

- 12 Starten Sie Ihr System neu und melden Sie sich an.

## Konfigurieren der Smartcard-Umleitung für Ubuntu-Desktops

Um die Smartcard-Umleitung für einen Ubuntu-Desktop einzurichten, müssen Sie zuerst den Desktop in eine Active Directory-Domäne integrieren. Installieren Sie dann die erforderlichen Bibliotheken und das Root-CA-Zertifikat, bevor Sie Horizon Agent installieren.

### Integrieren eines Ubuntu-Desktops in Active Directory für die Smartcard-Umleitung

Integrieren Sie den Desktop mithilfe von Samba und Winbind in eine Active Directory (AD)-Domäne, um die Smartcard-Umleitung auf einem Ubuntu-Desktop zu unterstützen.

Wenden Sie das folgende Verfahren an, um einen Ubuntu-Desktop für die Smartcard-Umleitung in eine AD-Domäne zu integrieren.

In einigen der Beispiele im Verfahren werden Platzhalterwerte verwendet, um Entitäten in Ihrer Netzwerkconfiguration darzustellen, z. B. den DNS-Namen Ihrer Active Directory-Domäne. Ersetzen Sie die Platzhalterwerte durch spezifische Informationen für Ihre Konfiguration, wie in der folgenden Tabelle gezeigt.

Platzhalterwert	Beschreibung
dns_IP_ADDRESS	IP-Adresse Ihres DNS-Namensservers
mydomain.com	DNS-Name Ihrer Active Directory-Domäne
MYDOMAIN.COM	DNS-Name Ihrer Active Directory-Domäne in Großbuchstaben
MYDOMAIN	DNS-Name der Arbeitsgruppe oder NT-Domäne, in der sich Ihr Samba-Server befindet, in Großbuchstaben
ads-hostname	Hostname Ihres AD-Servers
ads-hostname.mydomain.com	Vollqualifizierter Domänenname (FQDN) Ihres AD-Servers
mytimeserver.mycompany.com	DNS-Name Ihres NTP-Zeitserver
AdminUser	Benutzername des Linux-Desktop-Administrators

## Verfahren

- 1 Definieren Sie auf Ihrem Ubuntu-Desktop den Hostnamen des Desktops, indem Sie die Konfigurationsdatei `/etc/hostname` bearbeiten.
- 2 DNS konfigurieren.
  - a Fügen Sie den DNS-Servernamen und die IP-Adresse zur Konfigurationsdatei `/etc/hosts` hinzu.
  - b Fügen Sie die IP-Adresse Ihres DNS-Namensservers und den DNS-Namen Ihrer AD-Domäne zur Konfigurationsdatei `/etc/network/interfaces` hinzu, wie im folgenden Beispiel gezeigt.

```
dns-nameservers dns_IP_ADDRESS
dns-search mydomain.com
```

- 3 Installieren Sie das Paket `resolvconf`.
  - a Führen Sie den Installationsbefehl aus.

```
# apt-get install -y resolvconf
```

Erlauben Sie dem System, das Paket zu installieren und einen Neustart durchzuführen.

- b Überprüfen Sie Ihre DNS-Konfiguration in der Datei `/etc/resolve.conf` wie im folgenden Beispiel gezeigt.

```
# cat /etc/resolve.conf
...
nameserver dns_IP_ADDRESS
search mydomain.com
```

#### 4 Konfigurieren Sie die Synchronisierung der Netzwerkzeit.

- a Installieren Sie das Paket `ntpdate`.

```
# apt-get install -y ntpdate
```

- b Fügen Sie die NTP-Server Informationen zur Konfigurationsdatei `/etc/systemd/timesyncd.conf` hinzu, wie im folgenden Beispiel gezeigt.

```
[Time]
NTP=mytimeserver.mycompany.com
```

#### 5 Starten Sie den NTP-Dienst neu.

```
sudo service ntpdate restart
```

#### 6 Installieren Sie die erforderlichen AD-Join-Pakete.

- a Führen Sie den Installationsbefehl aus.

```
# apt-get install -y samba krb5-config krb5-user winbind libpam-winbind
libnss-winbind
```

- b Geben Sie bei der Installationsaufforderung nach dem Standard-Kerberos-Bereich den DNS-Namen Ihrer AD-Domäne in Großbuchstaben ein (z. B. `MYDOMAIN.COM`). Wählen Sie dann **Ok** aus.

#### 7 Bearbeiten Sie die Konfigurationsdatei `/etc/krb5.conf`, wie im folgenden Beispiel.

```
[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    default_realm = MYDOMAIN.COM
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
    MYDOMAIN.COM = {
        kdc = ads-hostname.mydomain.com
        admin_server = ads-hostname.mydomain.com
        default_domain = ads-hostname.mydomain.com
        pkinit_anchors = FILE:/etc/pki/nssdb/certificate.pem
        pkinit_cert_match = <KU>digitalSignature
        pkinit_kdc_hostname = ads-hostname.mydomain.com
    }

[domain_realm]
    .mydomain.com = MYDOMAIN.COM
    mydomain.com = MYDOMAIN.COM
```

- 8 Führen Sie die folgenden Befehle aus, um die Kerberos-Zertifizierung zu überprüfen.

```
# kinit Administrator@MYDOMAIN.COM

# klist
```

Stellen Sie sicher, dass die Befehle die Ausgabe ähnlich dem folgenden Beispiel zurückgeben.

```
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: Administrator@MYDOMAIN.COM
principal
2019-05-27T17:12:03    2019-05-28T03:12:03    krbtgt/MYDOMAIN.COM@MYDOMAIN.COM
renew until 2019-05-28T17:12:03
```

- 9 Bearbeiten Sie die Konfigurationsdatei `/etc/samba/smb.conf`, wie im folgenden Beispiel.

```
[global]
    workgroup = MYDOMAIN
    realm = MYDOMAIN.COM
    password server = ads-hostname.mydomain.com
    security = ads
    kerberos method = secrets only
    winbind use default domain = true
    winbind offline logon = false
    template homedir = /home/%D/%U
    template shell = /bin/bash
    client use spnego = yes
    client ntlmv2 auth = yes
    encrypt passwords = yes
    passdb backend = tdbsam
    winbind enum users = yes
    winbind enum groups = yes
    idmap uid = 10000-20000
    idmap gid = 10000-20000
```

- 10 Treten Sie der AD-Domäne bei und überprüfen Sie die Integration.

- a Führen Sie die AD-Join-Befehle aus.

```
# net ads join -U AdminUser@mydomain.com
# systemctl stop samba-ad-dc
# systemctl enable smbd nmbd winbind
# systemctl restart smbd nmbd winbind
```

- b Passen Sie die Konfigurationsdatei `/etc/nsswitch.conf` an, wie im folgenden Beispiel gezeigt.

```
passwd:    compat systemd winbind
group:     compat systemd winbind
shadow:    compat
gshadow:   files
```



- c Um das Ergebnis des AD-Beitritts zu überprüfen, führen Sie die folgenden Befehle aus und prüfen Sie, ob die richtige Ausgabe zurückgegeben wird.

```
# wbinfo -u

# wbinfo -g
```

- d Führen Sie zum Prüfen des Winbind Name Service Switch die folgenden Befehle aus und prüfen Sie, ob die Ausgabe stimmt.

```
# getent group|grep 'domain admins'

# getent passwd|grep 'ads-hostname'
```

- 11 Aktivieren Sie alle PAM-Profile.

```
# pam-auth-update
```

Wählen Sie im Bildschirm „PAM-Konfiguration“ alle PAM-Profile aus, einschließlich **Home-Verzeichnis bei Anmeldung erstellen**, und wählen Sie dann **Ok** aus.

- 12 Aktivieren Sie unter Ubuntu 16.04 den Benutzer-Switch im Anmeldebildschirm. Ändern Sie die Datei `/usr/share/lightdm/lightdm.conf.d/50-Ubuntu.conf` wie im folgenden Beispiel gezeigt.

```
user-session=ubuntu
greeter-show-manual-login=true
```

## Nächste Schritte

### Einrichten der Smartcard-Umleitung für einen Ubuntu-Desktop

## Einrichten der Smartcard-Umleitung für einen Ubuntu-Desktop

Um die Smartcard-Umleitung auf einem Ubuntu-Desktop zu konfigurieren, installieren Sie die Bibliotheken, von denen die Funktion abhängt, und das Stamm-CA-Zertifikat, um die vertrauenswürdige Authentifizierung von Smartcards zu unterstützen. Außerdem müssen Sie einige Konfigurationsdateien bearbeiten, um das Einrichten der Authentifizierung abzuschließen.

In einigen der Beispiele im Verfahren werden Platzhalterwerte verwendet, um Entitäten in Ihrer Netzwerkconfiguration darzustellen, z. B. den DNS-Namen Ihrer Active Directory-Domäne. Ersetzen Sie die Platzhalterwerte durch spezifische Informationen für Ihre Konfiguration, wie in der folgenden Tabelle gezeigt.

Platzhalterwert	Beschreibung
<code>dns_IP_ADDRESS</code>	IP-Adresse Ihres DNS-Namensservers
<code>mydomain.com</code>	DNS-Name Ihrer Active Directory-Domäne
<code>MYDOMAIN.COM</code>	DNS-Name Ihrer Active Directory-Domäne in Großbuchstaben
<code>MYDOMAIN</code>	DNS-Name der Arbeitsgruppe oder NT-Domäne, in der sich Ihr Samba-Server befindet, in Großbuchstaben

Platzhalterwert	Beschreibung
ads-hostname	Hostname Ihres AD-Servers
ads-hostname.mydomain.com	Vollqualifizierter Domänenname (FQDN) Ihres AD-Servers
mytimeserver.mycompany.com	DNS-Name Ihres NTP-Zeitserver
AdminUser	Benutzername des Linux-Desktop-Administrators

## Voraussetzungen

### Integrieren eines Ubuntu-Desktops in Active Directory für die Smartcard-Umleitung

## Verfahren

- 1 Installieren Sie die erforderlichen Bibliotheken.

```
# apt-get install -y pcscd pcsc-tools pkg-config libpam-pkcs11 opensc
libengine-pkcs11-openssl libnss3-tools
```

- 2 Installieren Sie ein Stamm-CA-Zertifikat.

- a Laden Sie ein Stamm-CA-Zertifikat herunter und speichern Sie es in /tmp/certificate.cer auf Ihrem Desktop. Siehe [How to export Root Certification Authority Certificate](#).
- b Übertragen Sie das heruntergeladene Stamm-CA-Zertifikat in eine .pem-Datei.

```
# openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

- c Verwenden Sie den Befehl certutil, um das Stamm-CA-Zertifikat in der Systemdatenbank /etc/pki/nssdb zu installieren.

```
# certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

- d Kopieren Sie das Stamm-CA-Zertifikat in das Verzeichnis /etc/pam\_pkcs11/cacerts.

```
# mkdir -p /etc/pam_pkcs11/cacerts

# cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
```

- 3 Erstellen Sie eine pkcs11-Hash-Datei.

```
# chmod a+r certificate.pem
# pkcs11_make_hash_link
```

- 4 Kopieren Sie die erforderlichen Treiber und fügen Sie die benötigten Bibliotheksdateien zum Verzeichnis `nssdb` hinzu.

- a Führen Sie die folgenden Befehle aus.

```
# cp libcmP11.so /usr/lib/
# mkdir -p /etc/pki/nssdb
# certutil -N -d /etc/pki/nssdb
# certutil -A -n rootca -i certificate.pem -t "CT,CT,CT" -d /etc/pki/nssdb
# modutil -dbdir /etc/pki/nssdb/ -add "piv card 2.0" -libfile /usr/lib/libcmP11.so
```

- b Stellen Sie sicher, dass das erwartete Zertifikat erfolgreich geladen wurde.

```
# certutil -L -d /etc/pki/nssdb

Certificate Nickname

rootca
```

- c Stellen Sie sicher, dass die erwarteten Bibliotheken erfolgreich hinzugefügt wurden.

```
modutil -dbdir /etc/pki/nssdb -list

Listing of PKCS #11 Modules
-----
1. NSS Internal PKCS #11 Module
   slots: 2 slots attached
   status: loaded

   slot: NSS Internal Cryptographic Services
   token: NSS Generic Crypto Services

   slot: NSS User Private Key and Certificate Services
   token: NSS Certificate DB

2. piv card 2.0
   library name: /usr/lib/libcmP11.so
   slots: There are no slots attached to this module
   status: loaded
-----
```

## 5 Konfigurieren Sie die pam\_pkcs11-Bibliothek.

- a Erstellen Sie eine pam\_pkcs11.conf-Datei mit dem standardmäßigen Beispieldinhalt.

```
# mkdir /etc/pam_pkcs11
# zcat /usr/share/doc/libpam-pkcs11/examples/pam_pkcs11.conf.example.gz |
tee /etc/pam_pkcs11/pam_pkcs11.conf
```

- b Bearbeiten Sie die Datei /etc/pam\_pkcs11/pam\_pkcs11.conf, wie im folgenden Beispiel gezeigt.

```
use_pkcs11_module = mysc;

pkcs11_module mysc {
    module = /usr/lib/libcMP11.so;
    description = "LIBCMP11";
    slot_num = 0;
    ca_dir = /etc/pki/cacerts;
    nss_dir = /etc/pki/nssdb;
    cert_policy = ca;
}
...
use_mappers = cn, null;
...
mapper cn {
    debug = false;
    module = internal;
    # module = /lib/pam_pkcs11/cn_mapper.so;
    ignorecase = true;
    mapfile = file:///etc/pam_pkcs11/cn_map;
    # mapfile = "none";
}
```

- c Bearbeiten Sie die Datei /etc/pam\_pkcs11/cn\_map , damit sie die folgende Zeile enthält.

```
ads-hostname -> ads-hostname
```

## 6 Konfigurieren Sie die PAM-Authentifizierung.

- a Bearbeiten Sie die Konfigurationsdatei `/etc/pam.d/gdm-password`. Platzieren Sie die Autorisierungszeile `pam_pkcs11.so` vor der Zeile `common-auth`, wie im folgenden Beispiel gezeigt.

```
#%PAM-1.0
auth    requisite      pam_nologin.so
auth    required       pam_succeed_if.so user != root quiet_success
auth    sufficient
pam_pkcs11.so
@include common-auth
auth    optional       pam_gnome_keyring.so
@include common-account
```

- b Bearbeiten Sie für Ubuntu 16.04 die Konfigurationsdatei `/etc/pam.d/lightdm`. Platzieren Sie die Autorisierungszeile `pam_pkcs11.so` vor der Zeile `common-auth`, wie im folgenden Beispiel gezeigt.

```
#%PAM-1.0
auth    requisite      pam_nologin.so debug
auth    sufficient     pam_succeed_if.so user ingroup nopasswdlogin debug
auth    [success=3 default=ignore] pam_pkcs11.so
@include common-auth
auth    optional       pam_gnome_keyring.so
auth    optional       pam_kwallet.so
```

- c Bearbeiten Sie für Ubuntu 16.04 die Konfigurationsdatei `/etc/pam.d/unity`. Platzieren Sie die Autorisierungszeile `pam_pkcs11.so` vor der Zeile `common-auth`, wie im folgenden Beispiel gezeigt.

```
auth    [success=3 default=ignore] pam_pkcs11.so
@include common-auth
auth    optional       pam_gnome_keyring.so
```

- ## 7 Führen Sie die folgenden Befehle aus, um die Smartcard-Hardware und die auf der Smartcard installierten Zertifikate zu überprüfen.

```
# pcsc_scan

# pkcs11_listcerts

# pkcs11_inspect
```

## 8 Konfigurieren Sie den Gnome Screensaver so, dass er beim Entfernen der Smartcard gesperrt wird.

### a Installieren Sie das Screensaver-Paket.

```
# apt-get install gnome-screensaver
```

### b Um den Screensaver zu konfigurieren, bearbeiten Sie die Datei `/etc/pam_pkcs11/pkcs11_eventmgr.conf`, wie im folgenden Beispiel gezeigt.

```
pkcs11_eventmgr {
    # Run in background? Implies debug=false if true
    daemon = true;

    # show debug messages?
    debug = false;

    # polling time in seconds
    polling_time = 1;

    # expire time in seconds
    # default = 0 ( no expire )
    expire_time = 0;

    # pkcs11 module to use
    pkcs11_module = /usr/lib/libcmP11.so;

    #
    # list of events and actions
    # Card inserted
    event card_insert {
        # what to do if an action fail?
        # ignore : continue to next action
        # return : end action sequence
        # quit : end program
        on_error = ignore ;

        # You can enter several, comma-separated action entries
        # they will be executed in turn
        action = "gnome-screensaver-command --poke";
    }

    # Card has been removed
    event card_remove {
        on_error = ignore;
        action = "gnome-screensaver-command --lock";
    }

    # Too much time card removed
    event expire_time {
```

```

    on_error = ignore;
    action = "/bin/false";
}
}

```

- c Führen Sie `pkcs11_eventmgr` aus.

```
# /usr/bin/pkcs11_eventmgr &
```

- 9 Installieren Sie das Paket Horizon Agent mit aktivierter Smartcard-Umleitung.

```
# sudo ./install_viewagent.sh -m yes
```

**Hinweis** Sie müssen Horizon Agent 7.9 oder höher installieren.

- 10 Starten Sie Ihr System neu und melden Sie sich an.

## Konfigurieren der Smartcard-Umleitung für SLED/SLES-Desktops

Um die Smartcard-Umleitung für einen SLED/SLES-Desktop einzurichten, müssen Sie zuerst den Desktop in eine Active Directory-Domäne integrieren. Installieren Sie dann die erforderlichen Bibliotheken und das Root-CA-Zertifikat, bevor Sie Horizon Agent installieren.

### Integrieren eines SLED/SLES-Desktops in Active Directory für die Smartcard-Umleitung

Integrieren Sie den Desktop mithilfe von Samba und Winbind in eine Active Directory (AD)-Domäne, um die Smartcard-Umleitung auf einem SLED/SLES-Desktop zu unterstützen.

Wenden Sie das folgende Verfahren an, um einen SLED/SLES-Desktop für die Smartcard-Umleitung in eine AD-Domäne zu integrieren.

In einigen der Beispiele im Verfahren werden Platzhalterwerte verwendet, um Entitäten in Ihrer Netzwerkkonfiguration darzustellen, z. B. den DNS-Namen Ihrer Active Directory-Domäne. Ersetzen Sie die Platzhalterwerte durch spezifische Informationen für Ihre Konfiguration, wie in der folgenden Tabelle gezeigt.

Platzhalterwert	Beschreibung
<code>dns_IP_ADDRESS</code>	IP-Adresse Ihres DNS-Namensservers
<code>mydomain.com</code>	DNS-Name Ihrer Active Directory-Domäne
<code>MYDOMAIN.COM</code>	DNS-Name Ihrer Active Directory-Domäne in Großbuchstaben
<code>MYDOMAIN</code>	DNS-Name der Arbeitsgruppe oder NT-Domäne, in der sich Ihr Samba-Server befindet, in Großbuchstaben
<code>ads-hostname</code>	Hostname Ihres AD-Servers
<code>ads-hostname.mydomain.com</code>	Vollqualifizierter Domänenname (FQDN) Ihres AD-Servers
<code>mytimeserver.mycompany.com</code>	DNS-Name Ihres NTP-Zeitservers
<code>AdminUser</code>	Benutzername des Linux-Desktop-Administrators

## Verfahren

- 1 Konfigurieren Sie die Netzwerkeinstellungen für Ihren SLED/SLES-Desktop.
  - a Definieren Sie den Hostnamen des Desktops, indem Sie die Konfigurationsdateien `/etc/hostname` und `/etc/hosts` bearbeiten.
  - b Konfigurieren Sie die IP-Adresse des DNS-Servers und deaktivieren Sie **Automatisches DNS**. Deaktivieren Sie für SLES 12 SP3 auch **Hostnamen über DHCP ändern**.
  - c Um die Synchronisierung der Netzwerkzeit zu konfigurieren, fügen Sie Ihre NTP-Server Informationen der Datei `/etc/ntp.conf` hinzu, wie im folgenden Beispiel gezeigt.

```
server mytimeserver.mycompany.com
```

- 2 Installieren Sie die erforderlichen AD-Join-Pakete.

```
# zypper in krb5-client samba-winbind
```



### 3 Bearbeiten Sie die erforderlichen Konfigurationsdateien.

- a Bearbeiten Sie die Datei `/etc/samba/smb.conf`, wie im folgenden Beispiel gezeigt.

```
[global]
    workgroup = MYDOMAIN
    usershare allow guests = NO
    idmap gid = 10000-20000
    idmap uid = 10000-20000
    kerberos method = secrets and keytab
    realm = MYDOMAIN.COM
    security = ADS
    template homedir = /home/%D/%U
    template shell = /bin/bash
    winbind use default domain=true
    winbind offline logon = yes
    winbind refresh tickets = yes

[homes]
    ...
```

- b Bearbeiten Sie die Datei `/etc/krb5.conf`, wie im folgenden Beispiel gezeigt.

```
[libdefaults]
    default_realm = MYDOMAIN.COM
    clocks skew = 300

[realms]
    MYDOMAIN.COM = {
        kdc = ads-hostname.mydomain.com
        default_domain = mydomain.com
        admin_server = ads-hostname.mydomain.com
    }

[logging]
    kdc = FILE:/var/log/krb5/krb5kdc.log
    admin_server = FILE:/var/log/krb5/kadmind.log
    default = SYSLOG:NOTICE:DAEMON

[domain_realm]
    .mydomain.com = MYDOMAIN.COM
    mydomain.com = MYDOMAIN.COM

[appdefaults]
    pam = {
        ticket_lifetime = 1d
        renew_lifetime = 1d
        forwardable = true
        proxiable = false
        minimum_uid = 1
    }
```

- c Bearbeiten Sie die Datei `/etc/security/pam_winbind.conf`, wie im folgenden Beispiel gezeigt.

```
cached_login = yes
krb5_auth = yes
krb5_ccache_type = FILE
```

- d Bearbeiten Sie die Datei `/etc/nsswitch.conf`, wie im folgenden Beispiel gezeigt.

```
passwd: compat winbind
group: compat winbind
```

- 4 Treten Sie der AD-Domäne bei, wie im folgenden Beispiel gezeigt.

```
# net ads join -U AdminUser
```

- 5 Aktivieren Sie den Winbind-Dienst.

- a Um Winbind zu aktivieren und zu starten, führen Sie die folgende Befehlssequenz aus.

```
# pam-config --add --winbind
# pam-config -a --mkhomedir
# systemctl enable winbind
# systemctl start winbind
```

- b Um sicherzustellen, dass sich AD-Benutzer beim Desktop anmelden können, ohne den Linux-Server neu starten zu müssen, führen Sie die folgende Befehlssequenz aus.

```
# systemctl stop nscd
# nscd -i passwd
# nscd -i group
# systemctl start nscd
```

- 6 Um den erfolgreichen AD-Beitritt zu prüfen, führen Sie die folgenden Befehle aus und prüfen Sie, ob die richtige Ausgabe zurückgegeben wird.

```
# wbinfo -u

# wbinfo -g
```

## Nächste Schritte

### [Einrichten der Smartcard-Umleitung für einen SLED/SLES-Desktop](#)

## Einrichten der Smartcard-Umleitung für einen SLED/SLES-Desktop

Um die Smartcard-Umleitung auf einem SLED/SLES-Desktop zu konfigurieren, installieren Sie die Bibliotheken, von denen die Funktion abhängt, und das Stamm-CA-Zertifikat, um die vertrauenswürdige Authentifizierung von Smartcards zu unterstützen. Außerdem müssen Sie einige Konfigurationsdateien bearbeiten, um das Einrichten der Authentifizierung abzuschließen.

In einigen der Beispiele im Verfahren werden Platzhalterwerte verwendet, um Entitäten in Ihrer Netzwerkkonfiguration darzustellen, z. B. den DNS-Namen Ihrer Active Directory-Domäne. Ersetzen Sie die Platzhalterwerte durch spezifische Informationen für Ihre Konfiguration, wie in der folgenden Tabelle gezeigt.

Platzhalterwert	Beschreibung
dns_IP_ADDRESS	IP-Adresse Ihres DNS-Namenservers
mydomain.com	DNS-Name Ihrer Active Directory-Domäne
MYDOMAIN.COM	DNS-Name Ihrer Active Directory-Domäne in Großbuchstaben
MYDOMAIN	DNS-Name der Arbeitsgruppe oder NT-Domäne, in der sich Ihr Samba-Server befindet, in Großbuchstaben
ads-hostname	Hostname Ihres AD-Servers
ads-hostname.mydomain.com	Vollqualifizierter Domänenname (FQDN) Ihres AD-Servers
mytimeserver.mycompany.com	DNS-Name Ihres NTP-Zeitserver
AdminUser	Benutzername des Linux-Desktop-Administrators

## Voraussetzungen

### Integrieren eines SLED/SLES-Desktops in Active Directory für die Smartcard-Umleitung

## Verfahren

### 1 Installieren Sie die erforderlichen Bibliothekspakete.

- a Installieren Sie die PAM-Bibliothek und die anderen Pakete.

```
# zypper install pam_pkcs11 mozilla-nss mozilla-nss-tools
pcsc-lite pcsc-ccid opensc coolkey pcsc-tools
```

- b Um die PC/SC-Tools zu installieren, führen Sie die folgende Befehlssequenz aus.

```
# SUSEConnect --list-extensions
# SUSEConnect -p PackageHub/12.3/x86_64
# zypper in pcsc-tools
```

### 2 Installieren Sie ein Stamm-CA-Zertifikat.

- a Laden Sie ein Stamm-CA-Zertifikat herunter und speichern Sie es in `/tmp/certificate.cer` auf Ihrem Desktop. Siehe [How to export Root Certification Authority Certificate](#).
- b Suchen Sie das heruntergeladene Stamm-CA-Zertifikat, übertragen Sie es in eine `.pem`-Datei und erstellen Sie eine Hash-Datei.

```
# openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
# cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
# chmod a+r /etc/pam_pkcs11/cacerts/certificate.pem
# cd /etc/pam_pkcs11/cacerts
# pkcs11_make_hash_link
```

- c Installieren Sie vertrauenswürdige Anker in der NSS-Datenbank.

```
# mkdir /etc/pam_pkcs11/nssdb
# certutil -N -d /etc/pam_pkcs11/nssdb
# certutil -L -d /etc/pam_pkcs11/nssdb
# certutil -A -n rootca -i certificate.pem -t "CT,CT,CT" -d /etc/pam_pkcs11/nssdb
```

- d Installieren Sie die erforderlichen Treiber.

```
# cp libcmP11.so /usr/lib64/
# modutil -add "piv card 2.0" -libfile /usr/lib64/libcmP11.so -dbdir /etc/pam_pkcs11/nssdb/
```

- 3 Bearbeiten Sie die Datei `/etc/pam_pkcs11/pam_pkcs11.conf`.

- a Löschen Sie die Zeile `use_pkcs11_module = nss`. Fügen Sie an dieser Stelle die Zeile `use_pkcs11_module = mysc` hinzu.
- b Fügen Sie das `mysc`-Modul hinzu, wie im folgenden Beispiel gezeigt.

```
pkcs11_module mysc {
    module = /usr/lib64/libcmP11.so;
    description = "MY Smartcard";
    slot_num = 0;
    nss_dir = /etc/pam_pkcs11/nssdb;
    cert_policy = ca, ocsp_on, signature, crl_auto;
}
```

- c Aktualisieren Sie die Konfiguration des Zuordnungsprogramms für allgemeine Namen, wie im folgenden Beispiel gezeigt.

```
# Assume common name (CN) to be the login
mapper cn {
    debug = false;
    module = internal;
    # module = /usr/lib64/pam_pkcs11/cn_mapper.so;
    ignorecase = true;
    mapfile = file:///etc/pam_pkcs11/cn_map;}
```

- d Löschen Sie die Zeile `use_mappers = ms`. Fügen Sie an dieser Stelle die Zeile `use_mappers = cn, null` hinzu.

- 4 Bearbeiten Sie die Konfigurationsdatei `/etc/pam_pkcs11/cn_map`, damit sie die folgende Zeile enthält.

```
ads-hostname -> ads-hostname
```

**5** Bearbeiten Sie die PAM-Konfiguration.

- a Um die Konfiguration der Smartcard-Authentifizierung zu ermöglichen, deaktivieren Sie zunächst das Tool `pam_config`.

```
# find /etc/pam.d/ -type l -iname "common-*" -delete
# for X in /etc/pam.d/common-*-pc; do cp -ivp $X ${X:0:-3}; done
```

- b Erstellen Sie eine Datei mit dem Namen `common-auth-smartcard` im Verzeichnis `/etc/pam.d/`. Fügen Sie der Datei den folgenden Inhalt hinzu.

```
auth    required      pam_env.so
auth    sufficient    pam_pkcs11.so
auth    optional      pam_gnome_keyring.so
auth    [success=1 default=ignore] pam_unix.so nullok_secure try_first_pass
auth    required      pam_winbind.so use_first_pass
```

- c Ersetzen Sie für SLED/SLES 12 SP3 die Zeile `auth include common-auth` durch die Zeile `auth include common-auth-smartcard` in den beiden folgenden Dateien: `/etc/pam.d/gdm` und `/etc/pam.d/xscreensaver`.

**6** Deaktivieren Sie die Firewall.

```
# rcSuSEfirewall2 stop
# chkconfig SuSEfirewall2_setup off
# chkconfig SuSEfirewall2_init off
```

---

**Hinweis** Die Smartcard-Umleitung schlägt manchmal fehl, wenn die Firewall aktiviert ist.

---

**7** Installieren Sie die für die Smartcard-Umleitung erforderlichen Bibliothekspakete.

- a Führen Sie für SLED/SLES 12 SP3 die folgenden Installationsbefehle aus.

```
# SUSEConnect -p sle-sdk/12.3/x86_64
# zypper in git autoconf automake libtool flex libudev-devel gcc
```

- b Installieren Sie für SLES 12 SP3 `systemd-devel`.

```
# zypper in systemd-devel
```

**8** Installieren Sie das Paket Horizon Agent mit aktivierter Smartcard-Umleitung.

```
# sudo ./install_viewagent.sh -m yes
```

---

**Hinweis** Sie müssen Horizon Agent 7.9 oder höher installieren.

---

**9** Starten Sie Ihr System neu und melden Sie sich an.

## Einrichten von True SSO für Linux-Desktops

Die Funktion „True Single Sign-On“ (True SSO) gewährt Benutzern Zugriff auf einen virtuellen Linux-Desktop, einen veröffentlichten Desktop oder eine veröffentlichte Anwendung, nachdem sie sich zum ersten Mal bei VMware Identity Manager angemeldet haben. Benutzer können sich mit einer Smartcard-, RSA SecurID- oder RADIUS-Authentifizierung bei VMware Identity Manager anmelden und dann auf Remote-Linux-Ressourcen zugreifen, ohne ihre Active Directory-Anmeldedaten einzugeben.

Wenn sich ein Benutzer mit den Anmeldedaten für Active Directory (AD) authentifiziert, ist die True SSO-Funktion nicht erforderlich. Sie können aber die Verwendung von True SSO auch für diesen Fall konfigurieren, damit der Desktop sowohl AD- als auch True SSO-Anmeldedaten unterstützen kann.

Bei der Herstellung einer Verbindung mit einem virtuellen Linux-Desktop oder einem veröffentlichten Desktop oder einer veröffentlichten Anwendung können Benutzer auswählen, ob sie den nativen Horizon Client oder HTML Access verwenden möchten.

Für True SSO gelten folgende Einschränkungen:

- Diese Funktion wird nur auf Desktops mit den folgenden Distributionen unterstützt: RHEL/CentOS 8.0, RHEL/CentOS 7.x, Ubuntu 16.04 und 18.04 und SLED/SLES 12.x SP3.
- Für RHEL/CentOS 7.x-Desktops wird die Funktion nur mit den folgenden Beitrittsmethoden unterstützt: die standardmäßigen Tools für den Domänenbeitritt, Samba, System Security Services Daemon (SSSD) und das Kerberos-Protokoll für die Netzwerkauthentifizierung.

Führen Sie folgende Aufgaben aus, um True SSO in Ihrer Linux-Umgebung einzurichten.

- 1 Konfigurieren Sie True SSO in Ihrer Horizon 7-Umgebung. Weitere Informationen finden Sie unter „Einrichten von True SSO“ im Dokument *Horizon 7-Verwaltung*.
- 2 Integrieren Sie Ihren Desktop in eine AD-Domäne, indem Sie die für Ihre Linux-Distribution erforderlichen Schritte ausführen.
- 3 Konfigurieren Sie True SSO auf Ihrem Desktop, indem Sie die für Ihre Linux-Distribution erforderlichen Schritte ausführen.

## Konfigurieren von True SSO auf RHEL/CentOS 8.0-Desktops

Um True SSO auf einem RHEL/CentOS 8.0-Desktop zu unterstützen, müssen Sie das System zuerst in Ihre Active Directory-Domäne (AD) integrieren. Anschließend müssen Sie bestimmte Konfigurationen auf dem System ändern, um die True SSO-Funktion zu unterstützen.

---

**Hinweis** True SSO wird auf Instant-Clone-Desktops mit RHEL 8.0 nicht unterstützt.

---

In einigen der Beispiele im Verfahren werden Platzhalterwerte verwendet, um Entitäten in Ihrer Netzwerkkonfiguration darzustellen, z. B. den DNS-Namen Ihrer Active Directory-Domäne. Ersetzen Sie die Platzhalterwerte durch spezifische Informationen für Ihre Konfiguration, wie in der folgenden Tabelle gezeigt.

Platzhalterwert	Beschreibung
mydomain.com	DNS-Name Ihrer Active Directory-Domäne
MYDOMAIN.COM	DNS-Name Ihrer Active Directory-Domäne in Großbuchstaben
MYDOMAIN	Name Ihrer NetBIOS-Domäne

### Voraussetzungen

- Stellen Sie sicher, dass der Active Directory(AD)-Server durch DNS auf dem RHEL/CentOS 8.0-System aufgelöst werden kann.
- Konfigurieren Sie den Hostnamen des Systems.
- Konfigurieren Sie das Network Time Protocol (NTP) auf dem System.

### Verfahren

- 1 Überprüfen Sie auf dem RHEL/CentOS 8.0-System die Netzwerkverbindung mit Active Directory.

```
# realm discover mydomain.com
```

- 2 Installieren Sie die erforderlichen Abhängigkeitspakete.

```
# yum install oddjob oddjob-mkhomedir sssd adcli samba-common-tools
```

- 3 Treten Sie der AD-Domäne bei.

```
# realm join --verbose mydomain.com -U administrator
```

- 4 Laden Sie das Root-CA-Zertifikat herunter und kopieren Sie es als PEM-Datei in das erforderliche Verzeichnis.

```
# openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
# cp /tmp/certificate.pem /etc/sssdpki/sssdpki_auth_ca_db.pem
```

- 5 Passen Sie die Konfigurationsdatei /etc/sssdpki/sssdpki.conf an, wie im folgenden Beispiel gezeigt.

```
[sssdpki]
domains = mydomain.com
config_file_version = 2
services = nss, pam

[domain/mydomain.com]
ad_domain = mydomain.com
krb5_realm = IMYDOMAIN.COM
realmd_tags = manages-system joined-with-adcli
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = False <----- Use short name for user
```

```

fallback_homedir = /home/%u@%d
access_provider = ad
ad_gpo_map_interactive = +gdm-vmwcred <----- Add this line for SSO

[pam] <----- Add pam section for certificate logon
pam_cert_auth = True <----- Add this line to enable certificate
logon for system
pam_p11_allowed_services = +gdm-vmwcred <----- Add this line to enable certificate
logon for VMware Horizon Agent

[certmap/mydomain.com/truesso] <----- Add this section and following lines to
set match and map rule for certificate user
matchrule = <EKU>msScLogin
maprule = (|(userPrincipal={subject_principal}))(samAccountName={subject_principal.short_name}))
domains = mydomain.com
priority = 10

```

- 6 Installieren Sie das Paket Horizon Agent mit aktiviertem True SSO.

**Hinweis** Sie müssen Horizon Agent 7.11 oder höher installieren.

```
# sudo ./install_viewagent.sh -T yes
```

- 7 Ändern Sie die Konfigurationsdatei `/etc/vmware/viewagent-custom.conf`, sodass sie die folgende Zeile enthält.

```
NetbiosDomain = MYDOMAIN
```

- 8 Starten Sie das System neu und melden Sie sich erneut an.

## Konfigurieren von True SSO für RHEL/CentOS 7.x-Desktops

Um True SSO für einen RHEL/CentOS 7.x-Desktop einzurichten, müssen Sie zuerst den Desktop in eine Active Directory-Domäne integrieren. Installieren Sie dann die erforderlichen Bibliotheken und das Root-CA-Zertifikat, bevor Sie Horizon Agent installieren.

### Integrieren eines RHEL/CentOS 7.x-Desktops in Active Directory für True SSO

Um True SSO auf einer Instant-Clone-VM in einer Horizon 7-Linux-Desktopumgebung auf einem RHEL/CentOS 7.x-System zu unterstützen, müssen Sie auf der Master-Linux-VM Samba konfigurieren.

Die RHEL/CentOS 7.x-Funktion `realmd` bietet eine einfache Möglichkeit zum Erkennen von und Beitreten zu Identitätsdomänen. Anstatt das System mit der Domäne selbst zu verbinden, konfiguriert `realmd` zugrunde liegende Linux-Systemdienste, wie z. B. SSSD oder Winbind, für die Verbindung mit der Domäne. Die folgenden Schritte beschreiben, wie Sie mithilfe von `realmd` und Samba einen Offline-Domänenbeitritt eines RHEL/CentOS 7.x-Desktops zu Active Directory durchzuführen.



## Voraussetzungen

- Das System Red Hat Enterprise Linux (RHEL) ist über Red Hat Network (RHN) abonniert oder das Tool yum ist darauf lokal installiert.
- Der Active Directory (AD)-Server kann auf dem Linux-System über das DNS aufgelöst werden.
- Das Network Time Protocol (NTP) ist auf dem Linux-System konfiguriert.

## Verfahren

- 1 Stellen Sie sicher, dass das RHEL/CentOS-System den AD-Server erkennen kann. Verwenden Sie das folgende Beispiel, bei dem *ADdomain.example.com* mit Ihren Active Directory-Serverinformationen ersetzt werden muss.

```
sudo realm discover ADdomain.example.com
```

- 2 Installieren Sie das Samba-tdb-tools-Paket.

Das Samba-tdb-tools-Paket kann nicht vom offiziellen Red Hat-Repository heruntergeladen werden. Sie müssen es manuell herunterladen. Verwenden Sie z. B. den folgenden Befehl, um es von einem CentOS 7.5-System herunterzuladen. Installieren Sie anschließend das heruntergeladene Paket in Ihrem RHEL-System.

```
yumdownloader tdb-tools
```

Wenn Sie nicht über ein CentOS-System verfügen, öffnen Sie <https://rpmfind.net/linux/rpm2html/search.php?query=tdb-tools&submit=Search+...&system=&arch=>, laden Sie das tdb-tools-1.3.15-1.el7.x86\_64.rpm-Paket herunter und installieren Sie es auf Ihrem RHEL-System.

- 3 Installieren Sie Samba und die Abhängigkeitspakete.

```
sudo yum install sssd-tools sssd adcli samba-common pam_ldap pam_krb5 samba samba-client krb5-workstation
```

- 4 Führen Sie den Befehl join anhand des folgenden Beispiels aus, bei dem *DNSdomain.example.com* durch den für Ihre Umgebung bestimmten Pfad der DNS-Domäne ersetzt werden muss.

```
sudo realm join DNSdomain.example.com -U administrator
```

Wenn der Befehl „Join“ erfolgreich durchgeführt wurde, erhalten Sie folgende Meldung.

```
Maschine im Bereich erfolgreich registriert
```

- 5 Starten Sie Ihr System neu und melden Sie sich an.

## Nächste Schritte

[Konfigurieren von True SSO auf RHEL/CentOS 7.x-Desktops](#)

## Konfigurieren von True SSO auf RHEL/CentOS 7.x-Desktops

Um die True SSO-Funktion auf einem RHEL/CentOS 7.x-Desktop zu aktivieren, installieren Sie die Bibliotheken, von denen die True SSO-Funktion abhängig ist, das Stamm-CA-Zertifikat für die vertrauenswürdige Authentifizierung und Horizon Agent. Außerdem müssen Sie einige Konfigurationsdateien bearbeiten, um des Einrichten der Authentifizierung abzuschließen.

Verwenden Sie das folgende Verfahren, um True SSO auf RHEL 7.x- und CentOS 7.x-Desktops zu aktivieren. Um True SSO auf diesen Desktops zu unterstützen, müssen Sie Horizon Agent 7.6 oder höher installieren.

In einigen der Beispiele im Verfahren werden Platzhalterwerte verwendet, um Entitäten in Ihrer Netzwerkconfiguration darzustellen, z. B. den DNS-Namen Ihrer Active Directory-Domäne. Ersetzen Sie die Platzhalterwerte durch spezifische Informationen für Ihre Konfiguration, wie in der folgenden Tabelle gezeigt.

Platzhalterwert	Beschreibung
dns_server	Pfad zu Ihrem DNS-Namensserver
mydomain.com	DNS-Name Ihrer Active Directory-Domäne
MYDOMAIN.COM	DNS-Name Ihrer Active Directory-Domäne in Großbuchstaben

### Voraussetzungen

- Konfigurieren Sie True SSO für VMware Identity Manager und Horizon Connection Server.
- [Integrieren eines RHEL/CentOS 7.x-Desktops in Active Directory für True SSO](#)
- Fordern Sie ein Stamm-CA-Zertifikat an und speichern Sie es auf Ihrem RHEL/CentOS 7.x-Desktop als /tmp/certificate.cer. Siehe [How to export Root Certification Authority Certificate](#).

### Verfahren

- 1 Installieren Sie die PKCS11-Support-Paket-Gruppe.

```
yum install -y nss-tools nss-pam-ldapd pam_krb5 krb5-libs krb5-workstation krb5-pkinit
```

## 2 Installieren Sie ein Stamm-CA-Zertifikat.

- a Suchen Sie das Stamm-CA-Zertifikat, das Sie heruntergeladen haben, und übertragen Sie es in eine .pem-Datei.

```
openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

- b Verwenden Sie den Befehl `certutil`, um das Stamm-CA-Zertifikat in der Systemdatenbank `/etc/pki/nssdb` zu installieren.

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

- c Fügen Sie das Stamm-CA-Zertifikat zur Liste der vertrauenswürdigen CA-Zertifikate auf Ihrem RHEL/CentOS 7.x-System hinzu und aktualisieren Sie die systemweite Trust Store-Konfiguration mit dem Befehl `update-ca-trust`.

```
cp /tmp/certificate.pem /etc/pki/ca-trust/source/anchors/ca_cert.pem
update-ca-trust
```

## 3 Ändern Sie den entsprechenden Abschnitt in der SSSD-Konfigurationsdatei Ihres Systems für Ihre Domäne, wie im folgenden Beispiel.

```
[domain/mydomain.com]
ad_domain = mydomain.com
krb5_realm = MYDOMAIN.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
#set the next line to false, so you can use the short name instead of the full domain name.
use_fully_qualified_names = False
fallback_homedir = /home/%u@%d
access_provider = ad
```

## 4 Ändern Sie die Kerberos-Konfigurationsdatei `/etc/krb5.conf`, wie im folgenden Beispiel.

```
[libdefaults]
dns_lookup_realm = false
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true
rdns = false
default_ccache_name = KEYRING:persistent:%{uid}
# Add following line, if the system doesn't add it automatically
default_realm = MYDOMAIN.COM

[realms]
MYDOMAIN.COM = {
    kdc = dns_server
    admin_server = dns_server
    # Add the following three lines for pkinit_*
```

```
pkinit_anchors = DIR:/etc/pki/ca-trust/source/anchors
pkinit_kdc_hostname = your_org_DNS_server
pkinit_eku_checking = kpServerAuth
}
[domain_realm]
mydomain.com = MYDOMAIN.COM
.mydomain.com = MYDOMAIN.COM
```

- 5 Installieren Sie das Paket Horizon Agent mit aktiviertem True SSO.

```
sudo ./install_viewagent.sh -T yes
```

**Hinweis** Sie müssen Horizon Agent 7.6 oder höher installieren.

- 6 Fügen Sie den folgenden Parameter zur benutzerdefinierten Horizon Agent-Konfigurationsdatei `/etc/vmware/viewagent-custom.conf` hinzu. Verwenden Sie das folgende Beispiel, in dem `NETBIOS_NAME_OF_DOMAIN` der NetBIOS-Name der Domäne Ihrer Organisation ist.

```
NetbiosDomain=NETBIOS_NAME_OF_DOMAIN
```

- 7 Starten Sie Ihr System neu und melden Sie sich an.

## Konfigurieren von True SSO für Ubuntu-Desktops

Um True SSO für einen Ubuntu-Desktop einzurichten, müssen Sie zuerst den Desktop in eine Active Directory-Domäne integrieren. Installieren Sie dann die erforderlichen Bibliotheken und das Root-CA-Zertifikat, bevor Sie Horizon Agent installieren.

### Integrieren eines Ubuntu-Desktops in Active Directory für True SSO

Integrieren Sie den Desktop in eine Active Directory-Domäne mithilfe von Samba und Winbind, um True SSO auf einem Desktop mit Ubuntu 16.04 oder 18.04 zu unterstützen.

Verfahren Sie wie folgt, um einen Ubuntu 16.04- oder 18.04-Desktop in eine Active Directory-Domäne zu integrieren.

In einigen der Beispiele im Verfahren werden Platzhalterwerte verwendet, um Entitäten in Ihrer Netzwerkconfiguration darzustellen, z. B. den Hostnamen Ihres Ubuntu-Desktops. Ersetzen Sie die Platzhalterwerte durch spezifische Informationen für Ihre Konfiguration, wie in der folgenden Tabelle gezeigt.

Platzhalterwert	Beschreibung
<code>dns_IP_ADDRESS</code>	IP-Adresse Ihres DNS-Namensservers
<code>mydomain.com</code>	DNS-Name Ihrer Active Directory-Domäne
<code>MYDOMAIN.COM</code>	DNS-Name Ihrer Active Directory-Domäne in Großbuchstaben
<code>myhost</code>	Hostname Ihres Ubuntu-Desktops
<code>MYDOMAIN</code>	DNS-Name der Arbeitsgruppe oder NT-Domäne, in der sich Ihr Samba-Server befindet, in Großbuchstaben

Platzhalterwert	Beschreibung
ads-hostname	Hostname Ihres AD-Servers
admin-user	Benutzername des Administrators der AD-Domäne

### Voraussetzungen

- Der Active Directory (AD)-Server kann auf dem Linux-System über das DNS aufgelöst werden.
- Das Network Time Protocol (NTP) ist auf dem Linux-System konfiguriert.

### Verfahren

- 1 Installieren Sie auf Ihrem Ubuntu 16.04- oder 18.04-Desktop die Pakete `samba` und `winbind`.

```
sudo apt install samba krb5-config krb5-user winbind libpam-winbind libnss-winbind
```

- 2 Wenn Sie dazu aufgefordert werden, konfigurieren Sie die Einstellungen für die Kerberos-Authentifizierung wie folgt.
  - a Geben Sie für einen **standardmäßigen Kerberos Version 5-Bereich** den DNS-Namen Ihrer Active Directory-Domäne in Großbuchstaben an.  
  
Wenn Ihr Active Directory-Domänenname z. B. `mydomain.com` lautet, geben Sie `MYDOMAIN.COM` ein.
  - b Geben Sie für **Kerberos-Server für Ihren Bereich** den Hostnamen Ihres AD-Servers ein (in den Beispielen für dieses Verfahren als `ads_hostname` angegeben).
  - c Geben Sie für **Verwaltungsserver für Ihren Kerberos-Bereich** erneut den Hostnamen Ihres AD-Servers ein.

- 3 Aktualisieren Sie die PAM-Konfiguration.

- a Öffnen Sie die Seite der PAM-Konfiguration.

```
pam-auth-update
```

- b Aktivieren Sie die Option **Home-Verzeichnis bei Anmeldung erstellen** und klicken Sie auf **OK**.

- 4 Bearbeiten Sie die Konfigurationsdatei `/etc/nsswitch.conf`, wie im folgenden Beispiel gezeigt.

```
passwd: compat winbind
group: compat winbind
shadow: compat
gshadow: files
```

- 5 Um sicherzustellen, dass die automatisch erstellte Datei `resolv.conf` auf Ihre AD-Domäne als Suchdomäne verweist, bearbeiten Sie die NetworkManager-Einstellungen für Ihre Systemverbindung.
  - a Öffnen Sie die Einstellungen von NetworkManager und navigieren Sie zu den **IPv4-Einstellungen** für Ihre Systemverbindung. Wählen Sie als Methode **Nur automatische (DHCP) Adressen** aus. Geben Sie im Textfeld **DNS-Server** die IP-Adresse Ihres DNS-Namenservers ein (in den Beispielen für dieses Verfahren als `dns_IP_ADDRESS` angegeben). Klicken Sie danach auf **Speichern**.
  - b Bearbeiten Sie die Konfigurationsdatei für Ihre Systemverbindung, die sich in `/etc/NetworkManager/system-connections` befindet. Verwenden Sie das folgende Beispiel.

```
[ipv4]
dns=dns_IP_ADDRESS
dns-search=mydomain.com
ignore-auto-dns=true
method=auto
```

**Hinweis** Beim Erstellen eines neuen virtuellen Instant-Clone-Desktops wird ein neuer virtueller Netzwerkadapter hinzugefügt. Wenn der neue Netzwerkadapter zum virtuellen Instant-Clone-Desktop hinzugefügt wird, gehen alle Einstellungen im Netzwerkadapter wie z. B. der DNS-Server in der Vorlage des virtuellen Desktops verloren. Um den Verlust der DNS-Server-Einstellung beim Hinzufügen des neuen Netzwerkadapters zu einem geklonten virtuellen Desktop zu vermeiden, müssen Sie für Ihr Linux-System einen DNS-Server angeben.

- c Geben Sie den DNS-Server an, indem Sie die Konfigurationsdatei `/etc/resolv.conf` wie im folgenden Beispiel bearbeiten.

```
nameserver dns_IP_ADDRESS

search mydomain.com
```

- d Starten Sie Ihr System neu und melden Sie sich an.

- 6 Bearbeiten Sie die Konfigurationsdatei `/etc/hosts`, wie im folgenden Beispiel.

```
127.0.0.1    localhost
127.0.1.1    myhost.mydomain.com myhost
```

- 7 Bearbeiten Sie die Konfigurationsdatei `/etc/samba/smb.conf`, wie im folgenden Beispiel.

```
[global]
security = ads
realm = MYDOMAIN.COM
workgroup = MYDOMAIN
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum group = yes
template homedir = /home/%D/%U
template shell = /bin/bash
```

```
client use spnego = yes
client ntlmv2 auth = yes
encrypt passwords = yes
winbind use default domain = yes
restrict anonymous = 2
kerberos method = secrets and keytab
winbind refresh tickets = true
```

## 8 Starten Sie den Dienst `smbd` neu.

```
sudo systemctl restart smbd.service
```

## 9 Bearbeiten Sie die Konfigurationsdatei `/etc/krb5.conf`, sodass sie über Inhalte ähnlich dem folgenden Beispiel verfügt.

```
[libdefaults]
    default_realm = MYDOMAIN.COM
    dns_lookup_realm = true
    dns_lookup_kdc = true

[realms]
    MYDOMAIN.COM = {
        kdc = ads-hostname
        admin_server = ads-hostname
    }

[domain_realm]
    .mydomain.com = MYDOMAIN.COMmydomain.com = MYDOMAIN.COM
```

## 10 Fügen Sie Ihren Ubuntu-Desktop zur Active Directory-Domäne hinzu.

### a Initiieren Sie ein Kerberos-Ticket.

```
sudo kinit admin-user
```

Geben Sie bei Aufforderung Ihr Administratorkennwort ein.

### b Stellen Sie sicher, dass das Ticket erfolgreich erstellt wurde.

```
sudo klist
```

Dieser Befehl liefert Informationen über das Ticket, einschließlich der gültigen Start- und Ablaufzeit.

### c Erstellen Sie eine Kerberos-Keytab-Datei.

```
sudo net ads keytab create -U admin-user
```

### d Treten Sie der AD-Domäne bei.

```
sudo net ads join -U admin-user
```

**11 Führen Sie einen Neustart durch und überprüfen Sie den Winbind-Dienst.**

- a Starten Sie den Winbind-Dienst neu.

```
sudo systemctl restart winbind.service
```

- b Führen Sie zum Prüfen des Winbind-Dienstes die folgenden Befehle aus und prüfen Sie, ob die Ausgabe stimmt.

- `wbinfo -u`
- `wbinfo -g`
- `getend passwd`
- `getend group`

**12 Starten Sie Ihr System neu und melden Sie sich an.****Nächste Schritte**[Konfigurieren von True SSO auf Ubuntu-Desktops](#)**Konfigurieren von True SSO auf Ubuntu-Desktops**

Um die True SSO-Funktion auf einem Ubuntu 16.04- oder 18.04-Desktop zu aktivieren, installieren Sie die Bibliotheken, von denen die True SSO-Funktion abhängig ist, das Stamm-CA-Zertifikat für die vertrauenswürdige Authentifizierung und Horizon Agent. Außerdem müssen Sie einige Konfigurationsdateien bearbeiten, um des Einrichten der Authentifizierung abzuschließen.

Verwenden Sie das folgende Verfahren, um True SSO in Ubuntu 16.04- und 18.04-Desktops zu aktivieren. Um True SSO auf diesen Desktops zu unterstützen, müssen Sie Horizon Agent 7.8 oder höher installieren.

**Voraussetzungen**

- Konfigurieren Sie True SSO für VMware Identity Manager und Horizon Connection Server.
- [Integrieren eines Ubuntu-Desktops in Active Directory für True SSO](#)
- Fordern Sie ein Stamm-CA-Zertifikat an und speichern Sie es auf Ihrem Desktop als `/tmp/certificate.cer`. Siehe [How to export Root Certification Authority Certificate](#).

**Verfahren**

- 1 Installieren Sie in Ihrem Ubuntu 16.04- oder 18.04-Desktop das Supportpaket `pkcs11`.

```
sudo apt install libpam-pkcs11
```

- 2 Installieren Sie das `libnss3-tools`-Paket.

```
sudo apt install libnss3-tools
```



**3** Installieren Sie ein Stamm-CA-Zertifikat.

- a Übertragen Sie das heruntergeladene Stamm-CA-Zertifikat in eine .pem-Datei.

```
openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

- b Verwenden Sie den Befehl `certutil`, um das Stamm-CA-Zertifikat in der Systemdatenbank `/etc/pki/nssdb` zu installieren.

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

- c Kopieren Sie das Stamm-CA-Zertifikat in das Verzeichnis `/etc/pam_pkcs11/cacerts`.

```
mkdir -p /etc/pam_pkcs11/cacerts

cp /tmp/certificate.pem /etc/pam_pkcs11/cacerts
```

- d Erstellen Sie einen Hash-Link für das Stamm-CA-Zertifikat. Führen Sie den folgenden Befehl im Verzeichnis `/etc/pam_pkcs11/cacerts` aus.

```
pkcs11_make_hash_link
```

**4** Installieren Sie das Paket Horizon Agent mit aktiviertem True SSO.

```
sudo ./install_viewagent.sh -T yes
```

**Hinweis** Damit Sie die True SSO-Funktion verwenden können, müssen Sie Horizon Agent 7.8 oder höher installieren.

- 5** Fügen Sie den folgenden Parameter zur benutzerdefinierten Horizon Agent-Konfigurationsdatei `/etc/vmware/viewagent-custom.conf` hinzu. Verwenden Sie das folgende Beispiel, in dem `NETBIOS_NAME_OF_DOMAIN` der NetBIOS-Name der Domäne Ihrer Organisation ist.

```
NetbiosDomain=NETBIOS_NAME_OF_DOMAIN
```

**6** Bearbeiten Sie die Konfigurationsdatei `/etc/pam_pkcs11/pam_pkcs11.conf`.

- a Erstellen Sie bei Bedarf die Konfigurationsdatei `/etc/pam_pkcs11/pam_pkcs11.conf`. Suchen Sie die Beispieldatei in `/usr/share/doc/libpam-pkcs11/examples`, kopieren Sie sie in das Verzeichnis `/etc/pam_pkcs11` und benennen Sie die Datei in `pam_pkcs11.conf` um. Fügen Sie gegebenenfalls Ihre Systeminformationen zum Inhalt der Datei hinzu.
- b Ändern Sie die Konfigurationsdatei `/etc/pam_pkcs11/pam_pkcs11.conf`, damit sie in etwa den im folgenden Beispiel gezeigten Inhalt enthält.

```
use_pkcs11_module = coolkey;
pkcs11_module coolkey {
    module = /usr/lib/vmware/viewagent/sso/libvmwpkcs11.so;
```

```
slot_num = 0;
ca_dir = /etc/pam_pkcs11/cacerts;
nss_dir = /etc/pki/nssdb;
}
```

7 Ändern Sie die auth-Parameter in der PAM-Konfigurationsdatei.

a Öffnen Sie die PAM-Konfigurationsdatei.

- Öffnen Sie für Ubuntu 16.04 /etc/pam.d/lightdm.
- Öffnen Sie für Ubuntu 18.04 /etc/pam.d/gdm-vmwcred.

b Bearbeiten Sie die PAM-Konfigurationsdatei, wie im folgenden Beispiel.

```
auth requisite pam_vmw_cred.so
auth sufficient pam_pkcs11.so try_first_pass
```

8 Starten Sie Ihr System neu und melden Sie sich an.

## Konfigurieren von True SSO für SLED/SLES-Desktops

Um True SSO für einen SLED/SLES-Desktop einzurichten, müssen Sie zuerst den Desktop in eine Active Directory-Domäne integrieren. Installieren Sie dann die erforderlichen Bibliotheken und das Root-CA-Zertifikat, bevor Sie Horizon Agent installieren.

### Integrieren eines SLED/SLES-Desktops in Active Directory für True SSO

Integrieren Sie den Desktop mithilfe von Samba und Winbind in eine Active Directory-Domäne, um True SSO auf einem Desktop mit SLED 12.x SP3 oder SLES 12.x SP3 zu unterstützen.

Verfahren Sie wie folgt, um einen SLED/SLES-Desktop in eine Active Directory-Domäne zu integrieren.

#### Voraussetzungen

- Der Active Directory (AD)-Server kann auf dem Linux-System über das DNS aufgelöst werden.
- Das Network Time Protocol (NTP) ist auf dem Linux-System konfiguriert.

#### Verfahren

1 Installieren Sie auf Ihrem SLED/SLES-Desktop die Pakete samba und winbind.

```
zypper install samba-winbind krb5-client samba-winbind-32bit
```

2 Öffnen Sie das YaST-Setuptools und navigieren Sie zu **Netzwerkdienste > Windows-Domänenmitgliedschaft**.

- 3 Konfigurieren Sie auf dem Bildschirm für die Windows-Domänenmitgliedschaft die folgenden Einstellungen.
  - a Geben Sie für **Domäne oder Arbeitsgruppe** den DNS-Namen der Arbeitsgruppe oder der NT-Domäne in Großbuchstaben an, in der sich Ihr Samba-Server befindet. Wenn der Arbeitsgruppenname z. B. **Mydomain** lautet, geben Sie **MYDOMAIN** ein.
  - b Aktivieren Sie **Zusätzlich SMB-Informationen für Linux-Authentifizierung verwenden**.
  - c Aktivieren Sie **Home-Verzeichnis bei Anmeldung erstellen**.
  - d Aktivieren Sie **Offline-Authentifizierung**.
  - e Aktivieren Sie **Single Sign-On für SSH**.
- 4 Klicken Sie auf **Ja**, wenn Sie gefragt werden, ob Sie der Domäne beitreten möchten.
- 5 Geben Sie den Administratornamen und das Kennwort für die angegebene Arbeitsgruppe ein und klicken Sie auf **OK**.

Eine Meldung bestätigt, dass Ihr SLED/SLES-Desktop der Domäne erfolgreich beigetreten ist. Klicken Sie auf **OK**.

- 6 Bearbeiten Sie die Konfigurationsdatei `/etc/samba/smb.conf`, damit sie folgenden Parameter enthält.

```
[global]
...
winbind use default domain = yes
```

- 7 Starten Sie Ihr System neu und melden Sie sich an.
- 8 Testen und überprüfen Sie Ihre SLED/SLES-Desktop-Integration.
 

Führen Sie die folgenden Testbefehle aus und prüfen Sie, ob die richtige Ausgabe zurückgegeben wird. Ersetzen Sie `mydomain` durch den Namen Ihrer Samba-Server-Arbeitsgruppe oder NT-Domäne.

  - `net ads testjoin`
  - `net ads info`
  - `wbinfo --krb5auth=mydomain\\open%open`
  - `ssh localhost -l mydomain\\open`

## Nächste Schritte

[Konfigurieren von True SSO auf SLED/SLES-Desktops](#)

## Konfigurieren von True SSO auf SLED/SLES-Desktops

Um die True SSO-Funktion auf einem SLED/SLES 12.x SP3-Desktop zu aktivieren, installieren Sie die Bibliotheken, von denen die True SSO-Funktion abhängt, das Stamm-CA-Zertifikat für die vertrauenswürdige Authentifizierung und Horizon Agent. Außerdem müssen Sie einige Konfigurationsdateien bearbeiten, um des Einrichten der Authentifizierung abzuschließen.

Wenden Sie das folgende Verfahren an, um True SSO in SLED 12.x SP3- und SLES 12.x SP3-Desktops zu aktivieren. Um True SSO auf diesen Desktops zu unterstützen, müssen Sie Horizon Agent 7.8 oder höher installieren.

### Voraussetzungen

- Konfigurieren Sie True SSO für VMware Identity Manager und Horizon Connection Server.
- [Integrieren eines SLED/SLES-Desktops in Active Directory für True SSO](#)
- Fordern Sie ein Stamm-CA-Zertifikat an und speichern Sie es auf Ihrem SLED/SLES 12.x SP3-Desktop als /tmp/certificate.cer. Siehe [How to export Root Certification Authority Certificate](#).

### Verfahren

- 1 Installieren Sie für einen SLES 12.x SP3-Desktop die erforderlichen Pakete, indem Sie den folgenden Befehl ausführen.

```
zypper install mozilla-nss-tools pam_krb5 krb5-client krb5-plugin-preauth-pkinit
```

- 2 Installieren Sie für einen SLED 12.x SP3-Desktop die erforderlichen Pakete, indem Sie die folgenden Schritte ausführen.

- a Laden Sie die SLES-ISO-Datei auf die lokale Festplatte Ihres SLED-Desktops herunter (z. B. /tmp/SLE-12-SP3-Server-DVD-x86\_64-GM-DVD1.iso).

Sie müssen die SLES-ISO-Datei als Paketquelle für Ihren SLED-Desktop hinzufügen, da das erforderliche Paket krb5-plugin-preauth-pkinit nur für SLES-Systeme verfügbar ist.

- b Stellen Sie die SLES-ISO-Datei auf Ihrem SLED-Desktop bereit und installieren Sie die erforderlichen Pakete.

```
sudo mkdir -p /mnt/sles
sudo mount -t iso9660 /tmp/SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso /mnt/sles
sudo zypper ar -f /mnt/sles sles
zypper install mozilla-nss-tools pam_krb5 krb5-client krb5-plugin-preauth-pkinit
```

- c Wenn die Installation abgeschlossen ist, heben Sie die Bereitstellung der SLES-ISO-Datei auf.

```
sudo umount /mnt/sles
```

### 3 Installieren Sie ein Stamm-CA-Zertifikat.

- a Übertragen Sie das heruntergeladene Stamm-CA-Zertifikat in eine .pem-Datei.

```
openssl x509 -inform der -in /tmp/certificate.cer -out /tmp/certificate.pem
```

- b Verwenden Sie den Befehl `certutil`, um das Stamm-CA-Zertifikat in der Systemdatenbank `/etc/pki/nssdb` zu installieren.

```
certutil -A -d /etc/pki/nssdb -n "root CA cert" -t "CT,C,C" -i /tmp/certificate.pem
```

- c Fügen Sie das Stamm-CA-Zertifikat zu `pam_pkcs11` hinzu.

```
cp /tmp/certificate.pem /etc/pki/ca-trust/source/anchors/ca_cert.pem
```

### 4 Bearbeiten Sie die Konfigurationsdatei `/etc/krb5.conf`, sodass sie über Inhalte ähnlich dem folgenden Beispiel verfügt.

```
[libdefaults]
    default_realm = MYDOMAIN.COM
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
    MYDOMAIN.COM = {
        kdc = ads-hostname
        admin_server = ads-hostname
        pkinit_anchors = DIR:/etc/pki/ca-trust/source/anchors
        pkinit_kdc_hostname = ads-hostname
        pkinit_eku_checking = kpServerAuth
    }

[domain_realm]
    .mydomain.com = MYDOMAIN.COMmydomain.com = MYDOMAIN.COM
```

Ersetzen Sie die Platzhalterwerte des Beispiels durch spezifische Informationen für Ihre Netzwerkconfiguration, wie in der folgenden Tabelle gezeigt.

Platzhalterwert	Beschreibung
mydomain.com	DNS-Name Ihrer Active Directory-Domäne
MYDOMAIN.COM	DNS-Name Ihrer Active Directory-Domäne (in Großbuchstaben)
ads-hostname	Hostname Ihres AD-Servers (Groß-/Kleinschreibung beachten)

- 5 Installieren Sie das Paket Horizon Agent mit aktiviertem True SSO.

```
sudo ./install_viewagent.sh -T yes
```

---

**Hinweis** Damit Sie die True SSO-Funktion verwenden können, müssen Sie Horizon Agent 7.8 oder höher installieren.

---

- 6 Fügen Sie den folgenden Parameter zur benutzerdefinierten Horizon Agent-Konfigurationsdatei `/etc/vmware/viewagent-custom.conf` hinzu. Verwenden Sie das folgende Beispiel, in dem `NETBIOS_NAME_OF_DOMAIN` der NetBIOS-Name der Domäne Ihrer Organisation ist.

```
NetbiosDomain=NETBIOS_NAME_OF_DOMAIN
```

- 7 Starten Sie Ihr System neu und melden Sie sich an.

# Einrichten von Grafiken für Linux-Desktops

# 4

Sie können die aktuell unterstützten Linux-Distributionen entsprechend konfigurieren, um die Vorteile der NVIDIA-Funktionen auf einem ESXi-Host oder einem Gastbetriebssystem nutzen zu können.

## Anforderungen für VM-Klone zur Einrichtung von 3D-Grafiken

Für die Einrichtung von 3D-Grafiken müssen die nachfolgend aufgeführten Anforderungen für VM-Klone erfüllt sein.

- Führen Sie für vGPU die Grafikeinrichtung in der Basis-VM durch. Klonen Sie die virtuellen Maschinen (VMs). Die Grafikeinstellungen gelten für alle geklonten VMs. Es sind keine weiteren Einstellungen erforderlich.
- Führen Sie für vDGA die Grafikeinrichtung in der Basis-VM durch. Klonen Sie die virtuellen Maschinen (VMs). Allerdings müssen Sie vor dem Einschalten der geklonten VMs das vorhandene NVIDIA-Passthrough-PCI-Gerät aus der geklonten VM entfernen und der geklonten VM das neue NVIDIA-Passthrough-PCI-Gerät hinzufügen. Das NVIDIA-Passthrough-PCI-Gerät kann nicht von den VMs gemeinsam genutzt werden. Jede virtuelle Maschine verwendet ein dediziertes NVIDIA-Passthrough-PCI-Gerät .

Dieses Kapitel enthält die folgenden Themen:

- [Konfigurieren unterstützter Linux-Distributionen für vGPU](#)
- [Konfigurieren von RHEL 6.x für vDGA](#)

## Konfigurieren unterstützter Linux-Distributionen für vGPU

Sie können eine unterstützte Linux-Distribution so einrichten, dass die NVIDIA vGPU-Funktionalität (gemeinsam genutzte GPU-Hardwarebeschleunigung) auf dem ESXi-Host zur Verfügung steht.

Sie müssen den NVIDIA Linux VM-Anzeigetreiber verwenden, der zum GPU-Treiber (.vib) des ESXi-Hosts passt. Informationen zu Treiberpaketen finden Sie auf der NVIDIA-Website.

**Hinweis** Informationen zu den NVIDIA-Grafikkarten und Linux-Distributionen, die vGPU unterstützen, finden Sie unter <https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html>.

**Vorsicht** Bevor Sie starten, stellen Sie sicher, dass Horizon Agent nicht auf der virtuellen Linux-Maschine installiert ist. Wenn Sie Horizon Agent vor der Konfiguration der Maschine zur Verwendung von NVIDIA vGPU installieren, werden die erforderlichen Parameter in der Datei `xorg.conf` überschrieben und NVIDIA vGPU funktioniert nicht. Sie müssen Horizon Agent nach dem Abschluss der NVIDIA vGPU-Konfiguration installieren.

## Installieren des VIB für die NVIDIA GRID vGPU-Grafikkarte auf dem ESXi-Host

Sie müssen das VIB für Ihre NVIDIA GRID-Grafikkarte herunterladen und auf dem ESXi 6.0 U1-Host oder höher installieren.

NVIDIA bietet ein vGPU-Softwarepaket mit einem vGPU Manager, den Sie in diesem Vorgang auf dem ESXi-Host installieren, und einen Linux-Anzeigetreiber, den Sie auf der virtuellen Linux-Maschine in einem späteren Vorgang installieren.

### Voraussetzungen

- Stellen Sie sicher, dass vSphere 6.0 U1 oder höher in Ihrer Umgebung installiert ist.
- Stellen Sie sicher, dass die erforderliche vGPU-Grafikkarte auf dem ESXi-Host installiert ist.

**Hinweis** Informationen zu den NVIDIA-Grafikkarten und Linux-Distributionen, die vGPU unterstützen, finden Sie unter <https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html>.

### Verfahren

- 1 Laden Sie das VIB für Ihre NVIDIA GRID vGPU-Grafikkarte von der Site [NVIDIA Treiber Downloads](#) herunter.

Wählen Sie aus den Dropdown-Menüs die geeignete VIB-Version aus.

Option	Beschreibung
Produkttyp	GRID
Produktserie	Wählen Sie <b>NVIDIA GRID vGPU</b> aus.
Produkt	Wählen Sie die Version aus, die auf dem ESXi-Host installiert ist (z. B. <b>GRID K2</b> ).
Betriebssystem	Wählen Sie die VMware vSphere ESXi-Version aus.

- 2 Dekomprimieren Sie die ZIP-Datei des vGPU-Softwarepakets.



- 3 Laden Sie den vGPU Manager-Ordner auf den ESXi-Host hoch.

---

**Hinweis** Der Linux-Anzeigetreiber wird später auf der virtuellen Linux-Maschine installiert.

---

- 4 Schalten Sie alle virtuellen Maschinen auf dem ESXi-Host aus oder halten Sie diese an.
- 5 Stellen Sie mithilfe von SSH eine Verbindung zum ESXi-Host her.
- 6 Beenden Sie den xorg-Dienst.

```
# /etc/init.d/xorg stop
```

- 7 Installieren Sie das NVIDIA VIB.

Beispiel:

```
# esxcli system maintenanceMode set --enable true
# esxcli software vib install -v /path-to-vib/NVIDIA-VIB-name.vib
# esxcli system maintenanceMode set --enable false
```

- 8 Starten Sie den ESXi-Host neu oder aktualisieren Sie diesen.
  - ◆ Bei einem installierten ESXi-Host starten Sie den Host neu.
  - ◆ Bei einem zustandsfreien ESXi-Host aktualisieren Sie den Host mit den folgenden Schritten. (Diese Schritte können auch auf einem installierten Host durchgeführt werden.)

```
Update vmkdevmgr:
# kill -HUP $(cat /var/run/vmware/vmkdevmgr.pid)

Wait for the update to complete:
# localcli --plugin-dir /usr/lib/vmware/esxcli/int deviceInternal bind

This is a new requirement with the NVIDIA 352.* host driver:
# /etc/init.d/nvidia-vgpu start

Restart xorg, which is used for GPU assignment:
# /etc/init.d/xorg start
```

- 9 Stellen Sie sicher, dass der xorg-Dienst nach dem Neustart des Hosts ausgeführt wird.

## Konfigurieren eines gemeinsam genutzten PCI-Geräts für vGPU auf der virtuellen Linux-Maschine

Zur Verwendung der NVIDIA vGPU müssen Sie ein gemeinsam genutztes PCI-Gerät für die virtuelle Linux-Maschine konfigurieren.

### Voraussetzungen

- Stellen Sie sicher, dass die virtuelle Linux-Maschine für eine Verwendung als Desktop vorbereitet ist. Siehe [Erstellen einer virtuellen Maschine und Installieren von Linux](#) und [Vorbereiten einer Linux-Maschine für die Remote-Desktop-Bereitstellung](#).
- Stellen Sie sicher, dass Horizon Agent nicht auf der virtuellen Linux-Maschine installiert ist.

- Stellen Sie sicher, dass das NVIDIA VIB auf dem ESXi-Host installiert ist. Siehe [Installieren des VIB für die NVIDIA GRID vGPU-Grafikkarte auf dem ESXi-Host](#).
- Machen Sie sich mit den virtuellen GPU-Typen vertraut, die mit NVIDIA vGPU verfügbar sind und die mit der Einstellung **GPU-Profil** ausgewählt werden. Die virtuellen GPU-Typen bieten unterschiedliche Funktionen für die physischen GPUs, die auf dem ESXi-Host installiert sind.

---

**Hinweis** Informationen zu den NVIDIA-Grafikkarten und Linux-Distributionen, die vGPU unterstützen, finden Sie unter <https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html>.

---

#### Verfahren

- 1 Schalten Sie die virtuelle Maschine aus.
- 2 Im vSphere Web Client wählen Sie die virtuelle Maschine aus und klicken auf der Registerkarte **VM-Hardware** auf **Einstellungen bearbeiten**.
- 3 Im Menü **Neues Gerät** wählen Sie **Gemeinsam genutztes PCI-Gerät** aus.
- 4 Klicken Sie auf **Hinzufügen** und wählen Sie **NVIDIA GRID vGPU** aus dem Dropdown-Menü aus.
- 5 Für die Einstellung **GPU-Profil** wählen Sie einen virtuellen GPU-Typ aus dem Dropdown-Menü aus.
- 6 Klicken Sie auf **Gesamten Arbeitsspeicher reservieren** und dann auf **OK**.

Um die GPU zur Unterstützung von NVIDIA GRID vGPU zu aktivieren, müssen Sie dafür den gesamten Arbeitsspeicher der virtuellen Maschine reservieren.

- 7 Schalten Sie die virtuelle Maschine ein.

## Installieren des NVIDIA GRID vGPU-Anzeigetreibers

Um den NVIDIA GRID vGPU-Anzeigetreiber zu installieren, müssen Sie den Standard-NVIDIA-Treiber deaktivieren, die NVIDIA-Anzeigetreiber herunterladen und das PCI-Gerät auf der virtuellen Maschine konfigurieren.

#### Voraussetzungen

- Stellen Sie sicher, dass Sie das vGPU-Softwarepaket von der NVIDIA-Download-Site heruntergeladen, das Paket dekomprimiert und den Linux-Anzeigetreiber (eine Paketkomponente) bereitgehalten haben. Siehe [Installieren des VIB für die NVIDIA GRID vGPU-Grafikkarte auf dem ESXi-Host](#).

Stellen Sie sicher, dass der virtuellen Maschine ein gemeinsam genutztes PCI-Gerät hinzugefügt wurde. Siehe [Konfigurieren eines gemeinsam genutzten PCI-Geräts für vGPU auf der virtuellen Linux-Maschine](#).

#### Verfahren

- 1 Kopieren Sie den NVIDIA Linux-Anzeigetreiber in die virtuelle Maschine.

- 2 Öffnen Sie einen Remoteterminal für die virtuelle Maschine oder wechseln Sie durch Drücken von Strg-Alt-F2 zu einer Textkonsole, melden Sie sich als Root an und führen Sie dann den `init 3`-Befehl zur Deaktivierung von X Windows aus.

- 3 Installieren Sie weitere für den NVIDIA-Treiber erforderliche Komponenten.

```
sudo yum install gcc-c++
sudo yum install kernel-devel-$(uname -r)
sudo yum install kernel-headers-$(uname -r)
```

- 4 Fügen Sie dem NVIDIA GRID vGPU-Treiberpaket ein ausführbares Attribut hinzu.

```
chmod +x NVIDIA-Linux-x86_64-Version-grid.run
```

- 5 Starten Sie das NVIDIA GRID vGPU-Installationsprogramm.

```
sudo ./NVIDIA-Linux-x86_64-Version-grid.run
```

- 6 Akzeptieren Sie die NVIDIA-Softwarelizenzvereinbarung und wählen Sie **Ja** aus, um die X-Konfigurationseinstellungen automatisch zu aktualisieren.

### Nächste Schritte

Installieren Sie Horizon Agent auf der virtuellen Linux-Maschine. Siehe [Installieren von Horizon Agent auf einer virtuellen Linux-Maschine](#).

Erstellen Sie einen Desktop-Pool mit den konfigurierten virtuellen Linux-Maschinen. Siehe [Erstellen eines manuellen Desktop-Pools für Linux](#).

## Überprüfen, ob der NVIDIA-Anzeigetreiber installiert ist

Sie können prüfen, ob der NVIDIA-Anzeigetreiber auf einer virtuellen Linux-Maschine installiert wurde, indem Sie die NVIDIA-Treiberausgabe in einer Horizon-Desktop-Sitzung darstellen.

### Voraussetzungen

- Überprüfen Sie, ob der NVIDIA-Anzeigetreiber installiert ist.
- Stellen Sie sicher, dass Horizon Agent auf der virtuellen Linux-Maschine installiert ist. Siehe [Installieren von Horizon Agent auf einer virtuellen Linux-Maschine](#).
- Stellen Sie sicher, dass die virtuelle Linux-Maschine in einem Desktop-Pool bereitgestellt wurde. Siehe [Erstellen eines manuellen Desktop-Pools für Linux](#).

### Verfahren

- 1 Starten Sie die virtuelle Linux-Maschine neu.

Das Startskript für Horizon Agent initialisiert den X-Server und stellt die Topologie dar.

Die Anzeige der virtuellen Maschine erscheint nicht mehr in der vSphere-Konsole.

- 2 Von Horizon Client aus stellen Sie eine Verbindung zum Linux-Desktop her.

- 3 In der Linux-Desktop-Sitzung stellen Sie sicher, dass der NVIDIA-Anzeigetreiber installiert ist.

Öffnen Sie ein Terminalfenster und führen Sie den Befehl `glxinfo | grep NVIDIA` aus.

Die Ausgabe des NVIDIA-Treibers wird dargestellt. Beispiel:

```
[root]# glxinfo | grep NVIDIA
server glx vendor string: NVIDIA Corporation
client glx vendor string: NVIDIA Corporation
OpenGL vendor string: NVIDIA Corporation
OpenGL version string: 4.5.0 NVIDIA 346.47
OpenGL shading language version string: 4.50 NVIDIA
```

Der Benutzer kann auf die NVIDIA-Grafikfunktionen auf dem Remote-Desktop zugreifen.

Nachdem Sie sichergestellt haben, dass der NVIDIA-Anzeigetreiber installiert ist, führen Sie die folgenden Schritte durch, um eine korrekte Installation zu gewährleisten.

- Wenn Sie ein Upgrade für den Linux-Kernel durchführen, kommuniziert Horizon Agent eventuell nicht mit dem Horizon-Verbindungsserver. Um dieses Problem zu beheben, installieren Sie den NVIDIA-Treiber erneut.
- Richten Sie die NVIDIA GRID-Lizenzierung in der Linux-VM ein. Weitere Informationen finden Sie in der NVIDIA-Dokumentation. Wenn die Lizenzierung nicht festgelegt ist, funktioniert der Linux-Desktop nicht korrekt. Beispielsweise ist dann keine automatische Anpassung möglich.

## Konfigurieren von RHEL 6.x für vDGA

Sie können durch entsprechende Einrichtung eines RHEL 6.x-Gastbetriebssystems die vDGA-Funktionalität auf dem ESXi-Host einem Horizon 7 für Linux-Desktop zur Verfügung stellen.

---

**Vorsicht** Bevor Sie starten, stellen Sie sicher, dass Horizon Agent nicht auf der virtuellen Linux-Maschine installiert ist. Wenn Sie Horizon Agent vor der Konfiguration der Maschine zur Verwendung von vDGA installieren, werden die erforderlichen Parameter in der Datei `xorg.conf` überschrieben und vDGA funktioniert nicht. Sie müssen Horizon Agent nach dem Abschluss der vDGA-Konfiguration installieren.

---

## Aktivieren von DirectPath I/O für NVIDIA GRID auf einem Host

Bevor Sie eine virtuelle Linux-Maschine für die Verwendung von vDGA konfigurieren können, müssen Sie die NVIDIA GRID GPU-PCI-Geräte für den DirectPath I/O-Passthrough auf dem ESXi-Host verfügbar machen.

### Voraussetzungen

- Stellen Sie sicher, dass vSphere 6.0 oder höher in Ihrer Umgebung installiert ist.
- Vergewissern Sie sich, dass die NVIDIA GRID K1- oder K2-Grafikkarte auf dem ESXi-Host installiert ist.

### Verfahren

- 1 Im vSphere Web Client suchen Sie nach dem ESXi-Host.

- 2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 3 Klicken Sie im Abschnitt „Hardware“ auf **PCI-Geräte**.
- 4 Um den DirectPath I/O-Passthrough für die NVIDIA GRID GPUs zu aktivieren, klicken Sie auf **Bearbeiten**.

Symbol	Beschreibung
Grünes Symbol	Das PCI-Gerät ist aktiv und kann aktiviert werden.
Oranges Symbol	Der Status des Geräts hat sich geändert. Sie müssen nun den Host neu starten, bevor Sie das Gerät verwenden können.

- 5 Wählen Sie die NVIDIA GRID GPUs aus und klicken Sie auf **OK**.  
Die PCI-Geräte werden der Tabelle der für VMs verfügbaren DirectPath I/O-PCI-Geräte hinzugefügt.
- 6 Um die PCI-Geräte den virtuellen Linux-Maschinen zur Verfügung zu stellen, starten Sie den Host neu.

## Hinzufügen eines vDGA-Passthrough-Geräts zu einer virtuellen RHEL 6.x-Maschine

Um eine virtuelle RHEL 6.x-Maschine für die Verwendung von vDGA zu konfigurieren, müssen Sie der virtuellen Maschine das PCI-Gerät hinzufügen. Damit kann das physische Gerät auf dem ESXi-Host für eine Verwendung auf der virtuellen Maschine weitergeleitet werden.

### Voraussetzungen

- Stellen Sie sicher, dass die virtuelle Linux-Maschine für eine Verwendung als Desktop vorbereitet ist. Siehe [Erstellen einer virtuellen Maschine und Installieren von Linux](#) und [Vorbereiten einer Linux-Maschine für die Remote-Desktop-Bereitstellung](#).
- Stellen Sie sicher, dass Horizon Agent nicht auf der virtuellen Linux-Maschine installiert ist.
- Vergewissern Sie sich, dass das NVIDIA GRID GPU-PCI-Gerät für den DirectPath I/O-Passthrough auf dem Host verfügbar ist. Siehe [Aktivieren von DirectPath I/O für NVIDIA GRID auf einem Host](#).

### Verfahren

- 1 Melden Sie sich beim RHEL 6.x-Gastbetriebssystem als lokaler Benutzer mit konfigurierten Sudo-Rechten an.
- 2 Im vSphere Web Client wählen Sie die virtuelle Maschine aus und klicken auf der Registerkarte **VM-Hardware** auf **Einstellungen bearbeiten**.
- 3 Im Menü **Neues Gerät** wählen Sie **PCI-Gerät** aus.
- 4 Klicken Sie auf **Hinzufügen** und wählen Sie das PCI-Gerät aus dem Dropdown-Menü aus.
- 5 Klicken Sie auf **Gesamten Arbeitsspeicher reservieren** und dann auf **OK**.

Um die GPU zur Unterstützung von vDGA zu aktivieren, müssen Sie dafür den gesamten Arbeitsspeicher der virtuellen Maschine reservieren.

- 6 Schalten Sie die virtuelle Maschine ein und öffnen Sie die vSphere-Konsole, um eine Verbindung zur Maschine herzustellen.
- 7 Stellen Sie sicher, dass das NVIDIA GRID-Gerät an die virtuelle Maschine weitergeleitet wird.

Öffnen Sie ein Terminalfenster und führen Sie den folgenden Befehl aus:

```
lspci | grep NVIDIA
```

Der VGA-kompatible XX:00.0-Controller wird dargestellt. Beispiel:

```
NVIDIA Corporation GK104GL [GRID K2]
```

## Installieren des NVIDIA-Anzeigetreibers für vDGA

Um den NVIDIA-Anzeigetreiber für vDGA zu installieren, müssen Sie den Standard-NVIDIA-Treiber deaktivieren, die NVIDIA-Anzeigetreiber herunterladen und das PCI-Gerät auf der virtuellen Maschine konfigurieren.

### Voraussetzungen

- Stellen Sie sicher, dass der virtuellen RHEL 6.x-Maschine das PCI-Gerät hinzugefügt wurde. Siehe [Hinzufügen eines vDGA-Passthrough-Geräts zu einer virtuellen RHEL 6.x-Maschine](#).

### Verfahren

- 1 Deaktivieren Sie den Standard-NVIDIA Nouveau-Treiber und sperren Sie diesen für eine weitere Verwendung.

- a Bearbeiten Sie die Datei `grub.conf`.

Bei RHEL 6.x ist das die Datei `/boot/grub/grub.conf`.

RHEL-Version	Befehl
6.x	<code>sudo vi /boot/grub/grub.conf</code>

- b Fügen Sie am Ende der Kernel-Optionen die Zeile `rdblacklist=nouveau` hinzu.
- c Bearbeiten Sie die Datei `blacklist.conf`.

```
sudo vi /etc/modprobe.d/blacklist.conf
```

- d Fügen Sie der Datei `blacklist.conf` die folgende Zeile an einer beliebigen Stelle hinzu.

```
blacklist nouveau
```

- 2 Starten Sie die virtuelle Maschine neu.

Die Art der Anzeige hat sich verändert.

- 3 (Optional) Stellen Sie sicher, dass der Nouveau-Treiber deaktiviert ist.

```
/sbin/lsmmod | grep nouveau
```

Dies ist dann der Fall, wenn die grep-Suche keine Ergebnisse ergibt.

- 4 Laden Sie den NVIDIA-Treiber von der Site [NVIDIA Treiber Downloads](#) herunter.

Wählen Sie aus den NVIDIA-Dropdown-Menüs die geeignete Treiberversion aus:

Option	Beschreibung
Produkttyp	GRID
Produktserie	GRID Series
Produkt	Wählen Sie die Version aus, die auf dem ESXi-Host installiert ist (z. B. <b>GRID K2</b> ).
Betriebssystem	Linux 64-Bit oder Linux 32-Bit

- 5 Um eine Verbindung mit der virtuellen Maschine herzustellen, öffnen Sie ein Remoteterminal oder verwenden Sie eine Textkonsole, indem Sie Strg-Alt-F2 drücken, melden Sie sich als Root-Benutzer an und führen Sie den Befehl `init 3` aus, um X Windows zu deaktivieren.
- 6 Installieren Sie weitere für den NVIDIA-Treiber erforderliche Komponenten.

```
sudo yum install gcc-c++
sudo yum install kernel-devel-$(uname -r)
sudo yum install kernel-headers-$(uname -r)
```

- 7 Fügen Sie dem NVIDIA-Treiberpaket für vDGA ein ausführbares Attribut hinzu.

```
chmod +x NVIDIA-Linux-x86_64-Version.run
```

- 8 Führen Sie das NVIDIA-Installationsprogramm aus.

```
sudo ./NVIDIA-Linux-x86_64-Version.run
```

- 9 Akzeptieren Sie die NVIDIA-Softwarelizenzvereinbarung und wählen Sie **Ja** aus, um die X-Konfigurationseinstellungen zu aktualisieren.

### Nächste Schritte

Installieren Sie Horizon Agent auf der virtuellen Linux-Maschine. Siehe [Installieren von Horizon Agent auf einer virtuellen Linux-Maschine](#).

Erstellen Sie einen Desktop-Pool mit den konfigurierten virtuellen Linux-Maschinen. Siehe [Erstellen eines manuellen Desktop-Pools für Linux](#).

## Überprüfen, ob der NVIDIA-Anzeigetreiber installiert ist

Sie können prüfen, ob der NVIDIA-Anzeigetreiber auf einer virtuellen Linux-Maschine installiert wurde, indem Sie die NVIDIA-Treiberausgabe in einer Horizon-Desktop-Sitzung darstellen.

## Voraussetzungen

- Überprüfen Sie, ob der NVIDIA-Anzeigetreiber installiert ist.
- Stellen Sie sicher, dass Horizon Agent auf der virtuellen Linux-Maschine installiert ist. Siehe [Installieren von Horizon Agent auf einer virtuellen Linux-Maschine](#).
- Stellen Sie sicher, dass die virtuelle Linux-Maschine in einem Desktop-Pool bereitgestellt wurde. Siehe [Erstellen eines manuellen Desktop-Pools für Linux](#).

## Verfahren

- 1 Starten Sie die virtuelle Linux-Maschine neu.

Das Startskript für Horizon Agent initialisiert den X-Server und stellt die Topologie dar.

Die Anzeige der virtuellen Maschine erscheint nicht mehr in der vSphere-Konsole.

- 2 Von Horizon Client aus stellen Sie eine Verbindung zum Linux-Desktop her.
- 3 In der Linux-Desktop-Sitzung stellen Sie sicher, dass der NVIDIA-Anzeigetreiber installiert ist.

Öffnen Sie ein Terminalfenster und führen Sie den Befehl `glxinfo | grep NVIDIA` aus.

Die Ausgabe des NVIDIA-Treibers wird dargestellt. Beispiel:

```
[root]# glxinfo | grep NVIDIA
server glx vendor string: NVIDIA Corporation
client glx vendor string: NVIDIA Corporation
OpenGL vendor string: NVIDIA Corporation
OpenGL version string: 4.5.0 NVIDIA 346.47
OpenGL shading language version string: 4.50 NVIDIA
```

Der Benutzer kann auf die NVIDIA-Grafikfunktionen auf dem Remote-Desktop zugreifen.

Nachdem Sie sichergestellt haben, dass der NVIDIA-Anzeigetreiber installiert ist, führen Sie die folgenden Schritte durch, um eine korrekte Installation zu gewährleisten.

- Wenn Sie ein Upgrade für den Linux-Kernel durchführen, kommuniziert Horizon Agent eventuell nicht mit dem Horizon-Verbindungsserver. Um dieses Problem zu beheben, installieren Sie den NVIDIA-Treiber erneut.
- Richten Sie die NVIDIA GRID-Lizenzierung in der Linux-VM ein. Weitere Informationen finden Sie in der NVIDIA-Dokumentation. Wenn die Lizenzierung nicht festgelegt ist, funktioniert der Linux-Desktop nicht korrekt. Beispielsweise ist dann keine automatische Anpassung möglich.



# Installieren von Horizon Agent

# 5

Sie müssen Horizon Agent auf den Linux-Desktops installieren, damit Horizon Connection Server mit den Desktops kommunizieren und sie verwalten kann.

Dieses Kapitel enthält die folgenden Themen:

- [Installieren von Horizon Agent auf einer virtuellen Linux-Maschine](#)
- [Konfigurieren des Zertifikats für den Linux Agent](#)
- [Durchführen eines Upgrades von Horizon Agent auf einer virtuellen Linux-Maschine](#)
- [Deinstallieren von Horizon 7 für Linux-Maschinen](#)

## Installieren von Horizon Agent auf einer virtuellen Linux-Maschine

Bevor Sie eine virtuelle Linux-Maschine als Remote-Desktop bereitstellen können, müssen Sie auf dieser Horizon Agent installieren.

Ab Horizon 7.0.1 verwendet Horizon Agent for Linux durch vCenter verwaltete virtuelle Maschinen. Die verwalteten virtuellen Maschinen bieten die folgenden Erweiterungen.

- vCenter ist für die Linux-Desktop-Bereitstellung erforderlich.
- Für die Horizon Agent-Installation auf Linux ist keine Registrierung erforderlich.
- Für eine Bereitstellung mit vielen Linux-Desktops können Sie Horizon Agent auf der virtuellen Basismaschine installieren.

---

**Vorsicht** Wenn Sie NVIDIA GRIDvGPU oder vDGA verwenden möchten, müssen Sie diese 3D-Funktionen auf der virtuellen Linux-Maschine vor der Installation von Horizon Agent konfigurieren. Wenn Sie Horizon Agent zuerst installieren, werden erforderliche Parameter in der Datei `xorg.conf` überschrieben und die 3D-Grafikfunktionen können nicht verwendet werden.

Siehe [Konfigurieren unterstützter Linux-Distributionen für vGPU](#) oder [Konfigurieren von RHEL 6.x für vDGA](#). Installieren Sie Horizon Agent erst nach dem Abschluss der 3D-Grafikkonfiguration.

Für die 2D-Grafikkonfiguration können Sie Horizon Agent nach dem Abschluss der unter [Vorbereiten einer Linux-Maschine für die Remote-Desktop-Bereitstellung](#) aufgeführten Schritte installieren.

---

## Voraussetzungen

- Stellen Sie sicher, dass das Linux-Gastbetriebssystem für die Desktop-Verwendung vorbereitet ist. Siehe [Vorbereiten einer Linux-Maschine für die Remote-Desktop-Bereitstellung](#).
- Machen Sie sich mit dem Installationsskript von Horizon Agent für Linux vertraut. Siehe [Befehlszeilenoptionen für install\\_viewagent.sh](#).

## Verfahren

- 1 Laden Sie die Installationsdatei für Horizon Agent für Linux von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunter.

Wählen Sie unter „Desktop & End-User Computing“ „Download-Komponenten für VMware Horizon anzeigen“. Wählen Sie unter Horizon 7 für Linux die Downloads-Seite für VMware Horizon 7 für 64-Bit-Linux-Systeme.

Der Dateiname des Installationsprogramms lautet `VMware-horizonagent-linux-x86_64-y.y.y-xxxxxxx.tar.gz` für 64-Bit-Linux. Hierbei ist `y.y.y` die Versionsnummer und `xxxxxxx` die Buildnummer.

- 2 Entpacken Sie das TAR-Archiv für Ihre Linux-Distribution auf dem Gastbetriebssystem.

Beispiel:

```
tar -xzf VMware-horizonagent-linux-x86_64-y.y.y-xxxxxxx.tar.gz
```

- 3 Wechseln Sie zum Ordner des TAR-Archivs.
- 4 Führen Sie das Skript `install_viewagent.sh` als Superuser aus.

Unter [Befehlszeilenoptionen für install\\_viewagent.sh](#) finden Sie eine Liste der Befehlszeilenoptionen.

Beispiel:

```
sudo ./install_viewagent.sh
```

- 5 Geben Sie **Yes** ein, um die EULA-Vereinbarung anzunehmen, wenn Sie `install_viewagent.sh` ohne Angabe der Option `-A` ausführen.

Das Installationsprogramm wird ohne Annahme der EULA-Vereinbarung nicht ausgeführt.

- 6 Führen Sie einen Linux-Neustart durch, damit die Änderungen wirksam werden.

Nach der Installation wird der Dienst `viewagent` gestartet. Stellen Sie sicher, dass der Dienst mithilfe von `sudo service viewagent status` gestartet wird.

## Nächste Schritte

Stellen Sie die virtuelle Maschine in einem Desktop-Pool bereit. Siehe [Erstellen eines manuellen Desktop-Pools für Linux](#).

## Befehlszeilenoptionen für install\_viewagent.sh

Das `install_viewagent.sh`-Skript installiert Horizon Agent auf einem Linux-Gastbetriebssystem.

Verwenden Sie für das `install_viewagent.sh`-Skript die folgende Syntax in einem Befehlsfenster der Gnome-Desktop-Umgebung.

```
install_viewagent.sh command_option argument [command_option argument] . . .
```

Das `install_viewagent.sh`-Skript enthält obligatorische und optionale Parameter.

**Tabelle 5-1. `install_viewagent.sh` Optionaler, aber erforderlicher Parameter**

Optionaler Parameter (erforderliche Informationen)	Beschreibung
-A yes no	Akzeptieren Sie die Nutzungsbedingungen (End User License Agreement, EULA) und die Verwendung der Federal Information Processing Standards (FIPS) oder lehnen Sie diese ab. Um die Installation fortzusetzen zu können, müssen Sie <b>yes</b> angeben.

**Tabelle 5-2. Optionale Parameter für `install_viewagent.sh`**

Optionale Parameter	Beschreibung
-a yes no	Installieren Sie die Unterstützung der Audio-Eingangsumleitung oder umgehen Sie diese. Die Standardeinstellung ist „yes“.
-f yes no	Installieren oder umgehen Sie die Unterstützung der kryptografischen Module, die auf FIPS 140-2-Kompatibilität (Federal Information Processing Standards) ausgelegt sind. Die Standardeinstellung ist <b>no</b> . Weitere Informationen finden Sie in der Beschreibung des FIPS 140-2-Modus unter <a href="#">Funktionen von Horizon Linux-Desktops</a> .
-j	JMS SSL-Schlüsselspeicherkennwort. Standardmäßig wird vom Installationsprogramm eine zufällige Zeichenfolge generiert.
-m yes no	Installieren oder umgehen Sie die Unterstützung für die Smartcard-Umleitung. Die Standardeinstellung ist <b>no</b> .
-r yes no	Automatischer Neustart des Systems nach der Installation. Die Standardeinstellung ist <b>no</b> .
-s	Subject DN des selbst signierten Zertifikats. Standardmäßig wird vom Installationsprogramm „Blast“ verwendet.
-C yes no	Installieren oder umgehen Sie die Unterstützung für die Zwischenablagenumleitung. Die Standardeinstellung ist <b>yes</b> .
-F yes no	Installieren oder umgehen Sie die CDR-Unterstützung. Die Standardeinstellung ist <b>yes</b> .
-M yes no	Aktualisieren Sie Linux Agent auf verwalteten oder nicht verwalteten Agenten. Die Standardeinstellung ist <b>yes</b> .
-S yes no	Installieren oder umgehen Sie die Single Sign-On-Unterstützung (SSO). Die Standardeinstellung ist <b>yes</b> .
-T yes no	Installieren oder umgehen Sie die True Single Sign-On-Unterstützung (True SSO). Die Standardeinstellung ist <b>no</b> .
-U yes no	Installieren oder umgehen Sie die USB-Unterstützung. Die Standardeinstellung ist <b>no</b> .

**Tabelle 5-3. Beispiele für install\_viewagent.sh -Parameter**

Bedingung	Beispiele
Neue Installation	<pre>sudo ./install_viewagent.sh -A yes</pre> <p>Für eine neue Installation ist immer die Erstellung eines neuen Desktop-Pools erforderlich.</p>
Upgrade einer nicht verwalteten virtuellen Maschine unter Beibehaltung der Charakteristika einer nicht verwalteten virtuellen Maschine	<pre>sudo ./install_viewagent.sh -A yes-M no</pre> <p>Für diesen Upgrade-Typ ist die Erstellung eines neuen Desktop-Pools nicht erforderlich. Sie können den vorhandenen Desktop-Pool erneut verwenden.</p> <p><b>Hinweis</b> Um die bestmögliche Leistung zu gewährleisten, sollten Sie keine nicht verwaltete virtuelle Maschine verwenden.</p>
Upgrade der Bereitstellung einer nicht verwalteten virtuellen Maschine und Umwandlung in Charakteristika einer verwalteten virtuellen Maschine. Für dieses Upgrade ist die Erstellung eines neuen Desktop-Pools auf dem Broker erforderlich.	<pre>sudo ./install_viewagent.sh -A yes</pre> <p>Für diesen Upgrade-Typ ist die Erstellung eines neuen Desktop-Pools erforderlich. Sie müssen den vorhandenen Desktop-Pool löschen.</p>

## Konfigurieren des Zertifikats für den Linux Agent

Wenn Sie den Linux Agent installieren, erstellt das Installationsprogramm ein selbstsigniertes Zertifikat für VMwareBlastServer.

- Wenn das Blast Security Gateway auf dem Broker deaktiviert ist, übergibt VMwareBlastServer dieses Zertifikat an den Browser, der mithilfe von HTML Access eine Verbindung mit dem Linux-Desktop herstellt.
- Wenn das Blast Security Gateway auf dem Broker aktiviert ist, wird das Zertifikat von Blast Security Gateway an den Browser übergeben.

Um die Einhaltung von Branchen- oder Sicherheitsbestimmungen sicherzustellen, können Sie das selbstsignierte Zertifikat durch ein von einer Zertifizierungsstelle (CA, Certificate Authority) signiertes Zertifikat ersetzen .

## Verfahren

- 1 Installieren Sie den privaten Schlüssel und das Zertifikat für VMwareBlastServer.
  - a Benennen Sie den privaten Schlüssel in `ru1.key` und das Zertifikat in `ru1.crt` um.
  - b Führen Sie `sudo chmod 550 /etc/vmware/ssl` aus.
  - c Kopieren Sie `ru1.crt` und `ru1.key` nach `/etc/vmware/ssl`.
  - d Führen Sie `chmod 440 /etc/vmware/ssl` aus.
- 2 Installieren Sie die Stamm- und Zwischenzertifizierungsstelle im Zertifizierungsstellen-Store des Linux-Betriebssystems.

---

**Hinweis** Erläuterungen zur Änderung der Linux-Systemeinstellungen finden Sie in der Dokumentation Ihrer Linux-Distribution.

---

## Durchführen eines Upgrades von Horizon Agent auf einer virtuellen Linux-Maschine

Sie können das Upgrade von Horizon Agent auf einer virtuellen Linux-Maschine durchführen, indem Sie die aktuelle Version von Horizon Agent installieren.

Nicht verwaltete virtuelle Maschine: Das Agent-Installationsprogramm registriert die virtuelle Maschine am Broker. Dies erfordert Broker-Administratorinformationen. Der Assistent zur **Erstellung von Desktop-Pools** verwendet **Andere Quellen** auf der Seite „Computerquelle“, um die registrierte virtuelle Maschine auszuwählen.

Verwaltete virtuelle Maschine: Das Installationsprogramm kommuniziert nicht mit dem Broker. Der Assistent zur **Erstellung von Desktop-Pools** verwendet **Virtuelle vCenter-Maschinen** auf der Seite „Computerquelle“, um die virtuellen Maschinen über vCenter auszuwählen. Die Bereitstellung der verwalteten virtuellen Maschine unterstützt die folgenden Funktionen.

- Betriebsrichtlinie für Remote-Computer
- Benutzern das Zurücksetzen ihrer Computer gestatten

---

**Hinweis** Horizon Agent for Linux 7.0.0 und frühere Versionen funktionierten als nicht verwaltete virtuelle Maschinen. Horizon Agent for Linux 7.0.1 funktioniert als Unterstützung für verwaltete virtuelle Maschinen.

---

Sie können mit den folgenden Methoden eine Aktualisierung der Bereitstellung einer nicht verwalteten zur Bereitstellung einer verwalteten virtuellen Maschine vornehmen.

- Behalten Sie die Bereitstellung der nicht verwalteten virtuellen Maschine bei und nehmen Sie eine Aktualisierung auf die erforderliche Version vor. Für diesen Aktualisierungstyp sind keine Konfigurationsänderungen auf Horizon Connection Server erforderlich.

- Nehmen Sie eine Aktualisierung von der Bereitstellung einer nicht verwalteten virtuellen Maschine auf die Bereitstellung einer verwalteten virtuellen Maschine einer beliebigen Version vor. Für diesen Upgrade-Typ ist die Erstellung eines neuen Desktop-Pools auf Horizon Connection Server erforderlich.

**Hinweis** Für die Aktualisierung der Bereitstellung einer verwalteten virtuellen Maschine können Sie die Bereitstellung einer verwalteten virtuellen Maschine beibehalten und eine Aktualisierung auf die erforderliche Version vornehmen. Das Konvertieren der Bereitstellung der verwalteten virtuellen Maschine zur Bereitstellung der nicht verwalteten virtuellen Maschine während der Aktualisierung wird nicht unterstützt.

Die folgenden Parameter stehen für die Aktualisierung zur Verfügung.

**Tabelle 5-4. Optionale Parameter für das Upgrade von Horizon Agent**

Parameter	Beschreibung
-A yes	Annahme der Nutzungsbedingungen und der FIPS-Erklärung Um die Installation fortzusetzen zu können, müssen Sie <b>yes</b> angeben. Wird dieser Parameter nicht angegeben, werden Sie vom Installationsprogramm dazu aufgefordert.
-a yes no	Installieren Sie die Unterstützung der Audio-Eingangsumleitung oder umgehen Sie diese.
-f yes no	Installieren oder umgehen Sie die Unterstützung der kryptografischen Module, die auf FIPS 140-2-Kompatibilität (Federal Information Processing Standards) ausgelegt sind. Die Standardeinstellung ist <b>no</b> . Weitere Informationen finden Sie in der Beschreibung des FIPS 140-2-Modus unter <a href="#">Funktionen von Horizon Linux-Desktops</a> .
-m yes no	Installieren oder umgehen Sie die Unterstützung für die Smartcard-Umleitung. Die Standardeinstellung ist <b>no</b> .
-r yes no	Starten Sie das Betriebssystem nach der Installation neu. Die Standardeinstellung ist <b>no</b> .
-C yes no	Installieren oder umgehen Sie die Unterstützung für die Zwischenablagenumleitung. Die Standardeinstellung ist <b>yes</b> .
-F yes no	Installieren oder umgehen Sie die CDR-Unterstützung. Die Standardeinstellung ist <b>yes</b> .
-M yes no	Aktualisieren Sie den Linux Agent auf den Agent managed unmanaged. Der Standardwert lautet <b>ja</b> .
-S yes no	Installieren oder umgehen Sie die Single Sign-On (SSO)-Unterstützung. Die Standardeinstellung ist <b>yes</b> .
-U yes no	Installieren oder umgehen Sie die USB-Unterstützung. Die Standardeinstellung ist <b>no</b> .

## Durchführen eines Upgrades von Horizon Agent auf einer virtuellen Linux-Maschine

Sie können das Upgrade von Horizon Agent auf einer Linux-Maschine durchführen, indem Sie die aktuelle Version von Horizon Agent installieren.

### Voraussetzungen

- Stellen Sie sicher, dass der VMwareBlastServer-Prozess nicht ausgeführt wird.

Um diesen Prozess anzuhalten, stellen Sie sicher, dass der Benutzer von der Maschine abgemeldet ist und keine Desktop-Sitzung aktiv ist, oder starten Sie die Maschine neu.

## Verfahren

- 1 Laden Sie die aktuelle Installationsdatei für Horizon Agent for Linux von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunter.

Wählen Sie unter „Desktop & End-User Computing“ den VMware Horizon 7-Download aus, der das Installationsprogramm für Horizon Agent for Linux enthält.

Der Dateiname des Installationsprogramms lautet `VMware-viewagent-linux-x86_64-y.y.y-xxxxxxx.tar.gz` für 64-Bit-Linux. Hierbei ist `y.y.y` die Versionsnummer und `xxxxxxx` die Buildnummer.

- 2 Entpacken Sie das TAR-Archiv für Ihre Linux-Distribution auf dem Gastbetriebssystem.

Beispiel:

```
tar -xzf <Horizon Agent-TAR-Archiv>
```

- 3 Wechseln Sie zum Ordner des TAR-Archivs.
- 4 Aktualisieren Sie nicht verwaltete Maschinen, indem Sie das Skript `install_viewagent.sh` nach einem der folgenden Bereitstellungsszenarien ausführen.

Option	Beschreibung
<b>Aktualisieren der Bereitstellung einer nicht verwalteten virtuellen Maschine und Beibehalten der Bereitstellung einer nicht verwalteten virtuellen Maschine</b>	<pre>sudo ./install_viewagent.sh -A yes -M no</pre> <p><b>Hinweis</b> Um die bestmögliche Leistung zu gewährleisten, sollten Sie keine nicht verwaltete virtuelle Maschine verwenden.</p>
<b>Aktualisieren der Bereitstellung einer nicht verwalteten virtuellen Maschine und Ändern zur Bereitstellung einer verwalteten virtuellen Maschine</b>	<pre>sudo ./install_viewagent.sh -A yes -M yes</pre> <p><b>Hinweis</b> Löschen Sie in Horizon Console den vorhandenen Desktop-Pool für die Bereitstellung der nicht verwalteten virtuellen Maschine und erstellen Sie einen Desktop-Pool für die Bereitstellung einer verwalteten virtuellen Maschine. Weitere Informationen finden Sie unter <a href="#">Erstellen eines manuellen Desktop-Pools für Linux</a>.</p>
<b>Aktualisieren der Bereitstellung einer verwalteten virtuellen Maschine</b>	<pre>sudo ./install_viewagent.sh -A yes -M yes</pre> <p><b>Hinweis</b> Nach dem Aktualisieren kann Ihr vorhandener Desktop-Pool erneut verwendet werden.</p>

## Deinstallieren von Horizon 7 für Linux-Maschinen

Zum Deinstallieren von Horizon 7 für Linux auf einer virtuellen Maschine müssen Sie den Horizon Agent deinstallieren und die Konfigurationsdateien entfernen.

## Voraussetzungen

Stellen Sie sicher, dass der VMwareBlastServer-Prozess nicht ausgeführt wird. Stellen Sie zum Beenden dieses Prozesses sicher, dass Sie sich von der Maschine abmelden und dass keine Desktop-Sitzung aktiv ist, oder starten Sie die Maschine neu.

## Verfahren

- 1 Öffnen Sie auf der virtuellen Maschine ein Terminalfenster und führen Sie das Deinstallationsskript für Horizon Agent aus.

```
sudo /usr/lib/vmware/viewagent/bin/uninstall_viewagent.sh
```

Das Skript beendet die Horizon Agent-Prozesse, löscht den Horizon Agent-Dienst und die Software aus dem Installationsverzeichnis `/usr/lib/vmware/viewagent`.

- 2 Löschen Sie die Horizon 7 for Linux-Konfigurationsdateien manuell aus dem Verzeichnis `/etc/vmware`.



# Konfigurationsoptionen für Linux-Desktops

# 6

Mithilfe von Konfigurationsdateien können Sie verschiedene Optionen konfigurieren, um die Benutzererfahrung anzupassen.

Dieses Kapitel enthält die folgenden Themen:

- [Einstellen der Optionen in Konfigurationsdateien auf einem Linux-Desktop](#)
- [Verwenden von Intelligente Richtlinien](#)
- [Beispiel für Blast-Einstellungen für Linux-Desktops](#)
- [Beispiel für Optionen der Clientlaufwerksumleitung für Linux-Desktops](#)

## Einstellen der Optionen in Konfigurationsdateien auf einem Linux-Desktop

Sie können verschiedene Optionen konfigurieren, indem Sie der Datei `/etc/vmware/config` oder `/etc/vmware/viewagent-custom.conf` Einträge hinzufügen.

Bei der Installation von Horizon Agent kopiert das Installationsprogramm die beiden Konfigurationsvorlagendateien `config.template` und `viewagent-custom.conf.template` in `/etc/vmware`. Außerdem kopiert das Installationsprogramm, wenn `/etc/vmware/config` und `/etc/vmware/viewagent-custom.conf` nicht vorhanden sind, `config.template` nach `config` und `viewagent-custom.conf.template` nach `viewagent-custom.conf`. In den Vorlagendateien sind alle Konfigurationsoptionen aufgelistet und dokumentiert. Um eine Option einzustellen, entfernen Sie einfach den Kommentar und ändern Sie den Wert wie gewünscht.

So aktiviert beispielsweise die folgende Zeile in `/etc/vmware/config` den Build-to-Lossless-PNG-Modus.

```
RemoteDisplay.buildToPNG=TRUE
```

Nachdem Sie Ihre Änderungen vorgenommen haben, müssen Sie Linux neu starten, damit die Änderungen wirksam werden.

## Konfigurationsoptionen in /etc/vmware/config

VMwareBlastServer und seine zugehörigen Plug-ins verwenden die Konfigurationsdatei /etc/vmware/config.

**Hinweis** Die folgende Tabelle enthält Beschreibungen für alle von Agent erzwungenen Richtlinieneinstellungen für USB in der Horizon Agent-Konfigurationsdatei. Horizon Agent verwendet die Einstellungen, um zu entscheiden, ob der USB-Anschluss zur Host-Maschine umgeleitet werden kann. Horizon Agent übergibt diese Einstellungen außerdem an Horizon Client zur Interpretation und Erzwingung. Die Erzwingung hängt davon ab, ob Sie den **(m)**-Modifizierer zur Anwendung der Horizon Agent-Filterrichtlinieneinstellung zusätzlich zur Horizon Client-Filterrichtlinieneinstellung festlegen oder den **(o)**-Modifizierer zur Verwendung der Horizon Agent-Filterrichtlinieneinstellung anstelle der Horizon Client-Filterrichtlinieneinstellung überschreiben.

**Tabelle 6-1. Konfigurationsoptionen in /etc/vmware/config**

Option	Wert/Format	Standard	Beschreibung
Clipboard.Direction	0, 1, 2, oder 3	2	Verwenden Sie diese Option zur Festlegung der Richtlinie für die Zwischenablagenumleitung. Folgende Werte sind gültig: <ul style="list-style-type: none"> <li>■ 0 - Zwischenablagenumleitung deaktivieren.</li> <li>■ 1 - Zwischenablagenumleitung in beide Richtungen aktivieren.</li> <li>■ 2 - Zwischenablagenumleitung nur vom Client zum Remote-Desktop aktivieren.</li> <li>■ 3 - Zwischenablagenumleitung nur vom Remote-Desktop zum Client aktivieren.</li> </ul>
RemoteDisplay.allowAudio	true oder false	true	Legen Sie diese Option fest, um die Audio-Ausgabe zu aktivieren/deaktivieren.
RemoteDisplay.allowH264	true oder false	true	Legen Sie diese Option zum Aktivieren oder Deaktivieren der H.264-Codierung fest.
RemoteDisplay.buildToPNG	true oder false	false	Grafische Anwendungen und insbesondere grafische Anwendungen zur Bildbearbeitung erfordern ein pixelgenaues Rendering von Bildern in der Clientanzeige eines Linux-Desktops. Sie haben die Möglichkeit, einen speziellen Build-to-Lossless-PNG-Modus für Bilder und die Videowiedergabe zu konfigurieren, die auf einem Linux-Desktop generiert und auf dem Clientgerät gerendert werden. Diese Funktion verwendet zusätzliche Bandbreite zwischen dem Client und dem ESXi-Host. Bei Aktivierung dieser Option wird die H.264-Codierung deaktiviert.
RemoteDisplay.enableNetworkContinuity	true oder false	true	Legen Sie diese Option fest, um die Funktion für durchgängige Netzwerke in Horizon Agent für Linux zu aktivieren oder zu deaktivieren.
RemoteDisplay.enableNetworkIntelligence	true oder false	true	Legen Sie diese Option fest, um die Funktion für intelligente Netzwerke in Horizon Agent für Linux zu aktivieren oder zu deaktivieren.

**Tabelle 6-1. Konfigurationsoptionen in /etc/vmware/config (Fortsetzung)**

Option	Wert/Format	Standard	Beschreibung
RemoteDisplay.enableStats	true oder false	false	Aktivieren oder deaktivieren Sie die VMware Blast-Anzeigeprotokollstatistik im MKS-Protokoll, beispielsweise Bandbreite, FPS, RTT usw.
RemoteDisplay.enableUDP	true oder false	true	Legen Sie diese Option fest, um die Unterstützung für das UDP-Protokoll in Horizon Agent für Linux zu aktivieren oder zu deaktivieren.
RemoteDisplay.maxBandwidthKbps	Eine Ganzzahl	1000000	Legt die maximale Bandbreite für eine VMware Blast-Sitzung in Kilobits pro Sekunde (KBit/s) fest. Die Bandbreite umfasst den gesamten Sitzungsdatenverkehr, Bilddarstellung, Audio, virtuelle Kanäle und VMware Blast-Steuerung eingeschlossen. Der gültige Wert muss kleiner als 4 Gbit/s (4096000) sein.
RemoteDisplay.minBandwidthKbps	Eine Ganzzahl	256	Legt die minimale Bandbreite für eine VMware Blast-Sitzung in Kilobits pro Sekunde (KBit/s) fest. Die Bandbreite umfasst den gesamten Sitzungsdatenverkehr, Bilddarstellung, Audio, virtuelle Kanäle und VMware Blast-Steuerung eingeschlossen.
RemoteDisplay.maxFPS	Eine Ganzzahl	30	Legt die maximale Rate der Bildschirmaktualisierungen fest. Mit dieser Einstellung steuern Sie die durchschnittliche Bandbreite, die Benutzer in Anspruch nehmen. Der gültige Wert muss zwischen 3 und 60 liegen. Die Standardeinstellung beträgt 30 Aktualisierungen pro Sekunde.
RemoteDisplay.maxQualityJPEG	Verfügbarer Wertebereich: 1–100	90	Legt die Bildqualität für die Desktop-Anzeige für die JPEG/PNG-Codierung fest. Die Einstellungen für eine hohe Bildqualität sind für eher statische Bereiche sinnvoll.
RemoteDisplay.midQualityJPEG	Verfügbarer Wertebereich: 1–100	35	Legt die Bildqualität für die Desktop-Anzeige für die JPEG/PNG-Codierung fest. Legt die Einstellungen für die mittlere Qualität der Desktop-Anzeige fest.
RemoteDisplay.minQualityJPEG	Verfügbarer Wertebereich: 1–100	25	Legt die Bildqualität für die Desktop-Anzeige für die JPEG/PNG-Codierung fest. Die Einstellungen für eine niedrige Bildqualität sind für Bereiche gedacht, die sich häufig ändern, z. B. durch einen Bildlauf.
RemoteDisplay.qpmaxH264	Verfügbarer Wertebereich: 0–51	36	Verwenden Sie diese Option, um den Quantisierungsparameter „H264minQP“ festzulegen, der die für die H.264-Codierung konfigurierte beste Bildqualität angibt. Geben Sie einen Wert an, der größer ist als der für „RemoteDisplay.qpminH264“ festgelegte Wert.
RemoteDisplay.qpminH264	Verfügbarer Wertebereich: 0–51	10	Verwenden Sie diese Option, um den Quantisierungsparameter „H264maxQP“ festzulegen, der die für die H.264-Codierung konfigurierte geringste Bildqualität angibt. Geben Sie einen Wert an, der kleiner ist als der für „RemoteDisplay.qpmaxH264“ festgelegte Wert.

**Tabelle 6-1. Konfigurationsoptionen in /etc/vmware/config (Fortsetzung)**

Option	Wert/Format	Standard	Beschreibung
UsbRedirPlugin.log.logLevel	error, warn, info, debug, trace oder verbose	info	Verwenden Sie diese Option zur Festlegung der Protokollebene des USB-Umleitungs-Plug-Ins.
UsbRedirServer.log.logLevel	error, warn, info, debug, trace oder verbose	info	Verwenden Sie diese Option zur Festlegung der Protokollebene des USB-Umleitungsservers.
VMWPKcs11Plugin.log.enable	true oder false	false	Legen Sie diese Option fest, um den Protokollierungsmodus für die True SSO-Funktion zu aktivieren oder zu deaktivieren.
VMWPKcs11Plugin.log.logLevel	error, warn, info, debug, trace oder verbose	info	Verwenden Sie diese Option, um die Protokollebene für die True SSO-Funktion festzulegen.
VVC.RTAV.Enable	true oder false	true	Legen Sie diese Option fest, um die Audio-Eingabe zu aktivieren/deaktivieren.
VVC.ScRedir.Enable	true oder false	true	Legen Sie diese Option fest, um die Smartcard-Umleitung zu aktivieren/deaktivieren.
VVC.logLevel	fatal error, warn, info, debug oder trace	info	Verwenden Sie diese Option zur Festlegung der Protokollebene des VVC-Proxy-Knotens.
cdrserver.cacheEnable	true oder false	true	Legen Sie diese Option fest, um die Funktion des Schreibcache von der Agentseite zur Clientseite zu aktivieren oder zu deaktivieren.
cdrserver.customizedSharedFolderPath	folder_path	/home/	<p>Verwenden Sie diese Option, um den Speicherort des freigegebenen Ordners für die Clientlaufwerksumleitung (Client Drive Redirection, CDR) aus dem Standardverzeichnis <code>/home/user/tsclient</code> in ein benutzerdefiniertes Verzeichnis zu ändern.</p> <p>Wenn beispielsweise der Benutzer test den freigegebenen CDR-Ordner auf <code>/mnt/test/tsclient</code> anstelle von <code>/home/test/tsclient</code> ablegen möchte, kann der Benutzer</p> <p><b><code>cdrserver.customizedSharedFolderPath=/mnt/</code></b> angeben.</p> <p><b>Hinweis</b> Damit diese Option wirksam wird, muss der angegebene Ordner vorhanden sein und mit den richtigen Benutzerberechtigungen konfiguriert werden.</p>
cdrserver.forcedByAdmin	true oder false	false	Legen Sie mit dieser Option fest, ob der Client zusätzliche Ordner gemeinsam nutzen kann, die nicht mit der Option <code>cdrserver.shareFolders</code> angegeben wurden.
cdrserver.logLevel	error, warn, info, debug, trace oder verbose	info	Verwenden Sie diese Option zur Festlegung der Protokollebene für die Datei <code>vmware-CDRserver.log</code> .

**Tabelle 6-1. Konfigurationsoptionen in /etc/vmware/config (Fortsetzung)**

Option	Wert/Format	Standard	Beschreibung
cdserver.permissions	R	RW	<p>Verwenden Sie diese Option zur Anwendung zusätzlicher Lese/Schreib-Berechtigungen, über die Horizon Agent für die von Horizon Client freigegebenen Ordner verfügt. Beispiel:</p> <ul style="list-style-type: none"> <li>■ Wenn der von Horizon Client freigegebene Ordner über die Berechtigungen <code>read</code> und <code>write</code> verfügt und Sie <b>cdserver.permissions=R</b> festlegen, verfügt Horizon Agent nur über <code>read</code>-Zugriffsberechtigungen.</li> <li>■ Wenn der von Horizon Client freigegebene Ordner nur über <code>read</code>-Berechtigungen verfügt und Sie <b>cdserver.permissions=RW</b> festlegen, verfügt Horizon Agent weiterhin nur über <code>read</code>-Zugriffsrechte. Horizon Agent kann nicht das Schreibschutzattribut „<code>read only</code>“ ändern, das von Horizon Client festgelegt wurde. Mit Horizon Agent lassen sich nur die Schreibzugriffsrechte entfernen.</li> </ul> <p>Eine typische Verwendung lautet:</p> <ul style="list-style-type: none"> <li>■ <b>cdserver.permissions=R</b></li> <li>■ <b>#cdserver.permissions=R</b> (z. B., um den Eintrag auszukommentieren oder zu löschen)</li> </ul>
cdserver.sharedFolders	<i>file_path1,R; file_path2,; file_path3,R; . .</i>	Nicht definiert	<p>Geben Sie einen oder mehrere Dateipfade zu den Ordnern an, die der Client mit dem Linux-Desktop gemeinsam nutzen kann. Beispiel:</p> <ul style="list-style-type: none"> <li>■ Für einen Windows-Client: <b>C:\spreadsheets,;D:\ebooks,R</b></li> <li>■ Für einen Nicht-Windows-Client: <b>/tmp/spreadsheets;/tmp/ebooks,; /home/finance,R</b></li> </ul>
collaboration.logLevel	error, info oder debug	info	<p>Verwenden Sie diese Option zur Festlegung der Protokollebene für die Zusammenarbeitssitzung. Wenn die Protokollebene <code>debug</code> ausgewählt ist, werden alle Aufrufe von <code>collabui</code>-Funktionen sowie die Inhalte der <code>collabor</code>-Liste protokolliert.</p>
collaboration.maxCollabors	Eine Ganzzahl kleiner 10	5	<p>Legt die maximale Anzahl der Benutzer fest, die Sie zur Teilnahme an einer Sitzung einladen können.</p>
collaboration.enableEmail	true oder false	true	<p>Legen Sie diese Option zum Aktivieren oder Deaktivieren der Einladungen zur Zusammenarbeit mithilfe einer installierten E-Mail-Anwendung fest. Ist diese Option deaktiviert, können Sie keine Einladungen zur Zusammenarbeit mit E-Mails versenden, auch wenn eine E-Mail-Anwendung installiert ist.</p>
collaboration.serverUrl	[URL]	Nicht definiert	<p>Spezifiziert die Server-URLs, die in Einladungen zur Zusammenarbeit enthalten sein sollen.</p>

**Tabelle 6-1. Konfigurationsoptionen in /etc/vmware/config (Fortsetzung)**

Option	Wert/Format	Standard	Beschreibung
collaboration.enableControlPassing	true oder false	true	Legen Sie diese Option fest, um die Kontrolle der Teilnehmer über die Linux-Desktops zuzulassen oder einzuschränken. Um für die Zusammenarbeitssitzung einen reinen Lesezugriff festzulegen, setzen Sie diese Option auf <b>false</b> .
mksVNCServer.useUIInputButtonMapping	true oder false	false	Legen Sie diese Option fest, um die Unterstützung einer Maus für Linkshänder auf Ubuntu oder RHEL 7.x zu aktivieren. CentOS und RHEL 6.x unterstützen Mäuse für Linkshänder, und Sie müssen diese Option nicht festlegen.
mksvhan.clipboardSize	Eine Ganzzahl	1024	Verwenden Sie diese Option, um die maximale Größe der Zwischenablage für das Kopieren und Einfügen anzugeben.
vdpservice.log.logLevel	fatal error, warn, info, debug oder trace	info	Verwenden Sie diese Option zum Festlegen der Protokollebene des vdpsservice.
viewusb.AllowAudioIn	{m o}: {true false}	Nicht definiert, entspricht true	Verwenden Sie diese Option, um die Umleitung für Audio-Eingabe-Geräte zuzulassen oder auszuschließen. Beispiel: <b>o:false</b>
viewusb.AllowAudioOut	{m o}: {true false}	Nicht definiert, entspricht false	Legen Sie diese Option fest, um die Umleitung für Audio-Ausgabe-Geräte zuzulassen oder auszuschließen.
viewusb.AllowAutoDeviceSplitting	{m o}: {true false}	Nicht definiert, entspricht false	Legen Sie diese Option fest, um das automatische Splitten von Composite USB-Geräten zuzulassen oder auszuschließen. Beispiel: <b>m:true</b>
viewusb.AllowDevDescFailsafe	{m o}: {true false}	Nicht definiert, entspricht false	Legen Sie diese Option fest, um die Umleitung für Geräte zuzulassen oder auszuschließen, auch wenn Horizon Client die Konfigurations-/Gerätebeschreibungen nicht abrufen kann. Um ein Gerät auch beim Scheitern des Abrufs der Konfigurations-/Gerätebeschreibungen zuzulassen, muss dieses in „Include“-Filter wie z. B. <b>IncludeVidPid</b> oder <b>IncludePath</b> eingeschlossen werden.
viewusb.AllowHIDBootable	{m o}: {true false}	Nicht definiert, entspricht true	Verwenden Sie diese Option, um die Umleitung anderer Eingabegeräte neben Tastatur und Maus, die zur Startzeit verfügbar sind (auch als „startfähige Eingabegeräte“ bezeichnet), zuzulassen oder auszuschließen.
viewusb.AllowKeyboardMouse	{m o}: {true false}	Nicht definiert, entspricht false	Verwenden Sie diese Option, um die Umleitung von Tastaturen mit eingebauten Zeigegeräten (Maus, Trackball oder Touchpad) zuzulassen oder auszuschließen.

**Tabelle 6-1. Konfigurationsoptionen in /etc/vmware/config (Fortsetzung)**

Option	Wert/Format	Standard	Beschreibung
viewusb.AllowSmartcard	<code>{m o}:</code> <code>{true false}</code>	Nicht definiert, entspricht <code>false</code>	Legen Sie diese Option fest, um die Umleitung für Smartcard-Geräte zuzulassen oder auszuschließen.
viewusb.AllowVideo	<code>{m o}:</code> <code>{true false}</code>	Nicht definiert, entspricht <code>true</code>	Verwenden Sie diese Option, um die Umleitung für Videogeräte zuzulassen oder auszuschließen.
viewusb.DisableRemoteConfig	<code>{m o}:</code> <code>{true false}</code>	Nicht definiert, entspricht <code>false</code>	Legen Sie diese Option fest, um die Verwendung von Horizon Agent-Einstellungen zuzulassen oder auszuschließen, wenn eine USB-Gerätefilterung durchgeführt wird.
viewusb.ExcludeAllDevices	<code>{true false}</code>	Nicht definiert, entspricht <code>false</code>	Verwenden Sie diese Option, um alle USB-Geräte von der Umleitung auszuschließen oder in die Umleitung einzubeziehen. Wenn für diese Einstellung <b>true</b> festgelegt ist, können Sie andere Richtlinieneinstellungen verwenden, um zuzulassen, dass bestimmte Geräte oder Gerätefamilien umgeleitet werden. Wenn für diese Einstellung <b>false</b> festgelegt ist, können Sie andere Richtlinieneinstellungen verwenden, um zu verhindern, dass bestimmte Geräte oder Gerätefamilien umgeleitet werden. Wenn Sie den Wert von <b>ExcludeAllDevices</b> in Horizon Agent auf <b>true</b> setzen und diese Einstellung an Horizon Client weitergegeben wird, überschreibt die Horizon Agent-Einstellung die Horizon Client-Einstellung.
viewusb.ExcludeFamily	<code>{m o}: family_name_1[;family_name_2;...]</code>	Nicht definiert	Verwenden Sie diese Option, um Gerätefamilien von der Umleitung auszuschließen oder in die Umleitung einzubeziehen. Beispiel: <b>m:bluetooth;smart-card</b> Wenn Sie das automatische Gerätesplitten aktiviert haben, prüft Horizon die Gerätefamilie jeder Schnittstelle eines Composite USB-Gerätes, um zu entscheiden, welche Schnittstelle ausgeschlossen werden muss. Wenn Sie das automatische Gerätesplitten deaktiviert haben, prüft Horizon die Gerätefamilie des gesamten Composite USB-Gerätes.  <b>Hinweis</b> Maus und Tastatur sind standardmäßig von der Umleitung ausgeschlossen und müssen deshalb nicht mit dieser Einstellung ausgeschlossen werden.
viewusb.ExcludePath	<code>{m o}: bus-x1[/y1].../ port-z1[;bus-x2[/y2].../port-z2;...]</code>	Nicht definiert	Verwenden Sie diese Option, um Geräte an bestimmten Hub- oder Portpfaden von der Umleitung auszuschließen. Bus- und Portnummern müssen im hexadezimalen Format angegeben werden. Sie können das Platzhalterzeichen nicht in Pfaden verwenden.  Beispiel: <b>m:bus-1/2/3_port- 02;bus-1/1/1/4_port-ff</b>

**Tabelle 6-1. Konfigurationsoptionen in /etc/vmware/config (Fortsetzung)**

Option	Wert/Format	Standard	Beschreibung
viewusb.ExcludeVidPid	<code>{m o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]</code>	Nicht definiert	Legen Sie diese Option fest, um Geräte mit einer bestimmten Anbieter- oder Produkt-ID von der Umleitung auszuschließen. Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden.  Beispiel: <b>o:vid-0781_pid-****;vid-0561_pid-554c</b>
viewusb.IncludeFamily	<code>{m o}:family_name_1[;family_name_2]...</code>	Nicht definiert	Legen Sie diese Option fest, um Gerätefamilien in die Umleitung einzubeziehen.  Beispiel: <b>o:storage; smart-card</b>
viewusb.IncludePath	<code>{m o}:bus-x1[/y1].../port-z1[;bus-x2[/y2].../portz2;...]</code>	Nicht definiert	Verwenden Sie diese Option, um Geräte an bestimmten Hub- oder Portpfaden in die Umleitung einzubeziehen. Bus- und Portnummern müssen im hexadezimalen Format angegeben werden. Sie können das Platzhalterzeichen nicht in Pfaden verwenden.  Beispiel: <b>m:bus-1/2_port- 02;bus-1/7/1/4_port-0f</b>
viewusb.IncludeVidPid	<code>{m o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]</code>	Nicht definiert	Legen Sie diese Option fest, um Geräte mit bestimmten Anbieter- oder Produkt-IDs in die Umleitung einzubeziehen. Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden.  Beispiel: <b>o:vid-***_pid-0001;vid-0561_pid-554c</b>



**Tabelle 6-1. Konfigurationsoptionen in /etc/vmware/config (Fortsetzung)**

Option	Wert/Format	Standard	Beschreibung
viewusb.SplitExcludeVidPid	<code>{m o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]</code>	Nicht definiert	Verwenden Sie diese Option, um ein bestimmtes Composite USB-Gerät für das Splitten nach Anbieter- und Produkt-IDs auszuschließen oder einzubeziehen. Das Format dieser Einstellung lautet <b>vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]</b> . ID-Nummern müssen in hexadezimaler Schreibweise angegeben werden. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: <b>m:vid-0f0f_pid-55**</b>
viewusb.SplitVidPid	<code>{m o}: vid-xxxx_pid-yyyy[exintf:zz[;exintf:ww]]</code>	Nicht definiert	Legen Sie diese Option fest, um die Komponenten eines Composite USB-Gerätes, die durch Anbieter- und Produkt-IDs angegeben sind, als separate Geräte zu behandeln. Das Format dieser Einstellung lautet <b>vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww])</b> . Sie können mit dem Stichwort <b>exintf</b> Komponenten durch Angabe ihrer Schnittstellennummer von der Umleitung ausschließen. Sie müssen hexadezimale ID-Nummern und dezimale Schnittstellennummern einschließlich der 0 am Anfang angeben. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: <b>o:vid-0f0f_pid-*** (exintf-01);vid-0781_pid-554c(exintf:01;exintf:02)</b>  <b>Hinweis</b> Horizon schließt nicht automatisch die Komponenten ein, die Sie nicht explizit ausgeschlossen haben. Sie müssen eine Filterrichtlinie wie z. B. <b>Include VidPid Device</b> (VidPid-Gerät einbeziehen) angeben, um diese Komponenten einzubeziehen.

## Konfigurationsoptionen in /etc/vmware/viewagent-custom.conf

Java Standalone Agent verwendet die Konfigurationsdatei /etc/vmware/viewagent-custom.conf.

**Tabelle 6-2. Konfigurationsoptionen in /etc/vmware/viewagent-custom.conf**

Option	Wert	Standard	Beschreibung
CDREnable	true oder false	true	Verwenden Sie diese Option, um die Funktion der Clientlaufwerksumleitung (Client Drive Redirection, CDR) zu aktivieren oder zu deaktivieren.
CollaborationEnable	true oder false	true	Legen Sie diese Option fest, um die Funktion „Session Collaboration“ in Linux Desktop zu aktivieren oder zu deaktivieren.

**Tabelle 6-2. Konfigurationsoptionen in /etc/vmware/viewagent-custom.conf (Fortsetzung)**

Option	Wert	Standard	Beschreibung
EndpointVPNEnable	true oder false	false	Legen Sie diese Option fest, um anzugeben, ob die IP-Adresse der physischen Client-Netzwerkkarte oder die VPN-IP-Adresse zur Überprüfung der IP-Adresse des Endpunkts anhand des Bereichs der in der Dynamic Environment Manager-Konsole verwendeten Endpunkt-IP-Adressen verwendet werden soll. Wenn die Option auf false festgelegt ist, wird die IP-Adresse der physischen Client-Netzwerkkarte verwendet. Andernfalls wird die VPN-IP-Adresse verwendet.
HelpDeskEnable	true oder false	true	Legen Sie diese Option fest, um die Helpdesk-Tool-Funktion zu aktivieren oder zu deaktivieren.
KeyboardLayoutSync	true oder false	true	<p>Verwenden Sie diese Option, um festzulegen, ob das Systemgebietsschema und das aktuelle Tastaturlayout eines Clients mit Horizon Agent for Linux-Desktops synchronisiert werden sollen.</p> <p>Wenn diese Einstellung aktiviert wurde oder nicht konfiguriert ist, ist eine Synchronisierung zugelassen. Wenn diese Einstellung deaktiviert ist, ist eine Synchronisierung nicht erlaubt.</p> <p>Diese Funktion wird nur für Horizon Client für Windows und nur für die Gebietsschemas Englisch, Französisch, Deutsch, Japanisch, Koreanisch, Spanisch, Chinesisch (vereinfacht) und Chinesisch (traditionell) unterstützt.</p>
LogCnt	Eine Ganzzahl	-1	<p>Verwenden Sie diese Option zur Festlegung der Anzahl der reservierten Protokolle in /tmp/vmware-root.</p> <ul style="list-style-type: none"> <li>■ -1 - alle beibehalten</li> <li>■ 0 - alle löschen</li> <li>■ &gt; 0 - Anzahl der reservierten Protokolle.</li> </ul>
NetbiosDomain	Eine Textzeich enfolge in Großbuc hstaben		Verwenden Sie diese Option bei der Konfiguration von True SSO, um den NetBIOS-Namen der Domäne Ihrer Organisation festzulegen.
OfflineJoinDomain	pbis oder samba	pbis	Mit dieser Option wird der Instant-Clone-Offline-Domänenbeitritt festgelegt. Die verfügbaren Methoden zum Durchführen eines Offline-Domänenbeitritts sind die PowerBroker Identity Services Open(PBISO)-Authentifizierung und der Samba-Offline-Domänenbeitritt. Wenn für diese Eigenschaft ein anderer Wert als pbis oder samba festgelegt ist, wird der Offline-Domänenbeitritt ignoriert.

**Tabelle 6-2. Konfigurationsoptionen in /etc/vmware/viewagent-custom.conf (Fortsetzung)**

Option	Wert	Standard	Beschreibung
RunOnceScript			<p>Mit dieser Option kann die geklonte virtuelle Maschine Active Directory erneut beitreten.</p> <p>Legen Sie das RunOnceScript fest, nachdem der Hostname geändert wurde. Das angegebene Skript wird nur einmal nach der ersten Änderung des Hostnamens ausgeführt. Das Skript wird mit der Stammberechtigung ausgeführt, wenn der Agentendienst gestartet wird und sich der Hostname seit der Agenteninstallation geändert hat.</p> <p>Zum Beispiel müssen Sie für die winbind-Lösung die virtuelle Basis-Maschine Active Directory mit winbind beitreten lassen und diese Option auf einen Skriptpfad festlegen. Das Skript muss den Befehl zum erneuten Domänenbeitritt /usr/bin/net ads join -U &lt;ADUserName&gt;%&lt;ADUserPassword&gt; enthalten. Nach dem VM-Klon ändert die Betriebssystemanpassung den Hostnamen. Wenn der Agentendienst gestartet wird, wird das Skript ausgeführt, damit die geklonte virtuelle Maschine Active Directory beitrifft.</p>
RunOnceScriptTimeout		120	<p>Verwenden Sie diese Option, um die Zeit bis zur Zeitüberschreitung in Sekunden für die Option „RunOnceScript“ festzulegen.</p> <p>Legen Sie z. B. RunOnceScriptTimeout=120 fest</p>
SSLCiphers	Eine Textzeich enfolge	!aNULL:kECDH +AESGCM:ECDH +AESGCM:RSA +AESGCM:kECDH +AES:ECDH+AES:RSA +AES	<p>Verwenden Sie diese Option zum Festlegen der Liste der Verschlüsselungen. Sie müssen das Format verwenden, das in <a href="https://www.openssl.org/docs/manmaster/man1/ciphers.html">https://www.openssl.org/docs/manmaster/man1/ciphers.html</a> definiert ist.</p>
SSLProtocols	Eine Textzeich enfolge	TLSv1_1:TLSv1_2	<p>Verwenden Sie diese Option zum Festlegen der Sicherheitsprotokolle. Die unterstützten Protokolle sind TLSv1.0, TLSv1.1 und TLSv1.2.</p>

**Tabelle 6-2. Konfigurationsoptionen in /etc/vmware/viewagent-custom.conf (Fortsetzung)**

Option	Wert	Standard	Beschreibung
SSODesktopType	UseGnomeClassic oder UseGnomeFlashback oder UseGnomeUbuntu oder UseMATE oder UseKdePlasma		<p>Über diese Option wird die Desktop-Umgebung festgelegt, die bei aktivierter SSO-Funktion anstelle der Standard-Desktop-Umgebung verwendet wird.</p> <p>Sie müssen zuerst sicherstellen, dass die ausgewählte Desktop-Umgebung auf Ihrem Desktop installiert ist, bevor Sie sie zur Verwendung auswählen. Nachdem Sie diese Option auf einem Ubuntu 16.04-/18.04-Desktop festgelegt haben, wird diese Option unabhängig davon, ob die SSO-Funktion aktiviert ist oder nicht, angewendet. Wenn diese Option auf einem RHEL.x/CentOS 7.x-Desktop festgelegt ist, wird die ausgewählte Desktop-Umgebung nur dann verwendet, wenn SSO aktiviert ist.</p> <p><b>Hinweis</b> Diese Option wird auf RHEL/CentOS 8.0- und RHEL/CentOS 6.x-Desktops nicht unterstützt. Horizon 7 unterstützt nur die Gnome-Desktop-Umgebung auf RHEL/CentOS 8.0-Desktops. Weitere Informationen zur Einrichtung von KDE als Standard-Desktop-Umgebung, wenn SSO auf RHEL/CentOS 6.x-Desktops ausgewählt ist, finden Sie unter <a href="#">Desktop-Umgebung</a>.</p>
SSOEnable	true oder false	true	Legen Sie diese Option fest, um Single Sign-On (SSO) zu aktivieren/deaktivieren.
SSOUserFormat	Eine Textzeich enfolge	[Benutzername]	<p>Verwenden Sie diese Option, um das Format des Anmeldenamens für das Single Sign-On anzugeben. Der Standard ist lediglich der Benutzername. Legen Sie diese Option fest, wenn auch der Domänenname erforderlich ist. Meist ist der Anmeldename der Domänenname plus einem Sonderzeichen, gefolgt vom Benutzernamen. Wenn das Sonderzeichen ein Rückschrägstrich ist, muss ein weiterer Rückschrägstrich als Escape-Zeichen verwendet werden. Beispiele für Formate von Anmeldenamen:</p> <ul style="list-style-type: none"> <li>■ SSOUserFormat=[Domäne]\\[Benutzername]</li> <li>■ SSOUserFormat=[Domäne]+[Benutzername]</li> <li>■ SSOUserFormat=[Benutzername]@[Domäne]</li> </ul>
Subnet	Ein Wert im CIDR- IP- Adressfor mat	[Subnetz]	<p>Legen Sie diese Option auf ein Subnetz fest, das andere Maschinen zur Verbindungsherstellung mit Horizon Agent for Linux verwenden können. Wenn mehr als eine lokale IP-Adresse mit unterschiedlichen Subnetzen vorhanden ist, wird die lokale IP-Adresse im konfigurierten Subnetz verwendet, um eine Verbindung mit Horizon Agent for Linux herzustellen. Sie müssen den Wert im CIDR-IP-Adressformat angeben. Beispielsweise Subnetz=123.456.7.8/24.</p>

**Tabelle 6-2. Konfigurationsoptionen in /etc/vmware/viewagent-custom.conf (Fortsetzung)**

Option	Wert	Standard	Beschreibung
UEMEnable	true oder false	false	Legen Sie diese Option zum Aktivieren oder Deaktivieren der intelligenten Dynamic Environment Manager-Richtlinien fest. Wenn die Option zum Aktivieren festgelegt ist und die Bedingung in der intelligenten Dynamic Environment Manager-Richtlinie erfüllt ist, werden die Richtlinien erzwungen.
UEMNetworkPath	Eine Textzeich enfolge		Diese Option muss auf denselben Netzwerkpfad festgelegt werden, der auch in der Dynamic Environment Manager-Konsole festgelegt ist. Der Pfad muss dem Format // 10.111.22.333/view/LinuxAgent/UEMConfig entsprechen.

**Hinweis** Die drei Sicherheitsoptionen SSLCiphers, SSLProtocols und SSLCipherServerPreference gelten für den VMwareBlastServer-Prozess. Beim Start des VMwareBlastServer-Prozesses durchläuft der Java Standalone Agent diese Optionen als Parameter. Wenn Blast Secure Gateway (BSG) aktiviert ist, wirken sich diese Optionen auf die Verbindung zwischen BSG und dem Linux-Desktop aus. Wenn BSG deaktiviert ist, wirken sich diese Optionen auf die Verbindung zwischen dem Client und dem Linux-Desktop aus.

## Verwenden von Intelligente Richtlinien

Sie können mit Intelligente Richtlinien Richtlinien zur Steuerung des Verhaltens der USB-Umleitung, der Zwischenablagenumleitung und der Clientlaufwerksumleitung auf bestimmten Linux-Remote-Desktops erstellen.

Sie können Richtlinien für Benutzerumgebungseinstellungen erstellen, die das Verhalten der USB-Umleitung, des virtuellen Drucks, der Zwischenablageumleitung, der Clientlaufwerksumleitung, der Web- und Chrome-Dateiübertragungsfunktionen sowie der Bandbreitenprofile in einem veröffentlichten Desktop oder einer veröffentlichten Anwendung bestimmen. Horizon Smart-Richtlinien für Benutzerumgebungseinstellungen werden während der Anmeldung angewendet und können während der erneuten Verbindung einer Sitzung aktualisiert werden. Um Horizon Smart-Richtlinien erneut anzuwenden, wenn Benutzer erneut eine Verbindung zu einer Sitzung herstellen, können Sie eine ausgelöste Aufgabe konfigurieren.

Sie können Richtlinien für Computerumgebungseinstellungen erstellen, die von Dynamic Environment Manager angewendet werden, während der Computer von Endbenutzern gestartet wird. Diese intelligenten Horizon-Richtlinien steuern das Verhalten der Flash-Multimediaumleitung, des integrierten Drucks und der USB-Umleitung. Horizon Smart-Richtlinien für Computerumgebungseinstellungen werden während des Computerstarts angewendet und können während der erneuten Verbindung einer Sitzung aktualisiert werden.

Mit Intelligente Richtlinien besteht die Möglichkeit, Richtlinien zu erstellen, die nur beim Eintreten bestimmter Bedingungen wirksam werden. Sie können beispielsweise eine Richtlinie konfigurieren, mit der die Clientlaufwerksumleitung dann deaktiviert wird, wenn ein Benutzer von einem Gerät außerhalb des Unternehmensnetzwerks eine Verbindung mit einem Remote-Desktop herstellt.

## Anforderungen für Intelligente Richtlinien

Für die Verwendung von Intelligente Richtlinien muss Ihre Horizon 7-Umgebung bestimmte Anforderungen erfüllen.

- Sie müssen Horizon Agent 7.5 oder höher und VMware Dynamic Environment Manager 9.4 oder höher auf den Remote-Desktops installieren, die mit Intelligente Richtlinien verwaltet werden sollen.
- Benutzer benötigen für die Herstellung einer Verbindung mit Linux-Remote-Desktops, die Sie mit Intelligente Richtlinien verwalten, Horizon Client 4.8 oder höher.
- Die Option `DEMEnable` muss aktiviert und die Option `DEMNetworkPath` muss in Datei `/etc/vmware/viewagent-custom.conf` festgelegt sein. Siehe [Einstellen der Optionen in Konfigurationsdateien auf einem Linux-Desktop](#).
- Sie müssen die Clientpakete für den Zugriff auf freigegebenen Netzwerkspeicher installieren. Installieren Sie auf einem Ubuntu 18.04-System beispielsweise das Paket `nfs-common` für NFS-fähigen freigegebenen Speicher und das Paket `cifs-utils` für Samba-fähigen Speicher.

## Installieren von Dynamic Environment Manager

Wenn Sie mit HorizonIntelligente Richtlinien das Verhalten der Funktionen auf einem Linux-Remote-Desktop steuern möchten, müssen Sie Dynamic Environment Manager 9.4 oder höher auf einem Windows-Remote-Desktop installieren.

Das Dynamic Environment Manager-Installationsprogramm steht auf der VMware-Downloads-Seite zum Herunterladen zur Verfügung. Sie können die Komponente der Dynamic Environment Manager-Verwaltungskonsole auf jedem Windows-Desktop installieren, von dem aus Sie die Dynamic Environment Manager-Umgebung verwalten möchten. Über die Dynamic Environment Manager-Verwaltungskonsole auf einem Windows-Desktop können Sie das Verhalten von Remote-Desktop-Funktionen auf einem Linux-Remote-Desktop steuern.

Für einen RDS-Desktop-Pool installieren Sie Dynamic Environment Manager auf dem RDS-Host, der die veröffentlichten Desktop-Sitzungen bereitstellt.

Informationen zu den Systemanforderungen von Dynamic Environment Manager und die kompletten Installationsanweisungen finden Sie im Dokument *Installieren und Konfigurieren von VMware Dynamic Environment Manager*.

## Konfigurieren von Dynamic Environment Manager

Sie müssen Dynamic Environment Manager konfigurieren, ehe Sie damit intelligente Richtlinien für Remote-Desktop-Funktionen erstellen können.

Zum Konfigurieren von Dynamic Environment Manager führen Sie die entsprechenden Anweisungen in *Administratorhandbuch zu VMware Dynamic Environment Manager* aus.

## Einstellungen für intelligente Horizon-Richtlinien

Sie können das Verhalten von Remote-Funktionen in Dynamic Environment Manager durch Erstellen einer intelligenten Horizon-Richtlinie steuern.

Sie können Richtlinien für Benutzerumgebungseinstellungen erstellen, die das Verhalten der USB-Umleitung, des virtuellen Drucks, der Zwischenablageumleitung, der Clientlaufwerksumleitung, der Web- und Chrome-Dateiübertragungsfunktionen sowie der Bandbreitenprofile in einem veröffentlichten Desktop oder einer veröffentlichten Anwendung bestimmen. Horizon Smart-Richtlinien für Benutzerumgebungseinstellungen werden während der Anmeldung angewendet und können während der erneuten Verbindung einer Sitzung aktualisiert werden. Um Horizon Smart-Richtlinien erneut anzuwenden, wenn Benutzer erneut eine Verbindung zu einer Sitzung herstellen, können Sie eine ausgelöste Aufgabe konfigurieren. Weitere Informationen finden Sie in der vollständigen Liste der Richtlinien im Thema „Konfigurieren von Horizon Smart-Richtlinien für Benutzerumgebungseinstellungen“ im *Administratorhandbuch für VMware Dynamic Environment Manager*.

Sie können Richtlinien für Computerumgebungseinstellungen erstellen, die von Dynamic Environment Manager angewendet werden, während der Computer von Endbenutzern gestartet wird. Diese intelligenten Horizon-Richtlinien steuern das Verhalten der Flash-Multimediaumleitung, des integrierten Drucks und der USB-Umleitung. Horizon Smart-Richtlinien für Computerumgebungseinstellungen werden während des Computerstarts angewendet und können während der erneuten Verbindung einer Sitzung aktualisiert werden. Weitere Informationen finden Sie in der vollständigen Liste der Richtlinien im Thema „Konfigurieren von Horizon Smart-Richtlinien für Computerumgebungseinstellungen“ im *Administratorhandbuch für VMware Dynamic Environment Manager*.

Im Allgemeinen überschreiben Einstellungen für intelligente Horizon-Richtlinien, die Sie für Remote-Funktionen in Dynamic Environment Manager konfiguriert haben, die entsprechenden Registrierungsschlüssel und Gruppenrichtlinieneinstellungen.

## Hinzufügen von Bedingungen zu intelligenten Horizon-Richtliniendefinitionen

Wenn Sie eine intelligente Horizon-Richtlinie in Dynamic Environment Manager definieren, können Sie Bedingungen hinzufügen, die erfüllt sein müssen, damit die Richtlinie wirksam wird. Sie können beispielsweise eine Bedingung hinzufügen, mit der die Clientlaufwerksumleitung nur dann deaktiviert wird, wenn ein Benutzer von einem Gerät außerhalb des Unternehmensnetzwerks eine Verbindung mit dem Remote-Desktop herstellt.

---

**Wichtig** Sie müssen der Definition einer intelligenten Horizon-Richtlinie die folgenden Bedingungen hinzufügen, damit die unterstützten Richtlinieneinstellungen an einem Linux-Remote-Desktop wirksam werden. Es werden aktuell nur diese Bedingungen unterstützt. Wenn andere Bedingungen festgelegt sind, lautet das Ergebnis der Bewertung der Bedingung „false“.

---

**Tabelle 6-3. Erforderliche Bedingungen für Linux-Remote-Desktops**

Bedingung	Beschreibung
Operating System Architecture	Prüft die Architektur des Betriebssystems. Der Wert muss auf „Linux“ festgelegt werden.
Endpoint IP address	Prüft, ob die IP-Adresse des Endpunkts im angegebenen Bereich liegt oder nicht. Leere Felder am Anfang des Bereichs werden als 0 interpretiert und leere Felder am Ende als 255.

Sie können jedoch mehrere Endpoint IP address-Bedingungen festlegen, wie im folgenden Beispiel gezeigt wird.

```
Operating system is Linux
AND Endpoint IP address is in range 11.22.33.44 – 11.22.33.54
OR Endpoint IP address is in range 11.22.33.66 – 11.22.33.77
```

Detaillierte Informationen zum Hinzufügen und Bearbeiten von Bedingungen in der Dynamic Environment Manager-Verwaltungskonsolle finden Sie unter *Administratorhandbuch zu VMware Dynamic Environment Manager*.

## Erstellen einer intelligenten Horizon-Richtlinie in Dynamic Environment Manager

Mit der Dynamic Environment Manager Management Console können Sie eine intelligente Horizon-Richtlinie in Dynamic Environment Manager erstellen. Wenn Sie eine intelligente Horizon-Richtlinie definieren, können Sie Bedingungen hinzufügen, die erfüllt sein müssen, damit die intelligente Richtlinie wirksam wird.

### Voraussetzungen

- Installieren und konfigurieren Sie Dynamic Environment Manager. Siehe [Installieren von Dynamic Environment Manager](#) und [Konfigurieren von Dynamic Environment Manager](#).
- Machen Sie sich mit den Bedingungen vertraut, die Sie den Definitionen einer intelligenten Horizon-Richtlinie hinzufügen können. Siehe [Hinzufügen von Bedingungen zu intelligenten Horizon-Richtliniendefinitionen](#).
- Aktivieren Sie die Option DEMEnable und konfigurieren Sie die Option DEMNetworkPath in Datei /etc/vmware/viewagent-custom.conf. Siehe [Einstellen der Optionen in Konfigurationsdateien auf einem Linux-Desktop](#).

**Hinweis** Warten Sie nach dem Speichern Ihrer neuen oder aktualisierten intelligenten Richtlinie in einem Netzwerk mit hoher Latenz mindestens eine Minute, bis der Dynamic Environment Manager die Verarbeitung der Änderungen abgeschlossen hat, bevor Sie die Endbenutzer anweisen, sich mit den betroffenen Desktops zu verbinden.

Sie können Richtlinien für Benutzerumgebungseinstellungen erstellen, die das Verhalten der USB-Umleitung, des virtuellen Drucks, der Zwischenablageumleitung, der Clientlaufwerksumleitung, der Web- und Chrome-Dateiübertragungsfunktionen sowie der Bandbreitenprofile in einem veröffentlichten Desktop oder einer veröffentlichten Anwendung bestimmen. Horizon Smart-Richtlinien für



Benutzerumgebungseinstellungen werden während der Anmeldung angewendet und können während der erneuten Verbindung einer Sitzung aktualisiert werden. Um Horizon Smart-Richtlinien erneut anzuwenden, wenn Benutzer erneut eine Verbindung zu einer Sitzung herstellen, konfigurieren Sie eine ausgelöste Aufgabe.

Sie können Richtlinien für Computerumgebungseinstellungen erstellen, die von Dynamic Environment Manager angewendet werden, während der Computer von Endbenutzern gestartet wird. Diese intelligenten Horizon-Richtlinien steuern das Verhalten der Flash-Multimediaumleitung, des integrierten Drucks und der USB-Umleitung. Horizon Smart-Richtlinien für Computerumgebungseinstellungen werden während des Computerstarts angewendet und können während der erneuten Verbindung einer Sitzung aktualisiert werden.

Umfassende Informationen zur Verwendung der Dynamic Environment Manager Management Console finden Sie im Dokument *Administratorhandbuch zu VMware Dynamic Environment Manager*.

## Verfahren

- 1 Wählen Sie in der Dynamic Environment Manager-Verwaltungskonsole die **Benutzerumgebung** aus, um eine Richtlinie für Benutzerumgebungseinstellungen zu erstellen, oder die Registerkarte **Computerumgebung**, um eine Richtlinie für Computerumgebungseinstellungen zu erstellen.

Falls Definitionen intelligenter Horizon-Richtlinien vorhanden sind, werden diese im Bereich „Intelligente Horizon-Richtlinien“ angezeigt.

- 2 Wählen Sie **Horizon Smart-Richtlinien** aus und klicken Sie auf **Erstellen**, um eine neue intelligente Richtlinie zu erstellen.

- 3 Aktivieren Sie die Registerkarte **Einstellungen**, und legen Sie die Einstellungen der intelligenten Richtlinie fest.

- a Geben Sie im Abschnitt „Allgemeine Einstellungen“ im Textfeld **Name** einen Namen für die intelligente Richtlinie ein.

Wenn beispielsweise die intelligente Richtlinie einen Einfluss auf die Clientlaufwerksumleitung hat, können Sie die intelligente Richtlinie „CLU“ nennen.

- b Wählen Sie im Abschnitt „Intelligente Horizon-Richtlinieneinstellungen“ die Remote-Desktop-Funktionen und -Einstellungen aus, die Sie in die intelligente Richtlinie aufnehmen möchten.

Sie können mehrere Remote-Desktop-Funktionen auswählen.

- 4 Geben Sie die Bedingungen ein, die zur Verwendung der neuen intelligenten Richtlinie an Linux Remote-Desktops erforderlich sind.

- a Wählen Sie die Registerkarte **Bedingungen** aus, klicken Sie auf **Hinzufügen** und wählen Sie die Bedingung **Betriebssystemarchitektur** aus.

- b Legen Sie den Wert auf **Linux** fest.

Operating System is Linux

- c Klicken Sie auf **Hinzufügen** und wählen Sie die Bedingung **IP-Adresse des Endpunkts** aus.

Der Operator **UND** wird standardmäßig hinzugefügt.

- d Legen Sie im Dialogfeld „IP-Adresse des Endpunkts“ den Bereich für die IP-Adresse des Endpunkts fest und klicken Sie auf **OK**.

Es folgt ein Beispiel der Bedingungsangabe.

```
Operating System is Linux
AND Endpoint IP address is in range 11.22.33.44 – 11.22.33.54
```

- 5 Klicken Sie auf **Speichern**, um die intelligente Richtlinie zu speichern.

Dynamic Environment Manager verarbeitet die intelligente Horizon-Richtlinie jedes Mal, wenn ein Benutzer eine Verbindung mit dem Remote-Desktop herstellt oder erneut herstellt.

Dynamic Environment Manager verarbeitet mehrere intelligente Richtlinien in alphabetischer Reihenfolge basierend auf den Richtliniennamen. Die intelligenten Horizon-Richtlinien werden im Bereich „Intelligente Horizon-Richtlinien“ in alphabetischer Reihenfolge angezeigt. Wenn es bei den intelligenten Richtlinien zu Konflikten kommt, hat die zuletzt verarbeitete intelligente Richtlinie Vorrang. Beispiel: Angenommen, es gibt eine intelligente Richtlinie namens „Sue“, die die USB-Umleitung aktiviert, und eine andere intelligente Richtlinie namens „Pool“, die die USB-Umleitung für einen Desktop-Pool „Ubuntu1604“ deaktiviert. Da die intelligente Richtlinie „Sue“ als Letztes verarbeitet wurde, wird die USB-Umleitungsfunktion aktiviert, wenn Sue eine Verbindung zu einem Remote-Desktop im Ubuntu1604-Desktop-Pool herstellt.

## Beispiel für Blast-Einstellungen für Linux-Desktops

Sie können die Bildqualität Ihrer Remote-Desktop-Anzeige anpassen, um die Benutzerfreundlichkeit zu verbessern. Durch die Anpassung der Bildqualität können Sie im Fall schlechter Netzwerkverbindungen eine durchgängige Benutzerfreundlichkeit sicherstellen.

## Beispiel für VMware Blast Extreme-Protokolleinstellungen

VMwareBlastServer und seine zugehörigen Plug-ins verwenden die Konfigurationsdatei `/etc/vmware/config`.

**Tabelle 6-4. Beispiel für Blast-Konfigurationsoptionen in `/etc/vmware/config`**

Name der Option	Parameter	Hochgeschwindigkeits-LAN	LAN	Dedizierte WAN	Breitband-WAN	Langsames WAN	Extrem langsam
Bandbreiteneinstellungen	RemoteDisplay.maxBandwidthKbps	1000000 (1 GBit/s)	1000000 (1 GBit/s)	1000000 (1 GBit/s)	5000 (5 MBit/s)	2000 (2 MBit/s)	1000 (1 MBit/s)
Maximale FPS	RemoteDisplay.maxFPS	60	30	30	20	15	5
Audiowiedergabe	RemoteDisplay.allowAudio	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE

**Tabelle 6-4. Beispiel für Blast-Konfigurationsoptionen in /etc/vmware/config (Fortsetzung)**

Name der Option	Parameter	Hochgeschwindigkeit-LAN		Dedizierte WAN	Breitband-WAN	Langsames WAN	Extrem langsam
		LAN	LAN				
Anzeigequalität (JPEG/PNG)	RemoteDisplay.maxQualityJPEG	90	90	90	70	60	50
Anzeigequalität (JPEG/PNG)	RemoteDisplay.midQualityJPEG	35	35	35	35	35	35
Anzeigequalität (JPEG/PNG)	RemoteDisplay.minQualityJPEG	25	25	25	20	20	20
Anzeigequalität (H.264)	RemoteDisplay.qpmaxH264	28	36	36	36	36	42
Anzeigequalität (H.264)	RemoteDisplay.qpminH264	10	10	10	10	10	10

## Beispiel für Optionen der Clientlaufwerksumleitung für Linux-Desktops

Durch Konfiguration der Optionen für die Clientlaufwerksumleitung (Client Drive Redirection, CDR) können Sie festlegen, ob auf die freigegebenen Ordner und Laufwerke eines lokalen Systems von Linux-Remote-Desktops aus zugegriffen werden kann.

Konfigurieren Sie CDR-Einstellungen durch Hinzufügen von Einträgen zur Datei /etc/vmware/config.

Mit dem nachfolgenden Konfigurationsbeispiel werden die Ordner D:\ebooks und C:\spreadsheets freigegeben, wobei beide Ordner schreibgeschützt sind. Außerdem können vom Client keine weiteren Ordner freigegeben werden.

```
cdserver.forcedByAdmin=true
cdserver.sharedFolders=d:\ebooks,;c:\spreadsheets,
cdserver.permissions=R
```

Im vorhergehenden Beispiel wurde das Komma „**,**“ nach **ebooks** platziert. **spreadsheets** ist obligatorisch für eine korrekte Optionsanalyse.

Ein „**R**“ in der `cdserver.sharedFolders`-Option hat Auswirkungen auf alle in dieser Einstellung aufgeführten Ordner. Im folgenden Beispiel sind die Ordner **ebooks** und **spreadsheets** schreibgeschützt, auch wenn der **R**-Wert nur nach dem Ordnerpfad **/home/jsmith** platziert wird.

```
cdserver.sharedFolders=d:\ebooks,;c:\spreadsheets,;/home/jsmith,R
```

# Erstellen und Verwalten von Linux-Desktop-Pools

# 7

Um virtuelle Linux-Maschinen für die Verwendung als Remote-Desktops zu konfigurieren, müssen Sie einen Desktop-Pool mit virtuellen Linux-Maschinen erstellen.

Horizon für Linux unterstützt die folgenden Typen von Desktop-Pools:

- Manueller Desktop-Pool mit virtueller vCenter-Maschine
- Automatisierter Full-Clone-Desktop-Pool
- Dynamischer Instant-Clone-Desktop-Pool

Um einen manuellen Desktop-Pool mit einer virtuellen vCenter-Maschine zu erstellen, müssen Sie auf allen virtuellen Maschinen Horizon Agent installieren. Verwenden Sie dann den Verbindungsserver-Assistenten für das Erstellen von Desktop-Pools, um die virtuellen Maschinen zum Desktop-Pool hinzuzufügen. Informationen zum Klonen einer großen Anzahl virtueller Maschinen finden Sie unter [Überblick über die Massenbereitstellung von Linux-Desktops](#).

Um einen automatisierten Full-Clone-Desktop-Pool zu erstellen, müssen Sie Horizon 7 auf einer Linux-VM-Vorlage installieren. Verwenden Sie dann den Verbindungsserver-Assistenten für das Erstellen von Desktop-Pools, um die vollständig virtuellen Maschinen zu klonen.

Um einen dynamischen Instant-Clone-Desktop-Pool zu erstellen, müssen Sie Horizon 7 Agent auf einer virtuellen Linux-Maschine mit eingerichteter PBISO-Umgebung installieren und daraus eine Vorlage erstellen. Erstellen Sie dann mit dem Assistenten zur Erstellung von Desktop-Pools des Verbindungsservers einen dynamischen Instant-Clone-Desktop-Pool.

Dieses Kapitel enthält die folgenden Themen:

- [Erstellen eines manuellen Desktop-Pools für Linux](#)
- [Verwalten von Linux-Desktop-Pools](#)
- [Erstellen eines automatisierten Full-Clone-Desktop-Pools für Linux](#)
- [Erstellen eines dynamischen Instant-Clone-Desktop-Pools für Linux](#)
- [Broker-PowerCLI-Befehle](#)

# Erstellen eines manuellen Desktop-Pools für Linux

Sie können einen manuellen Desktop-Pool für virtuelle Linux-Maschinen erstellen.

Das folgende Verfahren enthält Richtlinien zur Konfiguration der obligatorischen Einstellungen für einen Linux-basierten manuellen Desktop-Pool. Weitere Informationen zum Erstellen von manuellen Desktop-Pools finden Sie unter *Einrichten von virtuellen Desktops in Horizon Console*.

## Voraussetzungen

- Stellen Sie sicher, dass Horizon View Agent auf dem Linux-Gastbetriebssystem installiert ist. Siehe [Installieren von Horizon Agent auf einer virtuellen Linux-Maschine](#).
- Prüfen Sie, ob VMware vCenter Server zu Horizon Connection Server hinzugefügt wurde.

## Verfahren

- 1 Fügen Sie in Horizon Console einen manuellen Desktop-Pool hinzu.

Wählen Sie **Bestandsliste > Desktops > Hinzufügen** aus.

---

**Hinweis** Virtuelle Windows- und Linux-Maschinen dürfen nicht im selben Desktop-Pool erstellt werden.

---

- 2 Wählen Sie **Manueller Desktop-Pool** aus.
- 3 Wählen Sie virtuelle Maschinen aus, die von vCenter Server entweder verwaltet oder nicht verwaltet werden, und klicken Sie auf **Weiter**.
- 4 Wählen Sie entweder dedizierte oder flexible Benutzerzuweisungen für die Maschinen im Desktop-Pool aus und klicken Sie auf **Weiter**.
- 5 Folgen Sie den Anweisungen des Assistenten, um den Pool zu erstellen.

Legen Sie auf der Seite „Desktop-Pool-Einstellungen“ die folgenden Optionen fest.

Option	Beschreibung
Standardanzeigeprotokoll	VMware Blast
Benutzern die Wahl des Protokolls erlauben	Nein
3D-Renderer	Verwalten Sie vSphere Client für 2D- oder vDGA-Desktop und NVIDIA GRID vGPU für vGPU-Desktop.

---

**Hinweis** Die Pool-Einstellungen sind obligatorisch. Andernfalls treten bei der Verbindung zum Desktop möglicherweise Fehler auf und es wird ein Protokollfehler oder ein schwarzer Bildschirm angezeigt.

---

- 6 Erteilen Sie nach dem Erstellen des Desktop-Pools Benutzern die Berechtigung für die Maschinen im Desktop-Pool. Wählen Sie in Horizon Console den Desktop-Pool aus, wählen Sie **Berechtigungen > Berechtigung hinzufügen** und fügen Sie Benutzer oder Gruppen hinzu.

Die virtuellen Linux-Maschinen stehen dann für die Verwendung als Remote-Desktops in einer Horizon 7-Bereitstellung zur Verfügung.

## Verwalten von Linux-Desktop-Pools

Beim Erstellen eines manuellen Desktop-Pools und Hinzufügen von Linux-Maschinen zum Pool können Sie die manuellen Desktop-Pools verwalten, indem Sie die Einstellungen konfigurieren. Sie müssen nur Linux-Gastbetriebssysteme zum manuellen Desktop-Pool hinzufügen. Wenn der Pool sowohl virtuelle Windows- als auch virtuelle Linux-Gastbetriebssysteme enthält, wird der Pool als Windows-Pool behandelt und kann nicht mit Linux-Desktops verbunden werden.

## Unterstützung für das Verwalten von Vorgängen

- Deaktivieren oder Aktivieren eines Desktop-Pools
- Klonen eines automatisierten Desktop-Pools
- Löschen eines Desktop-Pools

Sie können virtuelle Maschinen aus Horizon 7 entfernen oder vom Datenträger löschen.

## Unterstützung für Remote-Einstellungen

**Tabelle 7-1. Remote-Einstellungen**

Remote-Einstellung	Optionen
Betriebsrichtlinie für Remote-Computer	<ul style="list-style-type: none"> <li>■ Keine Betriebsaktion vornehmen</li> <li>■ Computer müssen immer eingeschaltet sein</li> <li>■ Anhalten</li> <li>■ Ausschalten</li> </ul>
Automatic logoff after disconnect (Nach Verbindungstrennung automatisch abmelden)	<ul style="list-style-type: none"> <li>■ Sofort</li> <li>■ Nie</li> <li>■ Nach n Minuten</li> </ul>
Benutzern das Zurücksetzen/den Neustart ihrer Computer gestatten	<ul style="list-style-type: none"> <li>■ Ja</li> <li>■ Nein</li> </ul>
Benutzer darf separate Sitzungen von unterschiedlichen Client-Geräten aus starten	<ul style="list-style-type: none"> <li>■ Ja</li> <li>■ Nein</li> </ul>
Löschen der Maschine nach der Abmeldung für automatisierten Desktop-Pool mit Full-Clone und Floating	<ul style="list-style-type: none"> <li>■ Ja</li> <li>■ Nein</li> </ul>

## Unterstützung für Horizon Console-Vorgänge

- Sitzung trennen
- Logoff Session (Von Sitzung abmelden)
- Desktop neu starten/zurücksetzen

- Nachricht senden

Für einen dedizierten Desktop-Pool können Sie eine Benutzerzuweisung für jede virtuelle Maschine hinzufügen oder entfernen. Bei einer großen Anzahl an Vorgängen müssen Sie Horizon-PowerCLI-Cmdlets verwenden.

- Update-UserOwnership
- Remove-UserOwnership

**Hinweis** Lassen Sie die Einstellungen für das **Remote-Anzeigeprotokoll** unverändert. Diese Einstellungen müssen bei der Erstellung des Desktop-Pools identisch sein.

Einstellung	Option
Standardanzeigeprotokoll	VMware Blast
Benutzern die Wahl des Protokolls erlauben	Nein
3D-Renderer	<ul style="list-style-type: none"> <li>■ Verwaltung mithilfe von vSphere Client für 2D oder vDGA</li> <li>■ NVIDIA GRID vGPU</li> </ul>

Weitere Informationen finden Sie in der Dokumentation *Verwaltung der VMware Horizon Console*.

## Erstellen eines automatisierten Full-Clone-Desktop-Pools für Linux

Sie können einen automatisierten Full-Clone-Desktop-Pool für Linux erstellen. Nachdem Sie den automatisierten Full-Clone-Desktop-Pool erstellt haben, können Sie die virtuellen Linux-Maschinen als Remote-Desktops in einer Horizon 7-Bereitstellung verwenden.

Das folgende Verfahren enthält Richtlinien zur Konfiguration der obligatorischen Einstellungen für einen Linux-basierten automatisierten Full-Clone-Desktop-Pool. Weitere Informationen zum Erstellen automatisierter Full-Clone-Desktop-Pools finden Sie unter *Einrichten von virtuellen Desktops in Horizon Console*.

### Voraussetzungen

- Stellen Sie sicher, dass Horizon View Agent auf dem Linux-Gastbetriebssystem installiert ist. Siehe [Installieren von Horizon Agent auf einer virtuellen Linux-Maschine](#).
- Bevor Sie eine virtuelle Maschine klonen können, erstellen Sie als Grundlage für die Klone eine Vorlage für virtuelle Maschinen. Siehe [Erstellen einer Vorlage für virtuelle Maschinen zum Klonen von Linux-Desktop-Maschinen](#).
- Wenn Sie die Winbind-Lösung nutzen, um die virtuelle Linux-Maschine zu Active Directory beitreten zu lassen, müssen Sie die Konfiguration der Winbind-Lösung in der Vorlage der virtuellen Maschine durchführen.

- Wenn Sie die Winbind-Lösung verwenden, müssen Sie auf der virtuellen Maschine den Befehl für den Beitritt zur Domäne ausführen. Fügen Sie den Befehl in ein Shell-Skript ein und geben Sie den Skriptpfad zur Horizon Agent-Option RunOnceScript in `/etc/vmware/viewagent-custom.conf` an. Weitere Informationen finden Sie unter [Einstellen der Optionen in Konfigurationsdateien auf einem Linux-Desktop](#).
- Prüfen Sie, ob vCenter Server zum Horizon-Verbindungsserver hinzugefügt wurde.

## Verfahren

- 1 Erstellen Sie eine Anpassungsspezifikation für das Gastbetriebssystem.

Erläuterungen finden Sie unter „Erstellen einer Anpassungsspezifikation für Linux im vSphere Web Client“ im Dokument *Verwaltung virtueller vSphere-Maschinen*. Für die Erstellung einer Spezifikation müssen die folgenden Einstellungen korrekt festgelegt werden.

Einstellung	Wert
Betriebssystem der virtuellen Zielmaschine	Linux
Computername	Verwenden Sie den Namen der virtuellen Maschine.
Domäne	Geben Sie die Domäne der Horizon 7-Umgebung an.
Netzwerkeinstellungen	Verwenden Sie die Standardnetzwerkeinstellungen.
Primäres DNS	Geben Sie eine gültige Adresse an.

**Hinweis** Weitere Informationen zur Unterstützungsmatrix für die Gastbetriebssystemanpassung finden Sie unter <http://partnerweb.vmware.com/programs/guestOS/guest-os-customization-matrix.pdf>.

- 2 Fügen Sie in Horizon Console einen automatisierten Desktop-Pool hinzu.  
Wählen Sie **Bestandsliste > Desktops > Hinzufügen** aus.
- 3 Wählen Sie **Automatisierter Desktop-Pool** aus und klicken Sie auf **Weiter**.
- 4 Wählen Sie **Vollständige virtuelle Maschinen** aus und anschließend die vCenter Server-Instanz. Klicken Sie dann auf **Weiter**.



## 5 Folgen Sie den Anweisungen des Assistenten, um den Pool zu erstellen.

- a Legen Sie auf der Seite „Desktop-Pool-Einstellungen“ die folgenden Optionen fest.

Option	Beschreibung
Standardanzeigeprotokoll	VMware Blast
Benutzern die Wahl des Protokolls erlauben	Nein
3D-Renderer	Verwalten Sie vSphere Client für 2D- oder vDGA-Desktop und NVIDIA GRID vGPU für vGPU-Desktop.

- b Wenn Sie dazu aufgefordert werden, legen Sie die Optionen für die **Benennung virtueller Maschinen** fest.

Option	Beschreibung
Namen manuell angeben	Geben Sie Namen manuell ein.
Benennungsmuster	Geben Sie z. B. LinuxVM-{n} an. Sie müssen außerdem die folgenden Optionen für die Größe des Desktop-Pools angeben: <ul style="list-style-type: none"> <li>■ Maximale Anzahl an Maschinen</li> <li>■ Anzahl an eingeschalteten Reservemaschinen</li> </ul>

- c Wenn Sie dazu aufgefordert werden, wählen Sie die vCenter Server-Einstellungen nacheinander aus.

Sie können keine der vCenter Server-Einstellungen überspringen:

- 1 Vorlage
  - 2 Speicherort des VM-Ordners
  - 3 Host or cluster (Host oder Cluster)
  - 4 Ressourcenpool
  - 5 Datenspeicher
- 6 Erteilen Sie nach dem Erstellen des Desktop-Pools Benutzern die Berechtigung für die Maschinen im Desktop-Pool. Wählen Sie in Horizon Console den Desktop-Pool aus, wählen Sie **Berechtigungen** > **Berechtigung hinzufügen** und fügen Sie Benutzer oder Gruppen hinzu.
- 7 Warten Sie, bis alle virtuellen Linux-Maschinen im Desktop-Pool verfügbar sind.

## Erstellen eines dynamischen Instant-Clone-Desktop-Pools für Linux

Sie können einen dynamischen Instant-Clone-Desktop-Pool für virtuelle Linux-Maschinen mithilfe des Assistenten **Desktop-Pool hinzufügen** erstellen. Nach dem Erstellen eines dynamischen Instant-Clone-

Desktop-Pools haben Sie die Möglichkeit, die virtuellen Linux-Maschinen als Remote-Desktops in einer Horizon 7-Bereitstellung zu verwenden.

Horizon 7 Agent für Linux unterstützt Instant-Clone-Desktop-Pools nur auf Systemen mit Ubuntu 18.04/16.04, RHEL 7.1 oder höher, RHEL 8.0 oder SLED/SLES 12.x.

---

**Hinweis** vGPU-Grafikfunktionen werden auf Instant-Clone-Desktop-Pools, die von Linux-Desktops erstellt wurden, nicht unterstützt.

---

Das folgende Verfahren enthält Richtlinien zur Konfiguration der obligatorischen Einstellungen für einen Linux-basierten Instant-Clone-Desktop-Pool. Weitere Informationen zum Erstellen von Instant-Clone-Desktop-Pools finden Sie unter *Einrichten von virtuellen Desktops in Horizon Console*.

### Voraussetzungen

- Machen Sie sich mit den Schritten für das Erstellen virtueller Maschinen in vCenter Server und mit der Installation von Linux-Betriebssystemen vertraut. Weitere Informationen finden Sie unter [Erstellen einer virtuellen Maschine und Installieren von Linux](#).
- Machen Sie sich mit den Schritten zur AD-Integration mithilfe der PBISO-Authentifizierungslösung oder dem Samba Winbind-Offlinebeitritt vertraut. Weitere Informationen finden Sie unter [PowerBroker Identity Services Open\(PBISO\)-Authentifizierung konfigurieren](#) oder [Konfigurieren des Samba-Offline-Domänenbeitritts](#).

---

**Hinweis** Um einen Instant-Clone-Desktop-Pool von einer virtuellen Linux-Maschine zu erstellen, auf der RHEL 8.0 ausgeführt wird, führen Sie die AD-Integration mithilfe des Samba Winbind-Offlinebeitritts durch. Instant-Clone-Desktop-Pools werden für virtuelle RHEL 8.0-Maschinen, die die PBISO-Authentifizierung verwenden, nicht unterstützt.

---

- Machen Sie sich mit den Installationsschritten für Horizon 7 Agent for Linux vertraut. Weitere Informationen finden Sie unter [Installieren von Horizon Agent auf einer virtuellen Linux-Maschine](#).
- Machen Sie sich mit den Schritten zum Erstellen eines Snapshots einer ausgeschalteten Linux-VM mithilfe von VMware vSphere Web Client vertraut. Weitere Informationen finden Sie unter „Erstellen eines Snapshots in VMware Host Client“ in *Verwaltung eines einzelnen Hosts von vSphere – VMware Host Client*.
- Prüfen Sie, ob vCenter Server zum Horizon-Verbindungsserver hinzugefügt wurde.

### Verfahren

- 1 Erstellen Sie eine Linux-VM mit installiertem Ubuntu 18.04/16.04, RHEL 7.1 oder höher, RHEL 8.0 oder SLED/SLES 12.x.

Weitere Informationen finden Sie unter [Erstellen einer virtuellen Maschine und Installieren von Linux](#).

- 2 Installieren Sie Open VMware Tools (OVT) manuell auf Ihrem Ubuntu 18.04/16.04-Computer, indem Sie den folgenden Befehl ausführen:

```
# apt-get install open-vm-tools
```

Weitere Informationen finden Sie unter [Vorbereiten einer Linux-Maschine für die Remote-Desktop-Bereitstellung](#).

- 3 Installieren Sie alle für die Linux-Distribution erforderlichen Abhängigkeitspakete.

Weitere Informationen finden Sie unter [Installieren von Abhängigkeitspaketen für Horizon Agent](#).

- 4 Installieren Sie Horizon Agent for Linux in der Linux-VM.

```
# sudo ./install_viewagent.sh -A yes
```

Ausführliche Informationen dazu finden Sie unter [Installieren von Horizon Agent auf einer virtuellen Linux-Maschine](#).

- 5 Integrieren Sie Ihre Linux-VM in Active Directory.

- Für die Verwendung der PBISO-Authentifizierungslösung führen Sie die folgenden Schritte aus:

- a Laden Sie PBIS Open 8.5.6 oder höher aus <https://www.beyondtrust.com/products/powerbroker-identity-services-open/> herunter und installieren Sie es in Ihrer Linux-VM.

```
# sudo ./pbis-open-8.5.6.2029.linux.x86_64.deb.sh
```

- b Integrieren Sie Ihre Linux-VM in Active Directory mithilfe der Erläuterungen im Abschnitt „PBISO-Authentifizierung (PowerBroker Identity Services Open)“ im Dokument [Integrieren von Linux mit Active Directory](#).

- Um den Samba Winbind-Offlinebeitritt zu verwenden, setzen Sie `OfflineJoinDomain` in der Datei `/etc/vmware/viewagent-custom.conf` auf **samba**.

---

**Hinweis** Sie müssen Samba Winbind verwenden, um eine RHEL 8.0-VM in Active Directory zu integrieren. Andernfalls kann kein dynamischer Instant-Clone-Desktop-Pool erstellt werden.

---

- Wenn Sie den Offline-Domänenbeitritt deaktivieren möchten, müssen Sie in der Datei `/etc/vmware/viewagent-custom.conf` die Option `OfflineJoinDomain` auf **none** setzen. Andernfalls kann kein dynamischer Instant-Clone-Desktop-Pool erstellt werden.

- 6 Wenn Ihr DHCP-Server nicht an einen DNS-Server sendet, geben Sie einen DNS-Server für Ihr Linux-System an.

Beim Erstellen einer neuen Instant-Clone-VM wird ein neuer virtueller Netzwerkadapter hinzugefügt. Wenn der neue Netzwerkadapter der Instant-Clone-VM hinzugefügt wird, gehen alle Einstellungen im Netzwerkadapter wie z. B. der DNS-Server in der VM-Vorlage verloren. PBIS erfordert einen gültigen DNS-Server. Die FQDN-Zuordnung in `/etc/hosts` wird nicht akzeptiert. Um den Verlust der DNS-

Server-Einstellung beim Hinzufügen des neuen Netzwerkadapters zur geklonten VM zu vermeiden, müssen Sie in Ihrem Linux-System einen DNS-Server angeben. Geben Sie beispielsweise in einem Ubuntu 16.04-System den DNS-Server durch Hinzufügen der im Folgenden aufgeführten Zeilen in der Datei `/etc/resolvconf/resolv.conf.d/head` an.

```
nameserver 10.10.10.10
search mydomain.org
```

- 7 (Optional) Wenn Sie der Datei `/etc/fstab` ein NFS Mount vom Master-Linux-VDI-Instant-Clone-Agenten hinzufügen möchten, stehen Ihnen die im Folgenden aufgeführten Möglichkeiten zur Verfügung.

- Fügen Sie zu `/etc/fstab` ein „Soft“-Flag hinzu, z. B.:

```
10.111.222.333:/share /home/nfsmount nfs
size=8192,wsiz=8192,timeo=14,soft,intr,tcp
```

- Ohne „Soft“-Flag in `/etc/fstab` können Sie die Datei `/etc/fstab` im Master-Linux-VM-Image nicht konfigurieren. Sie können ein Ausschaltskript schreiben, um die Datei `/etc/fstab` zu konfigurieren, und dann dieses Ausschaltskript für das ClonePrep-Tool angeben. Weitere Informationen finden Sie im Dokument *Verwaltung der VMware Horizon Console*.

- 8 Fahren Sie die Linux-VM herunter und legen Sie ein Master-Image durch Erstellen eines Snapshots von Ihrer ausgeschalteten Linux-VM mithilfe von VMware vSphere® Web Client an.

Informationen dazu finden Sie unter „Erstellen eines Snapshots im VMware Host Client“ in *Verwaltung eines einzelnen Hosts von vSphere – VMware Host Client*.

- 9 Fügen Sie in Horizon Console einen automatisierten Desktop-Pool hinzu.

Wählen Sie **Bestandsliste > Desktops > Hinzufügen** aus.

- 10 Wählen Sie **Automatisierter Desktop-Pool** aus und klicken Sie auf **Weiter**.

- 11 Wählen Sie **Instant Clones** aus und anschließend die vCenter Server-Instanz. Klicken Sie dann auf **Weiter**.

## 12 Folgen Sie den Anweisungen des Assistenten, um den Pool zu erstellen.

- a Wenn Sie dazu aufgefordert werden, legen Sie die Optionen für die **Benennung virtueller Maschinen** fest.

Option	Beschreibung
<b>Bereitstellung aktivieren</b>	Wählen Sie diese Option aus.
<b>Bereitstellung bei Fehler abbrechen</b>	Wählen Sie diese Option aus.
<b>Benennungsmuster</b>	Geben Sie ein Muster an, dass Horizon 7 als Präfix in allen Desktop-VM-Namen verwendet, und zwar gefolgt von einer eindeutigen Zahl. Geben Sie z. B. <b>LinuxVM-{n}</b> ein.
<b>Maximale Anzahl an Computern</b>	Legen Sie gesamte Anzahl an Computern im Pool fest.
<b>Anzahl der (eingeschalteten) Reservemaschinen</b>	Legen Sie die Anzahl der Desktop-VMs fest, die für Benutzer verfügbar sein sollen.
<b>Alle Computer im Voraus bereitstellen</b>	Wählen Sie diese Option aus, damit Horizon 7 die Anzahl der VMs bereitstellt, die in <b>Maximale Anzahl an Maschinen</b> angegeben sind.

- b Wenn Sie dazu aufgefordert werden, wählen Sie **VMware Virtual SAN verwenden** als Speicherverwaltungsrichtlinie aus.
- c Wenn Sie dazu aufgefordert werden, geben Sie die Domäneneinstellung, den AD-Container und alle zusätzlichen Anpassungsskripts an, die ausgeführt werden müssen, nachdem die virtuelle Maschine geklont wurde.

**Wichtig** Wenn Sie zum Ausschalten oder nach der Synchronisierung ClonePrep-Skripts verwenden, stellen Sie sicher, dass sich die Skripts im Ordner mit `/var/userScript` im Besitz des Root-Benutzers befinden und für die Dateiberechtigungen „700“ festgelegt ist.

In Horizon Console können Sie die Desktop-VMs so anzeigen, wie sie dem Pool hinzugefügt werden. Wählen Sie hierzu **Bestandsliste > Desktops** aus.

Löschen Sie nach dem Erstellen des Pools nicht das Master-Image und entfernen Sie es auch nicht aus dem vCenter Server-Bestand, wenn der Pool vorhanden ist. Wenn Sie die Master-Image-VM versehentlich aus dem Bestand von vCenter Server entfernt haben, müssen Sie diese wieder hinzufügen und dann eine Image-Übertragung mit dem aktuellen Image durchführen.

### Nächste Schritte

Erteilen Sie Benutzern die Berechtigung für den Zugriff auf den Pool. Weitere Informationen finden Sie unter „Hinzufügen von Berechtigungen zu Desktop-Pools“ in *Einrichten von virtuellen Desktops in Horizon Console*.

## Broker-PowerCLI-Befehle

Die Horizon PowerCLI-Cmdlets, die zum Ausführen verschiedener Verwaltungsaufgaben auf dem Verbindungsserver und einem Windows-Desktop dienen, können auch auf Linux-Desktops verwendet werden.

## Erstellen eines manuellen Desktop-Pools

```
Add-ManualPool -DefaultProtocol Blast -AllowProtocolOverride $false -threadRender usevc|vgpu -
Pool_id <pool id> [more parameters]
```

Die folgenden Optionen und Werte sind für den Linux-Desktop obligatorisch.

- DefaultProtocol Blast
- AllowProtocolOverride \$false
- threadRender usevc|vgpu. Verwenden Sie bei einem vGPU-Desktop `-threadRender vgpu` und bei einem 2D-/DGA-Desktop `-threadRender usevc`.

### Beispiele

- Erstellen Sie einen dynamischen Linux-Desktop-Pool mit dem Namen „LinuxDesktop“ mit einer virtuellen Maschine (VM) namens „LinuxVM-01“.

```
Add-ManualPool -DefaultProtocol Blast -AllowProtocolOverride $false -threadRender usevc -Pool_id
LinuxDesktop -Id (Get-DesktopVM -Name LinuxVM-01).id -Persistence NonPersistent -Vc_name
myvc.myorg.org
```

- Erstellen Sie einen dedizierten Linux-vGPU-Desktop-Pool mit dem Namen „LinuxDesktop“ mit allen VMs, die mit einem VM-Namen wie „LinuxVM-“ beginnen.

```
Get-DesktopVM | Where-Object {$_.Name.StartsWith("LinuxVM-")} | Add-ManualPool -DefaultProtocol
Blast -AllowProtocolOverride $false -Persistence Persistent -threadRender vgpu -Pool_id
LinuxDesktop
```

- Erstellen Sie einen dynamischen Linux-Desktop-Pool mit dem Namen „LinuxDesktop“ mit dem ersten RHEL 6 x64 VM.

```
Get-DesktopVM | Where-Object {$_.GuestID -eq "rhel6_64Guest"} | Select-Object -Index 0 | Add-
ManualPool -DefaultProtocol Blast -AllowProtocolOverride $false -Persistence NonPersistent -
threadRender usevc -Pool_id LinuxDesktop
```

## Erstellen eines automatisierten Full-Clone-Desktop-Pools

```
Add-AutomaticPool -DefaultProtocol Blast -AllowProtocolOverride $false -threadRender usevc|vgpu `
-Pool_id <pool id> -Vc_id <vCenter id> `
-NamePrefix <VM Name Prefix> " `
-templatePath <Virtual Machine Template Path> `
-VmFolderPath <Virtual Machine Folder Path> `
-ResourcePoolPath <Resource Pool Path> `
-dataStorePaths <Datastore Path> `
-customizationSpecName <Customization Specification Name> `
[more parameters]
```

Die folgenden Optionen und Werte sind obligatorisch für Linux-Desktops.

- DefaultProtocol Blast

- `AllowProtocolOverride $false`
- `threadRender usevc|vgpu` Verwenden Sie bei einem vGPU-Desktop `-threadRender vgpu` und bei einem 2D-Desktop `-threadRender usevc`.

### Beispiel

```
Add-AutomaticPool -DefaultProtocol Blast -AllowProtocolOverride $false -threadrender usevc `
-pool_id FullClone-Linux `
-Vc_id (Get-ViewVC -serverName myvc.myorg.org).vc_id `
-NamePrefix "FullClone-{n:fixed=3}" `
-Persistence NonPersistent -deletePolicy DeleteOnUse `
-VmFolderPath "/LinuxVDI/vm/FullClone" `
-ResourcePoolPath "/LinuxVDI/host/LinuxVDICluster/Resources" `
-templatePath "/LinuxVDI/vm/LinuxTemplate" `
-dataStorePaths "/LinuxVDI/host/LinuxVDICluster/datastore" `
-customizationSpecName "linux-spec" `
-maximumCount 100
```

## Hinzufügen oder Entfernen von Desktop-Pool-Berechtigungen

- Gewähren Sie einer Domänenbenutzergruppe der Domäne „mydomain.org“ die Berechtigung für „LinuxDesktop“.

```
Add-PoolEntitlement -Pool_id LinuxDesktop -Sid (Get-User -Name "domain user" -Domain
"mydomain.org").sid
```

- Entfernen Sie die Berechtigung einer Domänenbenutzergruppe der Domäne „mydomain.org“ von „LinuxDesktop“.

```
Remove-PoolEntitlement -Pool_id LinuxDesktop -Sid (Get-User -Name "domain user" -Domain
"mydomain.org").sid
```

## Zuweisen eines Benutzers zur VM oder Entfernen eines Benutzers aus der VM in einem dedizierten Desktop-Pool

- Weisen Sie den Benutzer **myuser** der VM „LinuxVM-01“ zu, die sich in einem dedizierten Desktop-Pool befindet.

```
Update-UserOwnership -Machine_id (Get-DesktopVM -Name "LinuxVM-01").machine_id -Sid (Get-User -
Name "myuser" | Where-Object {$_.cn -eq "myuser"}).sid
```

- Entfernen Sie den Benutzer **myuser** aus der VM „LinuxVM-01“, die sich in einem dedizierten Desktop-Pool befindet.

```
Remove-UserOwnership -Machine_id (Get-DesktopVM -Name "LinuxVM-01").machine_id
```

## Abmelden der Desktop-Verbindung

- Melden Sie sich von der Desktop-Sitzung von „myuser“ ab.

```
Get-RemoteSession -Username "mydomain.org\myuser" | Send-SessionLogoff
```

Weitere Informationen zum Broker-PowerCLI-Cmdlet finden Sie unter „Verwenden des Horizon-View PowerCLI“ unter *Horizon 7-Integration*.



# Massenbereitstellung von Horizon 7 für manuelle Desktop-Pools

## 8

Mit Horizon Console können Sie automatisch einen Pool von Windows-Desktop-Maschinen erstellen, nicht jedoch von Linux-Desktop-Maschinen. Sie können jedoch Skripts entwickeln, die die Bereitstellung eines Pools von Linux-Desktop-Maschinen automatisieren.

Die zur Verfügung gestellten Beispielskripts dienen nur der Veranschaulichung. VMware übernimmt keine Verantwortung für Probleme, die im Zusammenhang mit der praktischen Anwendung der Beispielskripts auftreten.

Dieses Kapitel enthält die folgenden Themen:

- [Überblick über die Massenbereitstellung von Linux-Desktops](#)
- [Überblick über die Massenaktualisierung von Linux-Desktops](#)
- [Erstellen einer Vorlage für virtuelle Maschinen zum Klonen von Linux-Desktop-Maschinen](#)
- [Eingabedatei für die PowerCLI-Beispielskripts zur Bereitstellung von Linux-Desktops](#)
- [Beispielskript zum Klonen von virtuellen Linux-Maschinen](#)
- [Beispielskript zum Hinzufügen geklonter virtueller Maschinen zu einer AD-Domäne](#)
- [Beispielskript zum Hinzufügen geklonter virtueller Maschinen zu einer AD-Domäne mithilfe von SSH](#)
- [Beispielskript zum Hochladen von Konfigurationsdateien zu virtuellen Linux-Maschinen](#)
- [Beispielskript zum Hochladen von Konfigurationsdateien zu virtuellen Linux-Maschinen mithilfe von SSH](#)
- [Beispiel-PowerCLI-Skript zum Upgrade von Horizon Agent auf Linux-Desktop-Maschinen](#)
- [Beispielskript zur Durchführung eines Upgrades von Horizon Agent auf virtuellen Linux-Maschinen mithilfe von SSH](#)
- [Beispielskript zum Ausführen von Vorgängen auf virtuellen Linux-Maschinen](#)

# Überblick über die Massenbereitstellung von Linux-Desktops

Das Bereitstellen von manuellen Desktops für Linux umfasst verschiedene Schritte. Wenn Sie mehr als nur eine Handvoll Desktops bereitstellen möchten, können Sie einige dieser Schritte mithilfe von PowerCLI-Skripts automatisieren.

Für einige Vorgänge können Sie auswählen, ob entweder PowerCLI oder SSH die Befehle auf der Linux-Maschine ausführen soll. Die folgende Tabelle beschreibt die Unterschiede zwischen den beiden Vorgehensweisen.

PowerCLI	SSH
Es ist nicht erforderlich, zusätzliche Tools zu installieren.	<ul style="list-style-type: none"> <li>Für Ubuntu müssen Sie den SSH-Server mit dem Befehl <code>sudo apt-get install openssh-server</code> installieren. Für RHEL und CentOS wird <code>openssh-server</code> standardmäßig installiert. Sie müssen jedoch sicherstellen, dass die Firewall-Einstellungen SSH zulassen.</li> <li>Die SSH-Client-Anwendungen <code>pscp.exe</code> und <code>plink.exe</code> müssen heruntergeladen und im selben Ordner wie die PowerCLI-Skripts abgelegt werden.</li> </ul>
Das Hochladen von Dateien und die Befehlsausführung gehen langsamer vonstatten.	Das Hochladen von Dateien und die Befehlsausführung gehen schneller vonstatten.
Die Administrator-Anmeldedaten des ESXi-Hosts müssen angegeben werden.	Die Administrator-Anmeldedaten des ESXi-Hosts müssen nicht angegeben werden.
Es können keine Sonderzeichen im Administrator-Kennwort (bei Ausführung des Skripts zur Installation von Horizon Agent) oder im Kennwort des AD-Benutzers (bei Ausführung des Skripts zum Hinzufügen der Domäne) verarbeitet werden.	Es können Sonderzeichen im Administrator-Kennwort (bei Ausführung des Skripts zur Installation von Horizon Agent) oder im Kennwort des AD-Benutzers (bei Ausführung des Skripts zum Hinzufügen der Domäne) verarbeitet werden.

**Hinweis** Sowohl PowerCLI-basierte als auch SSH-basierte Skripts können Sonderzeichen in den Kennwörtern für den vCenter Server-Administrator und den Linux-Administrator verarbeiten. PowerCLI-basierte Skripts können Sonderzeichen auch im Kennwort des ESXi-Host-Administrators verarbeiten. In all diesen Fällen ist kein Escape-Zeichen erforderlich.

Weitere Informationen zu vSphere PowerCLI finden Sie unter <https://www.vmware.com/support/developer/PowerCLI>.

Die Massenbereitstellung eines Pools von Linux-Desktops umfasst die folgenden Schritte:

- 1 Erstellen Sie eine Vorlage für die virtuelle Maschine und installieren Sie Horizon Agent auf der virtuellen Maschine.  
Siehe [Erstellen einer Vorlage für virtuelle Maschinen zum Klonen von Linux-Desktop-Maschinen](#).
- 2 Erstellen Sie eine Anpassungsspezifikation für das Gastbetriebssystem.

Erläuterungen finden Sie unter „Erstellen einer Anpassungsspezifikation für Linux im vSphere Web Client“ im Dokument *Verwaltung virtueller vSphere-Maschinen*. Für die Erstellung einer Spezifikation müssen die folgenden Einstellungen korrekt festgelegt werden.

Einstellung	Wert
Betriebssystem der virtuellen Zielmaschine	Linux
Computername	Verwenden Sie den Namen der virtuellen Maschine.
Domäne	Geben Sie die Domäne der Horizon 7-Umgebung an.
Netzwerkeinstellungen	Verwenden Sie die Standardnetzwerkeinstellungen.
Primäres DNS	Geben Sie eine gültige Adresse an.

**Hinweis** Weitere Informationen zur Unterstützungsmatrix für die Gastbetriebssystemanpassung finden Sie unter <http://partnerweb.vmware.com/programs/guestOS/guest-os-customization-matrix.pdf>.

- 3 Klonen Sie virtuelle Maschinen.

Siehe [Beispielskript zum Klonen von virtuellen Linux-Maschinen](#).

- 4 Lassen Sie die geklonten VMs zur Active Directory-Domäne beitreten, sofern Sie die winbind-Lösung verwenden. Sie können den Befehl für den Beitritt zur Domäne mit den folgenden Beispielskripts ausführen oder die Option `RunOnceScript` in `/etc/vmware/viewagent-custom.conf` verwenden, die in der Vorlage für die virtuelle Maschine konfiguriert ist.

Siehe [Beispielskript zum Hinzufügen geklonter virtueller Maschinen zu einer AD-Domäne](#) oder [Beispielskript zum Hinzufügen geklonter virtueller Maschinen zu einer AD-Domäne mithilfe von SSH](#).

- 5 Aktualisieren Sie die Konfigurationsoptionen in virtuellen Maschinen.

Siehe [Beispielskript zum Hochladen von Konfigurationsdateien zu virtuellen Linux-Maschinen](#) oder [Beispielskript zum Hochladen von Konfigurationsdateien zu virtuellen Linux-Maschinen mithilfe von SSH](#).

- 6 Erstellen Sie einen Desktop-Pool.

Siehe [Erstellen eines manuellen Desktop-Pools für Linux](#).

Unter [Beispielskript zum Ausführen von Vorgängen auf virtuellen Linux-Maschinen](#) erhalten Sie ein Beispielskript, das Vorgänge wie das Einschalten, Herunterfahren, Neustarten oder Löschen virtueller Maschinen durchführt. Mit diesem Skript lassen sich virtuelle Maschinen aus vCenter Server löschen.

## Überblick über die Massenaktualisierung von Linux-Desktops

Die Massenaktualisierung von manuellen Desktops für Linux umfasst verschiedene Schritte. Sie können einige der Schritte mithilfe von PowerCLI-Skripts automatisieren.

## Massenaktualisierung eines nicht verwalteten Desktops

Um die nicht verwaltete virtuelle Maschine per Massenaktualisierung auf eine verwaltete oder nicht verwaltete virtuelle Maschine zu aktualisieren, müssen Sie das Beispielaktualisierungsskript verwenden, um den neuen Horizon Agent auf die vorhandenen virtuellen Maschinen hochzuladen, und den Aktualisierungsbefehl ausführen.

- Wenn Sie die nicht verwaltete virtuelle Maschine beibehalten, kann Ihr vorhandener Desktop-Pool wiederverwendet werden.
- Wenn Sie eine Aktualisierung von einer nicht verwalteten virtuellen Maschine auf eine verwaltete virtuelle Maschine vornehmen, müssen Sie den vorhandenen Desktop-Pool löschen und einen neuen Desktop-Pool erstellen. Weitere Informationen finden Sie unter [Durchführen eines Upgrades von Horizon Agent auf einer virtuellen Linux-Maschine](#).

## Massenaktualisierung eines verwalteten Desktops

Wählen Sie für die Massenaktualisierung der verwalteten virtuellen Maschine eine der folgenden Methoden aus.

Methode	Beschreibung
Installieren oder aktualisieren Sie in der Vorlagen-VM den neuen Horizon Agent und erstellen Sie einen Snapshot.	<ul style="list-style-type: none"> <li>■ Benutzerdaten und -profil gehen verloren, da die vorhandenen virtuellen Maschinen gelöscht wurden, außer die Benutzerdaten und das Benutzerprofil befinden sich auf dem Freigabeserver, zum Beispiel auf einem NFS-Server.</li> <li>■ Nach der VM-Ersetzung fehlt möglicherweise der Status der virtuellen Maschine auf View Administrator. Sie müssen den Broker-Dienst neu starten, um dies zu beheben.</li> </ul>
Verwenden Sie das Beispielskript der Aktualisierung, um den neuen Horizon Agent auf die vorhandenen virtuellen Maschinen hochzuladen, und führen Sie den Aktualisierungsbefehl aus.	Benutzerdaten und -profil werden beibehalten.

## Erstellen einer Vorlage für virtuelle Maschinen zum Klonen von Linux-Desktop-Maschinen

Bevor Sie eine virtuelle Maschine klonen können, müssen Sie als Grundlage für die Klone eine Vorlage für virtuelle Maschinen erstellen.

### Voraussetzungen

- Stellen Sie sicher, dass Ihre Bereitstellung den Anforderungen für die Unterstützung von Linux-Desktops entspricht. Siehe [Systemanforderungen für Horizon 7 for Linux](#).
- Machen Sie sich mit den Schritten für das Erstellen virtueller Maschinen in vCenter Server und mit der Installation von Gastbetriebssystemen vertraut. Unter „Erstellen und Vorbereiten virtueller Maschinen“ im *Einrichten von virtuellen Desktops in Horizon 7*-Dokument finden Sie dazu Erläuterungen.

- Informieren Sie sich über die erforderlichen Videospeicherwerte (vRAM) für die Monitore, die Sie mit der virtuellen Maschine verwenden müssen. Siehe [Einstellungen der virtuellen Maschine für 2D-Grafiken](#).
- Machen Sie sich mit den Schritten zur AD-Integration vertraut. Siehe [Kapitel 3 Einrichten der Active Directory-Integration für Linux-Desktops](#).
- Machen Sie sich mit den Schritten für das Installieren des Horizon Agent auf Linux vertraut. Siehe [Kapitel 5 Installieren von Horizon Agent](#).
- Machen Sie sich, falls erforderlich, mit den Schritten zur Konfiguration von Optionen mithilfe der Konfigurationsdateien von Horizon 7 vertraut. Siehe [Kapitel 6 Konfigurationsoptionen für Linux-Desktops](#).
- Wenn Sie planen, Grafiken einzurichten, machen Sie sich mit den entsprechenden Schritten vertraut. Siehe [Kapitel 4 Einrichten von Grafiken für Linux-Desktops](#).

## Verfahren

- 1 Erstellen Sie im vSphere Web Client oder vSphere Client eine neue virtuelle Maschine.
- 2 Konfigurieren Sie die benutzerdefinierten Konfigurationsoptionen.
  - a Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie auf **Einstellungen bearbeiten**.
  - b Geben Sie die Anzahl der vCPUs und die Größe des vMemory-Arbeitsspeichers an.  
  
Befolgen Sie die Größenrichtlinien für vCPUs und vMemory-Arbeitsspeicher im Installationshandbuch für Ihre Linux-Distribution.  
  
Ubuntu 18.04 erfordert beispielsweise die Konfiguration von 2.048 MB für den vMemory-Arbeitsspeicher und zwei vCPUs.
  - c Wählen Sie **Grafikkarte** aus und geben Sie die Anzahl der Anzeigegeräte sowie den gesamten Videospeicher (vRAM) ein.  
  
Legen Sie im vSphere Web Client die vRAM-Größe für virtuelle Maschinen mit 2D-Grafik fest. Diese verwenden den VMware-Treiber. Die vRAM-Größe hat keinen Einfluss auf vDGA- oder NVIDIA GRID vGPU-Maschinen. Diese verwenden NVIDIA-Treiber.  
  
Befolgen Sie die Anweisungen in [Einstellungen der virtuellen Maschine für 2D-Grafiken](#). Verwenden Sie nicht die Videospeicherberechnung.
- 3 Schalten Sie die virtuelle Maschine ein und installieren Sie die Linux-Distribution.
- 4 Erstellen Sie einen Benutzer mit Root-Rechten, z. B. „ViewBenutzer“. Mit diesem Benutzer wird nur Horizon Agent installiert und deinstalliert.
- 5 Bearbeiten Sie `/etc/sudoers` und fügen Sie die Zeile `viewUser ALL=(ALL) NOPASSWD:ALL` hinzu.  
  
Enthält `/etc/sudoers` diese Zeile ist kein Kennwort für die Ausführung von Sudo als „ViewBenutzer“ erforderlich. Wenn Sie für die Installation von Horizon Agent das in diesem Kapitel zur Verfügung gestellte Beispielskript verwenden, müssen Sie „ViewBenutzer“ als Eingabe angeben.

- 6 Bei Linux-Distributionen wie RHEL, CentOS oder NeoKylin bearbeiten Sie `/etc/sudoers` und kommentieren die folgenden Zeilen aus:

```
Defaults requiretty
Defaults !visiblepw
```

- 7 Wenn es sich bei der Linux-Distribution nicht um RHEL/CentOS 8.x, RHEL/CentOS 7.x oder SLED/SLES 12.x handelt, installieren Sie VMware Tools.

Für RHEL/CentOS 8.0, RHEL/CentOS 7.x und SLED/SLES 12.x wird Open VM Tools standardmäßig installiert.

- 8 Installieren und konfigurieren Sie die Abhängigkeitspakete.

- a Wenn in der Linux-Distribution eine Version von Open VM Tools vor 9.10 ausgeführt wird, installieren Sie das Plug-In `deployPkg`.

Die Anweisungen dazu finden Sie unter <http://kb.vmware.com/kb/2075048>.

- b Wenn die Linux-Distribution Ubuntu ist, bestimmen Sie anhand der folgenden KB-Artikel die Abhängigkeitspakete zum Installieren und Konfigurieren in der VM.

- Siehe KB-Artikel <https://kb.vmware.com/s/article/2051469> und <https://kb.vmware.com/s/article/59687> für Ubuntu 18.04 und 16.04.
- Für Ubuntu 18.04 siehe auch KB-Artikel <https://kb.vmware.com/s/article/56409>.

- 9 Für RHEL und CentOS aktivieren Sie die Netzwerkverbindungseinstellung **Automatisch verbinden**.

- 10 Führen Sie die Aufgaben zur AD-Integration aus.

- 11 Führen Sie die Schritte zum Einrichten von Grafiken durch.

- 12 Installieren Sie Horizon Agent.

```
sudo ./install_viewagent.sh -A yes
```

Siehe [Kapitel 5 Installieren von Horizon Agent](#).

- 13 Führen Sie zusätzliche Konfigurationen mithilfe der Konfigurationsdateien von Horizon 7 durch.

- 14 Fahren Sie die virtuelle Maschine herunter und erstellen Sie einen Snapshot.

## Eingabedatei für die PowerCLI-Beispielskripts zur Bereitstellung von Linux-Desktops

Die PowerCLI-Beispielskripts zur Bereitstellung von Linux-Desktops lesen eine Eingabedatei mit Informationen über die Desktop-Maschinen.

Die Eingabedatei ist vom Typ `csv` und enthält die folgenden Informationen:

- Name der virtuellen Desktop-Maschine
- Übergeordneter Name der virtuellen Maschine

- Anpassungsspezifikation des Gastbetriebssystems
- Datenspeicher mit den geklonten Desktop-Maschinen
- Host-ESXi-Server der Desktop-Maschine
- Snapshot der übergeordneten virtuellen Maschine für das Klonen
- Attribut für das Löschen der virtuellen Desktop-Maschine, wenn vorhanden

Das folgende Beispiel zeigt den möglichen Inhalt einer Eingabedatei.

```
VMName,Parentvm,CustomSpec,Datastore,Host,FromSnapshot,DeleteIfPresent
linux-001,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
linux-002,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
linux-003,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
linux-004,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
linux-005,Ubuntu1804x64,linuxagent,datastore1,10.117.44.172,snapshot1,TRUE
```

Das Beispielskript geht davon aus, dass der Name dieser Eingabedatei `CloneVMs.csv` lautet und dass die Datei im selben Ordner wie die Skripts enthalten ist.

## Beispielskript zum Klonen von virtuellen Linux-Maschinen

Sie können das im Folgenden aufgeführte Beispielskript für das Klonen einer beliebigen Anzahl virtueller Maschinen (VMs) anpassen und anwenden.

Für das Kopieren und Einfügen des Skriptinhalts ohne Seitenumbrüche verwenden Sie die HTML-Version dieses Themas, die auf der Dokumentationsseite von Horizon 7 unter [verfügbar ist](#).

### Skripteingabe

Dieses Skript liest eine Eingabedatei, die unter [Eingabedatei für die PowerCLI-Beispielskripts zur Bereitstellung von Linux-Desktops](#). Es gibt verschiedene Eingabeaufforderungen für die folgenden Informationen aus:

- IP-Adresse von vCenter Server
- Anmeldename des Administrators für vCenter Server
- Kennwort des Administrators für vCenter Server
- Klontyp, der nur voll sein kann
- Deaktivierung einer vSphere-VM-Konsole

### Skriptinhalt

```
<#
Create Clones from a Master VM

The Tool supports creation of Full clone from Master VM.
#>
#----- Functions -----
```

```

function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}

function IsVMExists ()
{
    Param($VMExists)
    Write-Host "Checking if the VM $VMExists already Exists"
    [bool]$Exists = $false

    #Get all VMS and check if the VMs is already present in VC
    $listvm = Get-vm
    foreach ($lvm in $listvm)
    {
        if($VMExists -eq $lvm.Name )
        {
            $Exists = $true
        }
    }
    return $Exists
}

function Disable_VM_Console()
{
    Param($VMToDisableConsole)
    $vmConfigSpec = New-Object VMware.Vim.VirtualMachineConfigSpec
    $extra = New-Object VMware.Vim.optionvalue
    $extra.Key="RemoteDisplay.maxConnections"
    $extra.Value="0"
    $vmConfigSpec.extraconfig += $extra
    $vm = Get-VM $VMToDisableConsole | Get-View
    $vm.ReconfigVM($vmConfigSpec)
}

function Delete_VM()
{
    Param($VMToDelete)

```



```

    Write-Host "Deleting VM $VMToDelete"
    Get-VM $VMToDelete | where { $_.PowerState -eq "PoweredOn" } | Stop-VM -confirm:$false
    Get-VM $VMToDelete | Remove-VM -DeleteFromDisk -confirm:$false
}

#----- Main Script -----

$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
$cloneType = GetInput -prompt 'Clone Type ("full")' -IsPassword $false
$disableVMConsole = GetInput -prompt 'Disable vSphere VM Console ("yes" or "no", recommend "yes")' -
IsPassword $false
"-----"
$csvFile = '.\CloneVMs.csv'

# Check that user passed only full clone
if (($CloneType.length > 0) -and ($CloneType -ne "full"))
{
    write-host -ForegroundColor Red "Clone type supports only 'full' (case sensitive)"
    exit
}
if (($disableVMConsole.length > 0) -and ($disableVMConsole -ne "yes" -or $disableVMConsole -ne "no"))
{
    write-host -ForegroundColor Red "Disable vSphere VM Console supports only 'yes' or 'no' (case
sensitive)"
    exit
}

#check if file exists
if (!(Test-Path $csvFile))
{
    write-host -ForegroundColor Red "CSV File $CSVFile not found"
    exit
}

# Connect to the VC (Parameterize VC)
#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile
#$csvData = Import-CSV $csvFile -
header("VMName","Parentvm","CustomSpec","Datastore","Host","FromSnapshot","DeleteIfPresent")
foreach ($line in $csvData)
{

```

```

" `n-----"
$VMName = $line.VMName
write-host -ForegroundColor Yellow "VM: $VMName`n"

$destVMName=$line.VMName
$srcVM = $line.Parentvm
$cSpec = $line.CustomSpec
$targetDSName = $line.Datastore
$destHost = $line.Host
$srcSnapshot = $line.FromSnapshot
$deleteExisting = $line.DeleteIfPresent
if (IsVMExists ($destVMName))
{
    Write-Host "VM $destVMName Already Exists in VC $vcAddress"
    if($deleteExisting -eq "TRUE")
    {
        Delete_VM ($destVMName)
    }
    else
    {
        Write-Host "Skip clone for $destVMName"
        continue
    }
}
$vm = get-vm $srcvm -ErrorAction Stop | get-view -ErrorAction Stop
$cloneSpec = new-object VMware.VIM.VirtualMachineCloneSpec
$cloneSpec.Location = new-object VMware.VIM.VirtualMachineRelocateSpec
Write-Host "Using Datastore $targetDSName"
$newDS = Get-Datastore $targetDSName | Get-View
$cloneSpec.Location.Datastore = $newDS.summary.Datastore
Set-VM -vm $srcVM -snapshot (Get-Snapshot -vm $srcVM -Name $srcSnapshot) -confirm:$false
$cloneSpec.Snapshot = $vm.Snapshot.CurrentSnapshot
$cloneSpec.Location.Host = (get-vmhost -Name $destHost).Extensiondata.MoRef
$cloneSpec.Location.Pool = (Get-ResourcePool -Name Resources -Location (Get-VMHost -Name
$destHost)).Extensiondata.MoRef
# Start the Clone task using the above parameters
$task = $vm.CloneVM_Task($vm.parent, $destVMName, $cloneSpec)
# Get the task object
$task = Get-Task | where { $_.id -eq $task }
#Wait for the taks to Complete
Wait-Task -Task $task

$newvm = Get-vm $destVMName
$customSpec = Get-OSCustomizationSpec $cSpec
Set-vm -OSCustomizationSpec $cSpec -vm $newvm -confirm:$false
if ($disableVMConsole -eq "yes")
{
    Disable_VM_Console($destVMName)
}
# Start the VM
Start-VM $newvm
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

## Skriptausführung

Die folgenden Meldungen resultieren aus einer Ausführung des Skripts:

```
PowerCLI C:\scripts> .\CloneVMs.ps1
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
Clone Type<"Full"> : Full
Disable vSphere VM Console ("yes" or "no", recommend "yes") : yes
```

Der für den Klonvorgang notwendige Zeitraum ist abhängig von der Anzahl der Desktop-Maschinen und kann von mehreren Minuten bis zu Stunden reichen. Um sicherzustellen, dass der Vorgang abgeschlossen ist, vergewissern Sie sich im vSphere Client, dass die letzte virtuelle Desktop-Maschine eingeschaltet ist und über ihren eigenen eindeutigen Hostnamen verfügt und dass VMware Tools ausgeführt wird.

## Beispielskript zum Hinzufügen geklonter virtueller Maschinen zu einer AD-Domäne

Sie können das folgende Beispielskript anpassen und verwenden, um geklonte virtuelle Maschinen (VMs) zu einer Active Directory-Domäne (AD-Domäne) hinzuzufügen.

Sie müssen dieses Skript ausführen, wenn Sie die Winbind-Lösung für die AD-Integration verwenden, weil dabei der Schritt des Hinzufügens zur Domäne für geklonte VMs fehlschlägt. Dieses Skript führt einen Befehl zum Hinzufügen zur Domäne auf jeder VM aus. Sie müssen dieses Skript nicht ausführen, wenn Sie die OpenLDAP-Lösung verwenden.

Für das Kopieren und Einfügen des Skriptinhalts ohne Seitenumbrüche verwenden Sie die HTML-Version dieses Themas, die auf der Dokumentationsseite von Horizon 7 unter [https://www.vmware.com/support/pubs/view\\_pubs.html](https://www.vmware.com/support/pubs/view_pubs.html) verfügbar ist.

## Skripteingabe

Dieses Skript liest eine Eingabedatei, die im Kapitel [Eingabedatei für die PowerCLI-Beispielskripts zur Bereitstellung von Linux-Desktops](#) beschrieben ist. Es gibt verschiedene Eingabeaufforderungen für die folgenden Informationen aus:

- IP-Adresse von vCenter Server
- Anmeldename des Administrators für vCenter Server
- Kennwort des Administrators für vCenter Server
- Anmeldename des Administrators für den ESXi-Host
- Kennwort des Administrators für den ESXi-Host
- Benutzeranmeldename für die Linux-VM
- Benutzerkennwort für die Linux-VM

- Anmeldenname eines AD-Benutzers, der autorisiert ist, Maschinen zur Domäne hinzuzufügen
- Kennwort des autorisierten AD-Benutzers

## Skriptinhalt

```
<#
.SYNOPSIS
run command "sudo /usr/bin/net ads join"

.DESCRIPTION
The tool is to run the command "sudo /usr/bin/net ads join" to join Linux to AD

.NOTES
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}
#----- Handle input -----
"-----"
$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$hostAdmin = GetInput -prompt 'Your ESXi host admin user name, such as root' -IsPassword $false
$hostPassword = GetInput -prompt "Your ESXi admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"
$adUser = GetInput -prompt 'Type the AD user name to join the AD' -IsPassword $false
""
"Please type the AD user password."
"Please note that special character in password may not work with the script"
$adUserPassword = GetInput -prompt 'Your AD user password' -IsPassword $true
"-----"
```

```

#$csvFile = Read-Host 'Csv File '
$csvFile = '.\CloneVMs.csv'

#----- Main Script -----

#Connect to vCenter
#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $cmd = "sudo /usr/bin/net ads join -U $adUser%$adUserPassword"
    Write-Host "Run cmd 'sudo /usr/bin/net ads join' in VM '$VMName' with user '$guestUser'"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
}

Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

## Skriptausführung

Die folgenden Meldungen resultieren aus einer Ausführung des Skripts:

```

PowerCLI C:\scripts> .\ClonedVMs_JoinDomain.ps1
-----
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your ESXi host admin user name, such as root: root
Your ESXi host admin user password: *****
-----
Your VM guest OS user name: ViewUser

```

```
Your VM guest OS user password: *****
```

```
-----
Type the AD user name to join the AD: viewadmin
```

```
Please type the AD user password.
```

```
Please note that special character in password may not work with the script.
```

```
Your AD user password: *****
```

## Beispielskript zum Hinzufügen geklonter virtueller Maschinen zu einer AD-Domäne mithilfe von SSH

Sie können das folgende Beispielskript anpassen und verwenden, um geklonte virtuelle Maschinen (VMs) zu einer Active Directory-Domäne (AD-Domäne) hinzuzufügen. Dieses Skript verwendet SSH zur Ausführung von Befehlen auf den Linux-VMs.

Sie müssen dieses Skript ausführen, wenn Sie die Winbind-Lösung für die AD-Integration verwenden, weil dabei der Schritt des Hinzufügens zur Domäne für geklonte VMs fehlschlägt. Dieses Skript führt einen Befehl zum Hinzufügen zur Domäne auf jeder VM aus. Sie müssen dieses Skript nicht ausführen, wenn Sie die OpenLDAP-Lösung verwenden.

Für das Kopieren und Einfügen des Skriptinhalts ohne Seitenumbrüche verwenden Sie die HTML-Version dieses Themas, die auf der Dokumentationsseite von Horizon 7 unter [https://www.vmware.com/support/pubs/view\\_pubs.html](https://www.vmware.com/support/pubs/view_pubs.html) verfügbar ist.

### Skripteingabe

Dieses Skript liest eine Eingabedatei, die im Kapitel [Eingabedatei für die PowerCLI-Beispielskripts zur Bereitstellung von Linux-Desktops](#) beschrieben ist. Es gibt verschiedene Eingabeaufforderungen für die folgenden Informationen aus:

- IP-Adresse von vCenter Server
- Anmeldename des Administrators für vCenter Server
- Kennwort des Administrators für vCenter Server
- Benutzeranmeldename für die Linux-VM
- Benutzerkennwort für die Linux-VM
- Anmeldename eines AD-Benutzers, der autorisiert ist, Maschinen zur Domäne hinzuzufügen
- Kennwort des autorisierten AD-Benutzers

### Skriptinhalt

```
<#
.SYNOPSIS
run command "sudo /usr/bin/net ads join" via SSH

.DESCRPTION
The tool is to run the command "sudo /usr/bin/net ads join" to join Linux machine to AD via SSH
```

```
.NOTES
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}

function Check_SSH_Client
{
    Param($IsPlink, $IsPSCP)
    if ($IsPlink)
    {
        if (Test-Path ".\plink.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "plink.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "plink.exe" not found, please download from
its official web site'
            exit
        }
    }
    if ($IsPSCP)
    {
        if (Test-Path ".\pscp.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "pscp.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "pscp.exe" not found, please download from its
official web site'
            exit
        }
    }
}
}
```

```

function RunCmdViaSSH
{
    Param($VM_Name, $User, $Password, $Cmd, $returnOutput = $false)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    write-host "Run cmd on $VM_Name ($IP)"
    if($returnOutput)
    {
        $command = "echo yes | .\plink.exe -ssh -l $user -pw $password $IP " + '"' + $cmd + '"'
        $output = Invoke-Expression $command
        return $output
    }
    else
    {
        echo yes | .\plink.exe -ssh -l $user -pw $password $IP "$cmd"
    }
}

function UploadFileViaSSH
{
    Param($VM_Name, $User, $Password, $LocalPath, $DestPath)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    $command = "echo yes | .\pscp.exe -l $User -pw $Password $LocalPath $IP" + ":" + "$DestPath"
    write-host "Upload file: $command"
    Invoke-Expression $command
}

#----- Handle input -----
"-----"
Check_SSH_Client -IsPlink $true -IsPSCP $false
"-----"
$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"
$adUser = GetInput -prompt 'Type the AD user name to join the AD' -IsPassword $false
""
"
Please type the AD user password."
[Console]::ForegroundColor = "Yellow"
"Please note that special character should be escaped. For example, $ should be \$ "
[Console]::ResetColor()
$adUserPassword = GetInput -prompt 'Your AD user password' -IsPassword $true
"-----"

#$csvFile = Read-Host 'Csv File '
$csvFile = '.\CloneVMs.csv'

```



```
#----- Main Script -----

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $cmd = "sudo /usr/bin/net ads join -U $adUser%$adUserPassword"
    Write-Host "Run cmd 'sudo /usr/bin/net ads join' in VM '$VMName' with user '$guestUser'"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
}

Disconnect-VIServer $vcAddress -Confirm:$false
exit
```

## Skriptausführung

Die folgenden Meldungen resultieren aus einer Ausführung des Skripts:

```
PowerCLI C:\scripts> .\ClonedVMs_JoinDomain_SSH.ps1

-----
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****
-----
Type the AD user name to join the AD: viewadmin
Please type the AD user password.
Please note that special character should be escaped. For example, $ should be \$
Your AD user password: *****
```

# Beispielskript zum Hochladen von Konfigurationsdateien zu virtuellen Linux-Maschinen

Sie können das folgende Beispielskript anpassen und verwenden, um die Konfigurationsdateien `config` und `viewagent-custom.conf` zu mehreren virtuellen Linux-Maschinen (VMs) hochzuladen.

Für das Kopieren und Einfügen des Skriptinhalts ohne Seitenumbrüche verwenden Sie die HTML-Version dieses Themas, die auf der Dokumentationsseite von Horizon 7 unter [https://www.vmware.com/support/pubs/view\\_pubs.html](https://www.vmware.com/support/pubs/view_pubs.html) verfügbar ist.

## Skripteingabe

Dieses Skript liest eine Eingabedatei, die im Kapitel [Eingabedatei für die PowerCLI-Beispielskripts zur Bereitstellung von Linux-Desktops](#) beschrieben ist. Es gibt verschiedene Eingabeaufforderungen für die folgenden Informationen aus:

- IP-Adresse von vCenter Server
- Anmeldename des Administrators für vCenter Server
- Kennwort des Administrators für vCenter Server
- Anmeldename des Administrators für den ESXi-Host
- Kennwort des Administrators für den ESXi-Host
- Benutzeranmeldename für die Linux-VM
- Benutzerkennwort für die Linux-VM

## Skriptinhalt

```
<#
Upload the configuration files config and viewagent-custom.conf to Linux VMs
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }
}
```

```

    [Console]::ResetColor()
    return $input
}

#----- Handle Input -----
"-----"
write-host -ForegroundColor Blue 'Please ensure your config file and viewagent-custom.conf file are
in current working directory'
$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$hostAdmin = GetInput -prompt 'Your ESXi host admin user name, such as root' -IsPassword $false
$hostPassword = GetInput -prompt "Your ESXi admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"

$csvFile = '.\CloneVMs.csv'
$setConfig = $false
$setCustomConf = $false
$config_File = "config"
$customConf_File = "viewagent-custom.conf"

#check if config file exists
if(Test-Path $config_File)
{
    $setConfig = $true
    write-host -ForegroundColor Yellow '"config" file found'
}
else
{
    write-host -ForegroundColor Yellow '"config" file not found, skip it'
}

if(Test-Path $customConf_File)
{
    $setCustomConf = $true
    write-host -ForegroundColor Yellow '"viewagent-custom.conf" file found'
}
else
{
    write-host -ForegroundColor Yellow '"viewagent-custom.conf" file not found, skip it'
}

if (($setConfig -eq $false)-AND ($setCustomConf -eq $false))
{
    write-host -ForegroundColor Red 'Both file not found, exit'
    exit
}

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword

```

```

if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    #Try to delete the configuration file from home folder on destination VM
    $cmd = "rm -rf config viewagent-custom.conf"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    if ($setConfig)
    {
        Write-Host "Upload File '$config_File' to '$destFolder' of VM '$VMName' with user '$guestUser'"
        Copy-VMGuestFile -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -LocalToGuest -Destination $destFolder -
Source $config_File

        $cmd = "sudo mv ./ $config_File /etc/vmware/";
        Write-Host "Move configuraton file: $cmd"
        Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
    }

    if ($setCustomConf)
    {
        Write-Host "Upload File '$customConf_File' to '$destFolder' of VM '$VMName' with user
'$guestUser'"
        Copy-VMGuestFile -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -LocalToGuest -Destination $destFolder -
Source $customConf_File

        $cmd = "sudo mv ./ $customConf_File /etc/vmware/";
        Write-Host "Move configuraton file: $cmd"
        Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
    }
}

```

```

    }
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

## Skriptausführung

Die folgenden Meldungen resultieren aus einer Ausführung des Skripts:

```

PowerCLI C:\scripts> .\UpdateOptionFile.ps1
-----
Please ensure your config file and view-agent.conf file are in current working directory.
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your ESXi host admin user name, such as root: root
Your ESXi host admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****

```

## Beispielskript zum Hochladen von Konfigurationsdateien zu virtuellen Linux-Maschinen mithilfe von SSH

Sie können das folgende Beispielskript anpassen und verwenden, um die Konfigurationsdateien `config` und `viewagent-custom.conf` zu mehreren virtuellen Linux-Maschinen (VMs) hochzuladen. Dieses Skript verwendet SSH zur Ausführung von Befehlen auf den Linux-VMs.

Für das Kopieren und Einfügen des Skriptinhalts ohne Seitenumbrüche verwenden Sie die HTML-Version dieses Themas, die auf der Dokumentationsseite von Horizon 7 unter [https://www.vmware.com/support/pubs/view\\_pubs.html](https://www.vmware.com/support/pubs/view_pubs.html) verfügbar ist.

## Skripteingabe

Dieses Skript liest eine Eingabedatei, die im Kapitel [Eingabedatei für die PowerCLI-Beispielskripts zur Bereitstellung von Linux-Desktops](#) beschrieben ist. Es gibt verschiedene Eingabeaufforderungen für die folgenden Informationen aus:

- IP-Adresse von vCenter Server
- Anmeldename des Administrators für vCenter Server
- Kennwort des Administrators für vCenter Server
- Benutzeranmeldename für die Linux-VM
- Benutzerkennwort für die Linux-VM

## Skriptinhalt

```
<#
Upload the configuration files config and viewagent-custom.conf to Linux VMs using SSH
#>
#----- Functions -----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}
function Check_SSH_Client
{
    Param($IsPlink, $IsPSCP)
    if ($IsPlink)
    {
        if (Test-Path ".\plink.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "plink.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "plink.exe" not found, please download from
its official web site'
            exit
        }
    }
    if ($IsPSCP)
    {
        if (Test-Path ".\pscp.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "pscp.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "pscp.exe" not found, please download from its
official web site'
            exit
        }
    }
}
```

```

    }
}

function RunCmdViaSSH
{
    Param($VM_Name, $User, $Password, $Cmd, $returnOutput = $false)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    write-host "Run cmd on $VM_Name ($IP)"
    if($returnOutput)
    {
        $command = "echo yes | .\plink.exe -ssh -l $user -pw $password $IP " + '"' + $cmd + '"'
        $output = Invoke-Expression $command
        return $output
    }
    else
    {
        echo yes | .\plink.exe -ssh -l $user -pw $password $IP "$cmd"
    }
}

function UploadFileViaSSH
{
    Param($VM_Name, $User, $Password, $LocalPath, $DestPath)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    $command = "echo yes | .\pscp.exe -l $User -pw $Password $LocalPath $IP" + ":" + "$DestPath"
    write-host "Upload file: $command"
    Invoke-Expression $command
}

#----- Handle Input -----
"-----"
Check_SSH_Client -IsPlink $true -IsPSCP $true
"-----"
write-host -ForegroundColor Blue 'Please ensure your config file and viewagent-custom.conf file are
in current working directory'
$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"

$csvFile = '.\CloneVMs.csv'
$setConfig = $false
$setCustomConf = $false
$config_File = "config"
$customConf_File = "viewagent-custom.conf"

#check if config file exists

```

```

if(Test-Path $config_File)
{
    $setConfig = $true
    write-host -ForegroundColor Yellow '"config" file found'
}
else
{
    write-host -ForegroundColor Yellow '"config" file not found, skip it'
}

if(Test-Path $customConf_File)
{
    $setCustomConf = $true
    write-host -ForegroundColor Yellow '"viewagent-custom.conf" file found'
}
else
{
    write-host -ForegroundColor Yellow '"viewagent-custom.conf" file not found, skip it'
}

if (($setConfig -eq $false)-AND ($setCustomConf -eq $false))
{
    write-host -ForegroundColor Red 'Both file not found, exit'
    exit
}

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    #Try to delete the configuration file from home folder on destination VM
    $cmd = "rm -rf config viewagent-custom.conf"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
}

```



```

if ($setConfig)
{
    Write-Host "Upload File '$config_File' to '$destFolder' of VM '$VMName' with user '$guestUser'"
    UploadFileViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -LocalPath
$config_File -DestPath $destFolder

    $cmd = "sudo mv ./ $config_File /etc/vmware/";
    Write-Host "Move configuraton file: $cmd"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
}

if ($setCustomConf)
{
    Write-Host "Upload File '$customConf_File' to '$destFolder' of VM '$VMName' with user
'$guestUser'"
    UploadFileViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -LocalPath
$customConf_File -DestPath $destFolder

    $cmd = "sudo mv ./ $customConf_File /etc/vmware/";
    Write-Host "Move configuraton file: $cmd"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
}
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

## Skriptausführung

Die folgenden Meldungen resultieren aus einer Ausführung des Skripts:

```

PowerCLI C:\scripts> .\UpdateOptionFile.ps1
-----
Please ensure your config file and view-agent.conf file are in current working directory.
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****

```

## Beispiel-PowerCLI-Skript zum Upgrade von Horizon Agent auf Linux-Desktop-Maschinen

Sie können das nachfolgend aufgeführte Beispielskript für ein Upgrade von Horizon Agent auf mehreren virtuellen Linux-Maschinen (VMs) anpassen und anwenden.

Dieses Skript lädt das TAR-Archiv des Installationsprogramms auf jede VM hoch, bevor Horizon Agent installiert wird. Die Upload-Aufgabe kann sehr viel Zeit in Anspruch nehmen, vor allem wenn eine große Anzahl von VMs beteiligt und die Netzwerkgeschwindigkeit langsam ist. Um Zeit zu sparen, können Sie das Skript ausführen, das SSH verwendet, oder das TAR-Archiv des Installationsprogramms an einem freigegebenen Speicherort ablegen, der für jede VM verfügbar ist, wodurch das Hochladen der Datei nicht erforderlich ist.

Für das Kopieren und Einfügen des Skriptinhalts ohne Seitenumbrüche verwenden Sie die HTML-Version dieses Themas, die auf der Dokumentationsseite von Horizon 7 unter <https://docs.vmware.com/de/VMware-Horizon-7/index.html> verfügbar ist.

## Skripteingabe

Dieses Skript liest eine Eingabedatei, die im Kapitel [Eingabedatei für die PowerCLI-Beispielskripts zur Bereitstellung von Linux-Desktops](#) beschrieben ist. Es gibt verschiedene Eingabeaufforderungen für die folgenden Informationen aus:

- Annahme der Horizon Agent-Endbenutzerlizenzvereinbarung (EULA)
- IP-Adresse von vCenter Server
- Anmeldename des Administrators für vCenter Server
- Kennwort des Administrators für vCenter Server
- Anmeldename des Administrators für den ESXi-Host
- Kennwort des Administrators für den ESXi-Host
- Anmeldename des Benutzers für das Linux-Gastbetriebssystem
- Kennwort des Benutzers für das Linux-Gastbetriebssystem
- Horizon Agent-TAR-Archiv-Pfad
- Aktualisieren auf verwaltete VM
- Installieren der Smartcard-Umleitungsfunktion

## Skriptinhalt

```
<#
Upload the Linux Agent installer tar ball and re-install
#>

#-----
Functions-----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
```

```

    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}
#-----Handle
input-----
"-----"
$acceptEULA = GetInput -prompt 'Accept Linux Horizon Agent EULA in tar bundle ("yes" or "no")' -
IsPassword $false
if ($acceptEULA -ne "yes")
{
    write-host -ForegroundColor Red "You need accept the EULA with 'yes'(case sensitive)"
    exit
}
$svcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$svcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$svcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$hostAdmin = GetInput -prompt 'Your ESXi host admin user name, such as root' -IsPassword $false
$hostPassword = GetInput -prompt "Your ESXi admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"
$agentInstaller = GetInput -prompt 'Type the Horizon Agent tar ball path' -IsPassword $false
"-----"
$UpgradeToManagedVM = GetInput -prompt 'Upgrade to managed VM ("yes" or "no")' -IsPassword $false
if (($UpgradeToManagedVM -ne "yes") -AND $UpgradeToManagedVM -ne "no")
{
    write-host -ForegroundColor Red "You need select 'yes' or 'no'(case sensitive)"
    exit
}
$installSmartcard = GetInput -prompt 'Install the Smartcard redirection feature ("yes" or "no")' -
IsPassword $false
if (($installSmartcard -ne "yes") -AND $installSmartcard -ne "no")
{
    write-host -ForegroundColor Red "You need select 'yes' or 'no'(case sensitive)"
    exit
}
"-----"

#csvFile = Read-Host 'Csv File '
$csvFile = '.\CloneVMs.csv'

#check if file exists

```

```

if (!(Test-Path $agentInstaller))
{
write-host -ForegroundColor Red "installer File not found"
exit
}

#check if file exists
if (!(Test-Path $csvFile))
{
write-host -ForegroundColor Red "CSV File not found"
exit
}
#-----
Functions-----
function GetSourceInstallerMD5()
{
    $agentInstallerPath = Convert-Path $agentInstaller;
    $md5 = New-Object -TypeName System.Security.Cryptography.MD5CryptoServiceProvider;
    $md5HashWithFormat =
[System.BitConverter]::ToString($md5.ComputeHash([System.IO.File]::ReadAllBytes($agentInstallerPath)))
;
    $md5Hash = ($md5HashWithFormat.replace("-", "")).ToLower();
    return $md5Hash;
}

#-----
Main-----
#Get installer MD5Sum
$installerMD5Hash = GetSourceInstallerMD5;

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $cmd = "rm -rf VMware-*linux-*"

```

```

Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

#Upload installer tar ball to Linux VM
Write-Host "Upload File '$agentInstaller' to '$destFolder' of VM '$VMName' with user '$guestUser'"
Copy-VMGuestFile -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -LocalToGuest -Destination $destFolder -
Source $agentInstaller

#Check the uploaded installer md5sum
$cmd = "md5sum VMware-*linux-*"
Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
$output = Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -
GuestUser $guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

if($output.Contains($installerMD5Hash))
{
    Write-Host $VMName": Uploaded installer's MD5Sum matches the local installer's MD5Sum";
    Write-Host $VMName": Extract the installer and do installation";
    $cmd = "tar -xzf VMware-*linux-*.tar.gz"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    $cmd = "sudo setenforce 0";
    Write-Host "Set the selinux to permissive mode: $cmd"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    $cmd = "sudo killall /usr/lib/vmware/viewagent/VMwareBlastServer/VMwareBlastServer"
    Write-Host "Stop VMwareBlastServer before upgrading: $cmd"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    #Run the upgrade command.
    $cmd = "cd VMware-*linux-* && sudo ./install_viewagent.sh -A yes -m $installSmartcard -M
$UpgradeToManagedVM"
    Write-Host "Run upgrade cmd in VM '$VMName' with user '$guestUser': $cmd"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd

    $cmd = "sudo shutdown -r +1&"
    Write-Host "Reboot to apply the Horizon Agent installation"
    Invoke-VMScript -HostUser $hostAdmin -HostPassword $hostPassword -VM $VMName -GuestUser
$guestUser -GuestPassword $guestPassword -Confirm:$false -ScriptType Bash -ScriptText $cmd
}
else
{
    Write-Host $VMName": Uploaded installer's MD5Sum does NOT match the local installer's MD5Sum";
    Write-Host $VMName": Skip the installation. Please check your network and VMware Tools
status";
    exit;
}

```

```

    }
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

## Skriptausführung

Die folgenden Meldungen resultieren aus einer Ausführung des Skripts:

```

PowerCLI C:\scripts> .\InstallAgent.ps1
-----
Accept Linux Horizon Agent EULA in tar bundle ("yes" or "no"): yes
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your ESXi host admin user name, such as root: root
Your ESXi host admin user password: *****
-----
Your VM guest OS user name: HorizonUser
Your VM guest OS user password: *****
-----
Type the Horizon Agent tar ball path. Please take care of the installer arch: .\VMware-viewagent-
linux-x86_64-x.y.z-1234567.tar.gz
-----
Upgrade to managed VM ("yes" or "no"): yes
Install the Smartcard redirection feature ("yes" or "no"): no

```

## Beispielskript zur Durchführung eines Upgrades von Horizon Agent auf virtuellen Linux-Maschinen mithilfe von SSH

Sie können das nachfolgend aufgeführte Beispielskript für ein Upgrade von Horizon Agent auf mehreren virtuellen Linux-Maschinen (VMs) anpassen und anwenden. Dieses Skript verwendet SSH zur Ausführung von Befehlen auf den Linux-VMs.

Für das Kopieren und Einfügen des Skriptinhalts ohne Seitenumbrüche verwenden Sie die HTML-Version dieses Themas, die auf der Dokumentationsseite von Horizon 7 unter [https://www.vmware.com/support/pubs/view\\_pubs.html](https://www.vmware.com/support/pubs/view_pubs.html) verfügbar ist.

## Skripteingabe

Dieses Skript liest eine Eingabedatei, die im Kapitel [Eingabedatei für die PowerCLI-Beispielskripts zur Bereitstellung von Linux-Desktops](#) beschrieben ist. Es gibt verschiedene Eingabeaufforderungen für die folgenden Informationen aus:

- Annahme der Horizon Agent-Endbenutzerlizenzvereinbarung (EULA)
- IP-Adresse von vCenter Server
- Anmeldename des Administrators für vCenter Server

- Kennwort des Administrators für vCenter Server
- Anmeldename des Administrators für den ESXi-Host
- Kennwort des Administrators für den ESXi-Host
- Anmeldename des Benutzers für das Linux-Gastbetriebssystem
- Kennwort des Benutzers für das Linux-Gastbetriebssystem
- Pfad für das Horizon Agent-TAR-Archiv
- Aktualisieren auf verwaltete VM
- Installieren der Smartcard-Umleitungsfunktion

## Skriptinhalt

```
<#
Upload the Linux Agent installer tar ball and re-install
#>

#-----
Functions-----
function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}
function Check_SSH_Client
{
    Param($IsPlink, $IsPSCP)
    if ($IsPlink)
    {
        if (Test-Path ".\plink.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "plink.exe" found'
        }
        else
    }
```

```

        {
            write-host -ForegroundColor Red 'SSH client "plink.exe" not found, please download from
its official web site'
            exit
        }
    }
    if ($IsPSCP)
    {
        if (Test-Path ".\pscp.exe")
        {
            write-host -ForegroundColor Yellow 'SSH client "pscp.exe" found'
        }
        else
        {
            write-host -ForegroundColor Red 'SSH client "pscp.exe" not found, please download from its
official web site'
            exit
        }
    }
}

function RunCmdViaSSH
{
    Param($VM_Name, $User, $Password, $Cmd, $returnOutput = $false)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    write-host "Run cmd on $VM_Name ($IP)"
    if($returnOutput)
    {
        $command = "echo yes | .\plink.exe -ssh -l $user -pw $password $IP " + "'" + $cmd + "'"
        $output = Invoke-Expression $command
        return $output
    }
    else
    {
        echo yes | .\plink.exe -ssh -l $user -pw $password $IP "$cmd"
    }
}

function UploadFileViaSSH
{
    Param($VM_Name, $User, $Password, $LocalPath, $DestPath)

    $VM= Get-VM $VM_Name
    $IP = $VM.guest.IPAddress[0]
    $command = "echo yes | .\pscp.exe -l $User -pw $Password $LocalPath $IP" + ":" + "$DestPath"
    write-host "Upload file $LocalPath to VM $VM_Name with user $User"
    Invoke-Expression $command
}

#-----Handle
input-----
"-----"

```



```

Check_SSH_Client -IsPlink $true -IsPSCP $true
"-----"
$acceptEULA = GetInput -prompt 'Accept Linux View Agent EULA in tar bundle ("yes" or "no")' -
IsPassword $false
if ($acceptEULA -ne "yes")
{
    write-host -ForegroundColor Red "You need accept the EULA with 'yes'(case sensitive)"
    exit
}
$svcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$svcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$svcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"
$guestUser = GetInput -prompt 'Your VM guest OS user name' -IsPassword $false
$guestPassword = GetInput -prompt 'Your VM guest OS user password' -IsPassword $true
"-----"
$agentInstaller = GetInput -prompt 'Type the View Agent tar ball path' -IsPassword $false
"-----"
$UpgradeToManagedVM = GetInput -prompt 'Upgrade to managed VM ("yes" or "no")' -IsPassword $false
if (($UpgradeToManagedVM -ne "yes") -AND $UpgradeToManagedVM -ne "no")
{
    write-host -ForegroundColor Red "You need select 'yes' or 'no'(case sensitive)"
    exit
}
$installSmartcard = GetInput -prompt 'Install the Smartcard redirection feature ("yes" or "no")' -
IsPassword $false
if (($installSmartcard -ne "yes") -AND $installSmartcard -ne "no")
{
    write-host -ForegroundColor Red "You need select 'yes' or 'no'(case sensitive)"
    exit
}
}
"-----"

#$csvFile = Read-Host 'Csv File '
$csvFile = '.\CloneVMs.csv'

#check if file exists
if (!(Test-Path $agentInstaller))
{
    write-host -ForegroundColor Red "installer File not found"
    exit
}

#check if file exists
if (!(Test-Path $csvFile))
{
    write-host -ForegroundColor Red "CSV File not found"
    exit
}
}
#-----
Functions-----
function GetSourceInstallerMD5()
{
    $agentInstallerPath = Convert-Path $agentInstaller;
    $md5 = New-Object -TypeName System.Security.Cryptography.MD5CryptoServiceProvider;

```

```

    $md5HashWithFormat =
[System.BitConverter]::ToString($md5.ComputeHash([System.IO.File]::ReadAllBytes($agentInstallerPath)))
;
    $md5Hash = ($md5HashWithFormat.replace("-", "").ToLower());
    return $md5Hash;
}

#-----
Main-----
#Get installer MD5Sum
$installerMD5Hash = GetSourceInstallerMD5;

#Connect to vCenter
$VC_Conn_State = Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
if([string]::IsNullOrEmpty($VC_Conn_State))
{
    Write-Host 'Exit since failed to login vCenter'
    exit
}
else
{
    Write-Host 'vCenter is connected'
}

#Read input CSV file
$csvData = Import-CSV $csvFile

$destFolder = "/home/$guestUser/"

#Handle VMs one by one
foreach ($line in $csvData)
{
    "`n-----"
    $VMName = $line.VMName
    write-host -ForegroundColor Yellow "VM: $VMName`n"

    $cmd = "rm -rf VMware-*linux-*"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

    #Upload installer tar ball to Linux VM
    Write-Host "Upload File '$agentInstaller' to '$destFolder' of VM '$VMName' with user '$guestUser'"
    UploadFileViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -LocalPath
$agentInstaller -DestPath $destFolder

    #Check the uploaded installer md5sum
    $cmd = "md5sum VMware-*linux-*"
    Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
    $output = RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd -
$returnOutput $true

    if($output.Contains($installerMD5Hash))
    {
        Write-Host $VMName": Uploaded installer's MD5Sum matches the local installer's MD5Sum";
    }
}

```

```

Write-Host $VMName": Extract the installer and do installation";

$cmd = "tar -xzf VMware-*linux-*.tar.gz"
Write-Host "Run cmd '$cmd' in VM '$VMName' with user '$guestUser'"
RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

$cmd = "sudo setenforce 0";
Write-Host "Set the selinux to permissive mode: $cmd"
RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

$cmd = "sudo killall /usr/lib/vmware/viewagent/VMwareBlastServer/VMwareBlastServer"
Write-Host "Stop VMwareBlastServer before upgrading: $cmd"
RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd

#Run the upgrade command.
$cmd = "cd VMware-*linux-* && sudo ./install_viewagent.sh -r yes -A yes -m $installSmartcard
-M $UpgradeToManagedVM"
Write-Host "Run upgrade cmd in VM '$VMName' with user '$guestUser': $cmd"
RunCmdViaSSH -VM_Name $VMName -User $guestUser -Password $guestPassword -Cmd $cmd
Write-Host -ForegroundColor Yellow "Linux Agent installer will reboot the Linux VM after
upgrade, and you may hit the ssh connection closed error message, which is expectation"
}
else
{
    Write-Host $VMName": Uploaded installer's MD5Sum does NOT match the local installer's MD5Sum";
    Write-Host $VMName": Skip the installation. Please check your network and VMware Tools
status";
    exit;
}
}
Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

## Skriptausführung

Die folgenden Meldungen resultieren aus einer Ausführung des Skripts:

```

PowerCLI C:\scripts> .\InstallAgent.ps1
-----
Accept Linux Horizon Agent EULA in tar bundle ("yes" or "no"): yes
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****
-----
Your VM guest OS user name: ViewUser
Your VM guest OS user password: *****
-----
Type the Horizon Agent tar ball path. Please take care of the installer arch: .\VMware-viewagent-
linux-x86_64-x.y.z-1234567.tar.gz
-----
-----
Upgrade to managed VM ("yes" or "no"): yes
Install the Smartcard redirection feature ("yes" or "no"): no

```

## Beispielskript zum Ausführen von Vorgängen auf virtuellen Linux-Maschinen

Sie können das im Folgenden aufgeführte Beispielskript für das Ausführen von Vorgängen auf mehreren virtuellen Linux-Maschinen (VMs) anpassen und anwenden. Zu diesen Vorgängen gehört das Einschalten, Ausschalten, Herunterfahren, Neustarten und Löschen der virtuellen Maschinen.

Dieses Skript löscht virtuelle Maschinen aus vCenter Server, aber nicht aus View.

Für das Kopieren und Einfügen des Skriptinhalts ohne Seitenumbrüche verwenden Sie die HTML-Version dieses Themas, die auf der Dokumentationsseite von Horizon 7 unter [https://www.vmware.com/support/pubs/view\\_pubs.html](https://www.vmware.com/support/pubs/view_pubs.html) verfügbar ist.

### Skripteingabe

Dieses Skript liest eine Eingabedatei, die im Kapitel [Eingabedatei für die PowerCLI-Beispielskripts zur Bereitstellung von Linux-Desktops](#) beschrieben ist. Es gibt verschiedene Eingabeaufforderungen für die folgenden Informationen aus:

- IP-Adresse von vCenter Server
- Anmeldename des Administrators für vCenter Server
- Kennwort des Administrators für vCenter Server
- Auszuführender Vorgang wie z. B. das Einschalten oder Ausschalten, das Herunterfahren des Gastbetriebssystems, das Neustarten der virtuellen Maschine, das Neustarten des VM-Gastbetriebssystems oder das Löschen einer virtuellen Maschine.
- Die Wartezeit (in Sekunden) zwischen den Vorgängen auf den VMs.

### Skriptinhalt

```
<#
.DESCRIPTION
The Tool supports:
1. Power off VMs
2. Power on VMs
3. Shutdown VMs
4. Restart VMs
5. Restart VM guest
6. Delete VMs from Disk
.NOTES
#>

#----- Functions -----

function GetInput
{
    Param($prompt, $IsPassword = $false)
    $prompt = $prompt + ": "
    Write-Host $prompt -NoNewLine
    [Console]::ForegroundColor = "Blue"
```

```

    if ($IsPassword)
    {
        $input = Read-Host -AsSecureString
        $input =
[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBS
TR($input))
    }
    else
    {
        $input = Read-Host
    }

    [Console]::ResetColor()
    return $input
}

function IsVMExists ($VMExists)
{
    Write-Host "Checking if the VM $VMExists Exists"
    [bool]$Exists = $false

    #Get all VMS and check if the VMs is already present in VC
    $listvm = Get-vm
    foreach ($lvm in $listvm)
    {
        if($VMExists -eq $lvm.Name )
        {
            $Exists = $true
            Write-Host "$VMExists is Exist"
        }
    }
    return $Exists
}

function Delete_VM($VMToDelete)
{
    Write-Host "Deleting VM $VMToDelete"
    Get-VM $VMToDelete | where { $_.PowerState -eq "PoweredOn" } | Stop-VM -confirm:$false
    Get-VM $VMToDelete | Remove-VM -DeleteFromDisk -confirm:$false
}

#----- Handle input -----
"-----"
$vcAddress = GetInput -prompt "Your vCenter address" -IsPassword $false
$vcAdmin = GetInput -prompt "Your vCenter admin user name" -IsPassword $false
$vcPassword = GetInput -prompt "Your vCenter admin user password" -IsPassword $true
"-----"

$action = GetInput -prompt 'Select action: 1). Power On 2). Power Off 3) Shutdown VM Guest 4).
Restart VM 5). Restart VM Guest 6). Delete VM' -IsPassword $false
$sleepTime = GetInput -prompt 'Wait time (seconds) between each VM' -IsPassword $false
"-----"

[Console]::ForegroundColor = "Yellow"
switch ($action)
{
    1

```

```

{
    "Your selection is 1). Power On"
}
2
{
    "Your selection is 2). Power Off"
}
3
{
    "Your selection is 3) Shutdown"
}
4
{
    "Your selection is 4). Restart VM"
}
5
{
    "Your selection is 5). Restart VM Guest"
}
6
{
    "Your selection is 6). Delete VM"
}
default
{
    "Invalid selection for action: $action"
    exit
}
}
[Console]::ResetColor()
$csvFile = '.\CloneVMs.csv'

#check if file exists
if (!(Test-Path $csvFile))
{
    write-host -ForegroundColor Red "CSV File not found"
    exit
}
"-----"

#----- Main -----
#Read input CSV file
Disconnect-VIServer $vcAddress -Confirm:$false
#Connect-VIServer $vcAddress -ErrorAction Stop -user $vcAdmin -password $vcPassword
Connect-VIServer $vcAddress -user $vcAdmin -password $vcPassword
$csvData = Import-CSV $csvFile

foreach ($line in $csvData)
{
    $VMName = $line.VMName
    switch ($action)
    {
        1
        {
            Get-VM $VMName | Start-VM -Confirm:$false

```

```

    }
    2
    {
        Get-VM $VMName | Stop-VM -Confirm:$false
    }
    3
    {
        Get-VM $VMName | Shutdown-VMGuest -Confirm:$false
    }
    4
    {
        Get-VM $VMName | Restart-VM -Confirm:$false
    }
    5
    {
        Get-VM $VMName | Restart-VMGuest -Confirm:$false
    }
    6
    {
        if (IsVMExists ($VMName))
        {
            Delete_VM ($VMName)
        }
    }
    default{}
}
Start-Sleep -s $sleepTime
}

Disconnect-VIServer $vcAddress -Confirm:$false
exit

```

## Skriptausführung

Die folgenden Meldungen resultieren aus einer Ausführung des Skripts:

```

PowerCLI C:\scripts> .\VMOperations.ps1
Your vCenter address: 10.117.44.17
Your vCenter admin user name: administrator
Your vCenter admin user password: *****

-----
Select action: 1). Power On 2). Power Off 3) Shutdown VM Guest 4). Restart VM 5). Restart VM Guest
6). Delete VM: 1
Wait time (seconds) between each VM: 20
-----

Your selection is 6). Delete VM

```

Für das Einschalten, das Neustarten einer VM oder das Neustarten eines VM-Gastbetriebssystems müssen Sie eine Wartezeit zwischen den virtuellen Maschinen von mindestens 20 Sekunden angeben, um einen „Boot Storm“ (Überlastung des Netzwerks durch zu viele Anmeldungen) zu vermeiden, durch den einige Vorgänge eventuell nicht ausgeführt werden könnten.

# Fehlerbehebung bei Linux-Desktops

# 9

Bei der Verwaltung von Linux-Desktops können bestimmte Probleme auftreten. Zur Diagnose und Behebung dieser Probleme stehen Ihnen verschiedene Vorgehensweisen zur Verfügung.

Dieses Kapitel enthält die folgenden Themen:

- [Verwenden des Horizon Help Desk Tool in Horizon Console](#)
- [Ermitteln von Diagnoseinformationen für eine Horizon 7 for Linux-Maschine](#)
- [Fehler beim Trennen der Verbindung auf dem Horizon Client für ein iPad Pro durch Horizon Agent](#)
- [SLES 12 SP1-Desktop wird nicht automatisch aktualisiert](#)
- [Fehlerhafte SSO-Verbindung zu einem PowerOff-Agenten](#)
- [Nicht erreichbare VM nach dem Erstellen eines manuellen Desktop-Pools für Linux](#)

## Verwenden des Horizon Help Desk Tool in Horizon Console

Horizon Help Desk Tool ist eine Webanwendung, mit der Sie den Status von Horizon 7-Benutzersitzungen abrufen und eine Fehlerbehebung sowie Wartungsvorgänge durchführen können.

In Horizon Help Desk Tool können Sie Benutzersitzungen zur Fehlerbehebung suchen und Vorgänge für die Desktop-Wartung wie den Neustart oder das Zurücksetzen von Desktops durchführen.

Um Horizon Help Desk Tool konfigurieren zu können, müssen die folgenden Anforderungen erfüllt sein:

- Lizenz für Horizon Enterprise Edition oder Horizon Apps Advanced Edition für Horizon 7. Informationen zur Prüfung, ob Sie über die richtige Lizenz verfügen, finden Sie im Dokument *Horizon 7-Verwaltung*.
- Eine Ereignisdatenbank zum Speichern von Informationen zu Horizon 7-Komponenten. Weitere Informationen zur Konfiguration einer Ereignisdatenbank finden Sie im Dokument *Horizon 7-Verwaltung*.
- Die Rolle „Helpdesk-Administrator“ oder „Helpdesk-Administrator (Nur Lesezugriff)“ zum Anmelden bei Horizon Help Desk Tool. Weitere Informationen zu diesen Rollen finden Sie im Dokument *Horizon 7-Verwaltung*.



- Aktivieren Sie den Zeitprofiler auf jeder Verbindungsserver-Instanz zur Anzeige der Anmeldesegmente.

Mit dem folgenden Befehl `vdmadmin` aktivieren Sie den Zeitprofiler auf jeder Verbindungsserver-Instanz:

```
vdmadmin -I -timingProfiler -enable
```

Mit dem folgenden Befehl `vdmadmin` aktivieren Sie den Zeitprofiler auf einer Verbindungsserver-Instanz, die einen Verwaltungspport verwendet:

```
vdmadmin -I -timingProfiler -enable -server {ip/server}
```

- Aktivieren Sie die `HelpDeskEnable`-Option in der Konfigurationsdatei `/etc/vmware/viewagent-custom.conf`.

## Starten des Horizon Help Desk Tool an der Horizon Console

Das Horizon Help Desk Tool ist in der Horizon Console enthalten. Sie können nach einem Benutzer suchen, für den Sie im Horizon Help Desk Tool Probleme beheben möchten.

### Verfahren

- 1 Sie können mit dem Textfeld „Benutzersuche“ nach einem Benutzernamen suchen oder direkt zum Horizon Help Desk Tool navigieren.
  - Geben Sie an der Horizon Console einen Benutzernamen im Textfeld „Benutzersuche“ ein.
  - Wählen Sie **Überwachen > Helpdesk** aus und geben Sie einen Benutzernamen in das Textfeld „Benutzersuche“ ein.

An der Horizon Console wird eine Liste der Benutzer in den Suchergebnissen angezeigt. Die Suche kann bis zu 100 übereinstimmende Ergebnisse zurückgeben.

- 2 Wählen Sie einen Benutzernamen aus.

Die Benutzerinformationen werden in einer Benutzerkarte angezeigt.

### Nächste Schritte

Um Probleme zu beheben, klicken Sie auf die verwandten Registerkarten in der Benutzerkarte.

## Fehlerbehebung bei Benutzern in Horizon Help Desk Tool

In Horizon Help Desk Tool können Sie in einer Benutzerkarte grundlegende Benutzerinformationen anzeigen. Durch Klicken auf Registerkarten auf der Benutzerkarte erhalten Sie weitere Details zu bestimmten Komponenten.

Benutzerdetails werden manchmal in Tabellen angezeigt. Sie können diese Benutzerdetails nach Spalten sortieren.

- Um eine Spalte in aufsteigender Reihenfolge zu sortieren, klicken Sie einmal auf die Spalte.
- Um eine Spalte in absteigender Reihenfolge zu sortieren, klicken Sie zweimal auf die Spalte.

- Um die Spalte nicht zu sortieren, klicken Sie dreimal auf die Spalte.

## Grundlegende Benutzerinformationen

Zeigt grundlegende Benutzerinformationen an wie z. B. Benutzername, Telefonnummer und E-Mail-Adresse sowie den Verbindungsstatus des Benutzers (verbunden oder getrennt). Wenn der Benutzer über eine Desktop-Sitzung verfügt, ist der Status des Benutzers „Verbunden“. Wenn der Benutzer über keine Desktop-Sitzung verfügt, ist der Status des Benutzers „Getrennt“.

Durch Klicken auf die E-Mail-Adresse können Sie dem Benutzer eine E-Mail senden.

## Sitzungen

Die Registerkarte **Sitzungen** zeigt Informationen zu den Desktop-Sitzungen an, mit denen der Benutzer verbunden ist.

Sie können mit dem Textfeld **Filter** Desktop-Sitzungen filtern.

**Hinweis** Auf der Registerkarte **Sitzungen** werden keine Sitzungsinformationen für Sitzungen angezeigt, die auf virtuelle Maschinen von vSphere Client oder ESXi aus zugreifen.

Die Registerkarte **Sitzungen** enthält die folgenden Informationen:

**Tabelle 9-1. Registerkarte „Sitzungen“**

Option	Beschreibung
Status	<p>Zeigt Informationen zum Status der Desktop-Sitzung an.</p> <ul style="list-style-type: none"> <li>■ Wenn die Sitzung verbunden ist, wird der Status „Grün“ angezeigt.</li> <li>■ L, wenn es sich bei der Sitzung um eine lokale Sitzung handelt oder um eine Sitzung, die im lokalen Pod ausgeführt wird.</li> </ul>
Computername	<p>Name der Desktop-Sitzung. Klicken Sie auf den Namen, um die Sitzungsinformationen auf einer Karte anzuzeigen.</p> <p>Um weitere Informationen anzuzeigen, klicken Sie auf die Registerkarten in der Sitzungskarte:</p> <ul style="list-style-type: none"> <li>■ Die Registerkarte <b>Details</b> zeigt die Benutzerinformationen wie z. B. die VM-Informationen und die CPU- bzw. Arbeitsspeicherauslastung an.</li> <li>■ Die Registerkarte <b>Prozesse</b> zeigt Informationen zu den Prozessen an, die CPU und Arbeitsspeicher betreffen.</li> </ul>
Protokoll	Das Anzeigeprotokoll für die Remote-Sitzung.
Typ	Zeigt an, ob es sich beim Desktop um einen veröffentlichten Desktop oder um einen Desktop einer virtuellen Maschine handelt.
Verbindungszeitpunkt	Der Zeitpunkt, an dem die Sitzung mit dem Verbindungsserver verbunden wurde.
Sitzungsdauer	Der Zeitraum, in dem die Sitzung mit dem Verbindungsserver verbunden war.

## Desktops

Die Registerkarte **Desktops** zeigt Informationen zu den veröffentlichten oder virtuellen Desktops an, für die der Benutzer über Berechtigungen verfügt.

**Tabelle 9-2. Desktops**

Option	Beschreibung
Status	<p>Zeigt Informationen zum Status der Desktop-Sitzung an.</p> <ul style="list-style-type: none"> <li>■ Wenn die Sitzung verbunden ist, wird der Status „Grün“ angezeigt.</li> </ul>
Name des Desktop-Pools	Name des Desktop-Pools für die Sitzung.
Desktop-Typ	<p>Zeigt an, ob es sich beim Desktop um einen veröffentlichten Desktop oder um einen Desktop einer virtuellen Maschine handelt.</p> <p><b>Hinweis</b> Wenn die Sitzung in einem anderen Pod im Pod-Verbund ausgeführt wird, werden nicht alle Informationen angezeigt.</p>
Typ	<p>Zeigt Informationen zum Typ der Desktop-Berechtigung an.</p> <ul style="list-style-type: none"> <li>■ „Lokal“ für eine lokale Berechtigung.</li> </ul>
vCenter	<p>Zeigt den Namen der virtuellen Maschine in vCenter Server an.</p> <p><b>Hinweis</b> Wenn die Sitzung in einem anderen Pod im Pod-Verbund ausgeführt wird, werden nicht alle Informationen angezeigt.</p>
Standardprotokoll	Das standardmäßige Anzeigeprotokoll für die Desktop-Sitzung.

## Aktivitäten

Die Registerkarte **Aktivitäten** zeigt die Ereignisprotokollinformationen über die Aktivitäten des Benutzers an. Sie können Aktivitäten zeitlich filtern, indem Sie z. B. als Zeitraum die letzten 12 Stunden oder die letzten 30 Tage angeben, oder nach Administraturname filtern. Klicken Sie auf **Nur Helpdesk-Ereignisse**, um nur nach Horizon Help Desk Tool-Aktivitäten zu filtern. Klicken Sie auf das Symbol „Aktualisieren“, um das Ereignisprotokoll zu aktualisieren. Klicken Sie auf das Symbol „Export“, um das Ereignisprotokoll in eine Datei zu exportieren.

**Hinweis** Die Ereignisprotokollinformationen werden nicht für Benutzer in einer Cloud-Pod-Architektur-Umgebung angezeigt.

Tabelle 9-3. Aktivitäten

Option	Beschreibung
Uhrzeit	<p>Ermöglicht die Auswahl eines Zeitraums. Standardmäßig sind die letzten 12 Stunden ausgewählt.</p> <ul style="list-style-type: none"> <li>■ Letzte 12 Stunden</li> <li>■ Letzte 24 Stunden</li> <li>■ Letzte 7 Tage</li> <li>■ Letzte 30 Tage</li> <li>■ Alle</li> </ul>
Administratoren	Name des Administratorbenutzers.
Meldung	Zeigt Meldungen für einen Benutzer oder Administrator zu den von ihm durchgeführten Aktivitäten an.
Ressourcenname	Zeigt Informationen zum Namen des Desktop-Pools oder der virtuellen Maschine an, für die die Aktivität ausgeführt wurde.

## Sitzungsdetails für das Horizon Help Desk Tool

Die Sitzungsdetails werden auf der Registerkarte **Details** angezeigt, wenn Sie in der Option **Computername** auf der Registerkarte **Sitzungen** auf den jeweiligen Benutzernamen klicken. Sie können die Details für Horizon Client, für den veröffentlichten oder virtuellen Desktop und CPU- bzw. Arbeitsspeicherdetails anzeigen.

### Client

Zeigt Informationen an, die vom Horizon Client-Typ abhängig sind. Sie enthalten Details wie den Benutzernamen, die Horizon Client-Version sowie die IP-Adresse und das Betriebssystem des Clientcomputers.

**Hinweis** Wenn Sie für Horizon Agent ein Upgrade durchgeführt haben, müssen Sie auch Horizon Client auf die aktuelle Version aktualisieren. Andernfalls wird keine Version für Horizon Client angezeigt. Weitere Informationen zum Upgrade von Horizon Client finden Sie im Dokument *Horizon 7-Upgrades*.

### VM

Zeigt Informationen zu virtuellen oder veröffentlichten Desktops an.

Tabelle 9-4. VM-Details

Option	Beschreibung
Computername	Name der Desktop-Sitzung.
Agent-Version	Version von Horizon Agent.
Betriebssystemversion	Betriebssystemversion.
Verbindungsserver	Der Verbindungsserver, mit dem die Sitzung verbunden ist.
Pool	Name des Desktop-Pools.
vCenter	Die IP-Adresse von vCenter Server.

**Tabelle 9-4. VM-Details (Fortsetzung)**

Option	Beschreibung
<b>Sitzungsstatus</b>	Status der Desktop-Sitzung. Der Sitzungsstatus kann „Verbunden“ oder „Verbindung getrennt“ lauten.
<b>Sitzungsdauer</b>	Der Zeitraum, in dem die Sitzung mit dem Verbindungsserver verbunden war.
<b>Statusdauer</b>	Der Zeitraum, in dem für eine Sitzung ein bestimmter Status gültig war.
<b>Anmeldezeitpunkt</b>	Der Zeitpunkt, an dem sich der Benutzer bei der Sitzung angemeldet hat.
<b>Anmeldedauer</b>	Der Zeitraum, in dem der Benutzer am Linux-Desktop angemeldet ist.

## Kennzahlen zur Benutzererfahrung

Zeigt Leistungsdetails für eine virtuelle oder veröffentlichte Desktop-Sitzung an, die das VMware Blast-Anzeigeprotokoll verwendet. Klicken Sie zum Anzeigen dieser Leistungsdetails auf **Mehr**. Klicken Sie zum Aktualisieren dieser Details auf das Symbol „Aktualisieren“.

**Tabelle 9-5. Blast-Anzeigeprotokolldetails**

Option	Beschreibung
<b>Frame-Rate</b>	Die Frame-Rate für eine Blast-Sitzung in Frames pro Sekunde.
<b>Skype-Status</b>	Für Linux-Desktop-Sitzungen wird diese Option als „Nicht verfügbar“ angezeigt.
<b>Blast-Sitzungszähler</b>	<ul style="list-style-type: none"> <li>■ <b>Geschätzte Bandbreite (Uplink).</b> Geschätzte Bandbreite für ein Uplink-Signal.</li> <li>■ <b>Paketverlust (Uplink).</b> Prozentsatz des Paketverlusts für ein Uplink-Signal.</li> </ul>
<b>Blast-Imagezähler</b>	<ul style="list-style-type: none"> <li>■ <b>Gesendete Byte.</b> Gesamtzahl der Bytes der Bildverarbeitungsdaten, die für eine Blast-Sitzung gesendet wurden.</li> <li>■ <b>Empfangene Byte.</b> Gesamtzahl der Bytes der Bildverarbeitungsdaten, die für eine Blast-Sitzung empfangen wurden.</li> </ul>
<b>Blast-Audiozähler</b>	<ul style="list-style-type: none"> <li>■ <b>Gesendete Byte.</b> Gesamtzahl der Bytes der Audiodaten, die für eine Blast-Sitzung gesendet wurden.</li> <li>■ <b>Empfangene Byte.</b> Gesamtzahl der Bytes der Audiodaten, die für eine Blast-Sitzung empfangen wurden.</li> </ul>
<b>Blast-CDR-Zähler</b>	<ul style="list-style-type: none"> <li>■ <b>Gesendete Byte.</b> Gesamtzahl der Bytes der Daten der Clientlaufwerksumleitung, die für eine Blast-Sitzung gesendet wurden.</li> <li>■ <b>Empfangene Byte.</b> Gesamtzahl der Bytes der Daten der Clientlaufwerksumleitung, die für eine Blast-Sitzung empfangen wurden.</li> </ul>

## CPU- und Arbeitsspeicherauslastung sowie Netzwerk- und Festplattenleistung

Zeigt Diagramme für die Auslastung von CPU und Arbeitsspeicher des virtuellen oder veröffentlichten Desktops sowie die Netzwerk- oder Festplattenleistung für das Blast-Anzeigeprotokoll an.

**Hinweis** Nach dem Start oder Neustart von Horizon Agent am Desktop zeigen die Leistungsdiagramme möglicherweise die Zeitachse nicht sofort an. Die Zeitachse erscheint nach wenigen Minuten.

**Tabelle 9-6. CPU-Auslastung**

Option	Beschreibung
Sitzungs-CPU	CPU-Auslastung der aktuellen Sitzung.
Host-CPU	CPU-Auslastung der virtuellen Maschine, der die Sitzung zugewiesen ist.

**Tabelle 9-7. Speicherauslastung**

Option	Beschreibung
Sitzungsarbeitsspeicher	Arbeitsspeicherauslastung der aktuellen Sitzung.
Hostarbeitsspeicher	Arbeitsspeicherauslastung der virtuellen Maschine, der die Sitzung zugewiesen ist.

**Tabelle 9-8. Netzwerkleistung**

Option	Beschreibung
Latenz	<p>Zeigt ein Diagramm der Latenz für die PCoIP- oder Blast-Sitzung an.</p> <p>Die Latenzzeit ist die Roundtripzeit in Millisekunden. Der Leistungsindikator, der diese Latenzzeit verfolgt, ist <b>VMware Blast-Sitzungszähler &gt; RTT</b>.</p>

**Tabelle 9-9. Festplattenleistung**

Option	Beschreibung
Lesen	Die Anzahl der Eingang/Ausgang (E/A)-Lesevorgänge pro Sekunde.
Schreiben	Die Anzahl der E/A-Schreibvorgänge pro Sekunde.
Festplattenlatenz	Zeigt ein Diagramm für die Festplattenlatenz an. Die Festplattenlatenz ist die Zeit in Millisekunden der Eingang/Ausgang-Vorgänge pro Sekunde (Input/Output Operations Per Second, IOPS), die von den Windows-Leistungsindikatoren abgerufen wurden.
Durchschnittliche Lesedauer	Die durchschnittliche Anzahl der zufälligen E/A-Lesevorgänge pro Sekunde.

**Tabelle 9-9. Festplattenleistung (Fortsetzung)**

Option	Beschreibung
Durchschnittliche Schreibdauer	Die durchschnittliche Anzahl der zufälligen E/A-Schreibvorgänge pro Sekunde.
Durchschnittliche Latenz	Die durchschnittliche Latenzzeit in Millisekunden von den IOPS-Daten, die von den Windows-Leistungsindikatoren abgerufen wurden.

## Segmente der Sitzungsanmeldung

Zeigt die Segmente für die Anmeldungsdauer und -nutzung an, die während der Anmeldung erstellt werden.

**Tabelle 9-10. Segmente der Sitzungsanmeldung**

Option	Beschreibung
<b>Anmeldedauer</b>	Die Anmeldedauer wird ermittelt von dem Zeitpunkt, an dem der Benutzer auf den Desktop-Pool klickt, bis zu dem Zeitpunkt, an dem sich der Benutzer beim Linux-Desktop angemeldet hat.
<b>Zeitpunkt der Sitzungsanmeldung</b>	Der Zeitraum, in dem der Benutzer bei der Sitzung angemeldet war.
<b>Anmeldesegmente</b>	<p>Zeigt die Segmente an, die während der Anmeldung erstellt werden.</p> <ul style="list-style-type: none"> <li>■ <b>Brokering.</b> Der gesamte Zeitraum, in dem der Verbindungsserver eine Verbindung für eine Sitzung herstellt oder trennt. Der Wert wird ermittelt von dem Zeitpunkt, an dem der Benutzer auf den Desktop-Pool klickt, bis zu dem Zeitpunkt, an dem die Tunnelverbindung eingerichtet ist. Enthält die Zeitangaben für Verbindungsserver-Vorgänge wie z. B. die Benutzerauthentifizierung, die Computerauswahl und die Computervorbereitung für die Einrichtung der Tunnelverbindung.</li> <li>■ <b>Interaktiv.</b> Der gesamte Zeitraum, in dem Horizon Agent eine Verbindung für eine Sitzung herstellt oder trennt. Die Anmeldedauer wird ermittelt von dem Zeitpunkt, an dem Blast Extreme die Tunnelverbindung verwendet bis zu dem Zeitpunkt, an dem sich der Benutzer beim Linux-Desktop angemeldet hat.</li> <li>■ <b>Protokoll der Verbindung.</b> Gesamtzeit für die Erstellung des PCoIP- oder Blast-Protokolls der Verbindung während des Anmeldevorgangs.</li> <li>■ <b>Anmeldeskript.</b> Gesamtzeit für die Ausführung des Anmeldeskripts vom Start bis zur Fertigstellung.</li> <li>■ <b>Authentifizierung.</b> Gesamtzeit für den Verbindungsserver zur Authentifizierung der Sitzung.</li> <li>■ <b>Start der VM.</b> Gesamtzeit zum Starten einer virtuellen Maschine. Dieser Zeitraum beinhaltet das Starten des Betriebssystems, das Fortsetzen einer angehaltenen Maschine und die Zeit, bis Horizon Agent signalisiert, dass es für eine Verbindung bereit ist.</li> </ul>

## Sitzungsprozesse für das Horizon Help Desk Tool

Die Sitzungsprozesse werden auf der Registerkarte **Prozesse** angezeigt, wenn Sie in der Option **Computernamen** auf der Registerkarte **Sitzungen** auf einen Benutzernamen klicken.

### Prozesse

Für jede Sitzung können Sie weitere ausführliche Informationen zu den Prozessen anzeigen, die CPU und Arbeitsspeicher betreffen. Wenn Sie feststellen, dass die CPU- und die Arbeitsspeicherauslastung für eine Sitzung ungewöhnlich hoch ist, können Sie die Details zum jeweiligen Prozess auf der Registerkarte **Prozesse** einsehen.



Für RDS-Host-Sitzungen zeigt die Registerkarte **Prozesse** die aktuellen RDS-Host-Sitzungsprozesse, die durch den aktuellen Benutzer oder den aktuellen Systemprozess gestartet wurden.

**Tabelle 9-11. Sitzungsprozessdetails**

Option	Beschreibung
Prozessname	Name des Sitzungsprozesses. Beispiel: chrome.exe.
CPU	CPU-Auslastung durch den Prozess in Prozent.
Arbeitsspeicher	Arbeitsspeicherauslastung durch den Prozess in KB.
Laufwerk	IOPS des Speicherdatenträgers. Wurde mit der folgenden Formel berechnet:  (Gesamte E/A-Bytes zum aktuellen Zeitpunkt) – (Gesamte E/A-Bytes eine Sekunde vor dem aktuellen Zeitpunkt).  Diese Berechnung kann einen Wert von 0 KB pro Sekunde ergeben, wenn im Task-Manager ein positiver Wert angezeigt wird.
Benutzername	Name des Benutzers, der für den Prozess zuständig ist.
Host-CPU	CPU-Auslastung der virtuellen Maschine, der die Sitzung zugewiesen ist.
Hostarbeitsspeicher	Arbeitsspeicherauslastung der virtuellen Maschine, der die Sitzung zugewiesen ist.
Prozesse	Anzahl der Prozesse in der virtuellen Maschine
Aktualisieren	Mit dem Symbol „Aktualisieren“ wird die Liste der Prozesse aktualisiert.
Prozess beenden	Beendet einen aktuell ausgeführten Prozess.  <b>Hinweis</b> Um einen Prozess beenden zu können, müssen Sie über die Rolle „Helpdesk-Administrator“ verfügen.  Um einen Prozess zu beenden, wählen Sie diesen aus und klicken Sie auf die Schaltfläche <b>Prozess beenden</b> .  Kritische Prozesse wie Windows-Kernprozesse, die unter Umständen auf der Registerkarte <b>Prozesse</b> aufgeführt werden, können nicht beendet werden. Wenn Sie einen kritischen Prozess beenden, zeigt Horizon Help Desk Tool eine Meldung, die besagt, dass der Systemprozess nicht beendet werden kann.

## Fehlerbehebung bei Linux-Desktop-Sitzungen in Horizon Help Desk Tool

Sie können in Horizon Help Desk Tool Fehlerbehebungen für Linux-Desktop-Sitzungen basierend auf dem Verbindungsstatus eines Benutzers durchführen.

### Voraussetzungen

- Starten Sie Horizon Help Desk Tool.

## Verfahren

- 1 Klicken Sie auf der Benutzerkarte auf die Registerkarte **Sitzungen**.

Eine Karte mit Leistungsinformationen wird angezeigt, die die CPU- sowie die Arbeitsspeicherauslastung und Informationen zu Horizon Client sowie zum virtuellen oder veröffentlichten Desktop enthält.

- 2 Wählen Sie eine Option für die Fehlerbehebung aus.

Option	Aktion
<b>Nachricht senden</b>	<p>Sendet eine Nachricht an den Benutzer auf dem veröffentlichten oder virtuellen Desktop. Sie können den Schweregrad der Nachricht durch Angabe von „Warnung“, „Info“ oder „Fehler“ auswählen.</p> <p>Klicken Sie auf <b>Nachricht senden</b>, geben Sie den Schweregrad und die Nachrichtendetails ein und klicken Sie auf <b>Absenden</b>.</p>
<b>Neustarten</b>	<p>Initiiert den Neustart auf dem virtuellen Desktop. Diese Funktion ist nicht für Sitzungen veröffentlichter Desktops verfügbar.</p> <p>Klicken Sie auf <b>VDI neu zu starten</b>.</p>
<b>Verbindung trennen</b>	<p>Trennt die Desktop- oder Anwendungssitzung.</p> <p>Klicken Sie auf <b>Mehr &gt; Trennen</b>.</p>
<b>Abmelden</b>	<p>Initiiert den Abmeldevorgang für einen veröffentlichten Desktop oder einen virtuellen Desktop.</p> <p>Klicken Sie auf <b>Mehr &gt; Abmelden</b>.</p>
<b>Zurücksetzen</b>	<p>Initiiert das Zurücksetzen der virtuellen Maschine. Diese Funktion ist nicht für veröffentlichte Desktops verfügbar.</p> <p>Klicken Sie auf <b>Mehr &gt; VM zurücksetzen</b>.</p> <p><b>Hinweis</b> Nicht gespeicherte Änderungen des Benutzers können verloren gehen.</p>

## Ermitteln von Diagnoseinformationen für eine Horizon 7 for Linux-Maschine

Mit der Ermittlung von Diagnoseinformationen können Sie den technischen Support von VMware bei der Diagnose und Behandlung von Problemen mit einer Horizon 7 for Linux-Maschine unterstützen. Dazu erstellen Sie ein DCT-Bundle (Data Collection Tool, Datenerfassungstool), in dem die Informationen zur Konfiguration der Maschine zusammengestellt und in einem komprimierten TAR-Archiv protokolliert werden.

## Verfahren

- 1 Melden Sie sich bei der virtuellen Linux-Maschine als Benutzer mit den erforderlichen Rechten an.
- 2 Öffnen Sie eine Eingabeaufforderung und führen Sie das `dct-debug.sh`-Skript aus.

```
sudo /usr/lib/vmware/viewagent/bin/dct-debug.sh
```

Das Skript generiert ein TAR-Archiv mit dem DCT-Bundle. Beispiel:

```
ubuntu-12-vdm-sdct-20150201-0606-agent.tgz
```

Das TAR-Archiv wird in dem Verzeichnis generiert, in dem das Skript ausgeführt wurde (das aktuelle Arbeitsverzeichnis).

## Fehler beim Trennen der Verbindung auf dem Horizon Client für ein iPad Pro durch Horizon Agent

Die SUSE-Horizon Agent-Verbindung kann nach einem Neustart oder Herunterfahren auf einem iPad Pro Horizon Client nicht getrennt werden.

### Problem

Wenn Sie eine virtuelle SUSE-Maschine auf einem iPad Pro Horizon Client neu starten oder herunterfahren, antwortet der Desktop nicht. Horizon Agent kann nicht getrennt werden.

### Ursache

Die SUSE-Maschine sendet nach dem Neustart oder Herunterfahren die Meldungen an Horizon Client möglicherweise nicht richtig.

### Lösung

- ◆ Trennen Sie die Desktop-Verbindung manuell vom iPad Pro Horizon Client

## SLES 12 SP1-Desktop wird nicht automatisch aktualisiert

SLES 12 SP1 wird in einem Modus mit mehreren Monitoren nicht automatisch aktualisiert, wenn Sie ein GNOME-Terminal hineinziehen.

### Problem

Wenn Sie SLES 12 SP1 in einem Modus mit mehreren Monitoren starten und zum Fenstermodus zurückkehren, wird der Desktop nicht automatisch aktualisiert, wenn Sie ein GNOME-Terminal hineinziehen.

### Ursache

Das GNOME-Terminal antwortet nicht auf das Hineinziehen.

### Lösung

- 1 Beenden Sie die GNOME-Shell-Sitzung.

```
kill -9 <process id of gnome-shell>
```

- 2 Starten Sie die GNOME-Shell-Sitzung erneut.

## Fehlerhafte SSO-Verbindung zu einem PowerOff-Agenten

Single Sign-On (SSO) stellt keine Verbindung zu einem PowerOff-Agenten her.

### Problem

Wenn Sie sich als Broker anmelden und eine Verbindung zu einem Agenten herstellen, treten beim Verbinden von SSO zum PowerOff-Agenten Fehler auf.

### Lösung

- ◆ Melden Sie sich manuell am Desktop an oder trennen Sie die Verbindung und stellen Sie eine erneute Verbindung zum Agenten her.

## Nicht erreichbare VM nach dem Erstellen eines manuellen Desktop-Pools für Linux

Der Status der virtuellen Maschine antwortet nicht.

### Problem

Nach dem Erstellen eines manuellen Desktop-Pools lautet der Status der virtuellen Maschine möglicherweise „Warten auf Agent“ oder „Nicht erreichbar“.

### Ursache

Es liegen möglicherweise verschiedene Benutzerfehlerkonfigurations- oder Setup-Probleme dahingehend vor, dass der Status der virtuellen Maschine „Nicht erreichbar“ oder „Warten auf Agent“ lautet.

- Stellen Sie sicher, dass die Option `machine.id` in der VMX-Konfigurationsdatei der virtuellen Maschine vorhanden ist.

Wenn sie nicht vorhanden ist, müssen Sie sicherstellen, dass die virtuelle Maschine richtig zum Desktop-Pool hinzugefügt wurde. Erstellen Sie ansonsten den Desktop-Pool, um dem Broker zu ermöglichen, die Option zur VMX-Konfigurationsdatei neu zu schreiben.

- Stellen Sie sicher, dass das VMware-Tool oder Open VM-Tool richtig installiert ist.

Wenn die Schritte zum Installieren des VMware-Tools oder Open VM-Tools nicht richtig ausgeführt wurden, ist der `vmware-rpctool`-Befehl unter PATH auf der virtuellen Linux-Maschine möglicherweise nicht vorhanden. Sie müssen die Anleitung befolgen, um das VMware Tool oder Open VM-Tool zu installieren.

Führen Sie den Befehl nach dem Abschließen der Installation aus.

```
#vmware-rpctool "machine.id.get"
```

Die `machine.id`-Werte werden aus der VMX-Konfigurationsdatei der virtuellen Maschinen aufgeführt.

- Überprüfen Sie, ob der vollqualifizierte Domänenname des Brokers in einer IP-Adresse in der virtuellen Linux-Maschine des Agenten aufgelöst werden kann.