# VMware Horizon FLEX-Administratorhandbuch

Horizon FLEX 1.6

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

DE-001873-00

vmware®

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

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

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

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

docfeedback@vmware.com



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

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

# Inhalt

# VMware Horizon FLEX -Administratorhandbuch

Das *VMware Horizon FLEX-Administratorhandbuch* erläutert die Installation und Verwaltung von VMware Horizon® FLEX™.

## Zielgruppe

Die vorliegenden Informationen richten sich an Benutzer, die Horizon FLEX installieren möchten. Die Erläuterungen sind für erfahrene Windows-Systemadministratoren gedacht, die mit der Technologie virtueller Maschinen vertraut sind.

# 1 Einführung in Horizon FLEX

Horizon FLEX ist eine richtlinienbasierte, Container-Desktop-Lösung, mit der IT-Administratoren lokale Desktops für Endbenutzer erstellen, sichern und verwalten können. Die Endbenutzer arbeiten dabei in einer eingeschränkten virtuellen Maschine namens „virtuelle Horizon FLEX-Maschine“ auf ihren eigenen Computern. Da virtuelle Horizon FLEX-Maschinen lokal auf Endbenutzercomputern gespeichert werden, kann auf die Unternehmensanwendungen offline zugegriffen werden.

Dieses Kapitel behandelt die folgenden Themen:



## Horizon FLEX -Komponenten

Horizon FLEX ist eine Kombination von VMware-Komponenten, inklusive Mirage, Fusion Pro und Workstation Player.

**VMware Mirage® für Horizon FLEX**

Der von Horizon FLEX verwendete Mirage-Server. Der Server stellt eine Verwaltung für virtuelle Horizon FLEX-Maschinen zur Verfügung. Sie können mithilfe der Layer-Technologie von Mirage für Horizon FLEX virtuelle Maschinen verwalten, sichern und erweitern. Die Verwendung von Mirage für Horizon FLEX ist optional. Sie haben auch die Möglichkeit, andere Image-Verwaltungs-Tools zum Verwalten virtueller Horizon FLEX-Maschinen verwenden.

**Horizon FLEX-Richtlinienserver**

Der Standard-Mirage-Server mit einer Horizon FLEX-spezifischen Erweiterung der Funktionalität. Horizon FLEX-Richtlinienserver wird nach der Anwendung der Horizon FLEX-Lizenz für Mirage für Horizon FLEX aktiviert.

**Horizon FLEX-Verwaltungskonsole**

Die Web Management-Benutzeroberfläche für Horizon FLEX-Richtlinienserver. Horizon FLEX-Verwaltungskonsole ist in der Mirage Web Manager-Komponente enthalten. Sie können mithilfe von Horizon FLEX-Verwaltungskonsole Verwaltungsaufgaben für virtuelle Maschinen durchführen, z. B.:

- Verwalten des Bestands an virtuellen Maschinen
- Durchsuchen einer Liste von Benutzern und Gruppen im Active Directory-Dienst

- Erteilen von Berechtigungen für Benutzer und Gruppen für eine oder mehrere virtuelle Maschinen
- Festlegen der Richtlinien für virtuelle Maschinen für eine vorhandene Berechtigung
- Verhindern des Zugriffs von Benutzern auf virtuelle Maschinen durch eine Remotesperre
- Prüfen der Details und des Status virtueller Maschinen zu jeder Zeit

**Horizon FLEX-Client**

Die Clientsoftware, mit der Endbenutzer die virtuellen Horizon FLEX-Maschinen auf ihre lokalen Computer herunterladen können. Clients sind VMware Fusion Pro® für Mac-Computer und VMware Workstation Player™ für Windows-Computer. Fusion Pro und Workstation Player sind im Horizon FLEX-Paket enthalten. Ein Lizenzschlüssel steht sowohl für Fusion Pro als auch für Workstation Player zur Verfügung.

**VirtuelleHorizon FLEX-Maschine**

Die virtuelle Maschine, die Endbenutzer auf Ihren eigenen Computern ausführen können. Mit Fusion Pro können Sie virtuelle Maschinen der Quelle für virtuelle Horizon FLEX-Maschinen erstellen. Fusion Pro ist im Horizon FLEX-Paket enthalten. Ein Horizon FLEX Server unterstützt bis zu 1.000 Benutzer.

**HINWEIS** Sie können auch mit VMware Workstation Pro™ eine virtuelle Maschine der Quelle erstellen. Workstation Pro ist nicht im Horizon FLEX-Paket enthalten.

### Über Mirage

Mirage ist ein wesentliches Element für den Betrieb und die Anwendung virtueller Horizon FLEX-Maschinen.

Horizon FLEX verwendet einen Teil der Funktionen von Mirage.

- Mirage-Server
  - Mirage Management Server
- Mirage Web Manager
  - Mirage Management Console

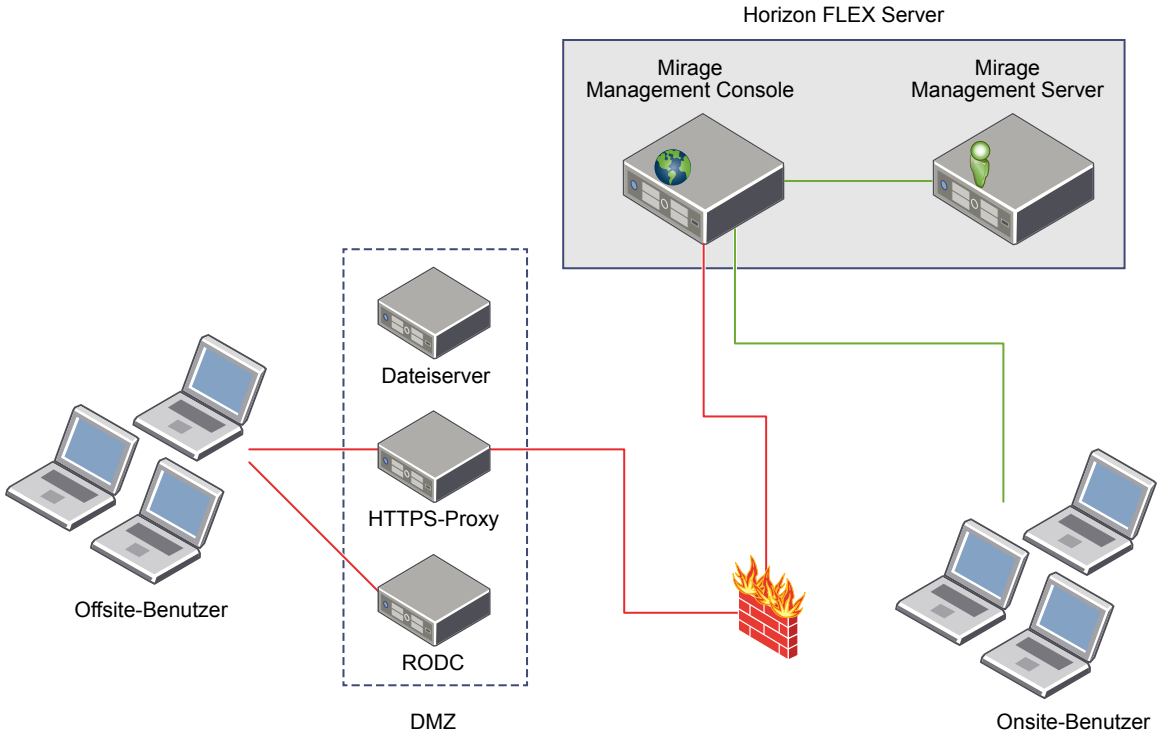
Dieses Handbuch erläutert dementsprechend nur einen Teilbereich von Mirage. Vollständige Informationen zu Mirage erhalten Sie in der Mirage-Dokumentation unter https://www.vmware.com/support/pubs/mirage_pubs.html.

## Horizon FLEX -Architektur

Zu einer typischen Horizon FLEX-Bereitstellung gehören der Horizon FLEX Server, ein Dateiserver, ein HTTPS-Proxy, ein schreibgeschützter Domänencontroller (RODC) sowie Offsite- und Onsite-Endbenutzersysteme.

Abbildung 1-1 zeigt die Beziehungen zwischen den Hauptkomponenten einer Horizon FLEX-Bereitstellung.

**Abbildung 1-1.** Beispiel- Horizon FLEX -Bereitstellung ohne Mirage




## Horizon FLEX -Server

Der Horizon FLEX Server besteht aus der Horizon FLEX Admin Console und dem Horizon FLEX Policy Server. Der Horizon FLEX Server bietet die im Folgenden aufgeführte Funktionalität.

- Zuweisung von virtuellen Horizon FLEX-Maschinen zu Benutzern und Gruppen aus einem Verzeichnisservice
- Protokollierung der aktuell von einzelnen Benutzern verwendeten virtuellen Horizon FLEX-Maschinen
- Bereitstellung einer Sicherheitszertifikatsverwaltung zur Sicherstellung einer sicheren und vertrauenswürdigen Kommunikation zwischen den bereitgestellten virtuellen Horizon FLEX-Maschinen und dem Horizon FLEX Server.
- Durchsetzung der Richtlinieneinstellungen für den Client
- Änderung der Richtlinieneinstellungen für die Kombination eines bestimmten Benutzers mit einer virtuellen Horizon FLEX-Maschine
- Überwachung des Status einer virtuellen Horizon FLEX-Maschine

Mirage Management Console ist die grafische Benutzeroberfläche, mit der bereitgestellte Endpunkte gewartet, verwaltet und überwacht werden können. Mirage Web Manager verfügt über die gleiche Funktionalität wie Mirage Management Console.

Standardmäßig wird Port 7443 vom Horizon FLEX Policy Server für den externen Zugriff und Port 8443 vom Mirage Management Server zur Kommunikation mit dem Horizon FLEX Policy Server verwendet. Um auf die erforderlichen Ports zugreifen zu können, müssen Sie Ihre Firewall-Richtlinie entsprechend konfigurieren. Eine vollständige Liste der von Mirage verwendeten Ports finden Sie in der Mirage-Dokumentation unter https://www.vmware.com/support/pubs/mirage_pubs.html.

### Dateiserver

Ein Dateiserver speichert die TAR-Dateien mit den Dateien der virtuellen Maschine der Quelle für virtuelle Horizon FLEX-Maschinen. Der Dateiserver kann sich auf jedem Server befinden, auf den ein Client-Benutzer ohne Eingabe von Anmeldeinformationen zugreifen kann. Der Dateiserver befindet sich in diesem Beispiel innerhalb der DMZ, aber dies ist nicht erforderlich.

### HTTPS-Proxy

Ein HTTPS-Proxy ermöglicht Offsite-Endbenutzersystemen die Verbindung mit Mirage Management Console und das Abrufen von Richtlinienaktualisierungen.

### RODC

Ein schreibgeschützter Domänencontroller (RODC) ermöglicht Endbenutzer-Bürosystemen die Anmeldung bei ihren virtuellen Horizon FLEX-Maschinen und den Beitritt zur Active Directory-Domäne beim ersten Start der virtuellen Maschine. Ein RODC ist nur erforderlich, wenn die Anmeldung externer Benutzer ohne VPN zulässig sein soll. Der RODC befindet sich innerhalb der DMZ.

### Lastausgleich

Horizon FLEX unterstützt den Lastausgleich mit mehreren Richtlinienservern. Richten Sie einen Aktiv/Passiv-Windows-Serversatz ein, um Fehlertoleranz für Ihre Horizon FLEX-Topologie zu erreichen.

## Systemanforderungen für Horizon FLEX

Jedes Produkt des Horizon FLEX-Pakets verfügt über spezielle Systemanforderungen.

| | |
|---|---|
| **Systemanforderungen für den Horizon FLEX Server und den Mirage-Server.** | Weitere Informationen finden Sie im Abschnitt „Systemanforderungen für den Horizon FLEX Server“, auf Seite 11. |
| **Mirage für Horizon FLEX** | Die Systemanforderungen für Horizon FLEX 1.6 entsprechen denen für Mirage 5.5. Erläuterungen dazu finden Sie in der Mirage-Dokumentation unter https://www.vmware.com/support/pubs/mirage_pubs.html. |
| **Horizon FLEX-Client für Mac** | Horizon FLEX 1.6 verwendet Fusion Pro 8.0 als Client-Software für Mac-Clients. Horizon FLEX 1.6 ist mit früheren Versionen von Fusion Pro nicht kompatibel.<br>Zu den Hardware- und Softwareanforderungen für Fusion Pro erhalten Sie ausführliche Informationen unter *VMware Horizon FLEX Client-Benutzerhandbuch*. |
| **Horizon FLEX-Client für Windows** | Horizon FLEX 1.6 verwendet Workstation Player 12.0 als Client-Software für Windows-Clients. Horizon FLEX 1.6 ist mit früheren Versionen von Player Pro nicht kompatibel.<br>Zu den Hardware- und Softwareanforderungen für Workstation Player erhalten Sie ausführliche Informationen unter *VMware Horizon FLEX Client-Benutzerhandbuch*. |
| **Workstation Pro** | Sie können mit Workstation Pro 12.0 eine virtuelle Maschine der Quelle erstellen und öffnen, aber Workstation Pro kann keine virtuelle Horizon FLEX-Maschine herunterladen.<br>Workstation Pro ist nicht im Horizon FLEX-Installationspaket enthalten. |

Zu den Hardware- und Softwareanforderungen für Workstation Pro erhalten Sie ausführliche Informationen in der Workstation Pro-Dokumentation unter https://www.vmware.com/support/pubs/ws_pubs.html.

# Systemanforderungen für den Horizon FLEX Server

Die Horizon FLEX-Umgebung umfasst Systemanforderungen für den Horizon FLEX Server und den Mirage-Server.

## Systemanforderungen für den Horizon FLEX Server

- CPU mindestens: 1 Quad-Core-Prozessor oder 2 vCPU
- 2,26 GHz Intel Core-Geschwindigkeit oder gleichwertig
- RAM mindestens: 512 MB; empfohlen 4 GB
- Festplattenspeicher mindestens: 10 GB+; empfohlen 40 GB+
- Windows 2008 R2, Windows 2012 oder höher
- .NET 4.5.1 und höher
- IIS 7.0+ mit IIS 6 Management Compatibility, mit ASP und ASP.NET
- Active Directory: Administratorkonto mit ausreichenden Berechtigungen, um Computerobjekte zur Domäne hinzuzufügen
- SQL 2008 Express oder SQL Server 2008 (erforderlich für die Mirage-Installation)
- HTTP-Dateifreigabe oder virtuelles IIS-Verzeichnis mit verfügbarem Platz für virtuelle Maschinen der Quelle
- Firewall-Ports für die Horizon FLEX Admin Console
  - Standard-Ports für IIS und Horizon FLEX Web App: HTTP – 7080, HTTPS – 7443 (Aufrufe für den HTTP-Port werden an den HTTPS-Port weitergeleitet.)
  - Der Mirage Management Server überwacht Anfragen von Windows Communication Foundation (WCF) auf dem folgenden Port: HTTP – 8443
- Bei Verwendung von SSL ist ein Zertifikat für den Horizon FLEX Server erforderlich.

## Anforderungen für den Mirage -Server

- CPU mindestens: 4 vCPU; empfohlen 8 vCPU
- RAM mindestens: 8 GB; empfohlen 16 GB
- 146 GB freier Festplattenspeicher
- Windows 2008 R2, Windows 2012 oder höher
- .NET 4.5.1 und höher

# Netzwerkanforderungen für Horizon FLEX

Horizon FLEX ermöglicht Endbenutzern die Ausführung von Unternehmensanwendungen, auch wenn keine Verbindung zum Netzwerk besteht. Virtuelle Horizon FLEX-Maschinen werden lokal für eine komplette Desktop-Anwendung gespeichert, für die keine Netzwerkverbindung notwendig ist.

Eine Netzwerkverbindung zwischen dem Horizon FLEX-Richtlinienserver und dem Horizon FLEX-Client ist in folgenden Fällen erforderlich:

- Beim ersten Herunterladen der virtuellen Horizon FLEX-Maschine auf den lokalen Computer des Benutzers.
- Für die Registrierung einer virtuellen Horizon FLEX-Maschine, die auf einem USB-Gerät oder auf dem lokalen Computer des Benutzers bereitgestellt wurde.
- Für den Erhalt von Aktualisierungen der Einschränkungen und Richtlinien für eine virtuelle Horizon FLEX-Maschine.

Wenn Sie eine virtuelle Maschine der Quelle für eine virtuelle Horizon FLEX-Maschine registrieren, geben Sie eine URL für den Standort zum Herunterladen des Pakets der virtuellen Maschine an. Die Computer der Endbenutzer müssen auf den Download-Ordner zugreifen können, damit diese virtuelle Maschinen herunterladen können.

# Unterstützte Host- und Gastbetriebssysteme

Der lokale Computer, auf dem Endbenutzer Horizon FLEX-Client anwenden, muss mit einem unterstützten Hostbetriebssystem ausgestattet sein. Für eine virtuelle Horizon FLEX-Maschine ist ein unterstütztes Gastbetriebssystem erforderlich.

## Unterstützte Hostbetriebssysteme

Mithilfe eines physischen Computers mit einem der im Folgenden aufgeführten Betriebssysteme können Ihre Endbenutzer Horizon FLEX-Client ausführen und auf ihre virtuellen Horizon FLEX-Maschinen zugreifen.

**Tabelle 1-1.** Unterstützte Hostbetriebssysteme

| Horizon FLEX-Client | Unterstützte Betriebssysteme |
|---|---|
| Workstation Player | ■ Windows 7<br>■ Windows 8.1 Enterprise<br>■ Windows Server 2012 R2<br>■ Windows 8<br>■ Windows 8.1 Pro<br>■ Windows 10<br>**Hinweis** Workstation Player unterstützt nur 64-Bit-Betriebssysteme. |
| Fusion Pro | ■ Mac OS X 10.11<br>■ Mac OS X 10.10<br>■ Mac OS X 10.9 |

## Unterstützte Gastbetriebssysteme

Eine virtuelle Horizon FLEX-Maschine kann eines der folgenden Gastbetriebssysteme enthalten.

- Windows 10
- Windows 8,1
- Windows 7

- Windows XP
- Windows Server 2012 R2
- Ubuntu 14.04

# Installieren von Horizon FLEX 2

Zur Installation von Horizon FLEX gehört das Installieren der Horizon FLEX Server- und -Client-Komponenten, das Erstellen von Ordnern zum Speichern virtueller Horizon FLEX-Maschinen, das Vorbereiten von Active Directory, das Einrichten von Zertifikaten sowie das Erstellen und Bereitstellen von virtuellen Horizon FLEX-Maschinen.

Dieses Kapitel behandelt die folgenden Themen:



## Übersicht über die Installation von Horizon FLEX

Horizon FLEX ist eine Kombination von VMware-Komponenten, inklusive Mirage, Fusion Pro und Workstation Player. Die Installation von Horizon FLEX umfasst die gesamte Installation dieser Komponenten und die Durchführung zusätzlicher Horizon FLEX-spezifischer Aufgaben. Für eine erfolgreiche Horizon FLEX-Bereitstellung ist die Kenntnis der Abfolge der erforderlichen Aufgaben notwendig.

Vor der Installation von Horizon FLEX müssen Sie sicherstellen, dass die gesamten Hardware- und Softwareanforderungen erfüllt sind, dass Sie über gültige Lizenzen verfügen und dass Sie die Installationsprogramme für die Horizon FLEX-Komponenten von der VMware Horizon FLEX-Produkt-Download-Seite heruntergeladen haben.

Zur Installation von Horizon FLEX müssen folgende Schritte durchgeführt werden:

1 Installieren Sie das Mirage-System.

  Weitere Informationen hierzu finden Sie unter „Installieren und Konfigurieren von Mirage für Horizon FLEX“, auf Seite 16.

2 Richten Sie die Zertifikate für die virtuellen Horizon FLEX-Maschinen ein.

  Weitere Informationen hierzu finden Sie unter Kapitel 3, „Einrichten von Zertifikaten für virtuelle Horizon FLEX-Maschinen“, auf Seite 25.

3 Erstellen Sie einen Download-Ordner für das Speichern der Pakete Ihrer virtuellen Horizon FLEX-Maschinen.

   Weitere Informationen hierzu finden Sie unter „Erstellen eines Download-Ordners für Pakete virtueller Horizon FLEX-Maschinen“, auf Seite 17.

4 Fügen Sie in IIS ein virtuelles Verzeichnis für den Download-Ordner Ihrer virtuellen Horizon FLEX-Maschine hinzu und bearbeiten Sie die Sitebindungen.

   Weitere Informationen hierzu finden Sie unter „Konfigurieren des IIS-SSL-Serverzertifikats für den Horizon FLEX Server“, auf Seite 18.

5 (Optional) Konfigurieren Sie Horizon FLEX zum Synchronisieren von Elementen nur in einer ausgewählten Active Directory-Organisationseinheit (OE).

   Weitere Informationen hierzu finden Sie unter „Konfigurieren von Active Directory-Einstellungen“, auf Seite 19.

6 Testen Sie die Verbindung zu Horizon FLEX-Verwaltungskonsole.

   Weitere Informationen hierzu finden Sie unter „Testen der Horizon FLEX-Verwaltungskonsole-Verbindung“, auf Seite 20.

7 Installieren Sie Horizon FLEX-Client auf jedem Endbenutzerhost oder zeigen Sie Endbenutzern, wie Horizon FLEX-Client auf ihren eigenen Computern installiert werden kann.

   Weitere Informationen hierzu finden Sie unter „Installieren des Horizon FLEX Client für Endbenutzer“, auf Seite 20.

8 Erstellen und Bereitstellen virtueller Horizon FLEX-Maschinen

   Weitere Informationen hierzu finden Sie unter Kapitel 4, „Erstellen und Bereitstellen virtueller Horizon FLEX-Maschinen“, auf Seite 35.

## Installieren und Konfigurieren von Mirage für Horizon FLEX

Der erste Schritt zur Installation von Horizon FLEX ist die Installation und Konfiguration des Mirage-Systems.

Das Horizon FLEX-Paket enthält die folgenden Komponenten:

- VMware Mirage für Horizon FLEX (die zentrale Mirage-Software)
- Mirage PowerCLI für Windows
- Mirage Gateway-Anwendungssoftware

Laden Sie die Installationsdateien von der Horizon FLEX Server-Produkt-Download-Seite herunter.

Zur Mirage-Bereitstellung gehört die Installation folgender Komponenten:

1 Mirage Management Server

2 Mirage Server

3 Mirage Management Console

4 Mirage Web Manager

Um das Mirage-System zu installieren und zu konfigurieren, folgen Sie der Installationsanleitung in der Mirage-Dokumentation unter https://www.vmware.com/support/pubs/mirage_pubs.html.

Wenn Sie das Mirage-System installieren, müssen Sie für einen reibungslosen Betrieb bestimmte Optionen für den Horizon FLEX Server auswählen.

- Die Mirage-Server und Mirage-Konsolen werden nur benötigt, wenn Sie den Mirage-Client in den virtuellen Maschinen der Quelle installieren.

- Wenn die Images der virtuellen Maschine auf demselben System wie der Horizon FLEX Server abgelegt werden, platzieren Sie die Images auf dem IIS-„Standard-Web“-Server.
- Der Web-Managementserver und der Mirage-Managementserver können auf demselben Server installiert werden, aber sie auf unterschiedlichen Servern zu installieren, verbessert die Skalierbarkeit. Der SQL Server sollte auf einem anderen Server installiert werden als der Web-Managementserver und der Mirage-Managementserver .
- Während der Installation von Mirage Server wählen Sie SSL als Übertragungssystem für Mirage Server. SSL ist für die Anwendung der Mirage Gateway-Funktion zum externen Zugriff und zur externen Verwaltung von Horizon FLEX-Systemen erforderlich. Vor der Konfiguration von Mirage Server für SSL müssen Sie das Server-SSL-Zertifikat installieren.
- Vor der Installation von Mirage Web Manager müssen Sie sicherstellen, dass .NET Framework 4.5.1 auf dem Server installiert ist.
- Mirage Management Server muss als Benutzer mit Leseberechtigungen für Active Directory ausgeführt werden. Wenn eine virtuelle Horizon FLEX-Maschine einer Active Directory-Domäne beitreten soll, muss Mirage Management Server als Benutzer mit Berechtigungen zum Beitritt in Domänen ausgeführt werden.

# Erstellen eines Download-Ordners für Pakete virtueller Horizon FLEX - Maschinen

Im Zuge der Bereitstellung einer virtuellen Horizon FLEX-Maschine müssen Sie Ihre Pakete virtueller Maschinen der Quelle in das TAR-Format (`.tar`) komprimieren, damit Endbenutzer Ihre virtuellen Horizon FLEX-Maschinen problemlos und schnell herunterladen können. Für das Speichern dieser TAR-Dateien ist das Erstellen eines Download-Ordners erforderlich.

### Vorgehensweise

1 Erstellen Sie den Download-Ordner auf dem Horizon FLEX Server oder auf einem anderen Server.

   Der Download-Ordner muss sich nicht auf dem Horizon FLEX Server befinden, die darin enthaltenen Dateien müssen jedoch ohne Authentifizierungsanforderung heruntergeladen werden können. Wenn Sie den Download-Ordner auf demselben IIS-Server erstellen wie den Horizon FLEX Server, können Sie den Ordner unter dem standardmäßigen IIS-Dokumentstammordner der Standardwebsite erstellen. Erstellen Sie den Download-Ordner nicht unter der VMware Mirage Management-Website.

2 Damit Benutzer die darin enthaltenen Dateien herunterladen können, müssen dem Download-Ordner entsprechende Berechtigungen zugewiesen werden.

3 (Optional) Geben Sie den Download-Ordner mit einer Administratorgruppe frei, z. B. für Horizon FLEX-Administratoren. Dabei kann es sich um eine Administratorgruppe für Benutzer zur Verwaltung von Horizon FLEX-Bereitstellungen handeln.

   Damit wird die Registrierung Ihrer virtuellen Maschine der Quelle mit Horizon FLEX-Richtlinienserver potenziell vereinfacht.

### Weiter

Weitere Informationen hierzu finden Sie unter „Konfigurieren des IIS-SSL-Serverzertifikats für den Horizon FLEX Server“, auf Seite 18.

# Einrichten eines Zertifikats für den Horizon FLEX Server mithilfe von OpenSSL

Sie können mithilfe von OpenSSL ein selbstsigniertes Zertifikat für den Horizon FLEX Server erstellen.

### Voraussetzungen

Die OpenSSL-Konfigurationsdatei wird auf dem Mirage Gateway-Server erstellt. Informationen dazu finden Sie in der Mirage-Dokumentation unter https://www.vmware.com/support/pubs/mirage_pubs.html

### Vorgehensweise

1 Erstellen Sie an der OpenSSL-Kommandozeile ein Zertifikat: **`$ openssl req –new –days Ablaufzeitpunkt –x509 –newkey rsa:2048 – keyout Schlüsseldateiname –outZertifikatsdateiname – nodes`**

*Ablaufzeitpunkt* steht für die Anzahl der Tage, die das Zertifikat gültig sein soll, *Schlüsseldateiname* stellt den Dateinamen für den Schlüssel dar und *Zertifikatsdateiname* den Namen des neuen Zertifikats.

Es werden ein selbstsigniertes Zertifikat und ein privater Schlüssel erstellt. Das Zertifikat verwendet einen 2048-Bit-RSA-Schlüssel und schützt den Schlüssel nicht mit einem Kennwort.

2 Wenn Sie dazu aufgefordert werden, geben Sie das Land, das Bundesland, den Ort sowie den Namen der Organisation und der Organisationseinheit an.

3 Im Textfeld „Allgemeiner Name“ geben Sie den Hostnamen des Horizon FLEX Servers ein, der geschützt werden soll.

Ein Eintrag in dieses Textfeld ist obligatorisch.

4 Geben Sie die E-Mail-Adresse ein.

Es werden ein selbstsigniertes Zertifikat und ein damit verknüpfter privater Schlüssel erstellt.

5 Wenn der private Schlüssel das `.pfx`-Format haben muss, geben Sie den folgenden Befehl mit den in den vorherigen Schritten erstellten Zertifikats- und Schlüsseldateinamen ein:
**`$ openSSL pkcs12 –export –outpfx–Ausgabedateiname –inkey Schlüsseldateiname –in Zertifikats–dateiname`**

Es wird eine neue kennwortgeschützte `.pfx`-Datei erstellt, die auf jedem Gerät bereitgestellt werden kann, das `.pfx`-Zertifikate anstelle von PEM-Zertifikaten verlangt.

# Konfigurieren des IIS-SSL-Serverzertifikats für den Horizon FLEX Server

Um die Zertifikatkette vom Horizon FLEX Server zu den virtuellen Horizon FLEX-Maschinen einzurichten, müssen Sie das IIS-SSL-Serverzertifikat für den Horizon FLEX Server konfigurieren.

### Voraussetzungen

- Installieren Sie Mirage für Horizon FLEX. Weitere Informationen hierzu finden Sie unter „Installieren und Konfigurieren von Mirage für Horizon FLEX“, auf Seite 16.
- Installieren Sie das Server-SSL-Zertifikat auf dem Mirage-Server. Informationen dazu finden Sie in der Mirage-Dokumentation unter https://www.vmware.com/support/pubs/mirage_pubs.html
- Konfigurieren Sie die Zertifikatauthentifizierung für Ihre virtuellen Horizon FLEX-Maschinen. Weitere Informationen hierzu finden Sie unter Kapitel 3, „Einrichten von Zertifikaten für virtuelle Horizon FLEX-Maschinen“, auf Seite 25.

- Erstellen Sie einen Download-Ordner für die Pakete Ihrer virtuellen Horizon FLEX-Maschine. Weitere Informationen hierzu finden Sie unter „Erstellen eines Download-Ordners für Pakete virtueller Horizon FLEX-Maschinen“, auf Seite 17.

### Vorgehensweise

1 Öffnen Sie den IIS-Manager.

2 Wechseln Sie zur **VMware Mirage Management-Website** und wählen Sie den Dateispeicherort für den Download-Ordner.

3 Klicken Sie mit der rechten Maustaste auf den Speicherort des Ordners und klicken Sie auf **Virtuelles Verzeichnis hinzufügen**.

4 Geben Sie einen Namen in das Textfeld **Alias** ein, wechseln Sie zum erstellten Ordner für die Pakete der virtuellen Horizon FLEX-Maschine und klicken Sie auf **OK**.

5 Wechseln Sie zum Stammknoten, dem für den Mirage-Server definierten Verbindungsknoten.

6 Auf der Seite Mirage Start doppelklicken Sie unter IIS auf **Serverzertifikate**.

Das Fenster IIS-SSL-Serverzertifikate wird geöffnet.

7 Klicken Sie in der rechten Spalte auf **Importieren**.

Mit diesem Schritt wird das erstellte SSL-Zertifikat importiert und ein Schlüssel zur Identifikation des Zertifikats zugewiesen.

8 Wählen Sie **VMware Mirage Management-Website** und klicken Sie auf **Bindungen bearbeiten** in der rechten Spalte.

9 Richten Sie den HTTPS-Port für die Verwendung Ihres Horizon FLEX Server-Zertifikats ein und klicken Sie auf **OK**.

## Konfigurieren von Active Directory-Einstellungen

Wenn Sie eine Berechtigung für eine virtuelle Horizon FLEX-Maschine erstellen, fügen Sie dieser Berechtigung Benutzer und Gruppen aus Ihrer vorhandenen Active Directory-Infrastruktur hinzu. Standardmäßig synchronisiert Horizon FLEX Ihre gesamte Active Directory-Infrastruktur mit der Horizon FLEX-Datenbank. Wahlweise können Sie die Horizon FLEX-Synchronisierung nur für eine bestimmte Organisationseinheit (OE) ausführen.

### Voraussetzungen

Installieren Sie Mirage für Horizon FLEX. Weitere Informationen hierzu finden Sie unter „Installieren und Konfigurieren von Mirage für Horizon FLEX“, auf Seite 16.

### Vorgehensweise

1 Starten Sie den Horizon FLEX-Verwaltungskonsole.

   a Geben Sie in einem Webbrowser **`https://WebManagerServer:7443/rvm`** ein, wobei *WebManagerServer* für den DNS-Namen oder die IP-Adresse des Hosts steht, auf dem Mirage Web Manager installiert ist.

   b Geben Sie den Benutzernamen und das Kennwort eines Domänenkontos ein, das einen Zugriff auf Mirage besitzt.

   c Klicken Sie auf **Anmelden**.

2 Klicken Sie in Horizon FLEX-Verwaltungskonsole auf das Symbol **Allgemeine Systemeinstellungen** und wählen Sie **Active Directory-Einstellungen**.

3 Geben Sie die Organisationseinheit, die synchronisiert werden soll, in das Textfeld **Organisationseinheit** ein.

   Während der Eingabe in das Textfeld erscheinen die in Ihrer Active-Directory-Infrastruktur verfügbaren Organisationseinheiten in einem Dropdown-Menü zur Auswahl.

4 Klicken Sie auf **OK**, um die Einstellungen der Organisationseinheit zu speichern.

   Der Horizon FLEX Server überprüft die Organisationseinheit, um zu überprüfen, ob diese vorhanden und zugänglich ist.

Der Horizon FLEX Server synchronisiert die Active Directory-Elemente, die nur zur ausgewählten Organisationseinheit gehören, einschließlich jener Elemente, die zu untergeordneten Organisationseinheiten gehören.

Immer wenn Sie eine neue Organisationseinheit konfigurieren, löscht der Horizon FLEX Server die zuvor synchronisierten Elemente aus der Datenbank und startet den gesamten Synchronisierungsprozess neu.

Sie können die Richtlinie für virtuelle Clientmaschinen so konfigurieren, dass das Einschaltkennwort dem Active Directory-Kennwort des Benutzers nach dem ersten Start entspricht. Weitere Informationen hierzu finden Sie unter „Konfigurieren einer allgemeinen Richtlinie für ein Horizon FLEX-Image“, auf Seite 44.

# Testen der Horizon FLEX-Verwaltungskonsole -Verbindung

Sie können Ihre Horizon FLEX-Bereitstellung durch Testen der Horizon FLEX-Verwaltungskonsole-Verbindung überprüfen.

### Voraussetzungen

- Installieren Sie Mirage für Horizon FLEX. Weitere Informationen hierzu finden Sie unter „Installieren und Konfigurieren von Mirage für Horizon FLEX“, auf Seite 16.
- Konfigurieren Sie die Zertifikatsauthentifizierung. Weitere Informationen hierzu finden Sie unter Kapitel 3, „Einrichten von Zertifikaten für virtuelle Horizon FLEX-Maschinen“, auf Seite 25.

### Vorgehensweise

1 Starten Sie den Horizon FLEX-Verwaltungskonsole.

   a Geben Sie in einem Webbrowser **`https://WebManagerServer:7443/rvm`** ein, wobei *WebManagerServer* für den DNS-Namen oder die IP-Adresse des Hosts steht, auf dem Mirage Web Manager installiert ist.

   b Geben Sie den Benutzernamen und das Kennwort eines Domänenkontos ein, das einen Zugriff auf Mirage besitzt.

   c Klicken Sie auf **Anmelden**.

2 Stellen Sie sicher, dass die Horizon FLEX-Verwaltungskonsole-Seite korrekt dargestellt wird.

   Die Schaltflächen **Images**, **Richtlinien**, **Berechtigungen** und **Virtuelle Maschinen** sollten im linken Navigationsbereich angezeigt werden.

# Installieren des Horizon FLEX Client für Endbenutzer

Endbenutzer können die virtuellen Horizon FLEX-Maschinen nur herunterladen, wenn auf ihren lokalen Computern die Horizon FLEX Client-Software installiert ist. Im Horizon FLEX-Paket sind die unterstützten Clients Fusion Pro für Mac OS X-Maschinen und Workstation Player für Windows-Maschinen enthalten.

Sie können mit der Erstellung einer Massenbereitstellung Horizon FLEX Client in einem Schritt auf vielen Systemen installieren. Alternativ haben Ihre Endbenutzer die Möglichkeit, Horizon FLEX Client von der VMware-Website herunterzuladen und selbst zu installieren. Außerdem lässt sich eine unbeaufsichtigte Workstation Player-Installation auf mehreren Windows-Computern durchführen.

## Erstellen eines Pakets für die Massenbereitstellung zur Installation von Fusion Pro

Sie können in Fusion Pro ein Paket für die Massenbereitstellung zum Installieren von Fusion Pro für eine beliebige Anzahl von Endbenutzer-Macs erstellen. Sie können mit Standardtools für die Paketbereitstellung, einschließlich Apple Remote Desktop Admin, das Massenbereitstellungspaket zur Verfügung stellen.

Wenn Sie ein Massenbereitstellungspaket konfigurieren, geben Sie Ihren Horizon FLEX-Lizenzschlüssel im Abschnitt `[Volumenlizenz]` der Datei `Deploy.ini` ein und erstellen eine Kopie der Fusion Pro-Anwendung im Ordner `00Fusion_Deployment_Items`.

Optional können Sie mit dem Parameter `connectAtStartupURL` im Abschnitt `[Locations]` der Datei `Deploy.ini` einen Benutzernamen und den Hostnamen Ihres Horizon FLEX Servers angeben, zum Beispiel:

```
connectAtStartupURL = vmware-rvm://johndoe@yourflexserver.com:7443
```

Wenn auf dem Mac des Benutzers keine virtuellen Maschinen installiert sind, öffnet sich beim Start von Fusion Pro das Verbindungsdialogfeld und die Textfelder **Server** und **Benutzername** sind bereits mit dem Hostnamen und Benutzernamen ausgefüllt, die Sie im Parameter `connectAtStartupURL` angegeben haben.

Schrittweise Informationen zum Erstellen eines Pakets für die Massenbereitstellung erhalten Sie im VMware-Knowledge Base-Artikel unter http://kb.vmware.com/kb/2058680.

## Bereitstellen eines Installationspakets von Workstation Player für Endbenutzer

Sie können Workstation Player mithilfe einer Befehlszeile auf Endbenutzercomputern installieren und die Einstellungen für die Horizon FLEX-Serververbindung mit einem URI (Uniform Resource Identifier) festlegen. Nach Abschluss der Installation von Workstation Player wird der Endbenutzer aufgefordert, eine Verbindung zu einem Server herzustellen und eine virtuelle Horizon FLEX-Maschine herunterzuladen.

### Voraussetzungen

- Übergeben Sie dem Endbenutzer ein Kennwort für den Server und den Workstation Player-Lizenzschlüssel zur Verwendung mit Horizon FLEX.

### Vorgehensweise

- Erstellen Sie einen URI zum Anlegen eines angepassten Workstation Player-Installations- und -Bereitstellungspakets.

  Die Befehlszeile verfügt über die folgende Struktur:

  ```
  VMware-player-x.x.x-xxxxxxx.exe /v PLAYER_RVM_URI="vmware-rvm://username@myserver.com:7443"
  ```

  Geben Sie die Version und die Build-Nummer der Workstation Player-.exe-Datei an. *Benutzername* ist der Anmeldename des Benutzers und *myserver.com* der Hostname des Servers. Die Serveradresse muss `vmware-rvm://` sowie `:7443` enthalten. Stellen Sie der Serveradresse nicht http oder https voran.

## Ausführen einer unbeaufsichtigten Workstation Player -Installation

Sie können mit der Funktion „Unbeaufsichtigte Installation“ des Microsoft Windows Installer (MSI) Workstation Player auf mehreren Windows-Hosts installieren, ohne auf die Aufforderungen eines Assistenten reagieren zu müssen. Diese Funktion ist besonders in großen Unternehmen komfortabel.

### Voraussetzungen

- Stellen Sie sicher, dass das Hostsystem die Hostsystemanforderungen erfüllt.
- Vergewissern Sie sich, dass der Hostcomputer über die Version 2.0 oder höher des MSI-Laufzeitmoduls verfügt. Diese Version des Installationsprogramms ist mit den Windows-Versionen ab Windows XP von Microsoft erhältlich. Auf der Microsoft-Website finden Sie weitere Informationen dazu.

### Vorgehensweise

1 Melden Sie sich beim Hostsystem als Administrator oder als Mitglied einer Administratorengruppe an.

Wenn Sie sich bei der Domäne anmelden, muss das Domänenkonto auch das eines lokalen Administrators sein.

2 Extrahieren Sie das Installations-Image des Administrators aus der Setup-Datei von Workstation Player.

Der Setup-Dateiname lautet `VMware-player-xxxx-xxxx.exe`, wobei *xxxx-xxxx* die Version und die Build-Nummer darstellt.

Beispiel: **`setup.exe /s /e install_temp_path`**

3 Geben Sie den Installationsbefehl in einer Zeile ein.

Diese Beispiele zeigen Optionen, die dem Befehl hinzugefügt werden können.

```
VMware-player-full-x.x.x-xxxxxx.exe /s /pass /v/qn REBOOT=ReallySuppress "EULAS_AGREED=1 IN-
STALLDIR=""path_to_program_directory"" ADDLOCAL=ALL SERIALNUMBER=""xxxxx-xxxxx-xxxxx-xxxxx-
xxxxx"" "
```

```
VMware-player-full-x.x.x-xxxxxx.exe /s /v/qn EULAS_AGREED=1 SERIALNUMBER="xxxxx-xxxxx-xxxxx-
xxxxx-xxxxx"
```

```
VMware-player-full-x.x.x-xxxxxx.exe /s /v/qn PLAYER_RVM_URI="vmware-rvm://username@myser-
ver.com:7443"
```

Mit der optionalen Eigenschaft `INSTALLDIR` lässt sich ein vom Standardspeicherort abweichender Dateipfad für die Installation angeben.

**Hinweis** Vergessen Sie nicht die Anführungszeichen für den Dateipfad. Alle MSI-Argumente werden mit der Option `/v` übergeben. Die äußeren Anführungszeichen gruppieren die MSI-Argumente und die inneren Anführungszeichen platzieren ein Anführungszeichen in diesem Argument.

Sie haben die Möglichkeit, mit der optionalen Eigenschaft `REMOVE` die Installation bestimmter Funktionen zu überspringen.

## Eigenschaften der unbeaufsichtigten Installation von Workstation Player

Sie können eine unbeaufsichtigte Installation von Workstation Player anpassen, indem Sie Installationseigenschaften im Installationsbefehl angeben.

Um eine Installationseigenschaft im Installationsbefehl anzugeben, verwenden Sie das Format `Property="value"`. Der Wert 1 steht für „true“ und der Wert 0 steht für „false“

**Tabelle 2-1.** Installationseigenschaften

| Eigenschaft | Beschreibung | Standardwert |
|---|---|---|
| `AUTHD_PORT` | Gibt an, über welchen Port der VMware-Autorisierungsservice kommuniziert. | 902 |
| `AUTOSOFTWAREUPDATE` | Ermöglicht automatische Upgrades für Workstation Player, wenn ein neuer Build verfügbar wird. | 1 |
| `DATACOLLECTION` | Sendet Informationen zur Anwendererfahrung an VMware. | 1 |
| `DESKTOP SHORTCUT` | Fügt bei der Installation von Workstation Player eine Verknüpfung auf dem Desktop hinzu. | 1 |

**Tabelle 2-1.** Installationseigenschaften (Fortsetzung)

| Eigenschaft | Beschreibung | Standardwert |
|---|---|---|
| EULAS_AGREED | Ermöglicht Ihnen ein unbeaufsichtigtes Akzeptieren der Produkt-EULAs. Legen Sie diese Eigenschaft auf 1 fest, um die Installation oder das Upgrade abzuschließen. | 0 |
| INSTALL_DIR | Installiert Workstation Player in einem anderen Verzeichnis als dem Standardspeicherort für Workstation Player. | C:\Programme (x86)\VMware\VMware Player |
| KEEP_LICENSE | Gibt an, ob Lizenzschlüssel bei der Installation von Workstation Player behalten oder entfernt werden sollen. | 1 |
| KEEP_SETTINGFILES | Gibt an, ob Einstellungsdateien bei der Deinstallation von Workstation Player behalten oder entfernt werden sollen. | 1 |
| PLAYER_RVM_URI | Gibt den URI (Uniform Resource Identifier) für den Horizon FLEX Server an. | VMware-player-full-x.x.x-xxxxxx.exe /s /v/qn PLAYER_RVM_URI="vmware-rvm://username@myserver.com:7443" |
| SERIALNUMBER | Ermöglicht die Eingabe des Lizenzschlüssels während der Installation von Workstation Player. Geben Sie den Lizenzschlüssel mit Bindestrichen ein, Beispiel: xxxxx-xxxxx-xxxxx-xxxxx-xxxxx. | |
| SIMPLIFIEDUI | Aktiviert oder deaktiviert bestimmte Merkmale der Benutzeroberfläche von Workstation Player. | 0 |
| SOFTWAREUPDATEURL | Gibt eine benutzerdefinierte URL für die Verwaltung von Software-Updates an (die nicht „vmware.com“ lautet). | |
| STARTMENU_SHORTCUT | Fügt bei der Installation von Workstation Player einen Eintrag zum Menü **Start** hinzu. | 1 |
| SUPPORTURL | Legt eine Support-URL oder einen E-Mail-Alias für den Support fest, damit Ihre Benutzer bei Produktproblemen über das Menü Workstation Player **Hilfe** einen spezifischen Support erreichen können. | |

# Einrichten von Zertifikaten für virtuelle Horizon FLEX -Maschinen 3

Bevor Sie virtuelle Horizon FLEX-Maschinen erstellen und bereitstellen, müssen Sie Zertifikate einrichten, damit Endbenutzer die Möglichkeit haben, ihre virtuellen Maschinen erfolgreich herunterzuladen und anzuwenden.

VMware empfiehlt die Anwendung eines Zertifikats auf Ihrem Horizon FLEX Server, das von einer Zertifizierungsstelle (ZS) wie Entrust oder Go Daddy herausgegeben wurde, oder das Zertifikat eines Drittanbieters. Wenn Sie ein selbstsigniertes Zertifikat oder ein Zertifikat von einer internen Zertifizierungsstelle anstelle eines allgemein vertrauenswürdigen Zertifikats verwenden, müssen Sie verschiedene Schritte durchführen, um sicherzustellen, dass das Zertifikat von allen Endbenutzercomputern als vertrauenswürdig eingestuft wird, die virtuelle Horizon FLEX-Maschinen herunterladen und anwenden.

Erläuterungen zur Einrichtung von Zertifikaten in Mirage für den Horizon FLEX Server finden Sie in der Mirage-Dokumentation unter https://www.vmware.com/support/pubs/mirage_pubs.html.

Dieses Kapitel behandelt die folgenden Themen:



## Erstellen einer Liste vertrauenswürdiger Zertifikate

Sie haben die Möglichkeit, eine Liste vertrauenswürdiger Zertifikate für virtuelle Horizon FLEX-Maschinen zu erstellen und diese in Horizon FLEX-Richtlinienserver zu importieren. Mit der Verwendung einer Liste vertrauenswürdiger Zertifikate müssen Sie keine Zertifikate mehr auf Endbenutzerhosts installieren.

Mit der Verwendung einer Liste vertrauenswürdiger Zertifikate lässt sich verhindern, dass böswillige Benutzer ihre eigenen selbstsignierten Zertifikate für denselben Hostnamen erstellen und diese Zertifikate ihrer Hostliste vertrauenswürdiger Zertifikate hinzufügen.

Wenn Sie Horizon FLEX-Richtlinienserver für die Verwendung einer Liste vertrauenswürdiger Zertifikate konfigurieren, ignoriert der Clienthost die Hostliste von Zertifikaten und verwendet stattdessen die Liste vertrauenswürdiger Zertifikate zur Überprüfung der Serververbindungen. Wenn der Clienthost ein Zertifikat nicht mithilfe der Liste vertrauenswürdiger Zertifikate überprüfen kann, ist keine Verbindung zum Server möglich.

Ist die Liste vertrauenswürdiger Zertifikate in der virtuellen Maschine der Quelle leer, führen Workstation Player und Fusion Pro die Authentifizierung mit der Hostliste vertrauenswürdiger Zertifikate durch.

Um die Liste vertrauenswürdiger Zertifikate zu erstellen, exportieren Sie jedes Zertifikat in eine eigene Datei und verknüpfen diese Dateien dann zu einer einzigen Datei. Mithilfe von Horizon FLEX-Verwaltungskonsole können Sie die Datei verknüpfter Zertifikate in Horizon FLEX-Richtlinienserver importieren.

Zertifikate müssen im PEM-Format (Privacy Enhanced Mail) exportiert werden. Auf Windows-Systemen wird die Verschlüsselung von PEM-Zertifikaten als Base-64-codiertes X.509 (.CER) bezeichnet. Es werden nur PEM-codierte Zertifikate unterstützt. Alle anderen Zertifikatsformate (DER, Serialized Certificate Store/SST, PKCS #12/PFX, PKCS #7/P7B) werden nicht akzeptiert.

## Über das PEM-Format

Das PEM-Format ist ein Base64-codiertes Standardzertifikatsformat.

Beispiel für ein Zertifikat im PEM-Format:

```
-----BEGIN CERTIFICATE-----
MIIDojCCAwugAwIBAgIJAMLM0CJRzPyzMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD
VQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJUGFsbyBBbHRv
MS8wLQYDVQQKEyZWTXdhcmUsIEluYy4gLSBXb3Jrc3RhdGlvbiBTU0wgVGVzdGlu
ZzEqMCgGA1UEAxMhV29ya3N0YXRpb24gQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTExMDcxNTAyMjY0OFoXDTE1MDcxNDAyMjY0OFowgZMxCzAJBgNVBAYTAlVTMRMw
EQYDVQQIEwpDYWxpZm9ybmlhMRIwEAYDVQQHEwlQYWxvIEFsdG8xLzAtBgNVBAoT
JlZNd2FyZSwgSW5jLiAtIFdvcmtzdGF0aW9uIFNTTCBUZXN0aW5nMSowKAYDVQQD
EyFXb3Jrc3RhdGlvbiBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAL/tBlngiEkCK7ssCBe8lZ30FlIHmpECmwEm3AaID1C0
lncb+LdRt2AmmQiknXBPxGBGyRNRNnashrzp1XXR/wL2b2AybT7NX+P/XSH2srDb
cGGCTNa/bwh/ArcirTLCjRwY55lAAH9xwzortRYR84IBJQpHzxcopTSI9o4ZVIqx
AgMBAAGjgfswgfgwHQYDVR0OBBYEFMoT527dtvlgR1EzYK4EnQHS6T2ZMIHIBgNV
HSMEgcAwgb2AFMoT527dtvlgR1EzYK4EnQHS6T2ZoYGZpIGWMIGTMQswCQYDVQQG
EwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJUGFsbyBBbHRvMS8w
LQYDVQQKEyZWTXdhcmUsIEluYy4gLSBXb3Jrc3RhdGlvbiBTU0wgVGVzdGluZzEq
MCgGA1UEAxMhV29ya3N0YXRpb24gQ2VydGlmaWNhdGUgQXV0aG9yaXR5ggkAwszQ
IlHM/LMwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOBgQBcoiwDWGWXzI+j
0gG/7BNzpNHzR1RGAF4nB9JrnCYWvB313kgYDMHogfiAoQchsu/py/OYBYVRjjFJ
YVaTJ7DVl/3Gpk3+tcdJfEmqIz76PVWfWbTnhuJEMYrMM4W06B/K2cs24bkZtcXQ
h8b4FYTVCg/l6TP5SWgei4VWgRfxgA==
-----END CERTIFICATE-----
```

Wenn Sie eine Liste vertrauenswürdiger Zertifikate erstellen, werden mehrere Zertifikate im PEM-Format zu einer Datei verbunden. Zeilenenden werden automatisch ermittelt. Das folgende Beispiel zeigt das Format einer Liste verbundener Zertifikate mit zwei Zertifikaten.

```
-----BEGIN CERTIFICATE-----
<Base64-Inhalt>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Base64-Inhalt>
-----END CERTIFICATE-----
```

## Erstellen von Zertifikaten im PEM-Format

Um Zertifikate im PEM-Format zu erstellen, laden Sie das Zertifikat von der Website der Zertifizierungsstelle herunter oder exportieren die Zertifikate von einem Hostsystem.

Beispielsweise lassen sich Zertifikate für Verisign von der Symantec-Website unter https://www.symantec.com/page.jsp?id=roots herunterladen.

### Exportieren von Zertifikaten im PEM-Format von einem Mac

Sie haben die Möglichkeit, Zertifikate von einem Mac im PEM-Format zu exportieren.

#### Voraussetzungen

Machen Sie sich mit der Anwendung der Schlüsselbundverwaltung auf einem Mac vertraut. Weitere Informationen dazu erhalten Sie auf der Apple-Support-Website unter http://support.apple.com.

#### Vorgehensweise

1 Auf dem Mac öffnen Sie die Schlüsselbundverwaltung.

2 In der Seitenleiste wählen Sie **System-Roots**.

3 Ermitteln Sie das Zertifikat, das exportiert werden soll.

4 Wählen Sie **Ablage > Elemente exportieren**.

5 Wählen Sie einen Speicherort für das Zertifikat und das Dateiformat **Privacy Enhanced Mail (.pem)**.

### Exportieren von Zertifikaten im PEM-Format von einem Windows-System

Sie haben die Möglichkeit, Zertifikate von einem Windows-System im PEM-Format zu exportieren. Unter Windows wird die Verschlüsselung von PEM-Zertifikaten als Base-64-codiertes X.509 (.CER) bezeichnet.

#### Voraussetzungen

Machen Sie sich mit der Anwendung der Zertifikatsverwaltung auf einem Windows-System vertraut. Weitere Informationen dazu erhalten Sie auf der Microsoft-TechNet-Website unter http://technet.microsoft.com.

#### Vorgehensweise

1 Auf dem Windows-System öffnen Sie den Zertifikat-Manager (`certmgr.exe`).

2 Klicken Sie mit der rechten Maustaste auf das Zertifikat, das exportiert werden soll, und wählen Sie im eingeblendeten Kontextmenü **Alle Aufgaben > Exportieren**.

3 Wählen Sie die gewünschten Optionen im Zertifikatexport-Assistenten.

   a Wählen Sie als Dateiexportformat **Base-64-codiert X.509 (.CER)**.

   Die Auswahl dieser Option obligatorisch, damit das Zertifikat mit Horizon FLEX angewendet werden kann.

   b Wählen Sie einen Speicherort für das Zertifikat und einen Dateinamen.

   c Überprüfen Sie die gewählten Einstellungen und klicken Sie auf **Fertig stellen**.

   Das Zertifikat wird dann am angegebenen Speicherort gespeichert.

## Erstellen und Importieren der Datei mit der Liste vertrauenswürdiger Zertifikate

Nach dem Export Ihrer Zertifikate im PEM-Format müssen Sie eine Liste vertrauenswürdiger Zertifikate erstellen und diese in Horizon FLEX-Richtlinienserver importieren.

#### Voraussetzungen

Exportieren Sie jedes Zertifikat im PEM-Format. Weitere Informationen hierzu finden Sie unter „Erstellen von Zertifikaten im PEM-Format“, auf Seite 26.

**Vorgehensweise**

1 Um die Datei mit der Liste vertrauenswürdiger Zertifikate zu erstellen, verknüpfen Sie jede Datei eines Zertifikats im PEM-Format zu einer einzigen Datei.

Dazu verwenden Sie den Befehl `cat` oder Sie kopieren die Inhalte der Zertifikatsdateien und fügen diese in eine Textdatei ein. Base64-Inhalt lässt sich sicher in einem Texteditor bearbeiten.

Beispiel: `$ cat mycert1.pem mycert2.pem mycert3.pem > list.pem`

2 Starten Sie den Horizon FLEX-Verwaltungskonsole.

a Geben Sie in einem Webbrowser **`https://WebManagerServer:7443/rvm`** ein, wobei *WebManagerServer* für den DNS-Namen oder die IP-Adresse des Hosts steht, auf dem Mirage Web Manager installiert ist.

b Geben Sie den Benutzernamen und das Kennwort eines Domänenkontos ein, das einen Zugriff auf Mirage besitzt.

c Klicken Sie auf **Anmelden**.

3 In Horizon FLEX-Verwaltungskonsole klicken Sie auf das Symbol **Allgemeine Systemeinstellungen** und wählen **Zertifikate**.

4 Klicken Sie auf **Importieren**, wechseln Sie zur Datei mit der Liste vertrauenswürdiger Zertifikate und klicken Sie auf **Öffnen**, um die Datei zu importieren.

## Aktualisieren von Zertifikaten auf dem Server

Ist ein Zertifikat abgelaufen und ein neues Zertifikat hat ein weit in der Zukunft liegendes Ablaufdatum, können Sie das neue Zertifikat als zweites Zertifikat der Liste vertrauenswürdiger Zertifikate in Horizon FLEX-Richtlinienserver hinzufügen.

Durch Hinzufügen des neuen Zertifikats zur Liste vertrauenswürdiger Zertifikate können alle virtuellen Horizon FLEX-Maschinen das neue Zertifikat herunterladen. Nach dem Wechsel des Zertifikats haben alle virtuellen Horizon FLEX-Maschinen, die die neue Liste von Zertifikaten erhalten haben, die Möglichkeit, eine Verbindung zum Horizon FLEX Server herzustellen. Sie können dann das alte vertrauenswürdige Zertifikat aus der Richtliniendatei entfernen.

Wenn Sie das Serverzertifikat ändern, nachdem die virtuellen Horizon FLEX-Maschinen bereits registriert und ausgeführt worden sind, muss Ihr Endbenutzer sicherstellen, dass das geänderte Zertifikat von Fusion Pro oder Workstation Player als vertrauenswürdig eingestuft wird. Handelt es sich beim neuen Serverzertifikat um ein selbstsigniertes Zertifikat, wird vom Horizon FLEX Client der Instanzenstatus nicht korrekt an den Horizon FLEX Server übermittelt. Der Endbenutzer muss dann die virtuelle Horizon FLEX-Maschine öffnen und auf **Verbinden** klicken, um eine Verbindung mit dem Server herzustellen. Erhält der Endbenutzer die Fehlermeldung

`Ungültiges Sicherheitszertifikat`

, muss der Endbenutzer sich die Gültigkeit des Zertifikats von Ihnen bestätigen lassen, und in diesem Fall das Kontrollkästchen **Immer diesem Host mit diesem Zertifikat vertrauen** aktivieren und auf **Verbindung trotzdem herstellen** klicken.

# Verwenden selbstsignierter Zertifikate

Wenn Sie das selbstsignierte Zertifikat nicht für die vorbereitete virtuelle Maschine der Quelle konfigurieren, müssen Sie das Zertifikat auf jedem Endbenutzerhost für die virtuellen Horizon FLEX-Maschinen installieren, damit es wie vorgesehen wirksam ist.

Ist die Zertifikatsliste in der Richtliniendatei leer, greifen Workstation Player und Fusion Pro für die Authentifizierung auf die Hostliste vertrauenswürdiger Zertifikate zurück.

Wenn Sie das selbstsignierte Zertifikat einer virtuellen Maschine der Quelle in Horizon FLEX-Richtlinienserver einbeziehen und das Zertifikat für Horizon FLEX-Client konfigurieren und installieren (entweder in der Richtliniendatei der virtuellen Maschine der Quelle oder in der Hostliste vertrauenswürdiger Zertifikate), müssen Sie das Zertifikat nicht mehr auf den Endbenutzerhosts installieren, wenn Zertifikatsaktualisierungen erforderlich sind, etwa wenn ein Zertifikat abläuft.

Informationen zum Konfigurieren von Zertifikaten in einer virtuellen Maschine finden Sie unter „Erstellen einer virtuellen Maschine der Quelle in Fusion Pro“, auf Seite 36.

Erläuterungen zum Erstellen einer Liste vertrauenswürdiger Zertifikate und zum Importieren dieser Liste in Horizon FLEX-Richtlinienserver erhalten Sie unter „Erstellen einer Liste vertrauenswürdiger Zertifikate“, auf Seite 25.

Informationen zum Aktualisieren von Zertifikaten finden Sie unter „Aktualisieren von Zertifikaten auf dem Server“, auf Seite 28.

## Installieren eines selbstsignierten Zertifikats auf einem Windows-Computer

Um ein selbstsigniertes Zertifikat auf einem Windows-Host zu installieren, müssen Sie das Zertifikat von Ihrem Horizon FLEX Server exportieren und auf Ihrem Windows-Computer importieren.

### Voraussetzungen

- Informieren Sie sich über die Installation und Anwendung des MMC-Zertifikate-Snap-In auf einem Windows-System. Weitere Informationen dazu erhalten Sie auf der Windows-TechNet-Website unter http://technet.microsoft.com.
- Installieren Sie Windows IIS.

### Vorgehensweise

1 Exportieren Sie das selbstsignierte Zertifikat von Ihrem Horizon FLEX-Server.

   a Auf dem Horizon FLEX-Server starten Sie MMC (`mmc.exe`), fügen das Zertifikate-Snap-In für ein Computerkonto hinzu und verwalten die Zertifikate für den lokalen Computer.

   b Wählen Sie **Datei > Snap-In hinzufügen/entfernen** aus.

   c Klicken Sie auf das **Zertifikat**-Snap-In und dann auf **Hinzufügen**.

   d Wählen Sie im Fenster **Zertifikat-Snap-In** die Option **Computerkonto** aus und klicken Sie auf **Weiter**.

   Diese Einstellung ist für den Horizon FLEX-Server obligatorisch.

   e Wählen Sie **Lokaler Computer** aus und klicken Sie auf **Fertig stellen** und dann auf **OK**.

   f Im linken Navigationsbereich erweitern Sie **Zertifikate (Lokaler Computer)**.

   g Klicken Sie mit der rechten Maustaste auf **Vertrauenswürdige Stammzertifizierungsstellen** und wählen Sie **Alle Aufgaben > Importieren** aus.

   Der Assistent für das Importieren von Zertifikaten wird geöffnet.

   h Klicken Sie auf **Weiter**.

   i Wechseln Sie zur Stammzertifikatsdatei und klicken Sie auf **Weiter**.

   j Wählen Sie **Alle Zertifikate in folgendem Speicher speichern: Vertrauenswürdige Stammzertifizierungsstellen**, klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

   k Klicken Sie mit der rechten Maustaste auf **Zwischenstammzertifizierungsstellen** und wählen Sie **Alle Aufgaben > Importieren** aus.

   l Der **Assistent für das Importieren von Zertifikaten** wird geöffnet.

m Wechseln Sie zur Stammzertifikatsdatei und klicken Sie auf **Weiter**.

n Wählen Sie **Alle Zertifikate in folgendem Speicher speichern: Zwischenstammzertifizierungsstellen**, klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

o Wiederholen Sie die Schritte m. und n. für jedes Zwischenzertifikat, das installiert werden soll.

p Wechseln Sie zu **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.

q Wählen Sie das selbstsignierte Zertifikat und exportieren Sie es.

Exportieren Sie das Zertifikat im Format DER-codiert-binär X.509 (.CER).

2 Kopieren Sie das selbstsignierte Zertifikat auf den Client-Windows-Computer.

3 Importieren Sie das selbstsignierte Zertifikat auf den Client-Windows-Computer.

a Auf dem Windows-Computer starten Sie MMC (`mmc.exe`).

b Fügen Sie das Zertifikate-Snap-In für das Computerkonto hinzu und verwalten Sie die Zertifikate für den lokalen Computer.

c Importieren Sie das selbstsignierte Zertifikat in **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.

Das selbstsignierte Zertifikat wird nun für alle Benutzer als vertrauenswürdig eingestuft.

## Installieren eines selbstsignierten Zertifikats auf einem Mac

Um ein selbstsigniertes Zertifikat auf einem Mac-Host zu installieren, müssen Sie das Zertifikat von Ihrem Horizon FLEX Server exportieren und auf Ihrem Mac importieren.

### Voraussetzungen

- Informieren Sie sich über die Installation und Anwendung des MMC-Zertifikate-Snap-In auf einem Windows-System. Weitere Informationen dazu erhalten Sie auf der Windows-TechNet-Website unter http://technet.microsoft.com.
- Machen Sie sich mit der Anwendung der Schlüsselbundverwaltung auf einem Mac vertraut. Weitere Informationen dazu erhalten Sie auf der Apple-Support-Website unter http://support.apple.com.
- Installieren Sie Windows IIS.

### Vorgehensweise

1 Exportieren Sie das selbstsignierte Zertifikat von Ihrem Horizon FLEX-Server.

a Auf dem Horizon FLEX-Server starten Sie MMC (`mmc.exe`), fügen das Zertifikate-Snap-In für ein Computerkonto hinzu und verwalten die Zertifikate für den lokalen Computer.

b Wählen Sie **Datei > Snap-In hinzufügen/entfernen** aus.

c Klicken Sie auf das **Zertifikat**-Snap-In und dann auf **Hinzufügen**.

d Wählen Sie im Fenster **Zertifikat-Snap-In** die Option **Computerkonto** aus und klicken Sie auf **Weiter**.

Diese Einstellung ist für den Horizon FLEX-Server obligatorisch.

e Wählen Sie **Lokaler Computer** aus und klicken Sie auf **Fertig stellen** und dann auf **OK**.

f Im linken Navigationsbereich erweitern Sie **Zertifikate (Lokaler Computer)**.

g Klicken Sie mit der rechten Maustaste auf **Vertrauenswürdige Stammzertifizierungsstellen** und wählen Sie **Alle Aufgaben > Importieren** aus.

Der Assistent für das Importieren von Zertifikaten wird geöffnet.

h Klicken Sie auf **Weiter**.

i Wechseln Sie zur Stammzertifikatsdatei und klicken Sie auf **Weiter**.

j Wählen Sie **Alle Zertifikate in folgendem Speicher speichern: Vertrauenswürdige Stammzertifizierungsstellen**, klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

k Klicken Sie mit der rechten Maustaste auf **Zwischenstammzertifizierungsstellen** und wählen Sie **Alle Aufgaben > Importieren** aus.

l Der **Assistent für das Importieren von Zertifikaten** wird geöffnet.

m Wechseln Sie zur Stammzertifikatsdatei und klicken Sie auf **Weiter**.

n Wählen Sie **Alle Zertifikate in folgendem Speicher speichern: Zwischenstammzertifizierungsstellen**, klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

o Wiederholen Sie die Schritte m. und n. für jedes Zwischenzertifikat, das installiert werden soll.

p Wechseln Sie zu **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.

q Wählen Sie das selbstsignierte Zertifikat und exportieren Sie es.

Exportieren Sie das Zertifikat im Format DER-codiert-binär X.509 (.CER).

2 Kopieren Sie das selbstsignierte Zertifikat auf den Mac.

3 Importieren Sie das selbstsignierte Zertifikat auf dem Mac.

a Doppelklicken Sie auf das selbstsignierte Zertifikat, um es in der Schlüsselbundverwaltung zu öffnen.

Das selbstsignierte Zertifikat erscheint unter **Anmeldung**.

b Kopieren Sie das selbstsignierte Zertifikat nach **System**.

Das Kopieren des selbstsignierten Zertifikats nach **System** ist Voraussetzung dafür, dass es von allen Benutzern und lokalen Systemprozessen als vertrauenswürdig eingestuft wird, inklusive der Prozesse der virtuellen Maschine (vmware-vmx) in Fusion Pro.

c Öffnen Sie das selbstsignierte Zertifikat in **System**, erweitern Sie **Vertrauen**, wählen Sie **System-Standards verwenden** und speichern Sie Ihre Änderungen.

d Öffnen Sie das selbstsignierte Zertifikat in **System** erneut, erweitern Sie **Vertrauen**, wählen Sie **Immer vertrauen** und speichern Sie Ihre Änderungen.

e Löschen Sie das selbstsignierte Zertifikat aus **Anmeldung**.

## Verwenden interner ZS-Zertifikate

Wenn Sie ein Zertifikat von einer internen statt von einer kommerziellen Zertifizierungsstelle wie Entrust oder Go Daddy verwenden und das Zertifikat nicht für die vorbereitete virtuelle Maschine der Quelle konfigurieren, müssen Sie das Stammzertifizierungsstellenzertifikat (Stamm-ZS-Zertifikat) auf jedem Endbenutzerhost für die virtuellen Horizon FLEX-Maschinen installieren, damit es wie vorgesehen wirksam ist.

**Hinweis** Da das Serverzertifikat durch das Stamm-ZS-Zertifikat signiert ist, müssen Sie das Serverzertifikat nicht in die Endbenutzerhosts importieren.

Ist die Zertifikatsliste in der Richtliniendatei leer, greifen Workstation Player und Fusion Pro für die Authentifizierung auf die Hostliste vertrauenswürdiger Zertifikate zurück.

Wenn Sie das interne ZS-Zertifikat einer virtuellen Maschine der Quelle in Horizon FLEX-Richtlinienserver einbeziehen und das Zertifikat für Horizon FLEX-Client konfigurieren und installieren (entweder in der Richtliniendatei der virtuellen Maschine der Quelle oder in der Hostliste vertrauenswürdiger Zertifikate), müssen Sie das Stamm-ZS-Zertifikat nicht mehr auf den Endbenutzerhosts installieren, wenn Zertifikatsaktualisierungen erforderlich sind, etwa wenn ein Zertifikat abläuft.

Informationen zum Konfigurieren von Zertifikaten in einer virtuellen Maschine finden Sie unter „Erstellen einer virtuellen Maschine der Quelle in Fusion Pro“, auf Seite 36.

Erläuterungen zum Erstellen einer Liste vertrauenswürdiger Zertifikate und zum Importieren dieser Liste in Horizon FLEX-Richtlinienserver erhalten Sie unter „Erstellen einer Liste vertrauenswürdiger Zertifikate“, auf Seite 25.

Informationen zum Aktualisieren von Zertifikaten finden Sie unter „Aktualisieren von Zertifikaten auf dem Server“, auf Seite 28.

## Installieren eines internen Stammzertifizierungsstellenzertifikats auf einem Windows-Computer

Um ein internes Stammzertifizierungsstellenzertifikat auf einem Windows-Host zu installieren, müssen Sie das Zertifikat von Ihrem Horizon FLEX-Server exportieren und auf Ihrem Windows-Computer importieren.

### Voraussetzungen

- Informieren Sie sich über die Installation und Anwendung des MMC-Zertifikate-Snap-In auf einem Windows-System. Weitere Informationen dazu erhalten Sie auf der Windows-TechNet-Website unter http://technet.microsoft.com.
- Fordern Sie ein internes Stammzertifizierungsstellenzertifikat an und installieren Sie dieses. Für die Anforderung eines Zertifikats steht das Windows MMC-Zertifikate-Snap-In zur Verfügung.
- Installieren Sie Windows IIS.

### Vorgehensweise

1 Exportieren Sie das Stammzertifizierungsstellenzertifikat von Ihrem Horizon FLEX-Server.

   a Auf dem Horizon FLEX-Server starten Sie MMC (`mmc.exe`), fügen das Zertifikate-Snap-In für ein Computerkonto hinzu und verwalten die Zertifikate für den lokalen Computer.

   b Wählen Sie **Datei > Snap-In hinzufügen/entfernen** aus.

   c Klicken Sie auf das **Zertifikat**-Snap-In und dann auf **Hinzufügen**.

   d Wählen Sie im Fenster **Zertifikat-Snap-In** die Option **Computerkonto** aus und klicken Sie auf **Weiter**.

   Diese Einstellung ist für den Horizon FLEX-Server obligatorisch.

   e Wählen Sie **Lokaler Computer** aus und klicken Sie auf **Fertig stellen** und dann auf **OK**.

   f Im linken Navigationsbereich erweitern Sie **Zertifikate (Lokaler Computer)**.

   g Klicken Sie mit der rechten Maustaste auf **Vertrauenswürdige Stammzertifizierungsstellen** und wählen Sie **Alle Aufgaben > Importieren**.

   Der Assistent für das Importieren von Zertifikaten wird geöffnet.

   h Klicken Sie auf **Weiter**.

   i Wechseln Sie zur Stammzertifikatsdatei und klicken Sie auf **Weiter**.

   j Wählen Sie **Alle Zertifikate in folgendem Speicher speichern: Vertrauenswürdige Stammzertifizierungsstellen**, klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

k Klicken Sie mit der rechten Maustaste auf **Zwischenstammzertifizierungsstellen** und wählen Sie **Alle Aufgaben > Importieren** aus.

l Der **Assistent für das Importieren von Zertifikaten** wird geöffnet.

m Wechseln Sie zur Stammzertifikatsdatei und klicken Sie auf **Weiter**.

n Wählen Sie **Alle Zertifikate in folgendem Speicher speichern: Zwischenstammzertifizierungsstellen**, klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

o Wiederholen Sie die Schritte m. und n. für jedes Zwischenzertifikat, das installiert werden soll.

p Wechseln Sie zu **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.

q Wählen Sie das Stammzertifizierungsstellenzertifikat und exportieren Sie dieses.

Exportieren Sie das Zertifikat im Format DER-codiert-binär X.509 (.CER).

2 Kopieren Sie das Stammzertifizierungsstellenzertifikat auf den Windows-Computer.

3 Importieren Sie das Stammzertifizierungsstellenzertifikat auf den Windows-Computer.

a Auf dem Windows-Computer starten Sie MMC (`mmc.exe`).

b Fügen Sie das Zertifikate-Snap-In für das Computerkonto hinzu und verwalten Sie die Zertifikate für den lokalen Computer.

c Importieren Sie das Stammzertifizierungsstellenzertifikat in **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.

Das Stammzertifizierungsstellenzertifikat wird nun für alle Benutzer als vertrauenswürdig eingestuft.

## Installieren eines internen Zertifizierungsstellen-Stammzertifikats auf einem Mac

Um ein internes Zertifizierungsstellen-Stammzertifikat auf einem Mac-Host zu installieren, müssen Sie das Zertifikat von Ihrem Horizon FLEX Server exportieren und auf Ihrem Mac importieren.

### Voraussetzungen

- Informieren Sie sich über die Installation und Anwendung des MMC-Zertifikate-Snap-In auf einem Windows-System. Weitere Informationen dazu erhalten Sie auf der Windows-TechNet-Website unter http://technet.microsoft.com.
- Machen Sie sich mit der Anwendung der Schlüsselbundverwaltung auf einem Mac vertraut. Weitere Informationen dazu erhalten Sie auf der Apple-Support-Website unter http://support.apple.com.
- Installieren Sie Windows IIS.

### Vorgehensweise

1 Exportieren Sie das Stammzertifizierungsstellenzertifikat von Ihrem Horizon FLEX-Server.

a Auf dem Horizon FLEX-Server starten Sie MMC (`mmc.exe`), fügen das Zertifikate-Snap-In für ein Computerkonto hinzu und verwalten die Zertifikate für den lokalen Computer.

b Wählen Sie **Datei > Snap-In hinzufügen/entfernen** aus.

c Klicken Sie auf das **Zertifikat**-Snap-In und dann auf **Hinzufügen**.

d Wählen Sie im Fenster **Zertifikat-Snap-In** die Option **Computerkonto** aus und klicken Sie auf **Weiter**.

Diese Einstellung ist für den Horizon FLEX-Server obligatorisch.

e Wählen Sie **Lokaler Computer** aus und klicken Sie auf **Fertig stellen** und dann auf **OK**.

f Im linken Navigationsbereich erweitern Sie **Zertifikate (Lokaler Computer)**.

g Klicken Sie mit der rechten Maustaste auf **Vertrauenswürdige Stammzertifizierungsstellen** und wählen Sie **Alle Aufgaben > Importieren**.

Der Assistent für das Importieren von Zertifikaten wird geöffnet.

h Klicken Sie auf **Weiter**.

i Wechseln Sie zur Stammzertifikatsdatei und klicken Sie auf **Weiter**.

j Wählen Sie **Alle Zertifikate in folgendem Speicher speichern: Vertrauenswürdige Stammzertifizierungsstellen**, klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

k Klicken Sie mit der rechten Maustaste auf **Zwischenstammzertifizierungsstellen** und wählen Sie **Alle Aufgaben > Importieren** aus.

l Der **Assistent für das Importieren von Zertifikaten** wird geöffnet.

m Wechseln Sie zur Stammzertifikatsdatei und klicken Sie auf **Weiter**.

n Wählen Sie **Alle Zertifikate in folgendem Speicher speichern: Zwischenstammzertifizierungsstellen**, klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

o Wiederholen Sie die Schritte m. und n. für jedes Zwischenzertifikat, das installiert werden soll.

p Wechseln Sie zu **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.

q Wählen Sie das Stammzertifizierungsstellenzertifikat und exportieren Sie dieses.

Exportieren Sie das Zertifikat im Format DER-codiert-binär X.509 (.CER).

2 Kopieren Sie das Zertifizierungsstellen-Stammzertifikat auf den Mac.

3 Importieren Sie das Zertifizierungsstellen-Stammzertifikat auf dem Mac.

a Doppelklicken Sie auf das Zertifizierungsstellen-Stammzertifikat, um es in der Schlüsselbundverwaltung zu öffnen.

Das Zertifizierungsstellen-Stammzertifikat erscheint unter **Anmeldung**.

b Kopieren Sie das Zertifizierungsstellen-Stammzertifikat nach **System**.

Das Kopieren des Zertifikats nach **System** ist Voraussetzung dafür, dass es von allen Benutzern und lokalen Systemprozessen als vertrauenswürdig eingestuft wird, inklusive der Prozesse der virtuellen Maschine (`.vmx`) in Fusion.

c Öffnen Sie das Zertifizierungsstellen-Stammzertifikat, erweitern Sie **Vertrauen**, wählen Sie **System-Standards verwenden** und speichern Sie Ihre Änderungen.

d Öffnen Sie das Zertifizierungsstellen-Stammzertifikat erneut, erweitern Sie **Vertrauen**, wählen Sie **Immer vertrauen** und speichern Sie Ihre Änderungen.

e Löschen Sie das Zertifizierungsstellen-Stammzertifikat aus **Anmeldung**.

# Erstellen und Bereitstellen virtueller Horizon FLEX -Maschinen

4

Sie können mehrere virtuelle Horizon FLEX-Maschinen erstellen und für diese einer Vielzahl an Endbenutzern eine Berechtigung erteilen, inklusive Mac-Benutzern. Für die Anwendung ihrer virtuellen Horizon FLEX-Maschinen können Benutzer mit dem Unternehmensnetzwerk verbunden oder von diesem getrennt sein. Wenn Sie eine virtuelle Maschine der Quelle für eine virtuelle Horizon FLEX-Maschine erstellen, müssen Sie bestimmte Optionen auswählen, um sicherzustellen, dass die virtuelle Maschine korrekt mit Horizon FLEX zusammenarbeitet.

Sie können mit Fusion Pro oder Workstation Pro (nicht im Horizon FLEX-Paket enthalten) eine virtuelle Maschine der Quelle erstellen.

Dieses Kapitel behandelt die folgenden Themen:



## Übersicht über die Bereitstellung virtueller Horizon FLEX -Maschinen

Um eine virtuelle Horizon FLEX-Maschine bereitstellen zu können, müssen Sie die dazu notwendigen Arbeitsschritte in einer bestimmten Reihenfolge ausführen.

1 Erstellen und konfigurieren Sie eine virtuelle Maschine der Quelle.

  Siehe „Erstellen einer virtuellen Maschine der Quelle in Fusion Pro“, auf Seite 36 oder „Erstellen einer virtuellen Maschine der Quelle in Workstation Pro (nicht in Horizon FLEX enthalten)“, auf Seite 38.

2 (Optional) Bereiten Sie die virtuelle Maschine der Quelle für eine Verbindung mit der Active Directory-Domäne vor.

  Weitere Informationen hierzu finden Sie unter „Vorbereiten einer virtuellen Maschine der Quelle für den Beitritt zu einer Active Directory-Domäne“, auf Seite 41.

3 Komprimieren Sie das Paket der virtuellen Maschine der Quelle und speichern Sie es in Ihrem Download-Verzeichnis.

   Weitere Informationen hierzu finden Sie unter „Komprimieren eines Pakets einer virtuellen Maschine der Quelle“, auf Seite 42.

4 Registrieren Sie die virtuelle Maschine der Quelle mit Horizon FLEX-Richtlinienserver.

   Weitere Informationen hierzu finden Sie unter „Registrieren einer virtuellen Maschine der Quelle mit Horizon FLEX-Richtlinienserver“, auf Seite 42.

5 Erstellen Sie eine Richtlinie für das Horizon FLEX-Image und erteilen Sie eine Berechtigung für das Image für Ihre Active Directory-Benutzer und -Gruppen.

   Weitere Informationen hierzu finden Sie unter „Erstellen von Richtlinien und Berechtigungen“, auf Seite 44.

6 (Optional) Erstellen Sie einen URI zur Bereitstellung einer virtuellen Horizon FLEX-Maschine

   Weitere Informationen hierzu finden Sie unter „Erstellen eines URI zur Bereitstellung einer virtuellen Horizon FLEX-Maschine“, auf Seite 53.

## Erstellen einer virtuellen Maschine der Quelle in Fusion Pro

Mit Fusion Pro können Sie eine virtuelle Maschine der Quelle für eine virtuelle Horizon FLEX-Maschine erstellen. Beim Erstellen einer virtuellen Maschine der Quelle müssen Sie Festlegungen für die Verschlüsselung und für Einschränkungen treffen, damit die Funktionen der virtuellen Maschine korrekt mit Horizon FLEX zusammenarbeiten.

Sie können auch mit Workstation Pro eine virtuelle Maschine der Quelle erstellen. Workstation Pro ist nicht im Horizon FLEX-Paket enthalten.

Wenn Sie die USB-Gerätefunktionen für die Verwendung, für „Drag-and-Drop“-Operationen sowie zum Kopieren und Einfügen beim Erstellen der virtuellen Maschine aktivieren, können Sie Richtlinien in Horizon FLEX-Verwaltungskonsole einrichten, um diese Funktionen für Endbenutzer zu aktivieren oder deaktivieren. Werden diese Funktionen beim Erstellen der virtuellen Maschine allerdings deaktiviert, ist es nicht möglich, die Einstellungen für die virtuelle Maschine durch Einrichten der Funktionen mithilfe von Richtlinien zu überschreiben.

Horizon FLEX unterstützt für virtuelle Maschinen ausschließlich Namen, die aus lateinischen Zeichen bestehen. Verwenden Sie in Namen für .vmx- oder .tar-Dateien keine Nicht-ASCII-Zeichen. Fusion Pro kann keine virtuellen Horizon FLEX-Maschinen auf Japanisch oder vereinfachtem Chinesisch erstellen.

---

**Hinweis** Stellen Sie bei der Vorbereitung einer virtuellen Horizon FLEX-Maschine sicher, dass die .vmx-Richtliniendatei sich im selben Ordner befindet wie alle .vmdk-Dateien (virtuellen Festplatten). Wenn die .vmx-Datei und die Dateien für die virtuellen Festplatten sich in unterschiedlichen Verzeichnissen auf dem Computer des Client-Benutzers befinden, erhält der Benutzer beim Versuch, die virtuelle Horizon FLEX-Maschine zu starten, eine Fehlermeldung.

---

### Voraussetzungen

- Machen Sie sich mit dem Erstellen einer virtuellen Maschine in Fusion Pro vertraut. Erläuterungen dazu finden Sie in der Fusion-Dokumentation unter https://www.vmware.com/support/pubs/fusion_pubs.html.
- Informieren Sie sich über die unterstützten Gastbetriebssysteme für virtuelle Horizon FLEX-Maschinen. Siehe „Unterstützte Host- und Gastbetriebssysteme“, auf Seite 12.
- Installieren Sie Fusion Pro mit einem Horizon FLEX-Lizenzschlüssel.

### Vorgehensweise

1 Öffnen Sie Fusion Pro und erstellen Sie eine virtuelle Maschine.

Wählen Sie ein Gastbetriebssystem, das für virtuelle Horizon FLEX-Maschinen unterstützt wird. Nach Erstellung der virtuellen Maschine versucht Fusion Pro, VMware Tools zu installieren. Konfigurieren Sie die virtuelle Maschine für die Verteilung an Ihre Endbenutzer.

2 Aus der Bibliothek der virtuellen Maschinen wählen Sie die neue virtuelle Maschine und anschließend **Einstellungen > Verschlüsselung und Einschränkungen**.

3 Wählen Sie **Verschlüsselung aktivieren** aus und legen Sie ein Kennwort für das Öffnen der virtuellen Maschine fest.

Das Kennwort muss aus mindestens sechs Zeichen bestehen. Dieses Verschlüsselungskennwort muss an Ihre Endbenutzer weitergegeben werden, damit diese die virtuelle Maschine öffnen können.

Sie müssen das Verschlüsselungskennwort aufbewahren. Ohne dieses Kennwort ist kein Zugriff auf die virtuelle Maschine möglich.

4 Aktivieren Sie **Einschränkungen aktivieren** und legen Sie ein Kennwort für die Bearbeitung der Einschränkungen für die virtuelle Maschine fest.

Dieses Kennwort muss sich von jenem zur Verschlüsselung der virtuellen Maschine unterscheiden.

Sie müssen das Kennwort für die Einschränkungen aufbewahren. Ohne dieses Kennwort lassen sich die Einschränkungen für die virtuelle Maschine nicht bearbeiten.

5 Klicken Sie auf **Konfigurieren**.

Das Fenster zur Konfiguration der Einschränkungen wird geöffnet.

6 Wählen Sie für **Einschränkungstyp** die Einstellung**Verwaltet**.

Mit **Verwaltet** wird sichergestellt, dass die virtuelle Maschine mit Horizon FLEX verteilt und angewendet werden kann .

7 Geben Sie in das Textfeld **Server für Einschränkungsmanagement** die URL des Horizon FLEX Servers ein, auf dem die virtuelle Maschine gehostet werden soll.

8 Klicken Sie auf **Server überprüfen**, um die Horizon FLEX Server-URL zu verifizieren.

9 (Optional) Um der virtuellen Maschine vertrauenswürdige Zertifikate hinzuzufügen, klicken Sie auf die Schaltfläche **+** und wechseln zum Standort jeder einzelnen Zertifikatsdatei.

Wenn Sie der virtuellen Maschine Zertifikate hinzufügen, verwendet Horizon FLEX-Client die Zertifikate der virtuellen Maschine und nicht jene auf dem Host. Zur Zertifikatsteuerung und zur Einrichtung auf dem Horizon FLEX-Richtlinienserver für alle virtuellen Horizon FLEX-Maschinen lassen Sie das Zertifikatfeld leer.

10 Klicken Sie auf **Speichern**.

11 Klicken Sie auf das Symbol **Sperren**, um zu verhindern, dass weitere Änderungen an den Einschränkungen der virtuellen Maschine vorgenommen werden.

Einschränkungen für die virtuelle Maschine lassen sich mithilfe des Einschränkungskennworts bearbeiten.

### Weiter

Wenn die virtuelle Horizon FLEX-Maschine einer Active Directory-Domäne beitreten soll, müssen Sie die virtuelle Maschine entsprechend vorbereiten. Siehe „Vorbereiten einer virtuellen Maschine der Quelle für den Beitritt zu einer Active Directory-Domäne“, auf Seite 41.

Zur Installation des Mirage-Clients in der virtuellen Maschine der Quelle finden Sie weitere Informationen unter „Installieren von Mirage Client in einer virtuellen Maschine der Quelle“, auf Seite 39.

# Erstellen einer virtuellen Maschine der Quelle in Workstation Pro (nicht in Horizon FLEX enthalten)

Mit Workstation Pro können Sie eine virtuelle Maschine der Quelle für eine virtuelle Horizon FLEX-Maschine erstellen. Workstation Pro ist nicht im Horizon FLEX-Paket enthalten. Für Workstation Pro ist kein Horizon FLEX-Lizenzschlüssel erforderlich.

Horizon FLEX unterstützt für virtuelle Maschinen ausschließlich Namen, die aus lateinischen Zeichen bestehen. Verwenden Sie in Namen für .vmx- oder .tar-Dateien keine Nicht-ASCII-Zeichen.

---

**HINWEIS** Stellen Sie bei der Vorbereitung einer virtuellen Horizon FLEX-Maschine sicher, dass die .vmx-Richtliniendatei sich im selben Ordner befindet wie alle .vmdk-Dateien (virtuellen Festplatten). Wenn die .vmx-Datei und die Dateien für die virtuellen Festplatten sich in unterschiedlichen Verzeichnissen auf dem Computer des Client-Benutzers befinden, erhält der Benutzer beim Versuch, die virtuelle Horizon FLEX-Maschine zu starten, eine Fehlermeldung.

---

### Voraussetzungen

- Informieren Sie sich über das Erstellen einer virtuellen Maschine in Workstation Pro. Informationen dazu finden Sie in der Workstation Pro-Dokumentation unter https://www.vmware.com/support/pubs/ws_pubs.html
- Informieren Sie sich über die unterstützten Gastbetriebssysteme für virtuelle Horizon FLEX-Maschinen. Weitere Informationen hierzu finden Sie unter „Unterstützte Host- und Gastbetriebssysteme“, auf Seite 12.
- Installieren Sie Workstation.

### Vorgehensweise

1. Öffnen Sie Workstation Pro und erstellen Sie eine virtuelle Maschine. Nach Erstellung der virtuellen Maschine versucht Workstation Pro, VMware Tools zu installieren.
2. Installieren Sie das Gastbetriebssystem.

   Wählen Sie ein Gastbetriebssystem, das für virtuelle Horizon FLEX-Maschinen unterstützt wird. Konfigurieren Sie die virtuelle Maschine für die Verteilung an Ihre Endbenutzer.
3. Verschlüsseln Sie die virtuelle Maschine und schränken Sie diese ein. Wählen Sie die virtuelle Maschine aus und dann die Option **VM > Einstellungen**.
4. Auf der Registerkarte **Optionen** wählen Sie **Zugriffssteuerung**.
5. Klicken Sie auf **Verschlüsseln**, geben Sie ein Verschlüsselungskennwort ein und klicken Sie auf **Verschlüsseln**.

   Das Verschlüsselungskennwort ist für den Zugriff auf die virtuelle Maschine erforderlich. Damit kann jedoch nicht verhindert werden, dass der Benutzer die Konfiguration der virtuellen Maschine ändert. Um die Änderung der Konfiguration der virtuellen Maschine zu sperren, aktivieren Sie die Einschränkungen und geben Sie ein Kennwort ein.

   ---

   **WICHTIG** Notieren Sie das verwendete Verschlüsselungskennwort. Workstation bietet keine Option zum erneuten Kennwortabruf, wenn Sie Ihr Kennwort vergessen.

   ---

   Workstation startet mit der Verschlüsselung der virtuellen Maschine. Nach Abschluss der Verschlüsselung können Sie ein Einschränkungskennwort einrichten.

6 Aktivieren Sie das Kontrollkästchen **Einschränkungen aktivieren** und legen Sie ein Kennwort für die Bearbeitung der Einschränkungen für die virtuelle Maschine fest.

Legen Sie ein vom Verschlüsselungskennwort der virtuellen Maschine abweichendes Kennwort fest.

Sie müssen das Kennwort für die Einschränkungen aufbewahren. Ohne dieses Kennwort lassen sich die Einschränkungen für die virtuelle Maschine nicht bearbeiten.

7 Wählen Sie für **Einschränkungstyp** die Einstellung**Verwaltet**.

Mit **Verwaltet** wird sichergestellt, dass die virtuelle Maschine mit Horizon FLEX verteilt und angewendet werden kann .

8 Geben Sie in das Textfeld **Server für Einschränkungsmanagement** die URL des Horizon FLEX Servers ein, auf dem die virtuelle Maschine gehostet werden soll.

9 Klicken Sie auf **Server überprüfen**, um die Horizon FLEX Server-URL zu verifizieren.

10 (Optional) Um der virtuellen Maschine vertrauenswürdige Zertifikate hinzuzufügen, klicken Sie auf das Symbol **Zertifikate verwalten** und wechseln Sie zum Standort jeder einzelnen Zertifikatsdatei.

Wenn Sie der virtuellen Maschine Zertifikate hinzufügen, verwendet Horizon FLEX-Client die Zertifikate der virtuellen Maschine und nicht jene auf dem Host. Zur Zertifikatsteuerung und zur Einrichtung auf dem Horizon FLEX-Richtlinienserver für alle virtuellen Horizon FLEX-Maschinen lassen Sie das Zertifikatfeld leer.

11 Klicken Sie auf **Speichern**.

### Weiter

Wenn die virtuelle Horizon FLEX-Maschine einer Active Directory-Domäne beitreten soll, müssen Sie die virtuelle Maschine entsprechend vorbereiten. Weitere Informationen hierzu finden Sie unter „Vorbereiten einer virtuellen Maschine der Quelle für den Beitritt zu einer Active Directory-Domäne“, auf Seite 41.

Zur Installation des Mirage-Clients in der virtuellen Maschine der Quelle finden Sie weitere Informationen unter „Installieren von Mirage Client in einer virtuellen Maschine der Quelle“, auf Seite 39.

## Installieren von Mirage Client in einer virtuellen Maschine der Quelle

Wenn die virtuelle Maschine der Quelle über ein Windows-Gastbetriebssystem verfügt, können Sie Mirage Client in der virtuellen Maschine installieren. Die Installation von Mirage Client ist optional.

Wenn Sie Mirage Client in einer virtuellen Maschine der Quelle installieren, können Sie, wenn Sie eine Berechtigung für die virtuelle Maschine erteilen, Szenarien der Notfallwiederherstellung auswählen. Beispielsweise haben Sie die Möglichkeit, mit einer Option festzulegen, dass der Mirage-Server eine CVD für die virtuellen Horizon FLEX-Maschinen erstellt, die der Endbenutzer herunterlädt. Mirage synchronisiert periodisch die Endbenutzerdaten mit dem Datencenter auf der Basis der gewählten Mirage-Richtlinie. Mit diesen Daten können Sie die CVD wiederherstellen oder auf Dateien der virtuellen Maschine mithilfe des Mirage-Dateiportals in Mirage Management Console zugreifen.

---

**Hinweis** Stellen Sie beim Konfigurieren des Mirage-Servers für die Disaster Recovery sicher, dass die MongoDB-Ports richtig konfiguriert sind. Weitere Informationen finden Sie im *VMware Mirage-Installationshandbuch*.

---

### Voraussetzungen

- Erstellen Sie die virtuelle Maschine der Quelle. Siehe „Erstellen einer virtuellen Maschine der Quelle in Fusion Pro“, auf Seite 36 oder „Erstellen einer virtuellen Maschine der Quelle in Workstation Pro (nicht in Horizon FLEX enthalten)“, auf Seite 38.
- Informieren Sie sich im *VMware Mirage-Installationshandbuch* für Mirage Client über die Arbeitsschritte der Installation.

### Vorgehensweise

1 Starten Sie in Fusion Pro oder Workstation Pro die virtuelle Maschine der Quelle und melden Sie sich beim Gastbetriebssystem an.

2 Installieren Sie die neueste Version von VMware Tools.

   a In der Menüleiste wählen Sie **Virtuelle Maschine > VMware Tools installieren**.

   b Klicken Sie zur Fortsetzung der Installation auf **Weiter**.

   c Wählen Sie **Vollständig**, wenn Sie nicht bestimmte Funktionen von VMware Tools ausschließen möchten, und klicken Sie auf **Weiter**.

   d Klicken Sie auf **Installieren**.

   e Nach Beendigung der Installation klicken Sie auf **Ja**, um die virtuelle Maschine neu zu starten.

3 Installieren Sie den Mirage-Client in der virtuellen Maschine der Quelle.

   Im *VMware Mirage-Installationshandbuch* finden Sie dazu weitere Informationen.

4 In Mirage Management Console vergewissern Sie sich, ob der Endpunkt als ausstehender Auftrag erscheint.

   **HINWEIS** Löschen Sie diesen ausstehenden Datensatz nicht, solange Sie diese virtuelle Maschine der Quelle verteilen.

5 Aktivieren Sie in Mirage Management Console die automatische CVD-Erstellung.

   a Klicken Sie mit der rechten Maustaste auf **Systemkonfiguration** und klicken Sie auf **Einstellungen**.

   b Klicken Sie auf die Registerkarte **Automatische CVD-Erstellung**.

   c Wählen Sie **Automatische CVD-Erstellung aktivieren** aus.

      Bei Bedarf können Sie die Benutzermeldung ändern.

   d Klicken Sie auf **OK**.

6 Schalten Sie die virtuelle Maschine der Quelle in Mirage aus, wenn diese sich im Status „Ausstehender Auftrag“ befindet.

   Geben Sie weder Benutzername noch Kennwort an und registrieren Sie nicht die virtuelle Maschine der Quelle an der Mirage-Client-Eingabeaufforderung. Wenn Sie die virtuelle Maschine der Quelle mit Mirage registrieren, wird die virtuelle Horizon FLEX-Maschine dupliziert, sobald der Endbenutzer darauf zugreift.

Wenn der Mirage-Client aktiv ist und Sie eine neue Horizon FLEX-Berechtigung für diese virtuelle Maschine der Quelle erstellen, sind Mirage-Kontrollen für diese virtuelle Maschine verfügbar.

# Vorbereiten einer virtuellen Maschine der Quelle für den Beitritt zu einer Active Directory-Domäne

Wenn eine virtuelle Horizon FLEX-Maschine einer bestimmten Active Directory-Domäne beitreten soll, müssen Sie die virtuelle Maschine der Quelle für den Beitritt zur Domäne vorbereiten, bevor Sie diese mit Horizon FLEX-Richtlinienserver registrieren können.

### Voraussetzungen

- Erstellen Sie die virtuelle Maschine. Siehe „Erstellen einer virtuellen Maschine der Quelle in Fusion Pro“, auf Seite 36 oder „Erstellen einer virtuellen Maschine der Quelle in Workstation Pro (nicht in Horizon FLEX enthalten)“, auf Seite 38.

  **HINWEIS** Installieren Sie nicht Windows 7 Home Edition oder ein Nicht-Windows-Gastbetriebssystem in der virtuellen Maschine der Quelle. Das Betriebssystem Windows 7 Home Edition oder ein Nicht-Windows-Gastbetriebssystem können keiner Domäne beitreten.

- Stellen Sie sicher, dass der Administrator über das Kennwort für die virtuelle Maschine der Quelle verfügt.
- In der Horizon FLEX-Verwaltungskonsole legen Sie die Richtlinie für die virtuelle Maschine zum Beitritt zur Active Directory-Domäne fest. Das Horizon FLEX-Administratorkonto muss über die Berechtigung zum Erstellen von Objekten in Active Directory verfügen.
- Außerdem muss ein RODC in der DMZ installiert sein.
- Konfigurieren Sie Active Directory zur Unterstützung des Domänenbeitritts.

### Vorgehensweise

1. In Fusion Pro starten Sie die virtuelle Maschine der Quelle und melden sich beim Gastbetriebssystem an.
2. (Optional) Schalten Sie **Windows Update** aus.
3. Installieren Sie die neueste Version von VMware Tools.
   a. In der Menüleiste wählen Sie **Virtuelle Maschine > VMware Tools installieren**.
   b. Klicken Sie zur Fortsetzung der Installation auf **Weiter**.
   c. Wählen Sie **Vollständig**, wenn Sie nicht bestimmte Funktionen von VMware Tools ausschließen möchten, und klicken Sie auf **Weiter**.
   d. Klicken Sie auf **Installieren**.
   e. Nach Beendigung der Installation klicken Sie auf **Ja**, um die virtuelle Maschine neu zu starten.
4. Führen Sie `install-rvmsetup.cmd` als Administrator aus, um den VMware-RVM-Setup-Dienst in der virtuellen Maschine der Quelle zu installieren.

   Der VMware-RVM-Setup-Dienst führt den Beitritt zur Domäne durch. `install-rvmsetup.cmd` ist in VMware Tools enthalten.
5. Öffnen Sie das Snap-In „Windows-Dienste“ (`services.msc`) und prüfen Sie, ob als Starttyp für den VMware-RVM-Setup-Dienst „Automatisch“ eingestellt ist.
6. Fahren Sie die virtuelle Maschine der Quelle herunter.

   Der VMware-RVM-Setup-Dienst wird gestartet, sobald Sie die virtuellen Maschine der Quelle das nächste Mal hochfahren.

# Komprimieren eines Pakets einer virtuellen Maschine der Quelle

Sie müssen das Paket einer virtuellen Maschine der Quelle im TAR-Format komprimieren (`.tar`), damit Endbenutzer die virtuelle Maschine problemlos und schnell herunterladen können. Das Paket für eine virtuelle Maschine (auch „Bundle“ genannt) enthält sämtliche Dateien der virtuellen Maschine, um diese ausführen zu können.

### Voraussetzungen

- Erstellen Sie die virtuelle Maschine der Quelle. Siehe „Erstellen einer virtuellen Maschine der Quelle in Fusion Pro“, auf Seite 36 oder „Erstellen einer virtuellen Maschine der Quelle in Workstation Pro (nicht in Horizon FLEX enthalten)“, auf Seite 38.
- Erstellen und konfigurieren Sie einen Download-Ordner für Ihre Pakete virtueller Horizon FLEX-Maschinen. Siehe „Erstellen eines Download-Ordners für Pakete virtueller Horizon FLEX-Maschinen“, auf Seite 17 und „Konfigurieren des IIS-SSL-Serverzertifikats für den Horizon FLEX Server“, auf Seite 18.

### Vorgehensweise

1 Wenn die virtuelle Maschine der Quelle ausgeführt wird, fahren Sie diese herunter.

2 In Fusion Pro oder Workstation Pro wechseln Sie zur virtuellen Maschine der Quelle.

3 Wählen Sie **Datei > Nach TAR exportieren** und exportieren Sie das Paket einer virtuellen Maschine in eine TAR-Datei.

Entfernen Sie alle Leerzeichen aus dem TAR-Dateinamen. Das Entfernen von Leerzeichen aus dem Dateinamen kann das Herstellen einer Verbindung zur Download-URL der virtuellen Maschine vereinfachen.

4 Exportieren Sie die TAR-Datei in den Download-Ordner für Ihre Pakete virtueller Horizon FLEX-Maschinen.

### Weiter

Registrieren Sie die virtuelle Maschine der Quelle bei Horizon FLEX-Richtlinienserver. Weitere Informationen hierzu finden Sie unter „Registrieren einer virtuellen Maschine der Quelle mit Horizon FLEX-Richtlinienserver“, auf Seite 42.

# Registrieren einer virtuellen Maschine der Quelle mit Horizon FLEX-Richtlinienserver

Sie müssen eine virtuelle Maschine der Quelle mit Horizon FLEX-Richtlinienserver als ein Horizon FLEX-Image registrieren, bevor Sie die virtuelle Maschine an Endbenutzer weitergeben können.

### Voraussetzungen

- Komprimieren Sie die Dateien der virtuellen Maschine der Quelle in einer TAR-Archivdatei (`.tar`). Weitere Informationen hierzu finden Sie unter „Komprimieren eines Pakets einer virtuellen Maschine der Quelle“, auf Seite 42.
- Vergewissern Sie sich, dass das Download-Verzeichnis für Ihre Pakete der virtuellen Horizon FLEX-Maschine korrekt eingerichtet ist. Siehe „Erstellen eines Download-Ordners für Pakete virtueller Horizon FLEX-Maschinen“, auf Seite 17 und „Konfigurieren des IIS-SSL-Serverzertifikats für den Horizon FLEX Server“, auf Seite 18.

- Überprüfen Sie, ob bereits Einschränkungen in der Konfigurationsdatei für die virtuelle Maschine der Quelle (`.vmx`) festgelegt sind. Wenn Sie eine virtuelle Maschine auswählen, für die noch keine Einschränkungen eingerichtet wurden, weist Horizon FLEX-Richtlinienserver die Datei `.vmx` als ungültig zurück. Informationen zum Einrichten von Einschränkungen in einer virtuellen Maschine finden Sie unter „Erstellen einer virtuellen Maschine der Quelle in Fusion Pro“, auf Seite 36.

### Vorgehensweise

1 Befindet sich die virtuelle Maschine der Quelle auf einem Mac, führen Sie die folgenden Schritte aus.

   a Ermitteln Sie die Paketdatei virtueller Maschinen (`.vmwarevm`) für die virtuelle Maschine, klicken Sie mit der rechten Maustaste auf den Dateinamen und wählen Sie aus dem eingeblendeten Kontextmenü die Option **Paketinhalt anzeigen**.

   b Kopieren Sie die Konfigurationsdatei für virtuelle Maschinen (`.vmx`) an einen Ort, auf den der Horizon FLEX Server über einen Zugriff verfügt.

2 Starten Sie den Horizon FLEX-Verwaltungskonsole.

   a Geben Sie in einem Webbrowser **`https://`*`WebManagerServer`*`:7443/rvm`** ein, wobei *WebManagerServer* für den DNS-Namen oder die IP-Adresse des Hosts steht, auf dem Mirage Web Manager installiert ist.

   b Geben Sie den Benutzernamen und das Kennwort eines Domänenkontos ein, das einen Zugriff auf Mirage besitzt.

   c Klicken Sie auf **Anmelden**.

3 Klicken Sie auf **Images** im linken Navigationsbereich.

4 Klicken Sie auf die Schaltfläche **Neu** (+).

5 Klicken Sie neben dem Textfeld **Image-Datei auswählen** auf **Auswählen** und wechseln Sie zur Konfigurationsdatei für virtuelle Maschinen (`.vmx`) für die virtuelle Maschine der Quelle.

6 Geben Sie für die Datei der virtuellen Horizon FLEX-Maschine im Textfeld **Image-Name** einen benutzerfreundlichen Namen ein.

   Beispiel: **`Windows 7 VM`**

7 (Optional) Geben Sie in das Textfeld **Beschreibung** eine Beschreibung der virtuellen Horizon FLEX-Maschine ein.

8 (Optional) Klicken Sie auf die Schaltfläche **Ändern** neben **Symbol** und laden Sie ein Symbol für die virtuelle Horizon FLEX-Maschine hoch.

   Bei hochgeladenen Symbolen muss es sich um PNG-Dateien (`.png`) handeln.

9 (Optional) In das Textfeld **Image-URL** geben Sie den gültigen Pfad für die TAR-Datei ein, die das Paket der virtuellen Maschine der Quelle enthält.

   Endbenutzer laden dann die virtuelle Horizon FLEX-Maschine von dieser URL herunter. Das URL-Format ist `http://`*`Server`*`:`*`Port`*`/`*`Download–Ordner`*`/`*`Dateiname.tar`*, wobei *Server* für den Hostnamen oder die IP-Adresse des Servers steht, auf dem die TAR-Datei gespeichert ist, Port für die Portnummer auf dem Server, *Download-Ordner* für den Namen des Download-Ordners der virtuellen Horizon FLEX-Maschine, der die TAR-Datei enthält, und *Dateiname.tar* für den Namen der TAR-Datei, die das Paket der virtuellen Maschine der Quelle enthält. Die URL kann mit „http“ oder „https“ beginnen.

   Beispiel: `https://flexserver.demo.local:7443/flexdownloads/windows7vm.tar`

10 (Optional) Geben Sie in das Textfeld **Haftungsausschluss (optional)** Text ein.

   Wenn Sie keinen Text eingeben, zeigt Horizon FLEX-Client keinen Haftungsausschlusstext an, wenn ein Benutzer die virtuelle Horizon FLEX-Maschine herunterlädt.

11 Klicken Sie auf **OK**, um die virtuelle Maschine der Quelle als Horizon FLEX-Image zu registrieren.

12 (Optional) Geben Sie die Image-URL in einen Webbrowser ein, um die URL zu überprüfen.

Beispiel: `https://flexserver.demo.local:7443/flexdownloads/windows7vm.tar`

Ist die URL korrekt, werden Sie zum Speichern der Datei aufgefordert. Wenn Sie einen Berechtigungsfehler erhalten, müssen Sie eventuell die NTFS-Berechtigungen für den Download-Ordner anpassen.

**Weiter**

Fügen Sie dem Horizon FLEX-Image Richtlinien hinzu. Weitere Informationen hierzu finden Sie unter „Konfigurieren einer allgemeinen Richtlinie für ein Horizon FLEX-Image“, auf Seite 44.

# Erstellen von Richtlinien und Berechtigungen

Mit Richtlinien haben Sie die Möglichkeit, ein Ablaufdatum festzulegen und die Funktionen in den Instanzen einer virtuellen Maschine zu steuern, die von einem Horizon FLEX-Image erstellt wurden. Mithilfe von Berechtigungen können bestimmte Benutzer und Gruppen Instanzen einer virtuellen Maschine von einem bestimmten Horizon FLEX-Image erstellen.

Mit jeder Berechtigung, die Sie erstellen, verbinden Sie eine Richtlinie. Diese Richtlinie definiert die Standardeinschränkungseinstellungen für die Instanzen der virtuellen Maschine, die vom Horizon FLEX-Image der Berechtigung erstellt wurde.

Dasselbe Horizon FLEX-Image lässt sich mehreren Berechtigungen hinzufügen und Sie können jede Berechtigung mit einer anderen Richtlinie verbinden. Derselbe Benutzer kann Mitglied mehrerer Berechtigungen sein.

Wenn die Instanz einer virtuellen Maschine erstellt wurde, legen die Richtlinien, die mit den Berechtigungen verbunden sind, die anfänglichen Einschränkungen der Instanz fest. Als Administrator können Sie die Einschränkungseinstellungen für eine bestimmte Instanz einer virtuellen Maschine ändern. Instanzenspezifische Einschränkungen wirken wie Einschränkungen für die Kombination aus einem bestimmten Benutzer und einer virtuellen Maschine. Informationen zum Bearbeiten von Einschränkungen in einer virtuellen Maschine finden Sie unter „Verwalten virtueller Horizon FLEX-Maschinen“, auf Seite 55.

## Konfigurieren einer allgemeinen Richtlinie für ein Horizon FLEX -Image

Sie können durch Konfiguration allgemeiner Richtlinien ein Ablaufdatum festlegen und die Funktionen in den Instanzen einer virtuellen Maschine steuern, die von einem Horizon FLEX-Image erstellt wurden.

---

**Wichtig** Wenn die Einstellungen für das Kopieren und Einfügen, die Anwendung von „Drag-and-Drop“-Vorgängen und die Ordnerfreigabe in der virtuellen Maschine der Quelle aktiviert sind, können Sie durch die entsprechende Konfiguration einer Richtlinie sicherstellen, dass sich diese Funktionen beim Herunterladen einer Instanz der virtuellen Maschine durch Benutzer aktivieren oder deaktivieren lassen. Sind diese Funktionen in der virtuellen Maschine der Quelle deaktiviert, ist es nicht möglich, die Einstellungen für die virtuelle Maschine durch Aktivieren der Funktionen in einer Richtlinie zu überschreiben.

---

Sie können die Richtlinie einem Horizon FLEX-Image zuweisen, wenn Sie Benutzern eine Berechtigung für das Image erteilen. Es besteht die Möglichkeit, dieselbe Richtlinie für mehrere Berechtigungen zu verwenden.

### Vorgehensweise

1 Starten Sie den Horizon FLEX-Verwaltungskonsole.

   a Geben Sie in einem Webbrowser **`https://WebManagerServer:7443/rvm`** ein, wobei *WebManagerServer* für den DNS-Namen oder die IP-Adresse des Hosts steht, auf dem Mirage Web Manager installiert ist.

   b Geben Sie den Benutzernamen und das Kennwort eines Domänenkontos ein, das einen Zugriff auf Mirage besitzt.

   c Klicken Sie auf **Anmelden**.

2 Klicken Sie auf **Richtlinien** im linken Navigationsbereich.

3 Klicken Sie auf die Registerkarte **Allgemein**, um eine Richtlinie hinzuzufügen, oder wählen Sie eine vorhandene Richtlinie aus und klicken Sie auf **Bearbeiten**, um diese zu ändern.

4 Geben Sie in das Textfeld **Richtlinienname** einen Namen für die Richtlinie ein.

5 (Optional) Geben Sie in das Textfeld **Beschreibung** eine Beschreibung für die Richtlinie ein.

6 Unter **Allgemeine Einschränkungen** konfigurieren Sie die Einschränkungen der virtuellen Maschine.

| Option | Aktion |
|---|---|
| **Ablaufdatum** | Mit dem Kalender-Widget können Sie ein Ablaufdatum für eine virtuelle Maschine festlegen. |
| **Operationen zum Kopieren und Einfügen** | Sie können festlegen, ob Operationen zum Kopieren und Einfügen in der virtuellen Maschine zulässig sind. Diese Richtlinie steuert die Operationen zum Kopieren und Einfügen zwischen dem Gastbetriebssystem und dem Host der virtuellen Maschine. Sie gilt nicht für das Kopieren und Einfügen in der virtuellen Maschine. |
| **„Drag-and-Drop"-Operationen** | Sie können festlegen, ob „Drag-and-Drop"-Operationen in der virtuellen Maschine zulässig sind. Diese Richtlinie steuert die „Drag-and-Drop"-Operationen zwischen dem Gastbetriebssystem und dem Host der virtuellen Maschine. Sie gilt nicht für „Drag-and-Drop"-Operationen in der virtuellen Maschine. |
| **Einstellungen für die Ordnerfreigabe** | Sie können festlegen, ob im Gastbetriebssystem der virtuellen Maschine die Verwendung freigegebener Ordner zulässig ist, wenn der Administrator freigegebene Ordner in der virtuellen Maschine konfiguriert hat. |
| **Ändern von Arbeitsspeicher- und CPU-Einstellungen** | Sie haben die Möglichkeit, festzulegen, ob Benutzer die Arbeitsspeicher- und CPU-Einstellungen der virtuellen Maschine ändern dürfen. |
| **Änderung des Verschlüsselungskennworts beim Verschieben oder Kopieren der virtuellen Maschine vom Benutzer anfordern** | Legen Sie fest, ob Benutzer das Verschlüsselungskennwort ändern müssen, wenn sie die virtuelle Maschine verschieben oder kopieren möchten. |
| **Legen Sie das Einschaltkennwort fest, das mit dem AD-Kennwort des Benutzers nach dem ersten Start übereinstimmen muss.** | Legen Sie fest, ob das von Benutzern beim Einschalten der virtuellen Maschine eingegebene Kennwort dem Active Directory-Kennwort entspricht. |
| **Sperren Sie die Möglichkeit der Erstellung mehrerer Kopien der virtuellen Maschine durch den Benutzer.** | Legen Sie fest, ob Benutzer mehrere Instanzen der virtuellen Maschine herunterladen oder bereits registrierte virtuelle Maschinen kopieren dürfen. |

7 (Optional) Unter **Endbenutzermitteilungen** konfigurieren Sie die Ablaufeinstellungen der virtuellen Maschine.

Die Standardmeldung lautet `Diese virtuelle Maschine ist abgelaufen.`

a Sie können eine zusätzliche benutzerdefinierte Meldung eingeben, die angezeigt wird, wenn die virtuelle Maschine abgelaufen ist.

b Aktivieren Sie das Kontrollfeld **Diese Meldung anzeigen**, wählen Sie die Anzahl von Tagen vor dem Ablaufdatum für die Anzeige der Meldung aus und geben Sie einen benutzerdefinierten Benachrichtigungstext ein.

8 Unter **Servereinstellungen** konfigurieren Sie die Horizon FLEXServer-Einstellungen.

| Option | Aktion |
|---|---|
| **FLEX-Server-URL** | Geben Sie die URL des Horizon FLEX-Servers ein, der das Paket der virtuellen Maschine hostet. Beispiel:<br>**`https://flexserver.demo.local:7443`**<br>**WICHTIG** Der URL darf am Ende nicht der Parameter **`/rvm`** hinzugefügt werden. |
| **Kontaktfrequenz des Servers** | Wählen Sie die Frequenz, in der die virtuelle Maschine Kontakt mit dem Server zur Synchronisierung aufnehmen soll. |
| **Offline-Zeitbeschränkung** | Legen Sie die Anzahl der Tage fest, an denen Benutzer die virtuelle Maschine verwenden können, ohne dass diese mit dem Horizon FLEX-Server verbunden sein muss.<br>Wenn die Offline-Zeitbeschränkung überschritten ist, muss die virtuelle Maschine eine Verbindung mit dem Horizon FLEX-Server herstellen, bevor sie eingeschaltet werden kann. |

9 Klicken Sie auf **OK**, um die Richtlinie zu speichern.

Die neue Richtlinie erscheint in der Richtlinienliste.

### Weiter

Erteilen Sie eine Berechtigung für die virtuelle Horizon FLEX-Maschine. Weitere Informationen hierzu finden Sie unter „Erteilen einer Berechtigung für ein Horizon FLEX-Image“, auf Seite 49.

## Konfigurieren einer USB-Geräterichtlinie für ein Horizon FLEX -Image

Sie haben die Möglichkeit, Richtlinien zu konfigurieren, mit denen festgelegt wird, ob USB-Geräte auf virtuellen Maschinen verwendet werden können, die von einem Horizon FLEX-Image erstellt wurden.

**WICHTIG** Wenn der USB-Gerätecontroller in der virtuellen Maschine der Quelle vorhanden ist, können Sie durch die entsprechende Konfiguration einer Richtlinie sicherstellen, dass sich diese Funktion beim Herunterladen einer Instanz der virtuellen Maschine durch Benutzer aktivieren oder deaktivieren lässt. Ist diese Funktion in der virtuellen Maschine der Quelle deaktiviert, ist es nicht möglich, die Einstellungen für die virtuelle Maschine durch Aktivieren dieser Funktion in einer Richtlinie zu überschreiben.

### Vorgehensweise

1 Starten Sie den Horizon FLEX-Verwaltungskonsole.

a Geben Sie in einem Webbrowser **`https://WebManagerServer:7443/rvm`** ein, wobei *WebManagerServer* für den DNS-Namen oder die IP-Adresse des Hosts steht, auf dem Mirage Web Manager installiert ist.

b Geben Sie den Benutzernamen und das Kennwort eines Domänenkontos ein, das einen Zugriff auf Mirage besitzt.

c Klicken Sie auf **Anmelden**.

2 Klicken Sie auf **Richtlinien** im linken Navigationsbereich.

3 Klicken Sie auf die Registerkarte **Gerätekontrolle**, um eine neue Geräterichtlinie hinzuzufügen.

4 Wählen Sie das Dropdown-Menü **Globale Verwendung von USB-Geräten** aus, um festzulegen, ob die Richtlinie die Verwendung aller USB-Geräte auf der virtuellen Maschine zulassen oder sperren soll.

   Alle USB-Geräteklassen werden abgeblendet dargestellt und können nicht geändert werden. Unter „Konfigurieren einer benutzerdefinierten USB-Geräterichtlinie für ein Horizon FLEX-Image“, auf Seite 47 finden Sie Erläuterungen zum Erstellen einer benutzerdefinierten Richtlinie, mit der bestimmte USB-Geräteklassen zugelassen werden.

5 Klicken Sie auf **OK**, um die Richtlinie zu speichern.

   Die neue oder aktualisierte Richtlinie erscheint in der Richtlinienliste.

### Weiter

Erteilen Sie eine Berechtigung für die virtuelle Horizon FLEX-Maschine. Weitere Informationen hierzu finden Sie unter „Erteilen einer Berechtigung für ein Horizon FLEX-Image“, auf Seite 49.

## Konfigurieren einer benutzerdefinierten USB-Geräterichtlinie für ein Horizon FLEX -Image

Sie haben die Möglichkeit, benutzerdefinierte Geräterichtlinien zu konfigurieren, mit denen festgelegt wird, ob bestimmte USB-Gerätetypen auf virtuellen Maschinen verwendet werden können, die von einem Horizon FLEX-Image erstellt wurden.

---

**Wichtig** Wenn der USB-Gerätecontroller in der virtuellen Maschine der Quelle vorhanden ist, können Sie durch die entsprechende Konfiguration einer Richtlinie sicherstellen, dass sich diese Funktion beim Herunterladen einer Instanz der virtuellen Maschine durch Benutzer aktivieren oder deaktivieren lässt. Ist diese Funktion in der virtuellen Maschine der Quelle deaktiviert, ist es nicht möglich, die Einstellungen für die virtuelle Maschine durch Aktivieren dieser Funktion in einer Richtlinie zu überschreiben.

---

### Vorgehensweise

1 Starten Sie den Horizon FLEX-Verwaltungskonsole.

   a Geben Sie in einem Webbrowser **`https://WebManagerServer:7443/rvm`** ein, wobei *WebManagerServer* für den DNS-Namen oder die IP-Adresse des Hosts steht, auf dem Mirage Web Manager installiert ist.

   b Geben Sie den Benutzernamen und das Kennwort eines Domänenkontos ein, das einen Zugriff auf Mirage besitzt.

   c Klicken Sie auf **Anmelden**.

2 Klicken Sie auf **Richtlinien** im linken Navigationsbereich.

3 Klicken Sie auf die Registerkarte **Gerätekontrolle**, um eine neue Geräterichtlinie hinzuzufügen.

4 Wählen Sie im Dropdown-Menü **Globale Verwendung von USB-Geräten** die Option **Benutzerdefiniert**, um festzulegen, ob bestimmte Klassen von USB-Geräten für die virtuelle Maschine zugelassen oder gesperrt werden sollen.

   Es werden die Textfelder für die USB-Geräteklassen angezeigt, mit denen Sie bestimmte Klassen zulassen oder sperren können.

5 Wählen Sie die USB-Klassen aus, die für die virtuelle Maschine zugelassen oder gesperrt werden sollen.

**Tabelle 4-1.** USB-Gerätetypen

| USB-Klasse | Basisklasse | Beispiele |
|---|---|---|
| Audio | 01h | USB-Soundkarte |
| Kommunikations- und CDC-Gerät | 02h | USB-Netzwerkadapter, serielle RS-232-Geräte |
| Physisch | 05h | Joystick |
| Bild | 06h | USB-Kamera, -Scanner, -Webcam |
| Drucker | 07h | USB-Drucker |
| Massenspeicher | 08h | USB-Festplatte |
| Smartcard | 0Bh | USB-Smartcard-Leser |
| Inhaltsicherheit | 0Dh | Fingerabdruckleser |
| Video | 0Eh | Webcam |
| Drahtlos-Controller | E0h | Bluetooth-Adapter, Microsoft RNDIS |
| Sonstiges | EFh | Mit der Option **Sonstiges** können Sie USB-Geräte zulassen oder sperren, die nicht unter die vorherigen Klassen fallen. Unter Tabelle 4-2 finden Sie die USB-Klassen, für die eine Einstellung unter **Sonstiges** erforderlich ist. |

**Tabelle 4-2.** Sonstige USB-Geräteklassen

| USB-Klasse | Basisklasse | Beispiele |
|---|---|---|
| Eingabegeräte (HID, Human Interface Devices) | 03h | USB-Tastatur, -Joystick, -Maus |
| Hub | 09h | USB-Hub |
| Persönliche Gesundheitsvorsorge | 0Fh | Pulsuhr |
| Diagnosegerät | DCh | USB-Gerät zum Kompatibilitätstest |
| Anwendungsspezifisch | FEh | IrDA-Brücke, Test- und Messklasse (USBTMC, Test and Measurement Class ), USB-Geräte-Firmware-Upgrade (DFU, Device Firmware Upgrade) |

6 Optional können Sie die Geräterichtlinie für die Zulassung bestimmter USB-Gerätetypen konfigurieren.

a Unter dem Textfeld **Virtuelle Maschine für die Verwendung folgender USB-Geräte zulassen** klicken Sie auf **Hinzufügen**.

b Geben Sie in das Textfeld **Name** den Namen des USB-Geräts ein.

c Geben Sie in das Textfeld **Anbieter-ID** die Anbieter-ID als Hexadezimalwert ein.

d Geben Sie in das Textfeld **Produkt-ID** die Produkt-ID als Hexadezimalwert ein.

e Klicken Sie auf **Hinzufügen** und dann auf **Aktualisieren**.

Um die USB-Geräteinformationen auf einem Windows-Computer verwenden zu können, klicken Sie auf **Systemprogramme** und wählen dann **Geräte-Manager** aus. Um die USB-Geräteinformationen auf einem Mac verwenden zu können, klicken Sie auf das **Apple**-Symbol, wählen **Über den Mac** aus, dann **Systembericht** sowie **USB** und klicken auf den Geräteeintrag.

7 Klicken Sie auf **OK**, um die Richtlinie zu speichern.

Die neue oder aktualisierte Richtlinie erscheint in der Richtlinienliste.

### Weiter

Erteilen Sie eine Berechtigung für die virtuelle Horizon FLEX-Maschine. Weitere Informationen hierzu finden Sie unter „Erteilen einer Berechtigung für ein Horizon FLEX-Image“, auf Seite 49.

## Aktualisieren einer Richtlinie für ein bereitgestelltes Horizon FLEX-Image

Nach der Bereitstellung eines Horizon FLEX-Image für Benutzer können Sie die Richtlinien für vorhandene Instanzen virtueller Maschinen aktualisieren.

**Wichtig** Wenn Sie eine vorhandene Richtlinie mithilfe der Schaltfläche **Richtlinien** im linken Navigationsbereich bearbeiten, gelten die Änderungen nur für neue Benutzer. Die bearbeitete Richtlinie gilt nicht für vorhandene Benutzer mit bereitgestellten Instanzen virtueller Maschinen. Wenn Sie beispielsweise in einem Szenario, in dem die ursprüngliche Richtlinie den Benutzer nicht daran hindert, mehrere Kopien der virtuellen Maschine zu erstellen, die Richtlinie bearbeiten, um diese Einschränkung hinzuzufügen, gilt sie nicht für vorhandene virtuelle Maschinen. Wenn ein Benutzer über eine virtuelle Maschine verfügt, die durch die ursprüngliche Richtlinie abgedeckt ist, kann der Benutzer weiterhin Kopien dieser virtuellen Maschine erstellen. Wenn dieser Benutzer eine zweite virtuelle Maschine herunterlädt, die durch die bearbeitete Richtlinie abgedeckt wird, kann der Benutzer diese zweite virtuelle Maschine nicht kopieren.

### Vorgehensweise

1 Starten Sie den Horizon FLEX-Verwaltungskonsole.

   a Geben Sie in einem Webbrowser **`https://WebManagerServer:7443/rvm`** ein, wobei *WebManagerServer* für den DNS-Namen oder die IP-Adresse des Hosts steht, auf dem Mirage Web Manager installiert ist.

   b Geben Sie den Benutzernamen und das Kennwort eines Domänenkontos ein, das einen Zugriff auf Mirage besitzt.

   c Klicken Sie auf **Anmelden**.

2 Klicken Sie auf **Virtuelle Maschinen** im linken Navigationsbereich.

3 Wählen Sie die betreffende virtuelle Maschine aus.

4 Klicken Sie auf **Bearbeiten**.

5 Aktualisieren Sie die Richtlinie für die virtuelle Maschine und klicken Sie am Ende auf **OK**.

### Weiter

Weitere Informationen finden Sie unter „Konfigurieren einer allgemeinen Richtlinie für ein Horizon FLEX-Image“, auf Seite 44 und „Konfigurieren einer USB-Geräterichtlinie für ein Horizon FLEX-Image“, auf Seite 46.

## Erteilen einer Berechtigung für ein Horizon FLEX -Image

Mithilfe von Berechtigungen können Sie bestimmten Benutzern und Gruppen das Herunterladen und Verwenden von Instanzen einer virtuellen Maschine von einem bestimmten Horizon FLEX-Image erlauben.

Benutzer können jede virtuelle Horizon FLEX-Maschine herunterladen, für die Sie eine Berechtigung erhalten haben. Bevor sich Benutzer registrieren und eine virtuelle Horizon FLEX-Maschine zum ersten Mal verwenden können, müssen sie ihre Active Directory-Anmeldeinformationen eingeben. Benutzer können sich am Horizon FLEX Server anmelden und die virtuelle Maschine herunterladen. Alternativ können sie die virtuelle Horizon FLEX-Maschine von einem USB-Gerät kopieren und die Anmeldeinformationen für Active Directory beim ersten Start der virtuellen Maschine eingeben.

### Voraussetzungen

- Stellen Sie sicher, dass die betreffenden Active Directory-Benutzer und -Gruppen in der Horizon FLEX-Datenbank synchronisiert wurden. Weitere Informationen hierzu finden Sie unter „Konfigurieren von Active Directory-Einstellungen“, auf Seite 19.
- Registrieren Sie die virtuelle Maschine der Quelle mit Horizon FLEX-Richtlinienserver. Weitere Informationen hierzu finden Sie unter „Registrieren einer virtuellen Maschine der Quelle mit Horizon FLEX-Richtlinienserver“, auf Seite 42.
- Konfigurieren Sie eine Richtlinie für ein Horizon FLEX-Image. Weitere Informationen hierzu finden Sie unter „Konfigurieren einer allgemeinen Richtlinie für ein Horizon FLEX-Image“, auf Seite 44.

### Vorgehensweise

1 Starten Sie den Horizon FLEX-Verwaltungskonsole.

   a Geben Sie in einem Webbrowser **`https://WebManagerServer:7443/rvm`** ein, wobei *WebManagerServer* für den DNS-Namen oder die IP-Adresse des Hosts steht, auf dem Mirage Web Manager installiert ist.

   b Geben Sie den Benutzernamen und das Kennwort eines Domänenkontos ein, das einen Zugriff auf Mirage besitzt.

   c Klicken Sie auf **Anmelden**.

2 Klicken Sie auf **Berechtigungen** im linken Bereich.

3 Klicken Sie auf die Schaltfläche **Neu** (+), um eine Berechtigung zu erstellen, oder wählen Sie eine vorhandene Berechtigung aus und klicken Sie auf **Bearbeiten**, um diese zu ändern, oder wählen Sie eine vorhandene Berechtigung aus und klicken Sie auf **Duplizieren**, um diese zu duplizieren.

4 Erstellen Sie den Berechtigungsnamen und weisen Sie ihn einem Horizon FLEX-Image zu.

   a Geben Sie in das Textfeld **Berechtigungsname** einen Namen für die Berechtigung ein.

   b Wählen Sie ein Horizon FLEX-Image aus, das der Berechtigung hinzugefügt werden soll.

   Mit dem Suchfeld können Sie die Liste der Horizon FLEX-Images filtern.

   Wenn Sie eine vorhandene Berechtigung dupliziert haben, müssen Sie die zweite Berechtigung vor dem Speichern umbenennen.

   Wenn Sie das Horizon FLEX-Image auswählen, wird die Download-URL für das Image automatisch in das Textfeld **Download-URL** eingetragen.

   c Ändern Sie im Textfeld **Download-URL** die URL, über die der Client das Horizon FLEX-Image herunterlädt.

   d Klicken Sie auf **Weiter**.

5 Wählen Sie die Active Directory-Benutzer und -Gruppen, denen die Berechtigung erteilt werden soll.

   a Wählen Sie mit dem Suchfeld die Benutzer und Gruppen aus, die der Berechtigung hinzugefügt werden sollen.

   Bei neuen Active Directory-Benutzern und -Gruppen kann es bis zu 15 Minuten dauern, bis diese in den Suchergebnissen erscheinen.

   b Klicken Sie auf **Hinzufügen**, um einen Benutzer oder eine Gruppe der Liste der berechtigten Mitglieder hinzuzufügen.

   Mit den Schaltflächen **Entfernen** und **Alle löschen** können Sie die Mitgliederliste verwalten.

   c Klicken Sie auf **Weiter**.

6 Wählen Sie eine Richtlinie für die Berechtigung aus und klicken Sie auf **Weiter**.

Mit dem Suchfeld haben Sie die Möglichkeit, die Richtlinienliste zu filtern. Die Schaltflächen **Filter löschen** und **Filter anzeigen** dienen der Verwaltung der Suchvorgänge.

7 (Optional) Um ein Benennungsmuster einer virtuellen Maschine zu verwenden, aktivieren Sie **Konfiguration des Maschinennamens verwenden** und konfigurieren das Benennungsmuster.

a Geben Sie das gewünschte Benennungsmuster in das Textfeld **Maschinennamensmuster** ein.

Um sicherzustellen, dass jede virtuelle Maschine einen anderen Namen erhält, damit sie der Domäne beitreten kann, verwenden Sie den Platzhalter {*username*}. Dieser Platzhalter wird beim Herunterladen der virtuellen Maschine durch den jeweiligen Benutzernamen ersetzt. Sie können auch ein Muster für laufende Nummern erstellen, indem Sie mit dem Platzhalter {*n*} aufsteigende Nummern virtueller Maschinen mit Benutzernamen erzeugen.

Weitere Informationen finden Sie im Abschnitt „Erstellen eines Benennungsmusters für virtuelle Maschinen“, auf Seite 52.

b Wählen Sie einen Domänennamen aus dem Dropdownmenü **Domänenname**.

c Geben Sie in das Textfeld **Organisationseinheit** eine Organisationseinheit (Organizational Unit, OU) ein.

Beispiel: `OU=hr1, OU=hr, OU=flex, DC=ws, DC=test, DC=com`

8 (Optional) Wenn Sie Mirage Client in der virtuellen Maschine installiert haben, geben Sie an, ob Sie die virtuelle Maschine mit Mirage verwalten möchten.

| Option | Beschreibung |
|---|---|
| **VMware Mirage für die Notfallwiederherstellung und für die Image-Verwaltung verwenden** | Mit dieser Option wählen Sie eine CVD-Richtlinie, einen Basis-Layer, einen Anwendungs-Layer und andere Konfigurationen aus.<br>Der Mirage-Server erstellt automatisch eine CVD für vom Endbenutzer heruntergeladene virtuelle Maschinen. Mirage synchronisiert periodisch die Endbenutzerdaten mit dem Datencenter auf der Basis der gewählten Mirage-Richtlinie. In Mirage Management Console können Sie mit diesen Daten die CVD wiederherstellen oder auf Dateien der virtuellen Maschine mithilfe des Mirage-Dateiportals zugreifen. Darüber hinaus stellt der Mirage-Server automatisch Basis- und Anwendungs-Layer für die virtuelle Maschine bereit, nachdem diese für die Image-Kompatibilität und die Lieferung der Remoteanwendung bereitgestellt wurde. |
| **VMware Mirage für die Notfallwiederherstellung verwenden** | Wählen Sie diese Option zur Auswahl einer CVD-Richtlinie. Der Mirage-Server erstellt eine CVD für vom Endbenutzer heruntergeladene virtuelle Maschinen. Mit diesen Daten können Sie die CVD wiederherstellen oder auf Dateien der virtuellen Maschine mithilfe des Mirage-Dateiportals in Mirage Management Console zugreifen. |
| **VMware Mirage nicht für die Verwaltung der virtuellen Maschinen verwenden** | Wählen Sie diese Option, um die Verwaltung der virtuellen Maschine mit Mirage auszuschließen. |

Wenn Sie eine virtuelle Maschine löschen, in der der Mirage-Client installiert ist, archiviert der Mirage-Server die CVD der gelöschten virtuellen Maschine.

9 Klicken Sie auf **Weiter** und überprüfen Sie die Einstellungen der Berechtigung.

10 Klicken Sie auf **Fertig stellen**, um die Berechtigung zu speichern, oder auf **Zurück**, um zur vorherigen Seite zurückzukehren und die Berechtigung zu bearbeiten.

## Erstellen eines Benennungsmusters für virtuelle Maschinen

Beim Erteilen von Berechtigungen für ein Horizon FLEX-Image können Sie ein Benennungsmuster für virtuelle Maschinen erstellen. Wenn virtuelle Maschinen für dieselbe Benutzerberechtigung erstellt werden, gibt Horizon FLEX ihnen nun eindeutige Namen.

Das Benennungsmuster für virtuelle Maschinen muss den Parameter {*username*} oder {*n*} enthalten. Der Parameter {*n*} ermöglicht die Erstellung eines Musters für laufende Nummern, damit zu den Namen virtueller Maschinen aufsteigende Nummern hinzugefügt werden. Die folgenden Muster sind gültig:

- VM-{*username*}
- VM-{*n*}

Die folgenden Muster sind nicht gültig:

- VM-(*username*}-{*username*}
- VM-{*username*}-{*n*}
- VM-{*n*}-{*n*}

Der Maschinenname ist auf 15 Zeichen begrenzt. Wenn der Maschinenname länger als 15 Zeichen ist, werden nur die ersten 15 Zeichen verwendet. Wenn das Muster beispielsweise „VM-1234567890-*username*“ lautet und der Benutzer „Jack“ heißt, wird der Name der virtuellen Maschine zu „VM-1234567890-J“ gekürzt.

Um sicherzustellen, dass jede virtuelle Maschine einen anderen Namen erhält, damit sie der Domäne beitreten kann, verwenden Sie den Platzhalter {*username*} oder {*n*} Der Platzhalter {*username*} wird beim Herunterladen der virtuellen Maschine durch den jeweiligen Benutzernamen ersetzt. Für {*n*} wird Active Directory nach Computern mit Namen durchsucht, die dem Muster entsprechen. Wenn kein Name dem Muster entspricht, lautet der Wert der laufenden Nummer 1. Andernfalls ist der Wert für die nächste laufende Nummer der Nachfolger der größten Nummer in allen Namen, die dem Muster entsprechen.

Beispielsweise wurden die Berechtigungen für eine virtuelle Maschine dem Benutzer „user1“ erteilt, und das Benennungsmuster für virtuelle Maschinen ist als „VM-*username- n*“ festgelegt. Wenn „user1“ die virtuelle Maschine herunterlädt, wird Active Directory durchsucht, um zu ermitteln, ob ein VM-Name dem Benennungsmuster entspricht, etwa „VM-user1-*x*“, wobei *x* die zugewiesene Nummer ist. Wenn die höchste bisher zugewiesene Nummer 25 lautet, der Name der entsprechenden virtuellen Maschine also „VM-user1-25“ ist, wird der Name dieser VM als „VM-user1-26“ festgelegt. Wenn keine vorhandene VM dem Muster entspricht, nennt Horizon FLEX diese virtuelle Maschine „VM-user1-1“.

Sie können einem Benutzer Berechtigungen für mehr als eine virtuelle Maschine erteilen. Beispielsweise können Sie „user1“ Berechtigungen für drei virtuelle Maschinen erteilen. Wenn „user1“ die virtuellen Maschinen herunterlädt, wird ihr Name zu „vm-*x*-user1“ geändert. Die zugewiesene Nummer für die virtuelle Maschine wird nicht für jeden einzelnen Benutzernamen hochgezählt, sondern basiert darauf, wann die virtuelle Maschine registriert wurde.

Beispielsweise kann „user1“ über drei virtuelle Maschinen mit den Namen „vm-10-user1“, „vm-26-user1“ und „vm-39-user1“ verfügen, abhängig davon, für welche anderen virtuellen Maschinen anderen Benutzern Berechtigungen erteilt wurden und wann „user1“ die einzelnen virtuellen Maschinen heruntergeladen hat. Die aufsteigende Nummer wird nur zur Nachverfolgung durch denHorizon FLEX-Administrator verwendet. Der Client-Benutzer sieht die aufsteigende Nummer nicht.

# Erstellen eines URI zur Bereitstellung einer virtuellen Horizon FLEX -Maschine

Sie haben die Möglichkeit, eine virtuelle Horizon FLEX-Maschine durch Erstellen eines URI (Uniform Resource Identifier) bereitzustellen. Mithilfe eines URI lässt sich eine E-Mail mit einem Link anlegen, mit dem der Endbenutzer eine Verbindung zu einem Server herstellen und eine virtuelle Horizon FLEX-Maschine herunterladen kann.

### Voraussetzungen

- Stellen Sie sicher, dass der Horizon FLEX Client auf dem Endbenutzersystem installiert ist.
- Übergeben Sie dem Endbenutzer ein Kennwort für den Server und das Verschlüsselungskennwort für die virtuelle Maschine.

### Vorgehensweise

1 Erstellen Sie einen URI für den Endbenutzer.

Ein URI verfügt über folgende Struktur:

`vmware-rvm://Benutzername@myserver.com:7443`

*Benutzername* ist der Anmeldename des Benutzers und *myserver.com* der Hostname des Servers. Die Serveradresse muss `vmware-rvm://` sowie `:7443` enthalten. Stellen Sie der Serveradresse nicht http oder https voran.

2 Geben Sie den Link-Text in eine E-Mail ein und dann die Hyperlink-Information für den URI.

Der Link kann mit jedem E-Mail-System versendet werden. Da allerdings das URI-Format nicht als eine Standard-URL erkannt wird, müssen Sie die Hyperlink-Informationen manuell eingeben.

3 Erstellen Sie eine E-Mail für den Benutzer und geben Sie den gewünschten Link-Text ein.

Beispiel: **`Ihre virtuelle Horizon FLEX-Maschine`**

4 Wählen Sie den Link-Text, klicken Sie mit der rechten Maustaste auf den ausgewählten Text und wählen Sie **Hyperlink** aus dem eingeblendeten Kontextmenü.

5 Wählen Sie **Verknüpfen mit: Vorhandene Datei oder Webseite**.

6 Geben Sie in das Textfeld **Adresse** den URI ein.

Beispiel: **`vmware-rvm://johndoe@yourserver.com:7443`**

Der Link ist damit aktiv.

7 Klicken Sie auf **OK**.

8 Senden Sie die E-Mail an den Benutzer.

Klickt der Benutzer den Link in der E-Mail an, startet der Horizon FLEX-Client des Benutzers und das Dialogfeld zur Herstellung der Verbindung mit dem Server wird geöffnet. Die Textfelder „Server“ und „Benutzername“ sind bereits mit den Werten ausgefüllt, die in der URL angegeben sind. Der Benutzer muss dann ein Kennwort eingeben, um eine Verbindung mit dem Server herzustellen und eine virtuelle Maschine herunterzuladen.

# Verwalten virtueller Horizon FLEX - Maschinen 5

Sie können für bereitgestellte virtuelle Horizon FLEX-Maschinen verschiedene Vorgänge zur Verwaltung durchführen: Bearbeiten, Sperren, Reaktivieren, Löschen und Archivieren.

## Verwalten virtueller Horizon FLEX -Maschinen

Nach der Bereitstellung virtueller Horizon FLEX-Maschinen können Sie für diese verschiedene Verwaltungsvorgänge durchführen. Sie können den Bestand an virtuellen Horizon FLEX-Maschinen in Horizon FLEX-Verwaltungskonsole anzeigen lassen.

Mithilfe des Textfeldes **Suchen** können Sie die Liste virtueller Maschinen und die sortierbaren Spaltentitel filtern, um eine spezifische virtuelle Maschine zu ermitteln. Mit dem Dropdown-Menü der Spaltentitel haben Sie die Möglichkeit, die Spalten für die Anzeige auszuwählen.

Bei der Auswahl einer virtuellen Maschine aus der Liste lässt sich das Fenster Eigenschaften unten auf der Seite erweitern, um die allgemeinen Einstellungen der virtuellen Maschine und der für sie geltenden Richtlinien anzuzeigen.

### Vorgehensweise

1 Starten Sie den Horizon FLEX-Verwaltungskonsole.

   a Geben Sie in einem Webbrowser **`https://WebManagerServer:7443/rvm`** ein, wobei *WebManagerServer* für den DNS-Namen oder die IP-Adresse des Hosts steht, auf dem Mirage Web Manager installiert ist.

   b Geben Sie den Benutzernamen und das Kennwort eines Domänenkontos ein, das einen Zugriff auf Mirage besitzt.

   c Klicken Sie auf **Anmelden**.

2 Klicken Sie auf **Virtuelle Maschinen** im linken Navigationsbereich.

   Der Bestand an bereitgestellten virtuellen Horizon FLEX-Maschinen erscheint auf der Seite der virtuellen Maschinen.

3 Um eine bestimmte virtuelle Maschine zu verwalten, wählen Sie diese in der Liste.

| Option | Aktion |
|---|---|
| **Bearbeiten** | Wählen Sie eine virtuelle Maschine und klicken Sie auf **Bearbeiten**, um die dieser virtuelle Maschine zugeordneten Richtlinien zu ändern. |
| **Sperren** | Wählen Sie eine virtuelle Maschine und klicken Sie auf **Sperren**, um den Benutzerzugriff auf diese virtuelle Maschine rückgängig zu machen. |
| **Reaktivieren** | Wählen Sie eine abgelaufene oder gesperrte virtuelle Maschine und klicken Sie auf **Reaktivieren**, um diese virtuelle Maschine wieder in die Ausgangsstellung zu bringen. |

| Option | Aktion |
|---|---|
| **Löschen** | Wählen Sie eine virtuelle Maschine aus und klicken Sie auf **Löschen**, um diese aus dem Dateisystem zu entfernen. |
| **Archiv** | Wählen Sie eine virtuelle Maschine und klicken Sie auf **Archivieren**, um diese virtuelle Maschine für die Anwendung zu deaktivieren und offline zu speichern.<br>Wählen Sie das Feld **Archivierte Instanzen anzeigen** unten auf der Seite der virtuellen Maschinen aus, um die bereits archivierten virtuellen Maschinen darzustellen. Durch Klicken auf **Reaktivieren** wird eine archivierte virtuelle Maschine wieder aktiviert. |
| **Löschen** | Wählen Sie eine archivierte virtuelle Maschine und klicken Sie auf **Löschen**. Es können nur virtuelle Maschinen mit dem Status „Archiviert“ gelöscht werden. |

4 Die möglichen Aktionen für eine virtuelle Maschine sind von ihrem Status in der Spalten „Status“ abhängig.

| Status | Beschreibung |
|---|---|
| **Aktiv** | Die virtuelle Maschine wird benutzt, hat Kontakt zum Server und ist nicht abgelaufen. |
| **Inaktiv** | Horizon FLEX-Client, mit dem der Benutzer die virtuelle Maschine geöffnet hat, hat länger keinen Kontakt mit dem Server, als es der in der Offline-Arbeitsrichtlinie festgelegt Zeitraum zulässt. |
| **Abgelaufen** | Das Ablaufdatum wurde erreicht und die virtuelle Maschine wurde deaktiviert. |
| **Ausstehender Ablauf** | Der Server wartet auf eine Bestätigung von Horizon FLEX-Client, dass die virtuelle Maschine abgelaufen ist. |
| **Gesperrt** | Ein Administrator hat den Benutzer der virtuellen Maschine gesperrt. |
| **Ausstehende Sperrung** | Es wurde eine Sperrung ausgelöst. Der Status verbleibt bei „Ausstehend“, bis Horizon FLEX-Client überprüft hat, dass die virtuelle Maschine gesperrt ist. |
| **Ausstehende Reaktivierung** | Der Server wartet auf eine Bestätigung von Horizon FLEX-Client, dass die virtuelle Maschine reaktiviert ist. |
| **Wird heruntergeladen** | Der Benutzer lädt die virtuelle Maschine herunter. |
| **Download abgebrochen** | Der Benutzer hat das Herunterladen abgebrochen. |
| **Download angehalten** | Der Benutzer hat das Herunterladen angehalten. |
| **Beitritt zur Domäne fehlgeschlagen** | Die virtuelle Maschine konnte nicht einer Domäne beitreten. Der häufigste Grund für das Scheitern des Beitritts einer virtuellen Maschine zu einer Domäne ist, dass das Objekt bereits im Active Directory vorhanden ist. In diesem Fall überprüfen Sie das Offline-Protokoll des Domänenbeitritts, das vom Betriebssystem verwaltet wird, um festzustellen, wie der Fehler gelöst werden kann. |
| **Benutzer gelöscht** | Der Benutzer hat die VM auf dem Client gelöscht. |
| **Gelöscht** | Die virtuelle Maschine wurde durch den Administrator gelöscht und aus dem Benutzersystem entfernt. |
| **Ausstehendes Löschen** | Der Server wartet auf die Bestätigung von Horizon FLEX-Client, dass die virtuelle Maschine aus dem Benutzersystem entfernt wurde. |
| **Archiviert** | Die virtuelle Maschine wurde archiviert.<br>**Hinweis** Sie müssen das Kontrollfeld **Archivierte Instanzen anzeigen** aktivieren, um archivierte, virtuelle Maschinen anzuzeigen. |

# Warten des Horizon FLEX-Systems 6

Sie können Wartungsvorgänge auf dem Horizon FLEX-System durchführen, inklusive eines Upgrades von vorherigen Horizon FLEX-Versionen.

Dieses Kapitel behandelt die folgenden Themen:



## Upgrade älterer Horizon FLEX-Versionen

Sie können für das Horizon FLEX-System ein Upgrade älterer Horizon FLEX-Versionen vornehmen.

### Voraussetzungen

- Alle Mirage-Server werden heruntergefahren
- Alle bereitgestellten virtuellen Horizon FLEX-Maschinen werden heruntergefahren.

### Vorgehensweise

1 Laden Sie die Installationsdateien von Horizon FLEX Server und Horizon FLEX Client für die Upgrade-Version herunter.

2 Führen Sie das Upgrade für die Horizon FLEX Server-Komponente durch.

   a So führen Sie das Upgrade für den Mirage Management Server durch. Doppelklicken Sie auf die Datei „mirage.management.server.64x.*buildnumber*.msi“ im Serverordner.

      Standardmäßig werden die von Ihnen bei der Erstinstallation ausgewählten Konfigurationseinstellungen angewendet. Sie können die Konfigurationseinstellungen während des Upgrades ändern.

   b Für das Upgrade des Mirage-Servers doppelklicken Sie auf die Datei „mirage.server.64x*buildnumber*.msi“.

      Standardmäßig werden die von Ihnen bei der Erstinstallation ausgewählten Konfigurationseinstellungen angewendet. Sie können die Konfigurationseinstellungen während des Upgrades ändern.

   c Für das Upgrade von Mirage Web Manager (Web Management Console) doppelklicken Sie auf die Datei „mirage.WebManagement.console.x64.*buildnumber*.msi“ im Ordner „WebManagement“.

      Setzen Sie den Vorgang ohne Änderungen fort.

   d Wenn Sie Mirage für die Verwaltung Ihrer virtuellen Windows-Maschinen verwenden, befolgen Sie die Anweisungen für das Upgrade von der früheren Mirage-Version im *VMware Mirage-Administratorhandbuch*.

3 Führen Sie das Upgrade für alle Horizon FLEX Clients auf die Version durch, die mit Horizon FLEX Server nach durchgeführtem Upgrade kompatibel ist.

- Stellen Sie Ihren Endbenutzern die Installationsdatei für die Upgrade-Version von Fusion Pro oder Workstation Player zur Verfügung oder zeigen Sie ihnen, wie sich die Software von der VMware-Website herunterladen lässt.
- Führen Sie das Upgrade für alle Horizon FLEX Clients mithilfe einer Massenbereitstellung durch.

**Weiter**

Die vollständigen Anleitungen zum Mirage-Upgrade erhalten Sie in der VMware-Mirage-Dokumentation unter https://www.vmware.com/support/pubs/mirage_pubs.html.

---

**HINWEIS** Verwenden Sie nicht die Option **Neue Speicherbereiche erstellen**, wenn Sie ein Upgrade des Mirage Management Servers durchführen. Wenn Sie diese Option auswählen und den Pfad zum ursprünglichen Speicherbereich eingeben, wird Ihre gesamte Mirage-Installation einschließlich Basis-Layer, Anwendungs-Layer, CVD-Daten usw. gelöscht und kann nicht wiederhergestellt werden, wenn keine Datensicherung verfügbar ist.

---

Unter „Installieren des Horizon FLEX Client für Endbenutzer“, auf Seite 20 erhalten Sie Informationen zur Verwendung einer Massenbereitstellung von Horizon FLEX Client für Endbenutzer.

# Horizon FLEX -Systemprotokolle

Horizon FLEX-Protokolldateien können zum Lösen von Systemproblemen verwendet werden.

Horizon FLEX-Systemprotokolle sind an den folgenden Speicherorten verfügbar:

- Web App-Protokolldatei

  `C:\ProgramData\Wanova Mirage\rvm\logs\webapp.log`

- Horizon FLEX-Serverprotokolle

  `C:\Programme\Wanova\Mirage Management Server\logs`

  Die wichtigste Protokolldatei ist die Datei `mgmtservice.log`.

- Horizon FLEX verwendet die Microsoft-Funktion für den Offline-Domänenbeitritt. Die Protokolldatei für Offline-Domänenbeitritte befindet sich unter:

  `C:\Windows\debug\NetSetup.LOG`

# Index

## R



## S



## T



## U



## V



## W



## Z