# Platform Services Controller-Verwaltung

Update 2
Geändert am 2. Mai 2022
VMware vSphere 6.7
VMware ESXi 6.7
vCenter Server 6.7

vmware®

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

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

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

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

# Inhalt

# Informationen zu *Platform Services Controller-Verwaltung*

In der Dokumentation zur *Platform Services Controller-Verwaltung* wird erläutert, wie sich der VMware® Platform Services Controller™ in Ihre vSphere-Umgebung einfügt. Außerdem erhalten Sie Unterstützung bei der Durchführung allgemeiner Aufgaben wie der Zertifikatsverwaltung und der Konfiguration von vCenter Single Sign On.

In *Platform Services Controller-Verwaltung* wird erläutert, wie Sie die Authentifizierung mit vCenter Single Sign-On einrichten und Zertifikate für vCenter Server und zugehörige Dienste verwalten können.

Tabelle 1-1. *Platform Services Controller-Verwaltung* – Schwerpunkte

| Themen | Inhaltliche Schwerpunkte |
|---|---|
| Erste Schritte mit Platform Services Controller | ■ vCenter Server- und Platform Services Controller-Bereitstellungsmodellen. HINWEIS: Diese Informationen ändern sich mit jeder Version des Produkts.<br>■ Platform Services Controller-Dienste unter Linux und Windows.<br>■ Verwalten von Platform Services Controller-Diensten.<br>■ Verwalten der Platform Services Controller-Appliance mithilfe von VAMI. |
| vSphere-Authentifizierung mit vCenter Single Sign-On | ■ Architektur des Authentifizierungsprozesses.<br>■ Informationen zum Hinzufügen von Identitätsquellen, sodass sich Benutzer in Ihrer Domäne authentifizieren können.<br>■ Zwei-Faktor-Authentifizierung.<br>■ Verwalten von Benutzern, Gruppen und Richtlinien. |
| vSphere-Sicherheitszertifikate | ■ Zertifikatmodell und Optionen für das Ersetzen von Zertifikaten.<br>■ Ersetzen von Zertifikaten über die Benutzeroberfläche (einfache Fälle).<br>■ Ersetzen von Zertifikaten mit dem Dienstprogramm Certificate Manager.<br>■ Ersetzen von Zertifikaten mithilfe der CLI (komplexe Situationen).<br>■ Referenz zur Zertifikatsverwaltungs-CLI. |

# Verwandte Dokumentation

Im Begleitdokument *vSphere-Sicherheit* werden die verfügbaren Sicherheitsfunktionen sowie die Maßnahmen beschrieben, die Sie zum Schutz Ihrer Umgebung vor Angriffen ergreifen können. In diesem Dokument wird außerdem erläutert, wie Sie Berechtigungen festlegen können, und es enthält einen Verweis auf Berechtigungen.

Zusätzlich zu diesen Dokumenten veröffentlicht VMware das Handbuch *vSphere Security Configuration Guide* (Handbuch für die vSphere-Sicherheitskonfiguration – früher bekannt als *Handbuch für Hardening*) für jede Version von vSphere. Die Handbücher stehen unter http://www.vmware.com/security/hardening-guides.html zur Verfügung. Das Handbuch *vSphere Security Configuration Guide* enthält Leitlinien zu Sicherheitseinstellungen, die vom Kunden festgelegt werden können bzw. sollten, und zu von VMware bereitgestellten Sicherheitseinstellungen, für die der Kunde prüfen sollte, ob sie noch auf die jeweiligen Standardwerte festgelegt sind.

# Zielgruppe

Diese Informationen richten sich an Administratoren, die den Platform Services Controller und zugehörige Dienste konfigurieren möchten. Die Informationen sind für erfahrene Systemadministratoren bestimmt, die mit der Windows- oder Linux-VM-Technologie und Datencenteroperationen vertraut sind.

# vSphere Client und vSphere Web Client

Die Anweisungen in diesem Handbuch beziehen sich auf den vSphere Client (eine HTML5-basierte Benutzeroberfläche). Sie können die Anweisungen auch nutzen, um die Aufgaben mithilfe des vSphere Web Client (einer Flex-basierten Benutzeroberfläche) durchzuführen.

Für Aufgaben, bei denen sich der Workflow zwischen dem vSphere Client und dem vSphere Web Client erheblich unterscheidet, sind doppelte Prozeduren vorhanden. Die Schritte der einzelnen Prozeduren beziehen sich auf die jeweilige Client-Benutzeroberfläche. Im Titel der Prozeduren, die sich auf den vSphere Web Client beziehen, ist vSphere Web Client angegeben.

**Hinweis** In vSphere 6.7 Update 1 sind fast alle Funktionen des vSphere Web Client im vSphere Client implementiert. Eine aktuelle Liste aller nicht unterstützten Funktionen finden Sie im Handbuch für Funktions-Updates für den vSphere Client.

# Aktualisierte Informationen

Dieses *Platform Services Controller-Verwaltung*-Dokument wird mit jeder Produktversion oder bei Bedarf aktualisiert.

Diese Tabelle enthält den Update-Verlauf für die Dokumentation *Platform Services Controller-Verwaltung*.

| Revision | Beschreibung |
|---|---|
| 2. Mai 2022 | ■ Ein Tippfehler in So schützt vCenter Single Sign On Ihre Umgebung wurde behoben.<br>■ Geringfügiges Update für Einstellungen der Active Directory-Identitätsquelle für LDAP-Server und OpenLDAP-Server.<br>■ Geringfügiges Update für Generieren eines neuen STS-Signaturzertifikats auf der Appliance.<br>■ Die Schritte im Abschnitt Ermitteln des Ablaufdatums eines LDAPS-SSL-Zertifikats wurden korrigiert.<br>■ Geringfügiges Update für Zertifikatsanforderungen für unterschiedliche Lösungspfade.<br>■ Geringfügiges Update für Neugenerieren eines neuen VMCA-Rootzertifikats und Ersetzen aller Zertifikate. |
| 08. OKT. 2021 | ■ Die Unleugbarkeit als Zertifikatanforderung wurde aus der Dokumentation entfernt.<br>■ Geringfügiges Update für Platform Services Controller-Dienste.<br>■ Die Beschreibungen für „Benutzername“ und „URL des primären Servers“ in Einstellungen der Active Directory-Identitätsquelle für LDAP-Server und OpenLDAP-Server wurden aktualisiert.<br>■ Es wurde ein Problem mit dem Bindestrich in `-securIDAuthn` in Einrichten der RSA SecurID-Authentifizierung behoben. Beim Kopieren wurde der Befehl nicht ordnungsgemäß ausgeführt.<br>■ Ein Tippfehler in Ersetzen des VMCA-Rootzertifikats durch ein benutzerdefiniertes Signaturzertifikat und Ersetzen aller Zertifikate wurde behoben.<br>■ Geringfügiges Update für Grundlegendes zum Beenden und Starten von Diensten.<br>■ Ein Tippfehler in Ersetzen der Maschinen-SSL-Zertifikate durch VMCA-signierte Zertifikate wurde behoben.<br>■ Ein Tippfehler in Befehlsreferenz für dir-cli wurde behoben. |
| 12. August 2020 | Wir bei VMware legen Wert auf die Verwendung neutraler Sprache. Um dieses Prinzip in unserer Kunden-, Partner- und internen Community zu fördern, ersetzen einen Teil der Terminologie in unseren Inhalten. Wir haben diesen Leitfaden aktualisiert, um Instanzen einer nicht inklusiven Sprache zu entfernen. |

| Revision | Beschreibung |
| --- | --- |
| 11. MAI 2020 | ■ Informationen über den Basis-DN für Benutzer und den Basis-DN für Gruppen wurden zu Einstellungen der Active Directory-Identitätsquelle für LDAP-Server und OpenLDAP-Server hinzugefügt<br>■ Es wurde ein Speicherort der Protokolle auf vCenter Server für Windows zu Platform Services Controller-Dienstprotokolle – Referenz hinzugefügt.<br>■ Geringfügiges Update für Anfordern von Zertifikaten und Importieren eines benutzerdefinierten Rootzertifikats.<br>■ Befehlsreferenz für die certool-Initialisierung wurde aktualisiert, um die Option `--gencsr` anstelle von `--initcsr` zu verwenden.<br>■ Ersetzen der Lösungsbenutzerzertifikate (Zwischenzertifizierungsstelle) wurde aktualisiert, um zu zeigen, dass der vpxd-Zertifikatspeicher nur auf der vCenter Server Appliance vorhanden ist.<br>■ Informationen zu Ereignis-ID 2889 wurden zu Einstellungen der Active Directory-Identitätsquelle hinzugefügt. |
| 26. August 2019 | ■ Der Speicherort der Datei `certool.cfg` in Ändern der certool-Konfigurationsoptionen wurde korrigiert.<br>■ Die Informationen zur Verwendung des Attributs „userPrincipalName“ wurden in Einrichten der RSA SecurID-Authentifizierung aktualisiert. |
| 11. APR 2019 | Erstversion. |

# Erste Schritte mit Platform Services Controller

1

Der Platform Services Controller stellt allgemeine Infrastrukturdienste für die vSphere-Umgebung zur Verfügung. Zu den Diensten zählen die Lizenzierung, die Zertifikatsverwaltung und die Authentifizierung mit vCenter Single Sign On.

Verbesserungen bei der Platform Services Controller-Schnittstelle (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_qcyuyhrt/uiConfId/49694343/)

Dieses Kapitel enthält die folgenden Themen:

- vCenter Server- und Platform Services Controller-Bereitstellungstypen
- Bereitstellungstopologien mit externen Platform Services Controller-Instanzen und Hochverfügbarkeit
- Grundlegende Informationen zu vSphere-Domänen, -Domänennamen und -Sites
- Platform Services Controller-Funktionen
- Verwalten von Platform Services Controller-Diensten
- Verwalten der Platform Services Controller-Appliance

## vCenter Server- und Platform Services Controller-Bereitstellungstypen

Sie können die vCenter Server Appliance bereitstellen oder vCenter Server für Windows mit einem eingebetteten oder externen Platform Services Controller installieren. Sie können auch einen Platform Services Controller als Appliance bereitstellen oder unter Windows installieren. Bei Bedarf können Sie eine Umgebung mit gemischten Betriebssystemen verwenden.

Bevor Sie die vCenter Server Appliance bereitstellen oder vCenter Server für Windows installieren, müssen Sie das für Ihre Umgebung geeignete Bereitstellungsmodell ermitteln. Für jede Bereitstellung oder Installation müssen Sie einen der drei Bereitstellungstypen auswählen.

Tabelle 1-1. vCenter Server- und Platform Services Controller-Bereitstellungstypen

| Bereitstellungstyp | Beschreibung |
|---|---|
| vCenter Server mit einem eingebetteten Platform Services Controller | Alle im Paket mit dem Platform Services Controller zur Verfügung gestellten Dienste werden zusammen mit den vCenter Server-Diensten auf derselben virtuellen Maschine oder demselben physischen Server bereitgestellt. |
| Platform Services Controller | Nur die Dienste, die im Paket mit dem Platform Services Controller zur Verfügung gestellt werden, werden auf der virtuellen Maschine oder dem physischen Server bereitgestellt. |
| vCenter Server mit einem externen Platform Services Controller<br>(Erfordert einen externen Platform Services Controller) | Nur die vCenter Server-Dienste werden auf der virtuellen Maschine oder dem physischen Server bereitgestellt.<br>Sie müssen eine solche vCenter Server-Instanz bei einer zuvor bereitgestellten oder installierten Platform Services Controller-Instanz registrieren. |

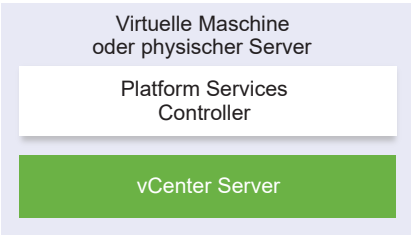
**Hinweis** vCenter Server-Bereitstellungen, die einen externen Platform Services Controller verwenden, werden in einer zukünftigen vSphere-Version nicht unterstützt. Stellen Sie vCenter Server mit einem eingebetteten Platform Services Controller bereit oder führen Sie ein entsprechendes Upgrade aus. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel http://kb.vmware.com/kb/60229.

## vCenter Server mit einem eingebetteten Platform Services Controller

Die Verwendung eines eingebetteten Platform Services Controller führt zu einer eigenständigen Bereitstellung, die über eine eigene vCenter Single Sign-On-Domäne mit einer einzelnen Site verfügt.

Ab vSphere 6.5 Update 2 können andere Instanzen von vCenter Server mit einem eingebetteten Platform Services Controller verbunden werden, um den erweiterten verknüpften Modus zu ermöglichen.

Abbildung 1-1. vCenter Server mit einem eingebetteten Platform Services Controller



Das Installieren von vCenter Server mit einem eingebetteten Platform Services Controller hat die folgenden Vorteile:

- Die Verbindung zwischen vCenter Server und dem Platform Services Controller erfolgt nicht über das Netzwerk und vCenter Server ist nicht für Ausfälle aufgrund von Verbindungs- und Namensauflösungsproblemen zwischen vCenter Server und dem Platform Services Controller anfällig.
- Wenn Sie vCenter Server auf virtuellen Windows-Maschinen oder physischen Servern installieren, benötigen Sie weniger Windows-Lizenzen.
- Sie verwalten weniger virtuelle Maschinen oder physische Server.

Sie können die vCenter Server Appliance mit einem eingebetteten Platform Services Controller in einer vCenter High Availability-Konfiguration konfigurieren. Weitere Informationen finden Sie unter *vSphere-Verfügbarkeit*.

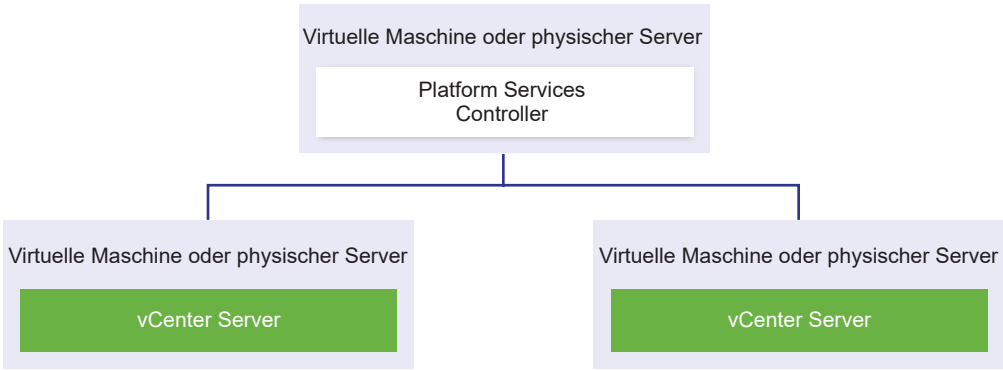
## Platform Services Controller und vCenter Server mit einem externen Platform Services Controller

Wenn Sie eine Platform Services Controller-Instanz bereitstellen oder installieren, können Sie eine vCenter Single Sign-On-Domäne erstellen oder einer bestehenden vCenter Single Sign-On-Domäne beitreten. Beigetretene Platform Services Controller-Instanzen replizieren ihre Infrastrukturdaten, wie beispielsweise Authentifizierungs- und Lizenzierungsinformationen, und können mehrere vCenter Single Sign-On-Sites umfassen. Weitere Informationen hierzu finden Sie unter Grundlegende Informationen zu vSphere-Domänen, -Domänennamen und -Sites.

**Hinweis** vCenter Server-Bereitstellungen, die einen externen Platform Services Controller verwenden, werden in einer zukünftigen vSphere-Version nicht unterstützt. Stellen Sie vCenter Server mit einem eingebetteten Platform Services Controller bereit oder führen Sie ein entsprechendes Upgrade aus. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel http://kb.vmware.com/kb/60229.

Sie können mehrere vCenter Server-Instanzen bei einer gemeinsamen externen Platform Services Controller-Instanz registrieren. Die vCenter Server-Instanzen übernehmen die vCenter Single Sign-On-Site der Platform Services Controller-Instanz, bei der sie registriert sind. Alle vCenter Server-Instanzen, die bei einer gemeinsamen oder verschiedenen beigetretenen Platform Services Controller-Instanzen registriert sind, sind im erweiterten verknüpften Modus verbunden.

**Abbildung 1-2. Beispiel für zwei vCenter Server-Instanzen mit einem gemeinsamen externen Platform Services Controller**




Die Installation von vCenter Server mit einem externen Platform Services Controller hat die folgenden Nachteile:

- Bei der Verbindung zwischen vCenter Server und dem Platform Services Controller treten möglicherweise Verbindungs- und Namensauflösungsprobleme auf.
- Wenn Sie vCenter Server auf virtuellen Windows-Maschinen oder physischen Servern installieren, benötigen Sie mehr Microsoft Windows-Lizenzen.
- Sie müssen mehr virtuelle Maschinen oder physische Server verwalten.

Informationen zu den Platform Services Controller- und vCenter Server-Maximalwerten finden Sie in der Dokumentation *Maximalwerte für die Konfiguration*.

Informationen zum Konfigurieren der vCenter Server Appliance mit einem externen Platform Services Controller in einer vCenter High Availability-Konfiguration finden Sie unter *vSphere-Verfügbarkeit*.

**Hinweis** Nachdem Sie vCenter Server mit einem externen Platform Services Controller bereitgestellt oder installiert haben, können Sie den Bereitstellungstyp neu konfigurieren und zu vCenter Server mit einem eingebetteten Platform Services Controller wechseln.

## Umgebung mit gemischten Betriebssystemen

Eine unter Windows installierte vCenter Server-Instanz kann entweder bei einem unter Windows installierten Platform Services Controller oder einer Platform Services Controller-Appliance registriert werden. Eine vCenter Server Appliance kann entweder bei einem unter Windows installierten Platform Services Controller oder einer Platform Services Controller-Appliance registriert werden. Sowohl vCenter Server als auch die vCenter Server Appliance können bei demselben Platform Services Controller registriert werden.

Abbildung 1-3. Beispiel einer Umgebung mit gemischten Betriebssystemen mit einem externen Platform Services Controller unter Windows

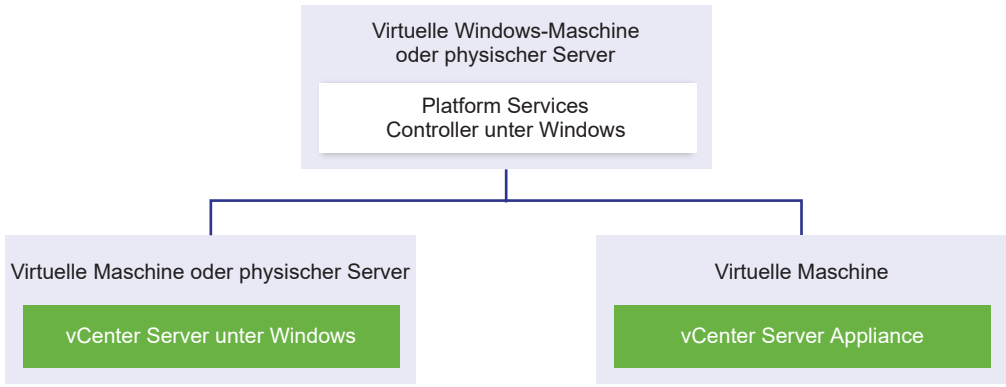
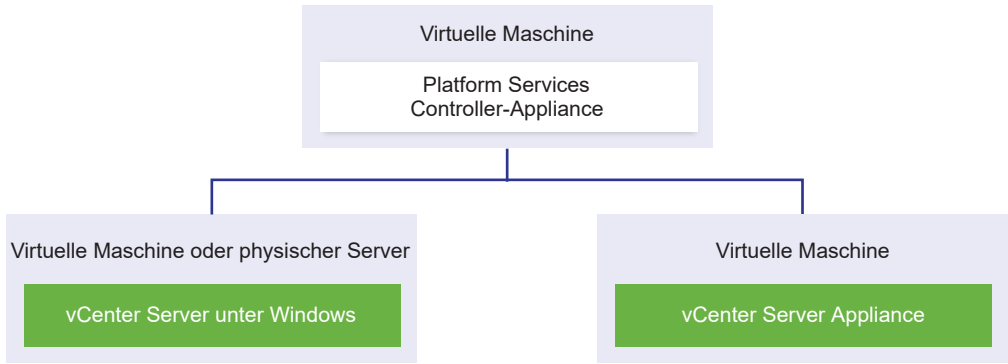



Abbildung 1-4. Beispiel einer Umgebung mit gemischten Betriebssystemen mit einer externen Platform Services Controller-Appliance




**Hinweis** Um Verwaltungsfreundlichkeit und problemlose Wartung zu gewährleisten, verwenden Sie nur Appliances oder nur Windows-Installationen von vCenter Server und Platform Services Controller.

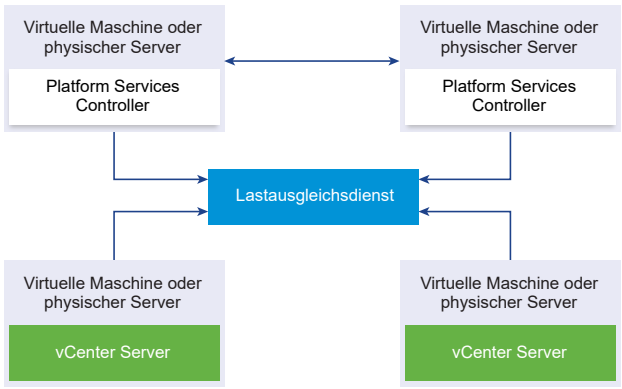
## Bereitstellungstopologien mit externen Platform Services Controller-Instanzen und Hochverfügbarkeit

Um Hochverfügbarkeit für den Platform Services Controller in externen Bereitstellungen zu gewährleisten, müssen Sie mindestens zwei hinzugefügte Platform Services Controller-Instanzen in Ihrer vCenter Single Sign-On-Domäne installieren oder bereitstellen. Wenn Sie einen Lastausgleichsdienst eines Drittanbieters verwenden, können Sie einen automatischen Failover ohne Ausfallzeit sicherstellen.

**Hinweis** vCenter Server-Bereitstellungen, die einen externen Platform Services Controller verwenden, werden in einer zukünftigen vSphere-Version nicht unterstützt. Stellen Sie vCenter Server mit einem eingebetteten Platform Services Controller bereit oder führen Sie ein entsprechendes Upgrade aus. Weitere Informationen finden Sie im Knowledgebase-Artikel 60229.

# Platform Services Controller mit Lastausgleichsdienst

**Abbildung 1-5. Beispiel für ein Paar von Platform Services Controller-Instanzen mit Lastausgleich**



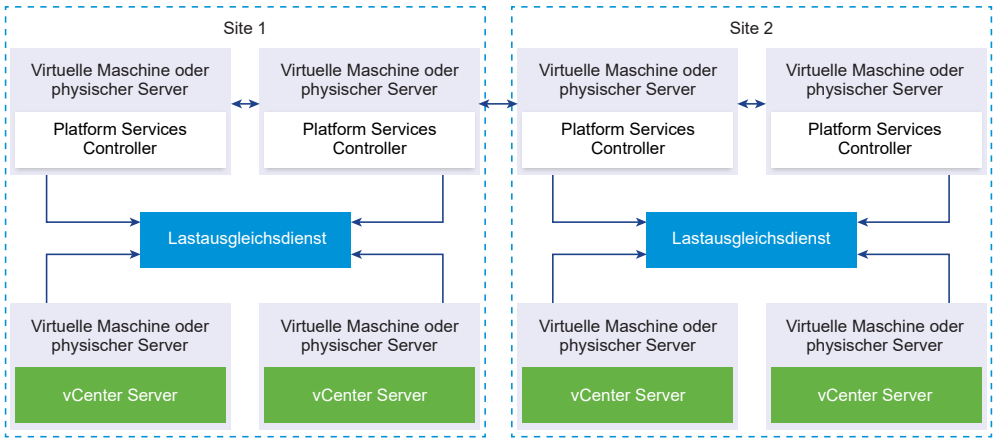

Sie können einen Drittanbieter-Lastausgleichsdienst pro Site verwenden, um Platform Services Controller-Hochverfügbarkeit mit automatischem Failover für diese Site zu konfigurieren. Informationen zur maximalen Anzahl von Platform Services Controller-Instanzen hinter einem Lastausgleichsdienst finden Sie in der Dokumentation *Maximalwerte für die Konfiguration*.

**Wichtig** Um die Hochverfügbarkeit für einen Platform Services Controller hinter einem Lastausgleichsdienst zu konfigurieren, müssen die Platform Services Controller-Instanzen den gleichen Betriebssystemtyp aufweisen. Platform Services Controller-Instanzen mit gemischten Betriebssystemen werden hinter einem Lastausgleichsdienst nicht unterstützt.

Die vCenter Server-Instanzen sind mit dem Lastausgleichsdienst verbunden. Wenn eine Platform Services Controller-Instanz nicht mehr reagiert, verteilt der Lastausgleichsdienst die Last automatisch ohne Ausfallzeit auf die übrigen funktionsfähigen Platform Services Controller-Instanzen.

# Platform Services Controller mit Lastausgleichsdiensten zwischen vCenter Single Sign-On-Sites

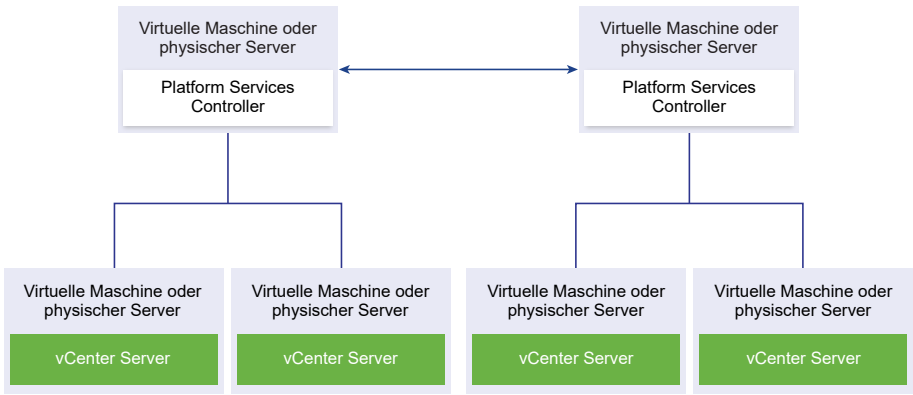
**Abbildung 1-6. Beispiel für zwei Platform Services Controller-Instanzen mit Lastausgleich zwischen zwei Sites**




Ihre vCenter Single Sign-On Domäne umfasst möglicherweise mehrere Sites. Um Platform Services Controller-Hochverfügbarkeit mit automatischem Failover in der gesamten Domäne sicherzustellen, müssen Sie einen separaten Lastausgleichsdient in jeder Site konfigurieren.

# Platform Services Controller ohne Lastausgleichsdienst

**Abbildung 1-7. Beispiel für zwei hinzugefügte Platform Services Controller-Instanzen ohne Lastausgleichsdienst**



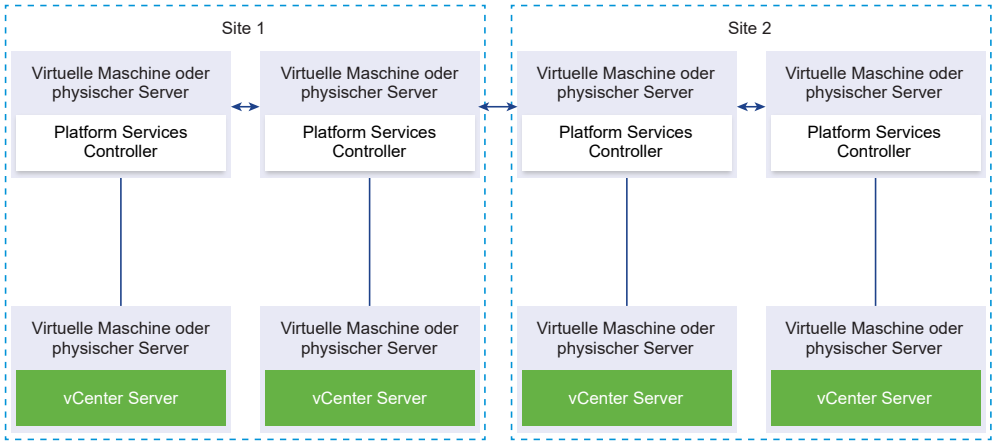

Wenn Sie zwei oder mehr Platform Services Controller-Instanzen in derselben Site ohne Lastausgleichsdienst hinzufügen, konfigurieren Sie Platform Services Controller-Hochverfügbarkeit mit manuellem Failover für diese Site.

Wenn eine Platform Services Controller-Instanz nicht mehr reagiert, müssen Sie für die dort registrierten vCenter Server-Instanzen ein manuelles Failover durchführen. Ein Failover von Instanzen wird durchgeführt, indem Sie neu auf andere, funktionsfähige Platform Services Controller-Instanzen auf der gleichen Site verweisen. Informationen zum Neuverweisen von vCenter Server-Instanzen auf einen anderen externen Platform Services Controller finden Sie unter *Installation und Einrichtung von vCenter Server*.

**Hinweis** Wenn Ihre vCenter Single Sign On-Domäne drei oder mehr Platform Services Controller-Instanzen umfasst, können Sie manuell eine Ringtopologie erstellen. Eine Ringtopologie stellt die Platform Services Controller-Zuverlässigkeit sicher, wenn eine der Instanzen fehlschlägt. Führen Sie zum Erstellen einer Ringtopologie den Befehl `/usr/lib/vmware-vmdir/bin/vdcrepadmin -f createagreement` für die erste und die letzte bereitgestellte Platform Services Controller-Instanz aus.

## Platform Services Controller ohne Lastausgleichsdienst zwischen vCenter Single Sign-On-Sites

**Abbildung 1-8. Beispiel für zwei hinzugefügte Paare von Platform Services Controller-Instanzen zwischen zwei Sites ohne Lastausgleichsdienst**




Ihre vCenter Single Sign-On Domäne umfasst möglicherweise mehrere Sites. Wenn kein Lastausgleichsdienst verfügbar ist, können Sie vCenter Server manuell von einem ausgefallenen zu einem funktionsfähigen Platform Services Controller in derselben Site neu verweisen. Informationen zum Neuverweisen von vCenter Server-Instanzen auf einen anderen externen Platform Services Controller finden Sie unter *Installation und Einrichtung von vCenter Server*.

# Grundlegende Informationen zu vSphere-Domänen, -Domänennamen und -Sites

Jeder Platform Services Controller ist mit einer vCenter Single Sign-On-Domäne verknüpft. Der Standarddomänenname lautet „vsphere.local“, Sie können diesen Namen jedoch bei der Installation des ersten Platform Services Controller ändern. Die Domäne bestimmt den Bereich

für die lokale Authentifizierung. Sie können die Domäne in mehrere Sites aufteilen und jeden Platform Services Controller und jede vCenter Server-Instanz einer Site zuordnen. Sites sind logische Konstrukte, bei denen es sich in der Regel um geografische Standorte handelt.

## Platform Services Controller-Domäne

Wenn Sie einen Platform Services Controller installieren, werden Sie zum Erstellen einer vCenter Single Sign-On-Domäne oder zum Beitritt zu einer vorhandenen Domäne aufgefordert.

Der Domänenname wird vom VMware Directory Service (vmdir) für die gesamte interne LDAP (Lightweight Directory Access Protocol)-Strukturierung verwendet.

In vSphere 6.0 und höher können Sie Ihrer vSphere-Domäne einen eindeutigen Namen geben. Verwenden Sie einen Namen, der nicht von OpenLDAP, Microsoft Active Directory und einem anderen Verzeichnisdienst verwendet wird, um Konflikte bei der Authentifizierung zu vermeiden.

**Hinweis** Sie können keine Domäne ändern, zu der eine Platform Services Controller- oder vCenter Server-Instanz gehört.

Nachdem Sie den Namen für Ihre Domäne angegeben haben, können Sie Benutzer und Gruppen hinzufügen. In der Regel ist es sinnvoller, eine Active Directory- oder LDAP-Identitätsquelle anzugeben und die Authentifizierung für die Benutzer und Gruppen in dieser Identitätsquelle zuzulassen. Sie können auch vCenter Server- oder Platform Services Controller-Instanzen oder andere VMware-Produkte wie vRealize Operations zur Domäne hinzufügen.

## Platform Services Controller-Sites

Sie können Platform Services Controller-Domänen in logische Sites organisieren. Eine Site in VMware Directory Service ist ein logischer Container, in dem Sie Platform Services Controller-Instanzen in einer vCenter Single Sign-On-Domäne gruppieren können.

Ab vSphere 6.5 gewinnen Sites an Bedeutung. Während des Platform Services Controller-Failovers werden vCenter Server-Instanzen von einem anderen Platform Services Controller in derselben Site verwendet. Um zu verhindern, dass Ihre vCenter Server-Instanzen von einem Platform Services Controller an einem weit entfernten geografischen Standort verwendet werden, können Sie mehrere Sites verwenden.

Bei der Installation oder beim Upgrade eines Platform Services Controller werden Sie zur Eingabe des Site-Namens aufgefordert. Informationen finden Sie in der Dokumentation *Installation und Einrichtung von vCenter Server*.

# Platform Services Controller-Funktionen

Platform Services Controller unterstützt Dienste wie Identitäts-, Zertifikat- und Lizenzverwaltung in vSphere.

## Kernfunktionen

Platform Services Controller umfasst verschiedene Dienste, die in Platform Services Controller-Dienste behandelt werden, und weist die folgenden Kernfunktionen auf.

- Authentifizierung durch vCenter Single Sign-On
- Bereitstellung von vCenter Server-Komponenten und ESXi-Hosts mit VMware Certificate Manager-Standardzertifikaten (VMCA)
- Verwendung benutzerdefinierter Zertifikate, die im VMware Endpoint Certificate Store (VECS) gespeichert werden

## Bereitstellungsmodelle

Sie können Platform Services Controller auf einem Windows-System installieren oder die Platform Services Controller-Appliance bereitstellen.

Das Bereitstellungsmodell hängt von der verwendeten Platform Services Controller-Version ab. Weitere Informationen hierzu finden Sie unter vCenter Server- und Platform Services Controller-Bereitstellungstypen.

Ab vSphere 6.7 Update 1 gilt, dass, wenn Sie eine vCenter Server-Instanz mit einem externen Platform Services Controller bereitgestellt oder installiert haben und Sie sie in eine vCenter Server-Instanz mit einem eingebetteten Platform Services Controllerkonvertieren möchten, Sie eine neue Platform Services Controller replizieren können, die in die vorhandene vCenter Server-Instanz eingebettet ist. Informationen finden Sie in der Dokumentation *Installation und Einrichtung von vCenter Server*.

Ab vSphere 6.7 Update 1 können Sie einen vCenter Server mit einem eingebetteten Platform Services Controller aus einer vSphere-Domäne in eine andere vSphere-Domäne verschieben. Dienste wie Tagging und Lizenzierung bleiben erhalten und werden auf die neue Domäne migriert. Informationen finden Sie in der Dokumentation *Installation und Einrichtung von vCenter Server*.

# Verwalten von Platform Services Controller-Diensten

Platform Services Controller-Dienste werden über den vSphere Client oder mithilfe der verfügbaren Skripts und CLIs verwaltet.

Verschiedene Platform Services Controller-Dienste unterstützen unterschiedliche Schnittstellen.

Tabelle 1-2. Schnittstellen für die Verwaltung von Platform Services Controller-Diensten

| Schnittstelle | Beschreibung |
|---|---|
| vSphere Client | Web-Benutzeroberfläche (HTML5-basierter Client). Die Terminologie, Topologie und der Workflow der vSphere Client-Benutzeroberfläche sind eng an denselben Aspekten und Elementen der vSphere Web Client-Benutzeroberfläche ausgerichtet. |
| vSphere Web Client | Webschnittstelle für die Verwaltung einiger Dienste. |
| Dienstprogramm für die Zertifikatsverwaltung | Befehlszeilenprogramm, das die CSR-Generierung und die Zertifikatsersetzung unterstützt. Weitere Informationen hierzu finden Sie unter Verwalten von Zertifikaten mit dem Dienstprogramm vSphere Certificate Manager. |
| CLIs für die Verwaltung von Platform Services Controller-Diensten | Befehlssatz für die Verwaltung von Zertifikaten, der VMware Endpoint Certificate Store (VECS) und VMware Directory Service (vmdir). Weitere Informationen hierzu finden Sie unter Kapitel 4 Verwalten von Diensten und Zertifikaten mit CLI-Befehlen. |

## Platform Services Controller-Dienste

Mit Platform Services Controller können alle VMware-Produkte innerhalb einer Umgebung die Authentifizierungsdomäne und andere Dienste gemeinsam verwenden. Zu den Diensten zählen beispielsweise Zertifikatverwaltung, Authentifizierung und Lizenzierung.

Platform Services Controller beinhaltet die folgenden Kerninfrastrukturdienste.

Tabelle 1-3. Platform Services Controller-Dienste

| Dienst | Beschreibung |
|---|---|
| `applmgmt`<br>(VMware Appliance Management Service) | Verarbeitet die Appliance-Konfiguration und stellt öffentliche API-Endpunkte für die Appliance-Lifecycle-Verwaltung bereit. Enthalten in der Platform Services Controller-Appliance. |
| `vmware-cis-license`<br>(VMware License Service) | Jeder Platform Services Controller enthält VMware License Service, der zentralisierte Lizenzverwaltungs- und Berichterstellungsfunktionen für VMware-Produkte in Ihrer Umgebung bereitstellt.<br>Die Lizenzdienstbestandsliste wird in 30-Sekunden-Intervallen auf alle Platform Services Controller in der Domäne repliziert. |

Tabelle 1-3. Platform Services Controller-Dienste (Fortsetzung)

| Dienst | Beschreibung |
| --- | --- |
| `vmware-stsd`<br>(VMware Security Token Service) | Der Dienst hinter der vCenter Single Sign On-Funktion, der sichere Authentifizierungsdienste für VMware-Softwarekomponenten und Benutzer bereitstellt.<br>vCenter Single Sign On ermöglicht die Kommunikation der VMware-Komponenten über einen sicheren Token-Austauschmechanismus. vCenter Single Sign On erstellt eine interne Sicherheitsdomäne (standardmäßig „vsphere.local“), in der die VMware-Softwarekomponenten während des Installations- oder Upgrade-Vorgangs registriert werden. |
| `vmware-rhttpproxy`<br>(VMware HTTP Reverse Proxy) | Der Reverse-Proxy wird auf jedem Platform Services Controller-Knoten und in jedem vCenter Server-System ausgeführt. Er stellt einen zentralen Einstiegspunkt in den Knoten dar und ermöglicht den auf dem Knoten ausgeführten Diensten die sichere Kommunikation. |
| `vmware-sca`<br>(VMware Service Control Agent) | Verwaltet Dienstkonfigurationen. Mit der `service-control`-CLI können Sie einzelne Dienstkonfigurationen verwalten. |
| `vmware-statsmonitor`<br>(VMware Appliance Monitoring Service) | Überwacht den Ressourcenverbrauch des vCenter Server Appliance-Gastbetriebssystems. |
| `vmware-vapi-endpoint`<br>(VMware vAPI Endpoint) | Der vSphere Automation-API-Endpoint bietet zentralen Zugriff auf vAPI-Dienste. Sie können die Eigenschaften des vAPI-Endpoint-Diensts in vSphere Client ändern. Details zu vAPI-Endpoints finden Sie im *vSphere Automation SDKs-Programmierhandbuch*. |
| `vmafdd`<br>VMware Authentication Framework | Dienst, der ein clientseitiges Framework für vmdir-Authentifizierung bereitstellt und dem VMware Endpoint Certificate Store (VECS) dient. |
| `vmcad`<br>VMware Certificate Service | Stellt allen VMware-Softwarekomponenten, die über vmafd-Clientbibliotheken verfügen, und allen ESXi-Hosts ein signiertes Zertifikat bereit, dessen Stammzertifizierungsstelle VMCA ist. Sie können die Standardzertifikate mithilfe des Certificate Manager-Dienstprogramms ändern.<br>Der VMware Certificate Service verwendet den VMware Endpoint Certificate Store (VECS) als lokales Repository für Zertifikate auf jeder Platform Services Controller-Instanz. Sie können zwar entscheiden, anstelle der VMCA benutzerdefinierte Zertifikate zu verwenden, Sie müssen diese Zertifikate aber zum VECS hinzufügen. |

Tabelle 1-3. Platform Services Controller-Dienste (Fortsetzung)

| Dienst | Beschreibung |
| --- | --- |
| `vmdird`<br>VMware Directory Service | Stellt einen LDAP-Verzeichnisdienst mit mehreren Mandanten und Peer-Replizierung zum Speichern von Authentifizierungs-, Zertifikat-, Lookup- und Lizenzinformationen zur Verfügung. Aktualisieren Sie keine Daten in `vmdird` mit einem LDAP-Browser.<br>Wenn Ihre Domäne mehr als eine Platform Services Controller-Instanz enthält, wird eine Aktualisierung des vmdir-Inhalts in einer vmdir-Instanz auf alle anderen Instanzen von vmdir propagiert. |
| `vmdnsd`<br>VMware Domain Name Service | Wird in vSphere 6.x nicht verwendet. |
| `vmonapi`<br>VMware Lifecycle Manager-API<br>`vmware-vmon`<br>VMware Service Lifecycle Manager | Startet und beendet vCenter Server-Dienste und überwacht die Dienst-API-Integrität. Der `vmware-vmon`-Dienst ist ein zentralisierter, plattformunabhängiger Dienst, der den Lebenszyklus von Platform Services Controller und vCenter Server verwaltet. Stellt APIs und CLIs für Drittanbieteranwendungen zur Verfügung. |
| `lwsmd`<br>Likewise Service Manager | Likewise erleichtert das Verbinden des Hosts mit einer Active Directory-Domäne und die nachfolgende Benutzerauthentifizierung. |
| `pschealth`<br>VMware Platform Services Controller-Systemüberwachung | Überwacht den Systemzustand und den Status aller wesentlichen Platform Services Controller-Infrastrukturdienste. |
| `vmware-analytics`<br>VMware-Analysedienst | Besteht aus Komponenten, die Telemetriedaten aus verschiedenen vSphere-Komponenten erfassen und in die VMware Analytics Cloud hochladen und das Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) verwalten. |

# Verwalten von Platform Services Controller-Diensten auf dem vSphere Client

Sie können die vCenter-Zugriffssteuerung, die Lizenzierung, Lösungen, verknüpfte Domänen, Zertifikate und Single Sign-On über den vSphere Client verwalten.

### Verfahren

1. Melden Sie sich bei der lokalen vCenter Single Sign-On-Domäne (standardmäßig „vsphere.local“) als Administrator bei einem vCenter Server an, der einem Platform Services Controller zugeordnet ist.
2. Wählen Sie **Administration** aus und klicken Sie auf das Element, das Sie verwalten möchten.

# Verwalten von Platform Services Controller-Diensten auf dem vSphere Web Client

Sie verwalten vCenter Single Sign-On und den Lizenzierungsdienst auf dem vSphere Web Client.

Verwenden Sie den vSphere Client oder CLIs anstelle des vSphere Web Client, um die folgenden Dienste zu verwalten.

- Zertifikate
- VMware Endpoint Certificate Store (VECS)
- Zweistufige Authentifizierung wie Authentifizierung mit einer allgemeinen Zugriffskarte (CAC-Authentifizierung)
- Anmelde-Banner

**Verfahren**

1. Melden Sie sich bei der lokalen vCenter Single Sign-On-Domäne (standardmäßig „vsphere.local“) als Administrator bei einem vCenter Server an, der einem Platform Services Controller zugeordnet ist.
2. Wählen Sie **Administration** aus und klicken Sie auf das Element, das Sie verwalten möchten.

| Option | Beschreibung |
|---|---|
| **Single Sign-On** | Konfigurieren von vCenter Single Sign-On<br>■ Festlegen von Richtlinien<br>■ Verwalten von Identitätsquellen<br>■ Verwalten des STS-Signierzertifikats<br>■ Verwalten von SAML-Dienstanbietern<br>■ Verwalten von Benutzern und Gruppen |
| **Lizenzierung** | Konfigurieren der Lizenzierung |

# Verwalten von Platform Services Controller-Diensten mithilfe von Skripts

Platform Services Controller enthält Skripts zum Generieren von CSRs und zum Verwalten von Zertifikaten und Diensten.

Sie können beispielsweise das Dienstprogramm `certool` zum Generieren von CSRs und zum Ersetzen von Zertifikaten sowohl bei Szenarios mit eingebettetem Platform Services Controller als auch für Szenarios mit externem Platform Services Controller verwenden. Weitere Informationen hierzu finden Sie unter Verwalten von Zertifikaten mit dem Dienstprogramm vSphere Certificate Manager.

Verwenden Sie die CLIs für Verwaltungsaufgaben, die die Webschnittstelle nicht unterstützt oder zum Erstellen von benutzerdefinierten Skripts für Ihre Umgebung.

Tabelle 1-4. Befehlszeilenschnittstellen für die Verwaltung von Zertifikaten und zugehörigen Diensten

| Befehlszeilenschnittstelle | Beschreibung | Links |
|---|---|---|
| `certool` | Generieren und verwalten Sie Zertifikate und Schlüssel. Bestandteil von VMCA. | Befehlsreferenz für die certool-Initialisierung |
| `vecs-cli` | Verwalten Sie die Inhalte von VMware-Zertifikatspeicherinstanzen. Bestandteil von VMAFD. | Befehlsreferenz für vecs-cli |
| `dir-cli` | Erstellen und aktualisieren Sie Zertifikate im VMware Directory Service. Bestandteil von VMAFD. | Befehlsreferenz für dir-cli |
| `sso-config` | Dienstprogramm zum Konfigurieren der Smartcard-Authentifizierung. | Grundlegendes zur zweistufigen vCenter Server-Authentifizierung |
| `service-control` | Befehl zum Starten, Anhalten und Auflisten von Diensten. | Führen Sie diesen Befehl aus, um Dienste anzuhalten, bevor Sie andere CLI-Befehle ausführen. |

### Verfahren

1 Melden Sie sich bei der Platform Services Controller-Shell an.

In den meisten Fällen müssen Sie der Root- oder Administratorbenutzer sein. Weitere Informationen finden Sie unter Erforderliche Rechte für die Ausführung von CLIs.

2 Greifen Sie an einem der folgenden Standard-Standorte auf eine CLI zu.

Die Rechte, die Sie benötigen, hängen von der Aufgabe ab, die Sie durchführen möchten. In einigen Fällen werden Sie zweimal zur Eingabe des Kennworts aufgefordert, um vertrauliche Informationen zu schützen.

#### Windows

```
C:\Programme\VMware\vCenter Server\vmafdd\vecs-cli.exe
C:\Programme\VMware\vCenter Server\vmafdd\dir-cli.exe
C:\Programme\VMware\vCenter Server\vmcad\certool.exe
C:\Programme\VMware\VCenter server\VMware Identity Services\sso-config
VCENTER_INSTALL_PATH\bin\service-control
```

#### Linux

```
/usr/lib/vmware-vmafd/bin/vecs-cli
/usr/lib/vmware-vmafd/bin/dir-cli
/usr/lib/vmware-vmca/bin/certool
/opt/vmware/bin
```

Unter Linux müssen Sie für den Befehl `service-control` den Pfad nicht angeben.

# Verwalten der Platform Services Controller-Appliance

Sie können die Platform Services Controller-Appliance über die Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) oder über die Appliance-Shell verwalten.

Wenn Sie eine Umgebung mit einem eingebetteten Platform Services Controller verwenden, verwalten Sie eine einzige Appliance, die sowohl den Platform Services Controller als auch den vCenter Server umfasst. Siehe *vCenter Server Appliance-Konfiguration*.

**Tabelle 1-5. Schnittstellen für die Verwaltung der Platform Services Controller-Appliance**

| Schnittstelle | Beschreibung |
|---|---|
| Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) für den Platform Services Controller | Verwenden Sie diese Schnittstelle, um die Systemeinstellungen einer Platform Services Controller-Bereitstellung neu zu konfigurieren. |
| Platform Services Controller-Appliance-Shell | Verwenden Sie diese Befehlszeilenschnittstelle, um Dienstverwaltungsvorgänge für VMCA, VECS und VMDIR durchzuführen. Siehe Verwalten von Zertifikaten mit dem Dienstprogramm vSphere Certificate Manager und Kapitel 4 Verwalten von Diensten und Zertifikaten mit CLI-Befehlen. |

## Verwalten der Appliance mit der Platform Services Controller-Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI)

In einer Umgebung mit einem externen Platform Services Controller können Sie mithilfe der Platform Services Controller-Verwaltungsschnittstelle für virtuelle Appliances (Virtual Appliance Management Interface, VAMI) die Appliance-Systemeinstellungen konfigurieren. Zu den verfügbaren Einstellungen zählen Zeitsynchronisierung, Netzwerkeinstellungen und SSH-Anmeldeeinstellungen. Sie können auch das Root-Kennwort ändern, die Appliance mit einer Active Directory-Domäne verbinden und eine Active Directory-Domäne verlassen.

In einer Umgebung mit einem eingebetteten Platform Services Controller verwalten Sie die Appliances, die sowohl den Platform Services Controller als auch den vCenter Server enthalten.

### Verfahren

1. Navigieren Sie in einem Webbrowser zur Webschnittstelle unter https://*platform_services_controller_ip*:5480.
2. Wenn eine Warnmeldung über ein nicht vertrauenswürdiges SSL-Zertifikat angezeigt wird, beheben Sie das Problem basierend auf der Unternehmenssicherheitsrichtlinie und dem Webbrowser, den Sie verwenden.
3. Melden Sie sich als „root“ an.

   Das Standard-Root-Kennwort ist das Root-Kennwort der virtuellen Appliance, das Sie bei der Bereitstellung der virtuellen Appliance festgelegt haben.

### Ergebnisse

Die Seite „Systeminformationen“ der Platform Services Controller-Appliance-Verwaltungsschnittstelle wird angezeigt.

## Verwalten der Appliance über die Appliance-Shell

Sie können Dienstverwaltungsprogramme und CLIs über die Appliance-Shell verwenden. Sie können TTY1 für die Anmeldung an der Konsole oder aber SSH zum Herstellen einer Verbindung zur Shell verwenden.

### Verfahren

1 Aktivieren Sie bei Bedarf die SSH-Anmeldung.

   a Melden Sie sich unter „https://*platform_services_controller_ip*:5480“ bei der Appliance-Verwaltungsschnittstelle (VAMI) an.

   b Wählen Sie im Navigator die Option **Zugriff** aus und klicken Sie auf **Bearbeiten**.

   c Aktivieren Sie die Option **SSH-Anmeldung aktivieren** und klicken Sie auf **OK**.

   Zum Aktivieren der Bash-Shell für die Appliance können Sie dieselben Schritte ausführen.

2 Greifen Sie auf die Appliance-Shell zu.

   - Wenn Sie Direktzugriff auf die Appliance-Konsole haben, wählen Sie **Anmelden** aus und drücken Sie die Eingabetaste.
   - Wenn Sie eine Remoteverbindung herstellen möchten, verwenden Sie SSH oder eine andere Remotekonsolenverbindung, um eine Sitzung mit der Appliance zu starten.

3 Melden Sie sich als Root-Benutzer mit dem Kennwort an, das Sie bei der erstmaligen Bereitstellung der Appliance verwendet haben.

   Wenn Sie das Root-Kennwort geändert haben, verwenden Sie das neue Kennwort.

## Hinzufügen einer Platform Services Controller-Appliance zu einer Active Directory-Domäne

Wenn Sie einem Platform Services Controller eine Active Directory-Identitätsquelle hinzufügen möchten, müssen Sie die Platform Services Controller-Appliance mit einer Active Directory-Domäne verbinden.

Wenn Sie eine unter Windows installierte Platform Services Controller-Instanz verwenden, können Sie die Domäne verwenden, zu der diese Maschine gehört.

### Verfahren

1 Melden Sie sich mithilfe von vSphere Client als Benutzer mit Administratorrechten bei einem mit Platform Services Controller verknüpften vCenter Server-System in der lokalen vCenter Single Sign-On-Domäne (standardmäßig „vsphere.local“) an.

2 Wählen Sie **Verwaltung** aus.

3 Erweitern Sie **Single Sign-On** und klicken Sie auf **Konfiguration**.

4 Klicken Sie auf **Active Directory-Domäne**.

5 Klicken Sie auf **AD beitreten**, geben Sie die Domäne, die optionale Organisationseinheit sowie den Benutzernamen und das Kennwort an und klicken Sie auf **Beitreten**.

### Nächste Schritte

Um Benutzer und Gruppen der Active Directory-Domäne anzuhängen, zu der der Beitritt erfolgte, fügen Sie die Domäne, der beigetreten wurde, als eine vCenter Single Sign-On-Identitätsquelle hinzu. Weitere Informationen hierzu finden Sie unter Hinzufügen oder Bearbeiten einer vCenter Single Sign On-Identitätsquelle.

# vSphere-Authentifizierung mit vCenter Single Sign On

2

vCenter Single Sign On ist ein Authentifizierungs-Broker und eine Austauschinfrastruktur für Sicherheitstoken. Wenn sich ein Benutzer bei vCenter Single Sign On authentifizieren kann, erhält der Benutzer ein SAML-Token. Der Benutzer kann dann das SAML-Token zum Authentifizieren bei vCenter-Diensten verwenden. Der Benutzer kann dann die Aktionen durchführen, für die er Berechtigungen hat.

Da der Datenverkehr für alle Kommunikationen verschlüsselt ist und nur authentifizierte Benutzer die Aktionen durchführen können, für die sie Berechtigungen haben, ist Ihre Umgebung sicher.

Ab vSphere 6.0 ist vCenter Single Sign On Teil des Platform Services Controller. Der Platform Services Controller enthält die gemeinsam genutzten Dienste, die vCenter Server und vCenter Server-Komponenten unterstützen. Zu diesen Diensten gehören vCenter Single Sign On, VMware Certificate Authority und Lizenzdienst. Siehe *Installation und Einrichtung von vCenter Server* für weitere Informationen zu den Platform Services Controller.

Für das anfängliche Handshake authentifizieren sich Benutzer mit einem Benutzernamen und einem Kennwort, und Lösungsbenutzer authentifizieren sich mit einem Zertifikat. Informationen zum Ersetzen von Lösungsbenutzerzertifikaten finden Sie unter Kapitel 3 vSphere-Sicherheitszertifikate.

Im nächsten Schritt autorisieren Sie die Benutzer, die die Durchführung bestimmter Aufgaben authentifizieren können. In den meisten Fällen weisen Sie vCenter Server-Berechtigungen zu, gewöhnlich durch Zuweisen des Benutzers zu einer Gruppe, die über eine Rolle verfügt. vSphere beinhaltet weitere Berechtigungsmodelle, wie zum Beispiel globale Berechtigungen. Informationen finden Sie in der Dokumentation *vSphere-Sicherheit*.

Dieses Kapitel enthält die folgenden Themen:

- Empfohlene Vorgehensweisen für die Sicherheit von vCenter Single Sign On

# Grundlegendes zu vCenter Single Sign On

Für die effiziente Verwaltung von vCenter Single Sign On müssen Sie mit der zugrunde liegenden Architektur und deren Auswirkungen auf Installation und Upgrades vertraut sein.

Domänen und Sites von vCenter Single Sign-On 6.0 (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_y9pxac75/uiConfId/49694343/)

## So schützt vCenter Single Sign On Ihre Umgebung

vCenter Single Sign On ermöglicht vSphere-Komponenten, über einen sicheren Token-Mechanismus miteinander zu kommunizieren.

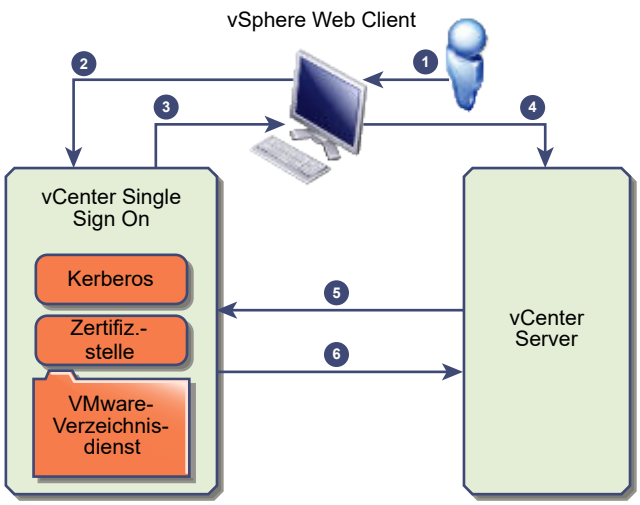
vCenter Single Sign On verwendet die folgenden Dienste.

- STS (Security Token Service)
- SSL für sicheren Datenverkehr.
- Authentifizierung für Personen als Benutzer mit Active Directory oder OpenLDAP.
- Authentifizierung von Lösungsbenutzern über Zertifikate.

### vCenter Single Sign On-Handshake für Personen als Benutzer

Die folgende Abbildung zeigt den Handshake für Personen als Benutzer.

**Abbildung 2-1. vCenter Single Sign On-Handshake für Personen als Benutzer**




1 Ein Benutzer muss sich mit einem Benutzernamen und einem Kennwort am vSphere Client anmelden, um auf das vCenter Server-System oder einen anderen vCenter-Dienst zugreifen zu können.

Der Benutzer hat auch die Möglichkeit, sich ohne ein Kennwort anzumelden. In diesem Fall muss er das Kontrollkästchen **Windows-Sitzungsauthentifizierung verwenden** aktivieren.

2 Der vSphere Client leitet die Anmeldeinformationen an den vCenter Single Sign On-Dienst weiter, der das SAML-Token des vSphere Client überprüft. Wenn der vSphere Client über ein gültiges Token verfügt, überprüft vCenter Single Sign On weiterhin, ob sich der Benutzer in der konfigurierten Identitätsquelle (z. B. , Active Directory) befindet.

   - Wenn nur der Benutzername verwendet wird, überprüft vCenter Single Sign On die Standarddomäne.
   - Ist ein Domänenname im Benutzernamen enthalten (*DOMÄNE*\Benutzer1 oder Benutzer1@*DOMÄNE*), überprüft vCenter Single Sign On diese Domäne.

3 Wenn sich der Benutzer bei der Identitätsquelle authentifizieren kann, gibt vCenter Single Sign On ein Token zurück, das für den vSphere Client den Benutzer darstellt.

4 Der vSphere Client leitet das Token an das vCenter Server-System weiter.

5 vCenter Server überprüft gemeinsam mit dem vCenter Single Sign On-Server, ob das Token gültig und noch nicht abgelaufen ist.

6 Der vCenter Single Sign On-Server gibt das Token an das vCenter Server-System zurück und nutzt das Autorisierungs-Framework von vCenter Server, um Benutzerzugriff zu ermöglichen.

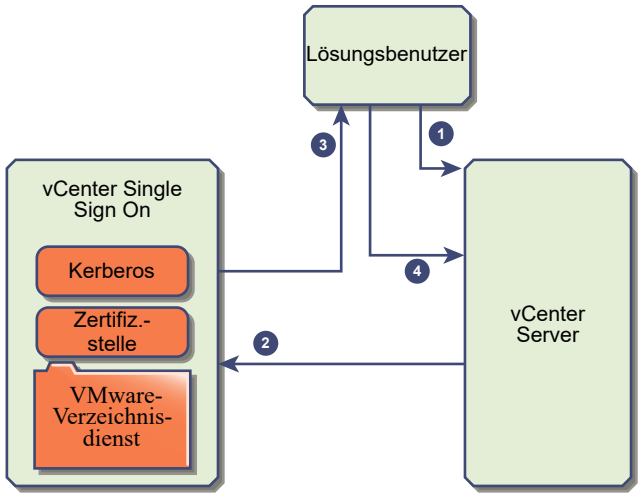
Der Benutzer kann sich nun authentifizieren und alle Objekte anzeigen und ändern, für die die Benutzerrolle über die entsprechenden Berechtigungen verfügt.

**Hinweis** Zu Beginn wird jedem Benutzer die Rolle „Kein Zugriff“ zugewiesen. Ein vCenter Server-Administrator muss dem jeweiligen Benutzer mindestens die Rolle für den Zugriff „Nur Lesen“ zuweisen, bevor sich der Benutzer anmelden kann. Informationen finden Sie in der Dokumentation *vSphere-Sicherheit*.

## vCenter Single Sign On-Handshake für Lösungsbenutzer

Lösungsbenutzer sind Sätze von Diensten, die in der vCenter Server-Infrastruktur verwendet werden, zum Beispiel der vCenter Server oder die vCenter Server-Erweiterungen. VMware-Erweiterungen und eventuell Erweiterungen von Drittanbietern können sich ebenfalls bei vCenter Single Sign On authentifizieren.

Abbildung 2-2. vCenter Single Sign On-Handshake für Lösungsbenutzer




Für Lösungsbenutzer verläuft die Interaktion folgendermaßen:

1 Der Lösungsbenutzer versucht, eine Verbindung mit einem vCenter-Dienst herzustellen.

2 Der Lösungsbenutzer wird an vCenter Single Sign On umgeleitet. Wenn der Lösungsbenutzer für vCenter Single Sign On neu ist, muss er ein gültiges Zertifikat vorweisen.

3 Wenn das Zertifikat gültig ist, weist vCenter Single Sign On dem Lösungsbenutzer ein SAML-Token (Bearer-Token) zu. Das Token wird durch vCenter Single Sign On signiert.

4 Der Lösungsbenutzer wird dann zu vCenter Single Sign On weitergeleitet und kann Aufgaben entsprechend seinen Berechtigungen ausführen.

5 Wenn sich der Lösungsbenutzer beim nächsten Mal authentifizieren muss, kann er das SAML-Token zum Anmelden bei vCenter Server verwenden.

Dieser Handshake erfolgt standardmäßig automatisch, weil VMCA beim Starten Zertifikate für Lösungsbenutzer bereitstellt. Wenn gemäß der Unternehmensrichtlinie Drittanbieterzertifikate einer Zertifizierungsstelle benötigt werden, können Sie die Lösungsbenutzerzertifikate durch Drittanbieterzertifikate einer Zertifizierungsstelle ersetzen. Wenn diese Zertifikate gültig sind, weist vCenter Single Sign On dem Lösungsbenutzer ein SAML-Token zu. Weitere Informationen hierzu finden Sie unter Verwenden benutzerdefinierter Zertifikate mit vSphere.

## Unterstützte Verschlüsselung

AES-Verschlüsselung, die den höchsten Verschlüsselungsgrad darstellt, wird unterstützt. Die unterstützte Verschlüsselung wirkt sich auf die Sicherheit aus, wenn vCenter Single Sign On Active Directory als Identitätsquelle verwendet.

Darüber hat sie immer dann eine Auswirkung auf die Sicherheit, wenn ein ESXi-Host oder vCenter Server zu Active Directory hinzugefügt wird.

# Komponenten für vCenter Single Sign On

vCenter Single Sign On umfasst den Security Token Service (STS), einen Verwaltungsserver, einen vCenter Lookup Service und den VMware-Verzeichnisdienst (vmdir). Der VMware-Verzeichnisdienst wird auch für die Zertifikatverwaltung eingesetzt.

Während der Installation werden die Komponenten als Teil einer eingebetteten Implementierung oder als Teil des Platform Services Controller bereitgestellt.

**STS (Security Token Service)**

Der STS-Dienst gibt Security Assertion Markup Language-Token (SAML) aus. Diese Sicherheitstoken stellen die Identität eines Benutzers in einem der von vCenter Single Sign On unterstützten Identitätsquellentypen dar. Die SAML-Token ermöglichen Benutzern und Lösungsbenutzern, die sich erfolgreich bei vCenter Single Sign On authentifizieren, jeden von vCenter Single Sign On unterstützten vCenter-Dienst zu verwenden, ohne sich erneut bei jedem Dienst authentifizieren zu müssen.

Der vCenter Single Sign On-Dienst signiert alle Token mit einem Signierzertifikat und speichert das Tokensignierzertifikat auf der Festplatte. Das Zertifikat für den Dienst selbst wird ebenfalls auf der Festplatte gespeichert.

**Verwaltungsserver**

Mithilfe des Verwaltungsservers können Benutzer, die über Administratorrechte für vCenter Single Sign On verfügen, den vCenter Single Sign On-Server konfigurieren und Benutzer und Gruppen auf dem vSphere Web Client verwalten. Anfänglich hat nur der Benutzer „administrator@*ihr_domänenname*“ diese Berechtigungen. In vSphere 5.5 war dieser Benutzer „administrator@vsphere.local“. In vSphere 6.0 können Sie die vSphere-Domäne ändern, wenn Sie vCenter Server installieren oder vCenter Server Appliance mit einem neuen Platform Services Controller bereitstellen. Benennen Sie die Domäne nicht mit Ihrem Microsoft Active Directory- oder OpenLDAP-Domänennamen.

**VMware Directory Service (vmdir)**

Der VMware Directory Service (vmdir) ist der Domäne zugeordnet, die Sie während der Installation angeben, und wird in jede eingebettete Bereitstellung sowie auf jedem Platform Services Controller eingeschlossen. Dieser Dienst ist ein mehrmandantenfähiger Multimaster-Verzeichnisdienst, der ein LDAP-Verzeichnis auf Port 389 zur Verfügung stellt. Der Dienst nutzt für Abwärtskompatibilität mit vSphere 5.5 und früheren Systemen nach wie vor Port 11711.

Wenn Ihre Umgebung mehr als eine Instanz des Platform Services Controller enthält, wird eine Aktualisierung des vmdir-Inhalts in einer vmdir-Instanz auf alle anderen Instanzen von vmdir propagiert.

Ab vSphere 6.0 speichert der VMware Directory Service nicht nur vCenter Single Sign On-Informationen, sondern auch Zertifikatsinformationen.

**Identitäts-Verwaltungsdienst**

Bearbeitete Identitätsquellen und STS-Authentifizierungsanforderungen.

## Auswirkungen von vCenter Single Sign On auf Installationen

vSphere beinhaltet ab Version 5.1 den vCenter Single Sign On-Dienst als Teil der vCenter Server-Managementinfrastruktur. Diese Änderung wirkt sich auf die vCenter Server-Installation aus.

Durch die Authentifizierung mit vCenter Single Sign On wird vSphere sicherer, da die vSphere-Softwarekomponenten miteinander über einen sicheren Token-Austauschmechanismus kommunizieren und sich alle anderen Benutzer ebenfalls mit vCenter Single Sign On authentifizieren.

Ab vSphere 6.0 ist vCenter Single Sign On entweder in einer eingebetteten Bereitstellung enthalten oder Bestandteil des Platform Services Controller. Der Platform Services Controller enthält alle Dienste, die für die Kommunikation zwischen vSphere-Komponenten erforderlich sind, darunter vCenter Single Sign On, VMware Certificate Authority, VMware Lookup Service und den Lizenzierungsdienst.

Die Installationsreihenfolge ist wichtig.

**Erste Installation**

Wenn Ihre Installation verteilt ist, müssen Sie den Platform Services Controller installieren, bevor Sie vCenter Server installieren oder die vCenter Server Appliance bereitstellen. Bei einer eingebetteten Bereitstellung wird die richtige Installationsreihenfolge automatisch eingehalten.

**Nachfolgende Installationen**

Für ca. bis zu vier vCenter Server-Instanzen kann ein Platform Services Controller die gesamte vSphere-Umgebung bedienen. Sie können die neuen vCenter Server-Instanzen mit dem gleichen Platform Services Controller verbinden. Für mehr als ca. vier vCenter Server-Instanzen können Sie einen zusätzlichen Platform Services Controller installieren, um die Leistung zu verbessern. Der vCenter Single Sign On-Dienst auf jedem Platform Services Controller synchronisiert Authentifizierungsdaten mit allen anderen Instanzen. Die genaue Zahl hängt neben anderen Faktoren davon ab, wie stark die vCenter Server-Instanzen genutzt werden.

Detaillierte Informationen über die Bereitstellungsmodelle und die Vor- und Nachteile der einzelnen Bereitstellungstypen finden Sie unter *Installation und Einrichtung von vCenter Server.*

## Verwenden von vCenter Single Sign On mit vSphere

Wenn sich ein Benutzer bei einer a vSphere-Komponente anmeldet oder wenn ein vCenter Server-Lösungsbenutzer auf einen anderen vCenter Server-Dienst zugreift, führt vCenter Single Sign On die Authentifizierung durch. Die Benutzer müssen bei vCenter Single Sign On authentifiziert sein und über die erforderlichen Rechte für die Interaktion mit vSphere-Objekten verfügen.

vCenter Single Sign On authentifiziert sowohl Lösungsbenutzer als auch andere Benutzer.

- Lösungsbenutzer stellen einen Satz von Diensten in Ihrer vSphere-Umgebung dar. Während der Installation weist VMCA standardmäßig jedem Lösungsbenutzer ein Zertifikat zu. Der Lösungsbenutzer authentifiziert sich mithilfe dieses Zertifikats bei vCenter Single Sign On. vCenter Single Sign On übergibt dem Lösungsbenutzer ein SAML-Token, und der Lösungsbenutzer kann dann mit anderen Diensten in der Umgebung interagieren.
- Wenn sich andere Benutzer bei der Umgebung anmelden, beispielsweise vom vSphere Client aus, werden sie von vCenter Single Sign On zur Eingabe eines Benutzernamens und Kennworts aufgefordert. Findet vCenter Single Sign On einen Benutzer mit diesen Anmeldedaten in der entsprechenden Identitätsquelle, wird dem Benutzer ein SAML-Token zugewiesen. Der Benutzer kann nun auf andere Dienste in der Umgebung zugreifen, ohne erneut zur Authentifizierung aufgefordert zu werden.

  vCenter Server-Berechtigungseinstellungen bestimmen in der Regel, welche Objekte der Benutzer anzeigen und welche Aufgaben er ausführen kann. vCenter Server-Administratoren weisen diese Berechtigungen über die Schnittstelle **Berechtigungen** im vSphere Web Client oder im vSphere Client zu, nicht über vCenter Single Sign On. Informationen finden Sie in der Dokumentation *vSphere-Sicherheit*.

## vCenter Single Sign On- und vCenter Server-Benutzer

Benutzer authentifizieren sich bei vCenter Single Sign On durch Eingabe ihrer Anmeldedaten auf der Anmeldeseite. Nach dem Herstellen der Verbindung mit vCenter Server können authentifizierte Benutzer alle vCenter Server-Instanzen oder andere vSphere-Objekte anzeigen, für die sie über die entsprechenden Rechte verfügen. Es ist keine weitere Authentifizierung erforderlich.

Nach der Installation hat der Administrator der vCenter Single Sign On-Domäne (standardmäßig „administrator@vsphere.local“) Administratorzugriff auf vCenter Single Sign On und vCenter Server. Dieser Benutzer kann anschließend Identitätsquellen hinzufügen, die standardmäßige Identitätsquelle festlegen und Benutzer und Gruppen in der vCenter Single Sign On-Domäne verwalten.

Alle Benutzer, die sich bei vCenter Single Sign On authentifizieren können, können ihr Kennwort zurücksetzen, selbst wenn das Kennwort abgelaufen ist. Sie müssen jedoch ihr Kennwort kennen. Weitere Informationen hierzu finden Sie unter Ändern des vCenter Single Sign On-Kennworts . Nur vCenter Single Sign On-Administratoren können das Kennwort für Benutzer zurücksetzen, die nicht mehr über ihr Kennwort verfügen.

**Hinweis** Wenn Sie das Kennwort für Ihr SDDC über den vSphere Client ändern, wird das neue Kennwort nicht mit dem Kennwort synchronisiert, das auf der Seite mit standardmäßigen vCenter-Anmeldedaten angezeigt wird. Auf dieser Seite werden nur die Standardanmeldedaten angezeigt. Wenn Sie die Anmeldedaten ändern, sind Sie dafür verantwortlich, das neue Kennwort zu speichern. Wenden Sie sich an den technischen Support und fordern Sie die Änderung des Kennworts an.

## vCenter Single Sign On-Administratorbenutzer

Die vCenter Single Sign On-Verwaltungsschnittstelle ist über den vSphere Client oder den vSphere Web Client zugänglich.

Um vCenter Single Sign On zu konfigurieren und vCenter Single Sign On-Benutzer und -Gruppen zu verwalten, muss sich der Benutzer „administrator@vsphere.local“ oder ein Benutzer in der vCenter Single Sign On-Administratorengruppe beim vSphere Client anmelden. Bei der Authentifizierung kann der Benutzer über den vCenter Single Sign On auf die vSphere Client-Verwaltungsschnittstelle zugreifen und Identitätsquellen und Standarddomänen verwalten, Kennwortrichtlinien angeben und andere Verwaltungsaufgaben durchführen.

**Hinweis** Sie können den vCenter Single Sign On-Administrator (standardmäßig „administrator@vsphere.local“ oder „administrator@*mydomain*“) nicht umbenennen, wenn Sie bei der Installation eine andere Domäne angegeben haben. Um die Sicherheit zu verbessern, können Sie zusätzliche benannte Benutzer in der vCenter Single Sign On-Domäne erstellen und ihnen Administratorrechte zuweisen. Verwenden Sie das Administratorkonto dann nicht mehr.

## ESXi-Benutzer

Eigenständige ESXi-Hosts werden nicht in vCenter Single Sign On oder im Platform Services Controller integriert. Weitere Informationen zum Hinzufügen eines ESXi-Hosts zu Active Directory finden Sie unter *vSphere-Sicherheit*.

Wenn Sie lokale ESXi-Benutzer für einen verwalteten ESXi-Host mit VMware Host Client, vCLI oder PowerCLI erstellen, erkennt vCenter Server diese Benutzer nicht. Das Erstellen von lokalen Benutzern kann daher verwirrend sein, insbesondere, wenn Sie dieselben Benutzernamen verwenden. Benutzer, die sich bei vCenter Single Sign On authentifizieren können, können ESXi-Hosts anzeigen und verwalten, wenn Sie über die erforderlichen Rechte für das ESXi-Hostobjekt verfügen.

**Hinweis** Verwalten Sie Berechtigungen für ESXi-Hosts nach Möglichkeit über vCenter Server.

## Vorgehensweise zum Anmelden bei vCenter Server-Komponenten

Sie können sich anmelden, indem Sie eine Verbindung zum vSphere Client oder zum vSphere Web Client herstellen.

Wenn sich ein Benutzer vom vSphere Client aus bei einem vCenter Server-System anmeldet, hängt das Anmeldeverhalten davon ab, ob der Benutzer sich in der Domäne befindet, die als Standard-Identitätsquelle festgelegt ist.

- Benutzer, die sich in der Standarddomäne befinden, können sich mit ihrem Benutzernamen und Kennwort anmelden.
- Benutzer in einer Domäne, die vCenter Single Sign On als Identitätsquelle hinzugefügt wurde, aber nicht die Standarddomäne ist, können sich bei vCenter Server anmelden, müssen dazu aber die Domäne mit einer der folgenden Methoden angeben.
  - Mit Präfix des Domänennamens, beispielsweise MEINEDOMÄNE\Benutzer1

  - Mit der Domäne, beispielsweise benutzer1@meinedomäne.com
- Benutzer in einer Domäne, die keine Identitätsquelle von vCenter Single Sign On ist, können sich nicht bei vCenter Server anmelden. Wenn die Domäne, die Sie in vCenter Single Sign On hinzufügen, zu einer Domänenhierarchie gehört, bestimmt Active Directory, ob die Benutzer anderer Domänen der Hierarchie authentifiziert werden oder nicht.

Wenn in Ihrer Umgebung eine Active Directory-Hierarchie vorhanden ist, finden Sie im VMware-Knowledgebase-Artikel 2064250 weitere Informationen zu unterstützten und nicht unterstützten Konfigurationen.

**Hinweis** Ab vSphere 6.0 Update 2 wird die zweistufige Authentifizierung unterstützt. Weitere Informationen hierzu finden Sie unter Grundlegendes zur zweistufigen vCenter Server-Authentifizierung.

## Gruppen in der vCenter Single Sign On-Domäne

Die vCenter Single Sign On-Domäne (standardmäßig „vsphere.local“) enthält verschiedene vordefinierte Gruppen. Fügen Sie einer dieser Gruppen Benutzer hinzu, damit sie die entsprechenden Aktionen ausführen können.

Weitere Informationen hierzu finden Sie unter Verwalten von vCenter Single Sign On-Benutzern und -Gruppen.

Berechtigungen für alle Objekte in der vCenter Server-Hierarchie können erteilt werden, indem ein Benutzer und eine Rolle einem Objekt zugewiesen werden. Sie können beispielsweise einen Ressourcenpool auswählen und einer Gruppe von Benutzern Leserechte für dieses Ressourcenpoolobjekt erteilen, indem Sie ihnen die entsprechende Rolle zuweisen.

Bei bestimmten Diensten, die nicht direkt von vCenter Serververwaltet werden, bestimmt die Mitgliedschaft in einer der vCenter Single Sign On -Gruppen die Berechtigungen. So kann ein Benutzer, der Mitglied der Administratorgruppe ist, vCenter Single Sign On verwalten. Ein Benutzer in der Gruppe CAAdmins kann die VMware Certificate Authority verwalten, ein Benutzer in der Gruppe LicenseService.Administrators kann Lizenzen verwalten.

Folgende Gruppen sind in vsphere.local vordefiniert.

**Hinweis** Viele davon bestehen nur innerhalb von vsphere.local oder geben Benutzern High-Level-Administratorrechte. Wägen Sie stets die Risiken ab, bevor Sie diesen Gruppen Benutzer hinzufügen.

**Hinweis** Löschen Sie keine vordefinierten Gruppen in der Domäne „vsphere.local“. Sollten Sie dies dennoch tun, treten möglicherweise Fehler bei der Authentifizierung oder Zertifikatbereitstellung auf.

Tabelle 2-1. Gruppen in der Domäne „vsphere.local“

| Recht | Beschreibung |
|---|---|
| Benutzer | Benutzer in der vCenter Single Sign On-Domäne (standardmäßig „vsphere.local“). |
| SolutionUsers | Gruppe der Lösungsbenutzer in vCenter-Diensten. Jeder Lösungsbenutzer authentifiziert sich mit einem Zertifikat einzeln bei vCenter Single Sign On. Standardmäßig liefert VMCA die Zertifikate für Lösungsbenutzer. Fügen Sie dieser Gruppe Mitglieder nicht explizit zu. |
| CAAdmins | Mitglieder der Gruppe CAAdmins besitzen Administratorrechte für VMCA. Fügen Sie dieser Gruppe ohne zwingende Gründe keine Mitglieder hinzu. |
| DCAdmins | Mitglieder der Gruppe DCAdmins dürfen Domänencontroller-Administratoraktionen im VMware Directory Service ausführen.<br>**Hinweis** Verwalten Sie den Domänencontroller nicht direkt. Verwenden Sie für die entsprechenden Aufgaben stattdessen die `vmdir`-CLI oder den vSphere Client. |
| SystemConfiguration.BashShellAdministrators | Diese Gruppe ist auf Bereitstellungen der vCenter Server Appliance beschränkt.<br>Ein Benutzer in dieser Gruppe kann den Zugriff auf die BASH-Shell aktivieren und deaktivieren. Standardmäßig können Benutzer, die sich über SSH mit der vCenter Server Appliance verbinden, nur Befehle in der eingeschränkten Shell verwenden. Benutzer in dieser Gruppe haben hingegen Zugriff auf die BASH-Shell. |
| ActAsUsers | Mitglieder der Gruppe „Act-As Users“ dürfen Act-As-Token aus vCenter Single Sign On abrufen. |
| ExternalIPDUsers | Diese interne Gruppe wird in vSphere nicht verwendet. VMware vCloud Air benötigt diese Gruppe. |
| SystemConfiguration.Administrators | Mitglieder der Gruppe „SystemConfiguration.Administrators“ können die Systemkonfiguration im vSphere Client anzeigen und verwalten. Diese Benutzer dürfen Dienste anzeigen, starten und neu starten, Fehlerbehebung in den Diensten ausführen und die verfügbaren Knoten anzeigen und verwalten. |
| DCClients | Diese Gruppe wird intern verwendet, um dem Verwaltungsknoten den Datenzugriff im VMware Directory Service zu ermöglichen.<br>**Hinweis** Nehmen Sie an dieser Gruppe keine Änderungen vor. Jedwede Änderung kann Ihre Zertifikatinfrastruktur beeinträchtigen. |
| ComponentManager.Administrators | Mitglieder der Gruppe ComponentManager.Administrators dürfen Component Manager-APIs abrufen, mit denen ein Dienst registriert oder dessen Registrierung aufgehoben werden kann. Das bedeutet, dass sie Dienste ändern können. Für einen reinen Lesezugriff auf die Dienste ist die Mitgliedschaft in dieser Gruppe nicht notwendig. |

Tabelle 2-1. Gruppen in der Domäne „vsphere.local“ (Fortsetzung)

| Recht | Beschreibung |
|---|---|
| LicenseService.Administrators | Mitglieder der Gruppe „LicenseService.Administrators“ haben vollständigen Schreibzugriff auf alle lizenzierungsbezogenen Daten und dürfen Seriennummernschlüssel für alle im Lizenzierungsdienst registrierten Produktassets hinzufügen, entfernen, zuweisen und widerrufen. |
| Administratoren | Administratoren des VMware Directory Service (vmdir). Mitglieder dieser Gruppe können Verwaltungsaufgaben in vCenter Single Sign On ausführen. Fügen Sie dieser Gruppe keine Mitglieder hinzu, es sei denn, Sie haben zwingende Gründe und kennen sich mit den Folgen aus. |

# Konfigurieren der vCenter Single Sign On-Identitätsquellen

Wenn sich ein Benutzer nur mit einem Benutzernamen anmeldet, überprüft vCenter Single Sign On für die Standardidentitätsquelle, ob sich dieser Benutzer authentifizieren kann. Wenn sich ein Benutzer anmeldet und einen Domänennamen im Anmeldebildschirm angibt, überprüft vCenter Single Sign On die angegebene Domäne, wenn diese Domäne als Identitätsquelle hinzugefügt wurde. Sie können Identitätsquellen hinzufügen und entfernen sowie den Standardwert ändern.

Sie konfigurieren vCenter Single Sign On über den vSphere Client. Um vCenter Single Sign On zu konfigurieren, müssen Sie über vCenter Single Sign On-Administratorrechte verfügen. vCenter Single Sign On-Administratorrechte unterscheiden sich von der Administratorrolle in vCenter Server oder ESXi. In einer neuen Installation kann sich nur der vCenter Single Sign On-Administrator (standardmäßig „administrator@vsphere.local“) bei vCenter Single Sign On authentifizieren.

- Identitätsquellen für vCenter Server mit vCenter Single Sign On

  Sie können Identitätsquellen verwenden, um vCenter Single Sign On eine oder mehrere Domänen hinzuzufügen. Bei einer Domäne handelt es sich um ein Repository für Benutzer und Gruppen, das der vCenter Single Sign On-Server für die Benutzerauthentifizierung verwenden kann.

- Festlegen der Standarddomäne für vCenter Single Sign On

  Jede vCenter Single Sign On-Identitätsquelle ist einer Domäne zugeordnet. vCenter Single Sign On verwendet die Standarddomäne zum Authentifizieren eines Benutzers, der sich ohne einen Domänennamen anmeldet. Benutzer, die einer Domäne angehören, bei der es sich nicht um die Standarddomäne handelt, müssen beim Anmelden den Domänennamen einschließen.

- Hinzufügen oder Bearbeiten einer vCenter Single Sign On-Identitätsquelle

  Benutzer können sich nur dann bei vCenter Server anmelden, wenn sie sich in einer Domäne befinden, die als vCenter Single Sign On-Identitätsquelle hinzugefügt wurde. vCenter Single Sign On-Benutzer mit Administratorrechten können Identitätsquellen hinzufügen oder die Einstellungen für Identitätsquellen ändern, die sie hinzugefügt haben.

- Verwenden von vCenter Single Sign On mit Windows-Sitzungsauthentifizierung

  Sie können vCenter Single Sign On mit der Windows-Sitzungsauthentifizierung (SSPI) verwenden. Sie müssen den Platform Services Controller mit einer Active Directory-Domäne verbinden, bevor Sie SSPI verwenden können.

## Identitätsquellen für vCenter Server mit vCenter Single Sign On

Sie können Identitätsquellen verwenden, um vCenter Single Sign On eine oder mehrere Domänen hinzuzufügen. Bei einer Domäne handelt es sich um ein Repository für Benutzer und Gruppen, das der vCenter Single Sign On-Server für die Benutzerauthentifizierung verwenden kann.

Ein Administrator kann Identitätsquellen hinzufügen, die Standardidentitätsquelle festlegen und Benutzer und Gruppen in der Identitätsquelle „vsphere.local“ erstellen.

Die Benutzer- und Gruppendaten werden in Active Directory, OpenLDAP oder lokal im Betriebssystem der Maschine, auf der vCenter Single Sign On installiert ist, gespeichert. Nach der Installation hat jede Instanz von vCenter Single Sign On die Identitätsquelle *your_domain_name*, z. B. „vsphere.local“. Diese Identitätsquelle ist für vCenter Single Sign On intern.

vCenter Server-Versionen vor Version 5.1 haben Active Directory und Benutzer des lokalen Betriebssystems als Benutzer-Repositorys unterstützt. Daher konnten lokale Betriebssystembenutzer sich immer beim vCenter Server-System authentifizieren. vCenter Server Version 5.1 und Version 5.5 verwenden vCenter Single Sign On für die Authentifizierung. Eine Aufstellung der für vSphere 5.1 unterstützten Identitätsquellen finden Sie in der Dokumentation zu vCenter Single Sign On 5.1. vCenter Single Sign On 5.5 unterstützt die folgenden Typen von Benutzer-Repositorys als Identitätsquellen, unterstützt aber nur eine einzige standardmäßige Identitätsquelle.

- Active Directory-Versionen 2003 und später. Wird als **Active Directory (integrierte Windows-Authentifizierung)** im vSphere Client angezeigt. Mit vCenter Single Sign On können Sie eine einzelne Active Directory-Domäne als Identitätsquelle angeben. Die Domäne kann untergeordnete Domänen haben, oder es kann sich dabei um eine Gesamtstruktur-Stammdomäne handeln. Im VMware-KB-Artikel 2064250 werden Microsoft Active Directory-Vertrauensstellungen behandelt, die von vCenter Single Sign On unterstützt werden.
- Active Directory über LDAP. vCenter Single Sign On unterstützt mehrere Active Directory-über LDAP-Identitätsquellen. Dieser Identitätsquellentyp wird zur Gewährleistung der Kompatibilität mit dem in vSphere 5.1 enthaltenen vCenter Single Sign On-Dienst bereitgestellt. Er wird als **Active Directory als ein LDAP-Server** im vSphere Client angezeigt.
- OpenLDAP Version 2.4 und höher. vCenter Single Sign On unterstützt mehrere OpenLDAP-Identitätsquellen. Wird als **OpenLDAP** im vSphere Client angezeigt.
- Benutzer des lokalen Betriebssystems. Benutzer des lokalen Betriebssystems sind lokale Benutzer in dem Betriebssystem, unter dem der vCenter Single Sign On-Server läuft. Die

Identitätsquelle des lokalen Betriebssystems existiert nur in einfachen vCenter Single Sign On-Serverbereitstellungen. In Bereitstellungen mit mehreren vCenter Single Sign On-Instanzen steht sie nicht zur Verfügung. Nur eine Identitätsquelle des lokalen Betriebssystems ist gestattet. Wird als **localos** im vSphere Client angezeigt.

**Hinweis** Verwenden Sie keine lokalen Betriebssystembenutzer, wenn sich der Platform Services Controller auf einer anderen Maschine als das vCenter Server-System befindet. Die Verwendung lokaler Betriebssystembenutzer kann bei einer eingebetteten Bereitstellung sinnvoll sein, wird jedoch nicht empfohlen.

- vCenter Single Sign On-Systembenutzer. Genau eine Systemidentitätsquelle wird bei der Installation von vCenter Single Sign On erstellt.

**Hinweis** Es ist jeweils immer nur eine Standarddomäne vorhanden. Wenn sich ein Benutzer aus einer Nicht-Standarddomäne anmeldet, muss dieser Benutzer den Domänennamen (*DOMAIN\user*) hinzufügen, um erfolgreich authentifiziert zu werden.

## Festlegen der Standarddomäne für vCenter Single Sign On

Jede vCenter Single Sign On-Identitätsquelle ist einer Domäne zugeordnet. vCenter Single Sign On verwendet die Standarddomäne zum Authentifizieren eines Benutzers, der sich ohne einen Domänennamen anmeldet. Benutzer, die einer Domäne angehören, bei der es sich nicht um die Standarddomäne handelt, müssen beim Anmelden den Domänennamen einschließen.

Wenn sich ein Benutzer vom vSphere Client aus bei einem vCenter Server-System anmeldet, hängt das Anmeldeverhalten davon ab, ob der Benutzer sich in der Domäne befindet, die als Standard-Identitätsquelle festgelegt ist.

- Benutzer, die sich in der Standarddomäne befinden, können sich mit ihrem Benutzernamen und Kennwort anmelden.
- Benutzer in einer Domäne, die vCenter Single Sign On als Identitätsquelle hinzugefügt wurde, aber nicht die Standarddomäne ist, können sich bei vCenter Server anmelden, müssen dazu aber die Domäne mit einer der folgenden Methoden angeben.
  - Mit Präfix des Domänennamens, beispielsweise MEINEDOMÄNE\Benutzer1
  - Mit der Domäne, beispielsweise benutzer1@meinedomäne.com
- Benutzer in einer Domäne, die keine Identitätsquelle von vCenter Single Sign On ist, können sich nicht bei vCenter Server anmelden. Wenn die Domäne, die Sie in vCenter Single Sign On hinzufügen, zu einer Domänenhierarchie gehört, bestimmt Active Directory, ob die Benutzer anderer Domänen der Hierarchie authentifiziert werden oder nicht.

### Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.

2 Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

   Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.

3 Navigieren Sie zur Benutzeroberfläche für die Konfiguration.

   a Wählen Sie im Menü **Home** die Option **Verwaltung** aus.

   b Klicken Sie unter **Single Sign-On** auf **Konfiguration**.

4 Klicken Sie auf **Identitätsquellen**, wählen Sie eine Identitätsquelle aus und klicken Sie auf **Als Standard festlegen**.

   In der Domänenansicht wird „(Standard)“ in der Spalte „Domäne“ für die Standarddomäne angezeigt.

## Hinzufügen oder Bearbeiten einer vCenter Single Sign On-Identitätsquelle

Benutzer können sich nur dann bei vCenter Server anmelden, wenn sie sich in einer Domäne befinden, die als vCenter Single Sign On-Identitätsquelle hinzugefügt wurde. vCenter Single Sign On-Benutzer mit Administratorrechten können Identitätsquellen hinzufügen oder die Einstellungen für Identitätsquellen ändern, die sie hinzugefügt haben.

Eine Identitätsquelle kann eine native Active Directory-Domäne (Integrierte Windows-Authentifizierung) oder ein OpenLDAP-Verzeichnisdienst sein. Active Directory ist als ein LDAP-Server verfügbar, um die Abwärtskompatibilität zu gewährleisten. Weitere Informationen hierzu finden Sie unter Identitätsquellen für vCenter Server mit vCenter Single Sign On.

Sofort nach der Installation sind die folgenden standardmäßigen Identitätsquellen und Benutzer verfügbar:

**localos**

Alle Benutzer des lokalen Betriebssystems. Wenn Sie ein Upgrade durchführen, können sich die `lokalen` Benutzer, die sich bereits authentifizieren können, auch weiterhin authentifizieren. Die Verwendung der `lokalen` Identitätsquelle ist für Umgebungen, in denen ein eingebetteter Platform Services Controller verwendet wird, nicht sinnvoll.

**vsphere.local**

Enthält die internen Benutzer von vCenter Single Sign On.

#### Voraussetzungen

Wenn Sie eine Active Directory-Identitätsquelle hinzufügen, muss sich die vCenter Server Appliance oder der Windows-Computer, auf dem vCenter Server ausgeführt wird, in der Active Directory-Domäne befinden. Weitere Informationen hierzu finden Sie unter Hinzufügen einer Platform Services Controller-Appliance zu einer Active Directory-Domäne.

Verfahren

1 Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.

2 Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

   Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.

3 Navigieren Sie zur Benutzeroberfläche für die Konfiguration.

   a Wählen Sie im Menü **Home** die Option **Verwaltung** aus.

   b Klicken Sie unter **Single Sign-On** auf **Konfiguration**.

4 Klicken Sie auf **Identitätsquellen** und anschließend auf **Identitätsquelle hinzufügen**.

5 Wählen Sie die Identitätsquelle aus und geben Sie die Einstellungen für die Identitätsquelle ein.

| Option | Beschreibung |
|---|---|
| **Active Directory (Integrierte Windows-Authentifizierung)** | Verwenden Sie diese Option für native Active Directory-Implementierungen. Die Maschine, auf der der vCenter Single Sign On-Dienst ausgeführt wird, muss sich in einer Active Directory-Domäne befinden, wenn Sie diese Option verwenden möchten.<br>Weitere Informationen hierzu finden Sie unter Einstellungen der Active Directory-Identitätsquelle. |
| **Active Directory über LDAP** | Diese Option ist verfügbar, um die Abwärtskompatibilität zu gewährleisten. Sie setzt voraus, dass Sie den Domänencontroller und andere Informationen angeben. Weitere Informationen hierzu finden Sie unter Einstellungen der Active Directory-Identitätsquelle für LDAP-Server und OpenLDAP-Server. |
| **OpenLDAP** | Verwenden Sie diese Option für eine OpenLDAP-Identitätsquelle. Weitere Informationen hierzu finden Sie unter Einstellungen der Active Directory-Identitätsquelle für LDAP-Server und OpenLDAP-Server. |
| **Lokales Betriebssystem des SSO-Servers** | Verwenden Sie diese Option für das lokale Betriebssystem des SSO-Servers. |

**Hinweis** Wenn das Benutzerkonto gesperrt oder deaktiviert ist, schlagen die Authentifizierungen sowie Gruppen- und Benutzersuchvorgänge in der Active Directory-Domäne fehl. Das Benutzerkonto muss über Nur-Lesen-Zugriff auf die Organisationseinheit (OU) „Benutzer und Gruppe“ verfügen und in der Lage sein, Benutzer- und Gruppenattribute zu lesen. Active Directory stellt diesen Zugriff standardmäßig zur Verfügung. Verwenden Sie einen speziellen Dienstbenutzer, um die Sicherheit zu verbessern.

6 Klicken Sie auf **Hinzufügen**.

### Nächste Schritte

Wenn eine Identitätsquelle hinzugefügt wird, können alle Benutzer authentifiziert werden, verfügen aber über die Rolle **Kein Zugriff**. Ein Benutzer mit vCenter Server**Modify.permissions**-Berechtigungen kann Benutzern oder Benutzergruppen Rechte erteilen. Die Rechte ermöglichen es Benutzern oder Gruppen, sich bei vCenter Server anzumelden und Objekte anzuzeigen und zu verwalten. Sie können Berechtigungen konfigurieren, damit Benutzer und Gruppen aus einer zusammengefügten Active Directory-Domäne auf die vCenter Server-Komponenten zugreifen können. Informationen finden Sie in der Dokumentation *vSphere-Sicherheit*.

## Einstellungen der Active Directory-Identitätsquelle

Wenn Sie den Identitätsquellentyp **Active Directory (Integrierte Windows-Authentifizierung)** auswählen, können Sie das Konto der lokalen Maschine als SPN (Service Principal Name, Dienstprinzipalname) auswählen oder einen SPN explizit angeben. Sie können diese Option nur verwenden, wenn der vCenter Single Sign On-Server einer Active Directory-Domäne beigetreten ist.

### Voraussetzungen für die Verwendung einer Active Directory-Identitätsquelle

Sie können vCenter Single Sign On so einrichten, dass nur dann eine Active Directory-Identitätsquelle verwendet wird, wenn diese Identitätsquelle verfügbar ist.

- Fügen Sie bei einer Windows-Installation den Windows-Computer der Active Directory-Domäne hinzu.
- Befolgen Sie für eine vCenter Server Appliance die Anweisungen in der Dokumentation zur *vCenter Server Appliance-Konfiguration*.

**Hinweis** Active Directory (integrierte Windows-Authentifizierung) verwendet immer der Stamm der Active Directory-Domänengesamtstruktur. Informationen zur Konfiguration der Identitätsquelle für integrierte Windows-Authentifizierung mit einer untergeordneten Domäne in der Active Directory-Gesamtstruktur finden Sie im VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/2070433.

Wählen Sie **Maschinenkonto verwenden** aus, um die Konfiguration zu beschleunigen. Wenn Sie die lokale Maschine, auf der vCenter Single Sign On ausgeführt wird, voraussichtlich umbenennen werden, empfiehlt sich die explizite Angabe eines SPN.

**Hinweis** In vSphere 5.5 verwendet vCenter Single Sign On das Maschinenkonto, selbst wenn Sie den SPN angeben. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/2087978.

Wenn Sie Protokollierung für Diagnoseereignisse in Active Directory aktiviert haben, um herauszufinden, an welcher Stelle Härtung notwendig sein könnte, wird unter Umständen ein Protokollereignis mit der Ereignis-ID 2889 auf diesem Verzeichnisserver angezeigt. Die Ereignis-ID 2889 wird bei Verwendung integrierter Windows-Authentifizierung eher als Anomalie denn als Sicherheitsrisiko erzeugt. Weitere Informationen zur Ereignis-ID 2889 finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/78644.

Tabelle 2-2. Hinzufügen von Einstellungen der Identitätsquelle

| Textfeld | Beschreibung |
| --- | --- |
| **Domänenname** | FQDN des Domänennamens, zum Beispiel „mydomain.com“. Geben Sie keine IP-Adresse an. Dieser Domänenname muss durch das vCenter Server-System per DNS auflösbar sein. Wenn Sie eine vCenter Server Appliance nutzen, verwenden Sie die Informationen zum Konfigurieren der Netzwerkeinstellungen, um die DNS-Servereinstellungen zu aktualisieren. |
| **Maschinenkonto verwenden** | Wählen Sie diese Option aus, um das Konto der lokalen Maschine als SPN zu verwenden. Mit dieser Option geben Sie nur den Domänennamen an. Verwenden Sie diese Option nicht, wenn Sie diese Maschine voraussichtlich umbenennen werden. |
| **SPN (Dienstprinzipalname) verwenden** | Wählen Sie diese Option aus, wenn Sie die lokale Maschine voraussichtlich umbenennen werden. Sie müssen einen SPN, einen Benutzer, der sich mit der Identitätsquelle authentifizieren kann, und ein Kennwort für den Benutzer angeben. |
| **SPN (Dienstprinzipalname)** | Der SPN, mit dem Kerberos den Active Directory-Dienst identifiziert. Schließen Sie die Domäne in den Namen ein. Beispiel: „`STS/example.com`“.<br>Der SPN muss innerhalb der Domäne eindeutig sein. Durch Ausführen von `setspn -S` wird sichergestellt, dass keine Duplikate erstellt werden. Weitere Informationen zu `setspn` finden Sie in der Microsoft-Dokumentation. |
| **UPN (Benutzerprinzipalname)**<br>**Kennwort** | Der Name und das Kennwort eines Benutzers, der sich mit dieser Identitätsquelle authentifizieren kann. Verwenden Sie beispielsweise folgendes E-Mail-Adressformat: „ `jchin@mydomain.com`“. Den Benutzerprinzipalnamen können Sie mit dem Active Directory-Dienstschnittstellen-Editor (ADSI Edit) überprüfen. |

## Einstellungen der Active Directory-Identitätsquelle für LDAP-Server und OpenLDAP-Server

Die Identitätsquelle „Active Directory über LDAP“ wird gegenüber der Option „Active Directory (Integrierte Windows-Authentifizierung)“ bevorzugt. Die Identitätsquelle für den OpenLDAP-Server ist für Umgebungen verfügbar, die OpenLDAP verwenden.

Wenn Sie eine OpenLDAP-Identitätsquelle konfigurieren, finden Sie weitere Informationen im VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/2064977.

**Hinweis** Ein zukünftiges Update auf Microsoft Windows ändert das Standardverhalten von Active Directory, sodass eine starke Authentifizierung und Verschlüsselung erforderlich sein wird. Diese Änderung wirkt sich auf die Authentifizierung von vCenter Server bei Active Directory aus. Wenn Sie Active Directory als Identitätsquelle für vCenter Server verwenden, müssen Sie die Aktivierung von LDAPS planen. Weitere Informationen zu diesem Microsoft-Sicherheitsupdate finden Sie unter https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023 und https://blogs.vmware.com/vsphere/2020/01/microsoft-ldap-vsphere-channel-binding-signing-adv190023.html.

Tabelle 2-3. Active Directory als LDAP-Server und OpenLDAP-Einstellungen

| Option | Beschreibung |
|---|---|
| Name | Name der Identitätsquelle |
| Basis-DN für Benutzer | Basis-DN (Distinguished Name) für Benutzer. Geben Sie den DN ein, von dem aus die Benutzersuche gestartet werden soll. Beispiel: cn=Users, dc=myCorp, dc=com. |
| Basis-DN für Gruppen | Der Basis-DN (Distinguished Name) für Gruppen. Geben Sie den DN ein, von dem aus die Gruppensuche gestartet werden soll. Beispiel: cn=Groups, dc=myCorp, dc=com. |
| Domänenname | Der vollständig qualifizierte Domänenname (FQDN) der Domäne. |
| Domänen-Alias | Für Active Directory-Identitätsquellen, der NetBIOS-Name der Domäne. Fügen Sie den NetBIOS-Namen der Active Directory-Domäne wie Alias der Identitätsquelle hinzu, wenn Sie SSPI-Authentifizierungen verwenden.<br>Für OpenLDAP-Identitätsquellen wird der Domänenname in Großbuchstaben hinzugefügt, wenn Sie keinen Alias angeben. |
| Benutzername | ID eines Benutzers in der Domäne, der über einen minimalen Base-DN-Zugriff (nur Lesen) für Benutzer und Gruppen verfügt Die ID kann in einem der folgenden Formate vorliegen:<br>■ UPN (user@domain.com)<br>■ NetBIOS (DOMAIN\user)<br>■ DN (cn=user,cn=Users,dc=domain,dc=com)<br>Der Benutzername muss vollqualifiziert sein. Ein Eintrag vom Typ „Benutzer“ funktioniert nicht. |
| Kennwort | Kennwort des Benutzers, der durch den **Benutzernamen** angegeben wird. |
| Verbinden mit | Domänencontroller, mit dem die Verbindung hergestellt werden soll. Kann ein beliebiger Domänencontroller in der Domäne oder ein bestimmter Controller sein. |

Tabelle 2-3. Active Directory als LDAP-Server und OpenLDAP-Einstellungen (Fortsetzung)

| Option | Beschreibung |
|---|---|
| URL des primären Servers | LDAP-Server des primären Domänencontrollers für die Domäne.<br>Verwenden Sie das Format **`ldap://hostname_or_IPaddress:port`** oder **`ldaps://hostname_or_IPaddress:port`**. Der Port ist in der Regel 389 für LDAP-Verbindungen und 636 für LDAPS-Verbindungen. Für Active Directory-Bereitstellungen über mehrere Domänencontroller ist der Port in der Regel 3268 für LDAP und 3269 für LDAPS.<br>Ein Zertifikat, das das Vertrauen für den LDAPS-Endpoint des Active Directory-Servers festlegt, ist erforderlich, wenn Sie **`ldaps://`** in der primären oder sekundären LDAP-URL verwenden. |
| URL des sekundären Servers | Adresse eines LDAP-Servers des sekundären Domänencontrollers, der für das Failover verwendet wird. |
| SSL-Zertifikate | Wenn Sie LDAPS mit Ihrer Identitätsquelle für den Active Directory-LDAP-Server oder -OpenLDAP-Server verwenden möchten, klicken Sie zum Auswählen eines Zertifikats auf **`Durchsuchen`**. Informationen zum Exportieren des Stammzertifikats aus Active Directory finden Sie in der Microsoft-Dokumentation. |

## Verwenden von vCenter Single Sign On mit Windows-Sitzungsauthentifizierung

Sie können vCenter Single Sign On mit der Windows-Sitzungsauthentifizierung (SSPI) verwenden. Sie müssen den Platform Services Controller mit einer Active Directory-Domäne verbinden, bevor Sie SSPI verwenden können.

Die Verwendung von SSPI beschleunigt das Anmeldeverfahren des Benutzers, der aktuell bei einem Computer angemeldet ist.

### Voraussetzungen

- Verbinden Sie die Platform Services Controller-Appliance oder den Windows-Computer, auf dem Platform Services Controller ausgeführt wird, mit einer Active Directory-Domäne. Weitere Informationen hierzu finden Sie unter Hinzufügen einer Platform Services Controller-Appliance zu einer Active Directory-Domäne.
- Vergewissern Sie sich, dass die Domäne ordnungsgemäß eingerichtet ist. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/2064250.
- Wenn Sie vSphere 6.0 und frühere Versionen verwenden, vergewissern Sie sich, dass das Client-Integrations-Plug-In installiert ist.

- Wenn Sie vSphere 6.5 und höher verwenden, vergewissern Sie sich, dass das Plug-In für erweiterte Authentifizierung installiert ist. Siehe *Installation und Einrichtung von vCenter Server*.

Verfahren

1 Navigieren Sie zur vSphere Client-Anmeldeseite.

2 Aktivieren Sie das Kontrollkästchen **Windows-Sitzungsauthentifizierung verwenden**.

3 Melden Sie sich mit dem Benutzernamen und dem Kennwort für Active Directory an.

   - Wenn es sich bei der Active Directory-Domäne um die Standard-Identitätsquelle handelt, melden Sie sich mit Ihrem Benutzernamen an, zum Beispiel „jlee“.
   - Schließen Sie andernfalls den Domänennamen ein, wie z. B. „jlee@example.com“.

# Grundlegendes zur zweistufigen vCenter Server-Authentifizierung

vCenter Single Sign On ermöglicht die Authentifizierung als Benutzer in einer Identitätsquelle, die vCenter Single Sign On bekannt ist, oder unter Verwendung der Windows-Sitzungsauthentifizierung. Sie können sich zudem mithilfe einer Smartcard (UPN-basierte allgemeine Zugriffskarte oder CAC) oder mithilfe eines RSA SecurID-Tokens authentifizieren.

## Zwei-Faktor-Authentifizierungsmethoden

Die Zwei-Faktor-Authentifizierungsmethoden sind oft bei staatlichen Behörden und großen Unternehmen erforderlich.

### Smartcard-Authentifizierung

Mit der Smartcard-Authentifizierung erhalten nur die Benutzer Zugriff, die eine physische Karte an das USB-Laufwerk des Computers anschließen, bei dem sie sich anmelden. Ein Beispiel ist die Authentifizierung mit einer allgemeinen Zugriffskarte (Common Access Card, CAC).

Der Administrator kann die PKI so bereitstellen, dass die Smartcard-Zertifikate die einzigen Clientzertifikate sind, die von der Zertifizierungsstelle ausgestellt werden. Für derartige Bereitstellungen werden dem Benutzer nur Smartcard-Zertifikate vorgelegt. Der Benutzer wählt ein Zertifikat aus und wird zur Eingabe der PIN aufgefordert. Es können sich nur diejenigen Benutzer anmelden, die sowohl über eine physische Karte als auch über die mit dem Zertifikat übereinstimmende PIN verfügen.

### RSA SecurID-Authentifizierung

Bei der RSA SecurID-Authentifizierung muss Ihre Umgebung einen ordnungsgemäß konfigurierten RSA Authentication Manager enthalten. Wenn der Platform Services Controller für den Verweis auf den RSA-Server konfiguriert wurde und die RSA SecurID-Authentifizierung aktiviert ist, können sich Benutzer mit ihren Benutzernamen und Token anmelden.

Informationen finden Sie in den zwei vSphere Blog-Beiträgen über die RSA SecurID-Einrichtung.

**Hinweis** vCenter Single Sign-On unterstützt nur die native SecurID-Authentifizierung. Die RADIUS-Authentifizierung wird nicht unterstützt.

## Angeben einer nicht standardmäßigen Authentifizierungsmethode

Administratoren können über den vSphere Client oder mit dem `sso-config`-Skript eine nicht standardmäßige Authentifizierungsmethode einrichten.

- Für die Smartcard-Authentifizierung können Sie das vCenter Single Sign-On-Setup über den vSphere Client oder unter Verwendung von `sso-config` vornehmen. Das Setup umfasst die Aktivierung der Smartcard-Authentifizierung und das Konfigurieren von Widerrufsrichtlinien für Zertifikate
- Bei RSA SecurID verwenden Sie das Skript `sso-config`, um RSA Authentication Manager für die Domäne zu konfigurieren und die RSA-Tokenauthentifizierung zu aktivieren. Sie können die RSA SecurID-Authentifizierung nicht über den vSphere Client konfigurieren. Wenn Sie RSA SecurID jedoch aktivieren, wird diese Authentifizierungsmethode im vSphere Client angezeigt.

## Kombinieren von Authentifizierungsmethoden

Mithilfe von `sso-config` können Sie jede Authentifizierungsmethode separat aktivieren bzw. deaktivieren. Lassen Sie anfänglich die Benutzernamen- und Kennwort-Authentifizierung aktiviert, während Sie eine zweistufige Authentifizierungsmethode testen, und aktivieren Sie nach dem Testen nur eine Authentifizierungsmethode.

## Anmeldung mit der Smartcard-Authentifizierung

Eine Chipkarte (Smartcard) ist eine kleine Plastikkarte mit einem integrierten Schaltkreis (Chip). Viele staatliche Behörden und große Unternehmen verwenden Smartcards wie die allgemeine Zugriffskarte (Common Access Card, CAC), um die Sicherheit ihrer Systeme zu erhöhen und bestehende Sicherheitsbestimmungen zu erfüllen. Eine Smartcard wird in Umgebungen verwendet, in denen an jeder Maschine ein Smartcard-Lesegerät vorhanden ist. Smartcard-Hardwaretreiber, die die Smartcard verwalten, sind üblicherweise vorinstalliert.

Benutzer, die sich bei einem vCenter Server- oder einem Platform Services Controller-System anmelden, werden dazu aufgefordert, sich wie folgt mit einer Smartcard und einer PIN-Kombination zu authentifizieren.

1 Wenn der Benutzer die Smartcard in ein Smartcard-Lesegerät einschiebt, liest vCenter Single Sign-On die Zertifikate auf der Karte.

2 vCenter Single Sign-On fordert den Benutzer zur Auswahl eines Zertifikats und anschließend zur Eingabe der PIN für dieses Zertifikat auf.

3 vCenter Single Sign-On überprüft, ob das Zertifikat auf der Smartcard bekannt und die PIN korrekt ist. Wenn die Überprüfung des Widerrufs eingeschaltet ist, überprüft vCenter Single Sign-On auch, ob das Zertifikat widerrufen wurde.

4 Wenn das Zertifikat bekannt ist und es sich nicht um ein widerrufenes Zertifikat handelt, wird der Benutzer authentifiziert und kann anschließend Aufgaben ausführen, über deren Berechtigungen er verfügt.

**Hinweis** Üblicherweise ist es sinnvoll, die Benutzernamen- und Kennwort-Authentifizierung während des Testens aktiviert zu lassen. Deaktivieren Sie nach Abschluss des Testens die Benutzernamen- und Kennwort-Authentifizierung und aktivieren Sie die Smartcard-Authentifizierung. Danach lassen der vSphere Client und der vSphere Web Client nur noch die Anmeldung per Smartcard zu. Nur Benutzer mit Root- oder Administratorberechtigungen auf der Maschine können die Benutzernamen- und Kennwort-Authentifizierung erneut aktivieren, indem sie sich direkt beim Platform Services Controller anmelden.

## Konfigurieren und Verwenden der Smartcard-Authentifizierung

Sie können Ihre Umgebung so einrichten, dass Smartcard-Authentifizierung erforderlich ist, wenn ein Benutzer eine Verbindung zu vCenter Server oder einem verknüpften Platform Services Controllerentweder über den vSphere Client oder den vSphere Web Client herstellt.

Die Art und Weise, wie Sie die Smartcard-Authentifizierung einrichten, hängt von der vSphere-Version ab, die Sie verwenden.

| vSphere-Version | Prozedur | Links |
|---|---|---|
| 6.0 Update 2<br>Neuere Versionen von vSphere 6.0 | 1 Richten Sie den Tomcat-Server ein.<br>2 Aktivieren und konfigurieren Sie die Smartcard-Authentifizierung. | vSphere 6.0-Dokumentationscenter |
| 6.5 und höher | 1 Richten Sie den Reverse-Proxy ein.<br>2 Aktivieren und konfigurieren Sie die Smartcard-Authentifizierung. | Konfigurieren des Reverse-Proxys zum Anfordern von Clientzertifikaten<br>Verwalten der Smartcard-Authentifizierung über die Befehlszeile<br>Verwalten der Smartcard-Authentifizierung |

### Konfigurieren des Reverse-Proxys zum Anfordern von Clientzertifikaten

Bevor Sie die Smartcard-Authentifizierung aktivieren, müssen Sie den Reverse-Proxy auf dem Platform Services Controller-System konfigurieren. Wenn in Ihrer Umgebung ein eingebetteter Platform Services Controller verwendet wird, führen Sie diese Aufgabe auf dem System aus, auf dem vCenter Server und der Platform Services Controller ausgeführt werden.

Eine Reverse-Proxy-Konfiguration ist in vSphere 6.5 und höher erforderlich.

### Voraussetzungen

Kopieren Sie die Zertifikate der Zertifizierungsstelle auf das Platform Services Controller-System.

### Verfahren

1 Melden Sie sich beim Platform Services Controller an.

| Betriebssystem | Beschreibung |
|---|---|
| **Appliance** | Melden Sie sich bei der Appliance-Shell als Root-Benutzer an. |
| **Windows** | Melden Sie sich bei einer Windows-Eingabeaufforderung als Administrator an. |

2 Erstellen Sie einen vertrauenswürdigen Client-Zertifizierungsstellenspeicher.

In diesem Speicher werden die Zertifikate der vertrauenswürdigen ausstellenden Zertifizierungsstelle für das Clientzertifikat gespeichert. Der Client ist hierbei der Browser, von dem aus der Smartcard-Prozess den Endbenutzer zur Eingabe von Informationen auffordert.

Im folgenden Beispiel wird verdeutlicht, wie Sie einen Zertifikatspeicher auf der Platform Services Controller-Appliance erstellen.

Für ein einzelnes Zertifikat:

```
cd /usr/lib/vmware-sso/
openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA.cer > /usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem
```

Für mehrere Zertifikate:

```
cd /usr/lib/vmware-sso/
openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA.cer >> /usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem
```

**Hinweis** Bei Platform Services Controller unter Windows verwenden Sie `C:\ProgramData\VMware\vCenterServer\runtime\VMwareSTSService\conf\` und ändern Sie den Befehl für die Verwendung von Rückwärtsschrägstrichen.

3 Erstellen Sie eine Sicherung der Datei `config.xml`, die die Reverse-Proxy-Definition enthält, und öffnen Sie `config.xml` in einem Editor.

| Betriebssystem | Beschreibung |
|---|---|
| **Appliance** | `/etc/vmware-rhttpproxy/config.xml` |
| **Windows** | `C:\ProgramData\VMware\vCenterServer\cfg\vmware-rhttpproxy\config.xml` |

4 Nehmen Sie die folgenden Änderungen vor und speichern Sie die Datei.

```
<http>
<maxConnections> 2048 </maxConnections>
```

```
<requestClientCertificate>true</requestClientCertificate>
<clientCertificateMaxSize>4096</clientCertificateMaxSize>
<clientCAListFile>/usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem</clientCAListFile>
</http>
```

Die Datei `config.xml` enthält einige dieser Elemente. Sie können nach Bedarf die Auskommentierung der Elemente aufheben, Elemente aktualisieren oder Elemente hinzufügen.

5 Starten Sie den Dienst neu.

| Betriebssystem | Beschreibung |
|---|---|
| **Appliance** | `/usr/lib/vmware-vmon/vmon-cli --restart rhttpproxy` |
| **Windows** | Starten Sie das Betriebssystem neu oder starten Sie VMware HTTP Reverse Proxy neu, indem Sie die folgenden Schritte ausführen:<br>a Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten.<br>b Führen Sie folgende Befehle aus:<br>`cd C:\Program Files\VMware\vCenter Server\bin`<br>`service-control --stop vmware-rhttpproxy`<br>`service-control --start vmware-rhttpproxy` |

## Verwalten der Smartcard-Authentifizierung über die Befehlszeile

Sie können das Dienstprogramm `sso-config` verwenden, um die Smartcard-Authentifizierung über die Befehlszeile zu verwalten. Das Dienstprogramm unterstützt alle Smartcard-Konfigurationsaufgaben.

Das `sso-config`-Skript befindet sich in folgenden Verzeichnissen:

| | |
|---|---|
| Windows | `C:\Programme\VMware\VCenter server\VMware Identity Services\sso-config.bat` |
| Linux | `/opt/vmware/bin/sso-config.sh` |

Die Konfiguration von unterstützten Authentifizierungstypen und Widerrufseinstellungen wird in VMware Directory Service gespeichert und über alle Platform Services Controller-Instanzen einer vCenter Single Sign-On-Domäne hinweg repliziert.

Wenn die Authentifizierung über den Benutzernamen und das Kennwort deaktiviert ist und falls Probleme mit der Smartcard-Authentifizierung auftreten, können sich die Benutzer nicht anmelden. In diesem Fall kann ein Root-Benutzer oder ein Administrator die Authentifizierung über den Benutzernamen und das Kennwort über die Platform Services Controller-Befehlszeile aktivieren. Mit dem folgenden Befehl wird die Authentifizierung über den Benutzernamen und das Kennwort aktiviert.

| Betriebssystem | Befehl |
| --- | --- |
| Windows | `sso-config.bat -set_authn_policy -pwdAuthn true -t <tenant_name>`<br><br>Wenn Sie den Standardmandanten verwenden, verwenden Sie „vsphere.local“ als Mandantenname. |
| Linux | `sso-config.sh -set_authn_policy -pwdAuthn true -t <tenant_name>`<br><br>Wenn Sie den Standardmandanten verwenden, verwenden Sie „vsphere.local“ als Mandantenname. |

Wenn Sie OCSP für den Zertifikatswiderruf verwenden, können Sie das in der AIA-Erweiterung des Smartcard-Zertifikats angegebene Standard-OCSP nutzen. Sie können die Standardeinstellung auch außer Kraft setzen und einen oder weitere alternative OCSP-Responder konfigurieren. Beispielsweise können Sie lokale OCSP-Responder für die vCenter Single Sign-On-Site einrichten, um die Anforderung des Zertifikatswiderrufs zu verarbeiten.

**Hinweis** Falls OCSP für Ihr Zertifikat nicht definiert ist, aktivieren Sie stattdessen CRL (Certificate Revocation List, Zertifikatswiderrufsliste).

Voraussetzungen

- Stellen Sie sicher, dass in Ihrer Umgebung Platform Services Controller Version 6.5 oder höher verwendet wird und dass Sie vCenter Server Version 6.0 oder höher verwenden. Platform Services Controller Version 6.0 Update 2 unterstützt die Smartcard-Authentifizierung, das Installationsverfahren ist aber unterschiedlich.
- Stellen Sie sicher, dass in Ihrer Umgebung ein Unternehmens-PKI-Schlüssel (Public Key Infrastructure) eingerichtet ist und die Zertifikate die folgenden Anforderungen erfüllen:
  - Ein Benutzerprinzipalname (User Principal Name, UPN) muss einem Active Directory-Konto in der Erweiterung „Alternativname für Betreff“ (SAN) entsprechen.
  - Im Zertifikat muss im Feld „Anwendungsrichtlinie“ oder „Erweiterte Schlüsselverwendung“ der Eintrag „Clientauthentifizierung“ angegeben sein, anderenfalls zeigt der Browser das Zertifikat nicht an.
- Stellen Sie sicher, dass das Platform Services Controller-Zertifikat für die Workstation des Endbenutzers vertrauenswürdig ist. Andernfalls unternimmt der Browser keinen Versuch zur Authentifizierung.
- Fügen Sie eine Active Directory-Identitätsquelle zu vCenter Single Sign-On hinzu.

- Weisen Sie die vCenter Server-Administratorrolle einem oder mehreren Benutzern in der Active Directory-Identitätsquelle zu. Diese Benutzer können nun Verwaltungsaufgaben durchführen, da sie berechtigt sind, sich zu authentifizieren und über Administratorrechte für vCenter Server verfügen.

  **Hinweis** Der Administrator der vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“, kann keine Smartcard-Authentifizierung durchführen.

- Richten Sie den Reverse-Proxy ein und starten Sie die physische oder die virtuelle Maschine neu.

**Verfahren**

1 Beziehen Sie die Zertifikate und kopieren Sie diese in einen Ordner, der für das `sso-config`-Dienstprogramm angezeigt wird.

| Option | Beschreibung |
|---|---|
| **Windows** | Melden Sie sich bei der Platform Services Controller-Windows-Installation an und verwenden Sie WinSCP oder ein ähnliches Dienstprogramm, um die Dateien zu kopieren. |
| **Appliance** | a Melden Sie sich bei der Appliance-Konsole entweder direkt oder mithilfe von SSH an.<br>b Aktivieren Sie die Appliance-Shell wie folgt:<br>`shell`<br>`chsh -s "/bin/bash" root`<br>c Kopieren Sie die Zertifikate mithilfe von WinSCP oder einem ähnlichen Dienstprogramm in das Verzeichnis `/usr/lib/vmware-sso/vmware-sts/conf` auf dem Platform Services Controller.<br>d Optional können Sie die Appliance-Shell wie folgt deaktivieren:<br>`chsh -s "/bin/appliancesh" root` |

2 Zur Aktivierung der Smartcard-Authentifizierung für VMware Directory Service (vmdir) führen Sie den folgenden Befehl aus:

```
sso-config.[bat|sh] -set_authn_policy -certAuthn true -cacerts
first_trusted_cert.cer,second_trusted_cert.cer  -t tenant
```

Beispiel:

```
sso-config.[bat|sh] -set_authn_policy -certAuthn true -cacerts
MySmartCA1.cer,MySmartCA2.cer  -t vsphere.local
```

Trennen Sie mehrere Zertifikate durch Kommas, aber fügen Sie nach den Kommas keine Leerzeichen ein.

3 Führen Sie zum Deaktivieren aller anderer Authentifizierungsmethoden die folgenden Befehle aus:

```
sso-config.[bat|sh] -set_authn_policy -pwdAuthn false -t vsphere.local
sso-config.sh -set_authn_policy -winAuthn false -t vsphere.local
sso-config.sh -set_authn_policy -securIDAuthn false -t vsphere.local
```

4 (Optional) Führen Sie zum Einrichten einer Whitelist der Zertifikatsrichtlinien den folgenden Befehl aus:

```
sso-config.[bat|sh] -set_authn_policy -certPolicies policies
```

Wenn Sie mehrere Richtlinien angeben möchten, trennen Sie diese durch ein Komma, z. B.:

```
sso-config.bat -set_authn_policy -certPolicies
2.16.840.1.101.2.1.11.9,2.16.840.1.101.2.1.11.19
```

In der Whitelist sind Objekt-IDs von Richtlinien angegeben, die in der Zertifikatsrichtlinienerweiterung das Zertifikat zugelassen sind. Ein X509-Zertifikat kann eine Zertifikatsrichtlinienerweiterung aufweisen.

5 (Optional) Aktivieren und konfigurieren Sie die Überprüfung des Widerrufs mittels OCSP.

a Aktivieren Sie die Überprüfung des Widerrufs mittels OCSP.

```
sso-config.[bat|sh]  -set_authn_policy -t tenantName  -useOcsp true
```

b Wenn der Link zum OCSP-Responder nicht von der AIA-Erweiterung der Zertifikate zur Verfügung gestellt wird, geben Sie die überschreibende OCSP-Responder-URL und das Zertifikat der OCSP-Zertifizierungsstelle an.

Das alternative OCSP wird für jede vCenter Single Sign-On-Site konfiguriert. Um ein Failover zu ermöglichen, können Sie mehrere alternative OCSP-Responder für Ihre vCenter Single Sign-On-Site angeben.

```
sso-config.[bat|sh] -t tenant -add_alt_ocsp  [-siteID yourPSCClusterID] -ocspUrl
http://ocsp.xyz.com/ -ocspSigningCert yourOcspSigningCA.cer
```

**Hinweis** Die Konfiguration wird standardmäßig auf die aktuelle vCenter Single Sign-On-Site angewendet. Geben Sie den Parameter `siteID` nur dann an, wenn Sie ein alternatives OCSP für andere vCenter Single Sign-On-Sites konfigurieren.

Betrachten Sie das folgende Beispiel.

```
 .sso-config.[bat|sh] -t vsphere.local -add_alt_ocsp
-ocspUrl http://failover.ocsp.nsn0.rcvs.nit.disa.mil/ -ocspSigningCert ./
DOD_JITC_EMAIL_CA-29__0x01A5__DOD_JITC_ROOT_CA_2.cer
 Adding alternative OCSP responder for tenant :vsphere.local
 OCSP responder is added successfully!
 [
 site::   78564172-2508-4b3a-b903-23de29a2c342
     [
     OCSP url::   http://ocsp.nsn0.rcvs.nit.disa.mil/
     OCSP signing CA cert:   binary value]
     ]
     [
     OCSP url::   http://failover.ocsp.nsn0.rcvs.nit.disa.mil/
     OCSP signing CA cert:   binary value]
     ]
 ]
```

c Führen Sie diesen Befehl aus, um die aktuellen Einstellungen für alternative OCSP-Responder anzuzeigen.

```
sso-config.[bat|sh] -t tenantName -get_alt_ocsp]
```

d Führen Sie diesen Befehl aus, um die aktuellen Einstellungen für alternative OCSP-Responder zu entfernen.

```
sso-config.[bat|sh] -t tenantName -delete_alt_ocsp [-allSite] [-siteID
pscSiteID_for_the_configuration]
```

6 (Optional) Führen Sie zum Auflisten der Konfigurationsinformationen den folgenden Befehl aus:

```
sso-config.[bat|sh] -get_authn_policy -t tenantName
```

## Verwalten der Smartcard-Authentifizierung

Über den vSphere Client können Sie die Smartcard-Authentifizierung aktivieren und deaktivieren, das Anmelde-Banner anpassen und die Widerrufsrichtlinie einrichten.

Wenn die Smartcard-Authentifizierung aktiviert ist und andere Authentifizierungsmethoden deaktiviert sind, müssen Benutzer sich mit der Smartcard-Authentifizierung anmelden.

Wenn die Authentifizierung über den Benutzernamen und das Kennwort deaktiviert ist und falls Probleme mit der Smartcard-Authentifizierung auftreten, können sich die Benutzer nicht anmelden. In diesem Fall kann ein Root-Benutzer oder ein Administrator die Authentifizierung über den Benutzernamen und das Kennwort über die Platform Services Controller-Befehlszeile aktivieren. Mit dem folgenden Befehl wird die Authentifizierung über den Benutzernamen und das Kennwort aktiviert.

| Betriebssystem | Befehl |
|---|---|
| Windows | `sso-config.bat -set_authn_policy -pwdAuthn true -t <tenant_name>`<br>Wenn Sie den Standardmandanten verwenden, verwenden Sie „vsphere.local“ als Mandantenname. |
| Linux | `sso-config.sh -set_authn_policy -pwdAuthn true -t <tenant_name>`<br>Wenn Sie den Standardmandanten verwenden, verwenden Sie „vsphere.local“ als Mandantenname. |

### Voraussetzungen

- Stellen Sie sicher, dass in Ihrer Umgebung Platform Services Controller Version 6.5 oder höher verwendet wird und dass Sie vCenter Server Version 6.0 oder höher verwenden. Platform Services Controller Version 6.0 Update 2 unterstützt die Smartcard-Authentifizierung, das Installationsverfahren ist aber unterschiedlich.
- Stellen Sie sicher, dass in Ihrer Umgebung ein Unternehmens-PKI-Schlüssel (Public Key Infrastructure) eingerichtet ist und die Zertifikate die folgenden Anforderungen erfüllen:
  - Ein Benutzerprinzipalname (User Principal Name, UPN) muss einem Active Directory-Konto in der Erweiterung „Alternativname für Betreff“ (SAN) entsprechen.
  - Im Zertifikat muss im Feld „Anwendungsrichtlinie“ oder „Erweiterte Schlüsselverwendung“ der Eintrag „Clientauthentifizierung“ angegeben sein, anderenfalls zeigt der Browser das Zertifikat nicht an.

- Stellen Sie sicher, dass das Platform Services Controller-Zertifikat für die Workstation des Endbenutzers vertrauenswürdig ist. Andernfalls unternimmt der Browser keinen Versuch zur Authentifizierung.
- Fügen Sie eine Active Directory-Identitätsquelle zu vCenter Single Sign-On hinzu.
- Weisen Sie die vCenter Server-Administratorrolle einem oder mehreren Benutzern in der Active Directory-Identitätsquelle zu. Diese Benutzer können nun Verwaltungsaufgaben durchführen, da sie berechtigt sind, sich zu authentifizieren und über Administratorrechte für vCenter Server verfügen.

  **Hinweis** Der Administrator der vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“, kann keine Smartcard-Authentifizierung durchführen.

- Richten Sie den Reverse-Proxy ein und starten Sie die physische oder die virtuelle Maschine neu.

**Verfahren**

1 Beziehen Sie die Zertifikate und kopieren Sie diese in einen Ordner, der für das `sso-config`-Dienstprogramm angezeigt wird.

| Option | Beschreibung |
|---|---|
| **Windows** | Melden Sie sich bei der Platform Services Controller-Windows-Installation an und verwenden Sie WinSCP oder ein ähnliches Dienstprogramm, um die Dateien zu kopieren. |
| **Appliance** | a Melden Sie sich bei der Appliance-Konsole entweder direkt oder mithilfe von SSH an.<br>b Aktivieren Sie die Appliance-Shell wie folgt:<br>`shell`<br>`chsh -s "/bin/bash" root`<br>`csh -s "bin/appliance/sh" root`<br>c Kopieren Sie die Zertifikate mithilfe von WinSCP oder einem ähnlichen Dienstprogramm in das Verzeichnis `/usr/lib/vmware-sso/vmware-sts/conf` auf dem Platform Services Controller.<br>d Optional können Sie die Appliance-Shell wie folgt deaktivieren:<br>`chsh -s "/bin/appliancesh" root` |

2 Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.

3 Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.

4 Navigieren Sie zur Benutzeroberfläche für die Konfiguration.

   a Wählen Sie im Menü **Home** die Option **Verwaltung** aus.

   b Klicken Sie unter **Single Sign-On** auf **Konfiguration**.

5 Klicken Sie unter **Smartcard-Authentifizierung** auf **Bearbeiten**.

6 Aktivieren oder deaktivieren Sie Authentifizierungsmethoden und klicken Sie auf **Speichern**.

   Sie können entweder nur die Smartcard-Authentifizierung oder sowohl die Smartcard-Authentifizierung als auch die Windows-Sitzungsauthentifizierung mit Kennwort auswählen.

   Das Aktivieren bzw. Deaktivieren der RSA SecurID-Authentifizierung ist über diese Webschnittstelle nicht möglich. Wenn RSA SecurID jedoch über die Befehlszeile aktiviert wurde, wird der Status in der Webschnittstelle angezeigt.

   Die Registerkarte **Zertifikate von vertrauenswürdiger Zertifizierungsstelle** wird angezeigt.

7 Klicken Sie auf der Registerkarte **Zertifikate von vertrauenswürdiger Zertifizierungsstelle** auf **Hinzufügen** und dann auf **Durchsuchen**.

8 Wählen Sie alle Zertifikate von vertrauenswürdigen Zertifizierungsstellen und klicken Sie auf **Hinzufügen**.

#### Nächste Schritte

Möglicherweise ist in Ihrer Umgebung die erweiterte OCSP-Konfiguration erforderlich.

- Falls Ihre OCSP-Antwort von einer anderen Zertifizierungsstelle als der signierenden Zertifizierungsstelle der Smartcard ausgegeben wird, geben Sie das OCSP-Signaturzertifikat der Zertifizierungsstelle an.
- Sie können einen oder mehrere lokale OCSP-Responder für jede Platform Services Controller-Site in einer Umgebung mit mehreren Sites konfigurieren. Diese alternativen OCSP-Responder können über die CLI konfiguriert werden. Weitere Informationen hierzu finden Sie unter Verwalten der Smartcard-Authentifizierung über die Befehlszeile.

## Festlegen von Widerrufsrichtlinien für die Smartcard-Authentifizierung

Sie können die Überprüfung des Zertifikatswiderrufs anpassen und angeben, wo vCenter Single Sign-On nach Informationen über widerrufene Zertifikate suchen soll.

Sie können das Verhalten mithilfe des vSphere Client oder mithilfe des Skripts `sso-config` anpassen. Die auszuwählenden Einstellungen hängen teilweise von der Unterstützung der Zertifizierungsstelle ab.

- Wenn die Überprüfung des Widerrufs deaktiviert ist, ignoriert vCenter Single Sign-On alle Einstellungen für die Zertifikatswiderrufsliste (Certificate Revocation List, CRL) oder das Onlinestatusprotokoll des Zertifikats (Online Certificate Status Protocol, OCSP). vCenter Single Sign-On führt keine Zertifikatüberprüfungen durch.

- Wenn die Überprüfung des Widerrufs aktiviert ist, hängt das empfohlene Setup vom PKI-Setup ab.

  **Nur OCSP**

  Wenn die ausstellende Zertifizierungsstelle einen OCSP-Responder unterstützt, aktivieren Sie **OCSP** und deaktivieren Sie **CRL als Failover für OCSP**.

  **Nur CRL**

  Wenn die ausstellende Zertifizierungsstelle OCSP nicht unterstützt, aktivieren Sie die **CRL-Überprüfung** und deaktivieren Sie die **OSCP-Überprüfung**.

  **OSCP und CRL**

  Wenn die ausstellende Zertifizierungsstelle sowohl einen OCSP-Responder als auch CRL unterstützt, überprüft vCenter Single Sign-On zuerst den OCSP-Responder. Wenn der Responder einen unbekannten Status zurückgibt oder nicht verfügbar ist, überprüft vCenter Single Sign-On die CRL. Aktivieren Sie in diesem Fall sowohl die **OCSP-Überprüfung** als auch die **CRL-Überprüfung** und aktivieren Sie **CRL als Failover für OCSP**.

- Wenn die Überprüfung des Widerrufs aktiviert ist, können fortgeschrittene Benutzer die folgenden zusätzlichen Einstellungen angeben.

  **OSCP-URL**

  vCenter Single Sign-On überprüft standardmäßig den Speicherort des OCSP-Responders, der im validierten Zertifikat definiert ist. Wenn die Erweiterung „Zugriff auf Zertifizierungsstelleninfos“ im Zertifikat nicht vorhanden ist oder Sie sie überschreiben möchten, können Sie explizit einen Speicherort angeben.

  **CRL aus Zertifikat verwenden**

  vCenter Single Sign-On überprüft standardmäßig den Speicherort der CRL, die im validierten Zertifikat definiert ist. Deaktivieren Sie diese Option, wenn im Zertifikat die Erweiterung „CRL-Verteilungspunkt“ nicht vorhanden ist oder Sie den Standard überschreiben möchten.

  **CRL-Speicherort**

  Verwenden Sie diese Eigenschaft, wenn Sie **CRL aus Zertifikat verwenden** deaktivieren und einen Speicherort angeben möchten (Datei oder HTTP-URL), an dem die CRL gespeichert wird.

Sie können durch das Hinzufügen einer Zertifikatsrichtlinie weiter einschränken, welche Zertifikate von vCenter Single Sign-On akzeptiert werden sollen.

Voraussetzungen

- Stellen Sie sicher, dass in Ihrer Umgebung Platform Services Controller Version 6.5 oder höher verwendet wird und dass Sie vCenter Server Version 6.0 oder höher verwenden. Platform Services Controller Version 6.0 Update 2 unterstützt die Smartcard-Authentifizierung, das Installationsverfahren ist aber unterschiedlich.

- Stellen Sie sicher, dass in Ihrer Umgebung ein Unternehmens-PKI-Schlüssel (Public Key Infrastructure) eingerichtet ist und die Zertifikate die folgenden Anforderungen erfüllen:
  - Ein Benutzerprinzipalname (User Principal Name, UPN) muss einem Active Directory-Konto in der Erweiterung „Alternativname für Betreff“ (SAN) entsprechen.
  - Im Zertifikat muss im Feld „Anwendungsrichtlinie“ oder „Erweiterte Schlüsselverwendung“ der Eintrag „Clientauthentifizierung“ angegeben sein, anderenfalls zeigt der Browser das Zertifikat nicht an.
- Stellen Sie sicher, dass das Platform Services Controller-Zertifikat für die Workstation des Endbenutzers vertrauenswürdig ist. Andernfalls unternimmt der Browser keinen Versuch zur Authentifizierung.
- Fügen Sie eine Active Directory-Identitätsquelle zu vCenter Single Sign-On hinzu.
- Weisen Sie die vCenter Server-Administratorrolle einem oder mehreren Benutzern in der Active Directory-Identitätsquelle zu. Diese Benutzer können nun Verwaltungsaufgaben durchführen, da sie berechtigt sind, sich zu authentifizieren und über Administratorrechte für vCenter Server verfügen.

**Hinweis** Der Administrator der vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“, kann keine Smartcard-Authentifizierung durchführen.

Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.
2. Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

   Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.
3. Navigieren Sie zur Benutzeroberfläche für die Konfiguration.
   a. Wählen Sie im Menü **Home** die Option **Verwaltung** aus.
   b. Klicken Sie unter **Single Sign-On** auf **Konfiguration**.
4. Klicken Sie auf **Smartcard-Authentifizierung**.
5. Klicken Sie auf **Zertifikatwiderruf** und dann auf **Bearbeiten**, um die Überprüfung des Widerrufs zu aktivieren oder zu deaktivieren.
6. Falls in Ihrer Umgebung Zertifikatsrichtlinien gelten, können Sie im Bereich **Zertifikatsrichtlinien** eine Richtlinie hinzufügen.

## Einrichten der RSA SecurID-Authentifizierung

Sie können Ihre Umgebung so einrichten, dass sich Benutzer mit einem RSA SecurID-Token anmelden müssen. Die Einrichtung von SecurID wird nur von der Befehlszeile unterstützt.

Informationen finden Sie in den zwei vSphere Blog-Beiträgen über die RSA SecurID-Einrichtung.

**Hinweis** RSA Authentication Manager gibt vor, dass die Benutzer-ID ein eindeutiger Bezeichner ist, der 1 bis 255 ASCII-Zeichen enthalten kann. Das Kaufmannszeichen (&), Prozentsymbol (%), Größer als (>), Kleiner als (<) und das einfache Anführungszeichen (`) sind nicht zulässig.

### Voraussetzungen

- Beim Konfigurieren von RSA SecurID unterstützt vCenter Single Sign-On (SSO) die Nutzung des Benutzerprinzipalnamens (Attribut „userPrincipalName“) nur als Benutzer-ID, wenn Integrated Windows Authentication (IWA) als Identitätsquelle für RSA-Benutzer konfiguriert ist.
- Stellen Sie sicher, dass in Ihrer Umgebung Platform Services Controller Version 6.5 oder höher verwendet wird und dass Sie vCenter Server Version 6.0 oder höher verwenden. Platform Services Controller Version 6.0 Update 2 unterstützt die Smartcard-Authentifizierung, das Installationsverfahren ist aber unterschiedlich.
- Stellen Sie sicher, dass RSA Authentication Manager in Ihrer Umgebung ordnungsgemäß konfiguriert wurde und dass Benutzer über RSA-Token verfügen. RSA Authentication Manager Version 8.0 oder höher ist erforderlich.
- Stellen Sie sicher, dass die von RSA Manager verwendete Identitätsquelle zu vCenter Single Sign-On hinzugefügt wurde. Weitere Informationen hierzu finden Sie unter Hinzufügen oder Bearbeiten einer vCenter Single Sign On-Identitätsquelle.
- Stellen Sie sicher, dass das RSA Authentication Manager-System den Platform Services Controller-Hostnamen auflösen kann und dass das Platform Services Controller-System den RSA Authentication Manager-Hostnamen auflösen kann.
- Exportieren Sie die Datei `sdconf.rec` aus dem RSA Manager, indem Sie **Zugriff > Authentifizierungsagenten > Konfigurationsdatei generieren** auswählen. Dekomprimieren Sie die resultierende Datei `AM_Config.zip` und suchen Sie nach der Datei `sdconf.rec`.
- Kopieren Sie die Datei `sdconf.rec` in den Platform Services Controller-Knoten.

### Verfahren

1 Wechseln Sie in das Verzeichnis, in dem sich das Skript `sso-config` befindet.

| Option | Beschreibung |
|---|---|
| **Windows** | `C:\Program Files\VMware\VCenter server\VMware Identity Services` |
| **Appliance** | `/opt/vmware/bin` |

2 Führen Sie zum Aktivieren der RSA SecurID-Authentifizierung den folgenden Befehl aus:

```
sso-config.[sh|bat]  -t tenantName  -set_authn_policy -securIDAuthn true
```

*tenantName* ist der Name der vCenter Single Sign-On-Domäne (standardmäßig „vsphere.local“).

3 (Optional) Führen Sie zum Deaktivieren anderer Authentifizierungsmethoden den folgenden Befehl aus:

```
sso-config.sh -set_authn_policy -pwdAuthn false -winAuthn false -certAuthn false -t
vsphere.local
```

4 Um die Umgebung so zu konfigurieren, dass der Mandant an der aktuellen Site die RSA-Site verwendet, führen Sie den folgenden Befehl aus.

```
sso-config.[sh|bat] -set_rsa_site [-t tenantName] [-siteID Location] [-agentName Name] [-
sdConfFile Path]
```

Beispiel:

```
sso-config.sh -set_rsa_site -agentName SSO_RSA_AUTHSDK_AGENT -sdConfFile /tmp/sdconf.rec
```

Sie können die folgenden Optionen angeben.

| Option | Beschreibung |
|---|---|
| **siteID** | Optionale Platform Services Controller-Site-ID. Platform Services Controller unterstützt eine RSA Authentication Manager-Instanz bzw. ein Cluster pro Site. Wenn Sie diese Option nicht explizit festlegen, gilt die RSA-Konfiguration für die aktuelle Platform Services Controller-Site. Verwenden Sie diese Option nur, wenn Sie eine andere Site hinzufügen. |
| **agentName** | Definiert in RSA Authentication Manager. |
| **sdConfFile** | Kopie der Datei `sdconf.rec`, die aus dem RSA Manager heruntergeladen wurde und Informationen zur Konfiguration für den RSA Manager enthält, wie z. B. die IP-Adresse. |

5 (Optional) Um die Mandantenkonfiguration auf nicht standardmäßige Werte zu ändern, führen Sie den folgenden Befehl aus.

```
sso-config.[sh|bat] -set_rsa_config [-t tenantName] [-logLevel Level] [-logFileSize
Size] [-maxLogFileCount Count] [-connTimeOut Seconds] [-readTimeOut Seconds] [-encAlgList
Alg1,Alg2,...]
```

Die Standardwerte sind normalerweise angemessen, z.B.:

```
sso-config.sh -set_rsa_config -t vsphere.local -logLevel DEBUG
```

6 (Optional) Wenn Ihre Identitätsquelle nicht den Benutzerprinzipalnamen als Benutzer-ID verwendet, konfigurieren Sie die Identitätsquelle als userID-Attribut. (Wird nur bei Active Directory über LDAP-Identitätsquellen unterstützt.)

Das Attribut „userID“ bestimmt, welches LDAP-Attribut als RSA-Benutzer-ID verwendet wird.

```
sso-config.[sh|bat] -set_rsa_userid_attr_map [-t tenantName] [-idsName Name] [-ldapAttr AttrName] [-siteID Location]
```

Beispiel:

```
sso-config.sh -set_rsa_userid_attr_map -t vsphere.local -idsName ssolabs.com -ldapAttr userPrincipalName
```

7 Um die aktuellen Einstellungen anzuzeigen, führen Sie den folgenden Befehl aus.

```
sso-config.sh -t tenantName -get_rsa_config
```

### Ergebnisse

Wenn die Authentifizierung mit Benutzername und Kennwort deaktiviert und die RSA-Authentifizierung aktiviert ist, müssen Benutzer sich mit ihrem Benutzernamen und dem RSA-Token anmelden. Die Anmeldung mit Benutzername und Kennwort ist nicht mehr möglich.

**Hinweis** Verwenden Sie das Benutzernamensformat ***BenutzerID@Domänenname*** oder ***BenutzerID@Domänen_UPN_Suffix***.

## Verwalten der Anmeldenachricht

In Ihre Umgebung können Sie eine Anmeldenachricht einschließen. Sie können die Anmeldenachricht aktivieren und deaktivieren sowie fordern, dass Benutzer für die ausdrückliche Zustimmung auf ein Kontrollkästchen klicken müssen.

### Verfahren

1 Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.

2 Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.

3 Navigieren Sie zur Benutzeroberfläche für die Konfiguration.

a Wählen Sie im Menü **Home** die Option **Verwaltung** aus.

b Klicken Sie unter **Single Sign-On** auf **Konfiguration**.

4 Klicken Sie auf die Registerkarte **Anmeldenachricht** .

5 Klicken Sie auf **Bearbeiten** und konfigurieren Sie die Anmeldenachricht.

| Option | Beschreibung |
|---|---|
| **Anmeldenachricht anzeigen** | Schalten Sie **Anmeldenachricht anzeigen** ein, um die Anmeldenachricht zu aktivieren. Sie können keine Änderungen an der Anmeldenachricht vornehmen, ohne vorher diesen Schalter umzulegen. |
| **Anmeldenachricht** | Titel der Nachricht. Wenn **Zustimmung durch Kontrollkästchen** eingeschaltet ist, lautet der Text der Anmeldenachricht standardmäßig `I agree to Terms and Conditions`. Sie müssen `Terms and Conditions` mit Ihrem eigenen Text ersetzen. Wenn das **Zustimmungskontrollkästchen** deaktiviert ist, erscheint `Login message`, über dem Sie Ihre Nachricht eingeben können. |
| **Kontrollkästchen für Zustimmung** | Schalten Sie **Zustimmung durch Kontrollkästchen** ein, damit der Benutzer vor der Anmeldung ein Kontrollkästchen aktivieren muss. Sie können auch eine Meldung ohne Kontrollkästchen anzeigen. |
| **Details der Anmeldenachricht** | Meldung, die angezeigt wird, wenn ein Benutzer auf die Anmeldenachricht klickt, z. B. der Text der Nutzungsbedingungen. Sie müssen einige Details in dieses Textfeld eingeben. |

6 Klicken Sie auf **Speichern**.

# Verwenden von vCenter Single Sign On als Identitätsanbieter für andere Identitätsanbieter

Der vSphere Web Client wird bei vCenter Single Sign-On automatisch als vertrauenswürdiger SAML 2.0-Dienstanbieter (SP) registriert. Sie können der Identity Federation weitere vertrauenswürdige Dienstanbieter hinzufügen, wobei vCenter Single Sign-On als SAML-Identitätsprovider (IDP) fungiert. Die Dienstanbieter müssen dem SAML 2.0-Protokoll entsprechen. Nachdem die Federation eingerichtet wurde, gewährt der Dienstanbieter einem Benutzer Zugriff, wenn dieser sich bei vCenter Single Sign On identifizieren kann.

**Hinweis** vCenter Single Sign On kann der IDP für andere SPs sein.vCenter Single Sign On kann kein SP sein, einen anderen IDP verwendet.

Ein registrierter SAML-Dienstanbieter kann einem Benutzerzugriff gewähren, der sich bereits in einer Live-Sitzung befindet, d. h. beim Identitätsprovider angemeldet ist. vRealize Automation 7.0 und höher unterstützt beispielsweise vCenter Single Sign On als Identitätsanbieter. Sie können eine Federation über vCenter Single Sign On und über vRealize Automation einrichten. Anschließend kann vCenter Single Sign On die Authentifizierung durchführen, wenn Sie sich bei vRealize Automation anmelden.

Um der Identity Federation einen SAML-Dienstanbieter hinzuzufügen, müssen Sie zwischen SP und IPD das Vertrauen einrichten, in dem Sie die SAML-Metadaten zwischen ihnen austauschen.

Sie müssen Integrationsaufgaben sowohl für vCenter Single Sign On als auch für den Dienst ausführen, der vCenter Single Sign On verwendet.

1 Exportieren Sie die IDP-Metadaten in eine Datei und importieren Sie sie anschließend in den SP.

2 Exportieren Sie die SP-Metadaten und importieren Sie sie in den IDP.

Zum Exportieren der IDP-Metadaten und zum Importieren der Metadaten vom SP können Sie die vSphere Web Client-Schnittstelle zu vCenter Single Sign On verwenden. Bei Verwendung von vRealize Automation als SP finden Sie Details zum Exportieren der SP-Metadaten und zum Importieren der IDP-Metadaten in der Dokumentation zu vRealize Automation.

**Hinweis** Der Dienst muss den Standard von SAML 2.0 vollständig unterstützen, da die Integration andernfalls nicht funktioniert.

## Hinzufügen eines VSAML-Dienstanbieters zur Identity Federation

Sie können den vSphere Web Client verwenden, um einen SAML-Dienstanbieter zu vCenter Single Sign On hinzuzufügen und vCenter Single Sign On als Identitätsanbieter zu diesem Dienst hinzuzufügen. Der Dienstanbieter authentifiziert Benutzer mit vCenter Single Sign On, wenn diese sich beim Dienstanbieter anmelden.

### Voraussetzungen

Der Zieldienst muss den SAML 2.0-Standard vollständig unterstützen, und die SP-Metadaten müssen das `SPSSODescriptor`-Element aufweisen.

Wenn die Metadaten das Metadatenschema von SAML 2.0 nicht exakt befolgen, müssen Sie die Metadaten vor dem Importieren möglicherweise bearbeiten. Wenn Sie z. B. Active Directory-Verbunddienste (Active Directory Federation Services, ADFS) als SAML-Dienstanbieter verwenden, müssen Sie die Metadaten bearbeiten, bevor Sie sie importieren können. Entfernen Sie die folgenden nicht standardmäßigen Elemente:

```
fed:ApplicationServiceType
fed:SecurityTokenServiceType
```

### Verfahren

1 Exportieren Sie die Metadaten aus dem Dienstanbieter in eine Datei.

2 Melden Sie sich mit dem vSphere Web Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.

3 Navigieren Sie zur Benutzeroberfläche für die Konfiguration.

   a Wählen Sie im Menü **Home** die Option **Verwaltung** aus.

   b Klicken Sie unter **Single Sign-On** auf **Konfiguration**.

4 Importieren Sie die SP-Metadaten in vCenter Single Sign On.

   a Gehen Sie zur Registerkarte **SAML-Dienstanbieter**.

   b Importieren Sie im Dialogfeld **Metadaten aus Ihrem SAML-Dienstanbieter** die Metadaten, indem Sie die XML-Zeichenfolge einfügen oder eine Datei importieren.

5 Exportieren Sie die vCenter Single Sign On-IDP-Metadaten.

   a Klicken Sie im Textfeld **Metadaten Ihres SAML-Dienstanbieters** auf **Herunterladen**.

   b Geben Sie einen Speicherort an.

6 Melden Sie sich beim SAML-Dienstanbieter, beispielsweise VMware vRealize Automation 7.0, an und befolgen Sie dessen Anweisungen zum Hinzufügen der vCenter Single Sign On-Metadaten zu diesem Dienstanbieter.

   Weitere Informationen zum Importieren von Metadaten in dieses Produkt finden Sie in der Dokumentation zu vRealize Automation.

# Security Token Service STS

Der Security Token Service (STS) von vCenter Single Sign On ist ein Webservice, der Sicherheitstoken ausstellt, validiert und erneuert.

Die Benutzer geben ihre primären Anmeldedaten bei der STS-Schnittstelle ein, um SAML-Token zu erhalten. Die primären Anmeldedaten hängen vom Benutzertyp ab.

**Benutzer**

In einer vCenter Single Sign On-Identitätsquelle verfügbarer Benutzername und verfügbares Kennwort.

**Anwendungsbenutzer**

Gültiges Zertifikat.

STS authentifiziert den Benutzer anhand der primären Anmeldedaten und erstellt ein SAML-Token mit Benutzerattributen. STS signiert das SAML-Token mit dem STS-Signaturzertifikat und weist das Token dem Benutzer zu. Standardmäßig wird das STS-Signaturzertifikat von VMCA generiert. Das standardmäßige STS-Signaturzertifikat können Sie über den vSphere Web Client ersetzen. Ersetzen Sie das STS-Signaturzertifikat nur dann, wenn die Sicherheitsrichtlinien Ihres Unternehmens das Ersetzen aller Zertifikate erfordern.

Nachdem ein Benutzer einen SAML-Token erhalten hat, wird er als HTTP-Anforderung des Benutzers versendet, möglicherweise über verschiedene Proxys. Nur der beabsichtigte Empfänger (Dienstanbieter) kann die Informationen im SAML-Token nutzen.

## Aktualisieren des Zertifikats für den Security Token Service

Der vCenter Single Sign On-Server enthält einen Security Token Service (STS). Der Security Token Service ist ein Webservice, der Sicherheitstoken ausstellt, validiert und erneuert. Sie können das

vorhandene Zertifikat für den Security Token Service manuell im vSphere Web Client aktualisieren, wenn es abläuft oder geändert wird.

Um einen SAML-Token abzurufen, gibt der Benutzer die primären Anmeldedaten im Secure Token Server (STS) ein. Diese hängen vom Objekttyp ab.

**Lösungsbenutzer**

Gültiges Zertifikat

**Andere Benutzer**

In einer vCenter Single Sign On-Identitätsquelle verfügbarer Benutzername und verfügbares Kennwort.

Der STS authentifiziert den Benutzer anhand der primären Anmeldedaten und erstellt einen SAML-Token mit Benutzerattributen. Der STS-Dienst signiert den SAML-Token mit dem STS-Signaturzertifikat und weist den Token einem Benutzer zu. Standardmäßig wird das STS-Signaturzertifikat von VMCA generiert.

Nachdem ein Benutzer einen SAML-Token erhalten hat, wird er als HTTP-Anforderung des Benutzers versendet, möglicherweise über verschiedene Proxys. Nur der beabsichtigte Empfänger (Dienstanbieter) kann die Informationen im SAML-Token nutzen.

Sie können das bestehende STS-Signaturzertifikat im vSphere Web Client ersetzen, wenn Ihre Unternehmensrichtlinien dies erfordern oder ein abgelaufenes Zertifikat aktualisiert werden soll.

**Vorsicht** Ersetzen Sie die Datei nicht im Dateisystem. Andernfalls treten unerwartete Fehler auf, die schwer zu debuggen sind.

**Hinweis** Nachdem Sie das Zertifikat ersetzt haben, müssen Sie den Knoten neu starten, damit der vSphere Web Client-Dienst und der STS-Dienst neu gestartet werden.

**Voraussetzungen**

Kopieren Sie das Zertifikat, das Sie gerade zum Java Keystore hinzugefügt haben, von Platform Services Controller auf Ihre lokale Arbeitsstation.

**Platform Services Controller-Appliance**

*Zertifikatspeicherort*/keys/root-trust.jks z. B.: /keys/root-trust.jks

Beispiel:

/root/newsts/keys/root-trust.jks

**Windows-Installation**

*Zertifikatspeicherort*\root-trust.jks

Beispiel:

```
C:\Programme\VMware\vCenter Server\jre\bin\root-trust.jks
```

Verfahren

1. Melden Sie sich beim vSphere Web Client als „administrator@vsphere.local“ oder als anderer Benutzer mit vCenter Single Sign On-Administratorrechten an.

   Benutzer mit Administratorrechten für vCenter Single Sign On sind in der Administratorgruppe in der lokalen vCenter Single Sign On-Domäne enthalten (standardmäßig „vsphere.local“).

2. Navigieren Sie zur Benutzeroberfläche für die Konfiguration.
   a. Wählen Sie im Menü **Home** die Option **Verwaltung** aus.
   b. Klicken Sie unter **Single Sign-On** auf **Konfiguration**.
3. Wählen Sie die Registerkarte **Zertifikate** und die Unterregisterkarte **STS-Signierung** und klicken Sie auf das Symbol **STS-Signaturzertifikat hinzufügen**.
4. Fügen Sie das Zertifikat hinzu.
   a. Klicken Sie auf **Durchsuchen**, um zur Keystore-Datei (JKS) zu navigieren, die das neue Zertifikat enthält, und klicken Sie auf **Öffnen**.
   b. Geben Sie das Kennwort ein, wenn Sie dazu aufgefordert werden.
   c. Klicken Sie ganz oben in die STS-Alias-Kette und dann auf **OK**.
   d. Geben Sie das Kennwort erneut ein, wenn Sie dazu aufgefordert werden.
5. Klicken Sie auf **OK**.
6. Starten Sie den Platform Services Controller-Knoten neu, damit der STS-Dienst und vSphere Web Client neu gestartet werden.

   Ohne einen Neustart funktioniert die Authentifizierung nicht ordnungsgemäß, daher ist der Neustart unerlässlich.

## Generieren eines neuen STS-Signaturzertifikats auf der Appliance

Bei dem signierenden Zertifikat des vCenter Single Sign-On Security Token Service (STS) handelt es sich um ein internes VMware-Zertifikat. Ersetzen Sie es daher nicht, außer wenn Ihr Unternehmen Sie zum Ersatz interner Zertifikate anweist. Wenn Sie das standardmäßige STS-Signaturzertifikat ersetzen möchten, müssen Sie ein neues Zertifikat generieren und zum Java Keystore hinzufügen. In diesem Thema werden die Schritte auf einer eingebetteten Bereitstellungs-Appliance oder einer externen Platform Services Controller-Appliance erläutert.

**Hinweis** Dieses Zertifikat ist zehn Jahre lang gültig und kein externes Zertifikat. Ersetzen Sie dieses Zertifikat nur, wenn die Sicherheitsrichtlinie des Unternehmens dies erfordert.

Weitere Informationen finden Sie unter Generieren eines neuen STS-Signaturzertifikats in einer Windows-Installation von vCenter, wenn eine Windows-Installation des Platform Services Controller ausgeführt wird.

Verfahren

1 Erstellen Sie ein Verzeichnis auf oberster Ebene, in dem das neue Zertifikat gespeichert wird, und überprüfen Sie den Verzeichnispfad.

```
mkdir newsts
cd newsts
pwd
#resulting output: /root/newst
```

2 Kopieren Sie die Datei `certool.cfg` in das neue Verzeichnis.

```
cp /usr/lib/vmware-vmca/share/config/certool.cfg /root/newsts
```

3 Öffnen Sie die Kopie der Datei `certool.cfg` und bearbeiten Sie sie so, dass die IP-Adresse und der Hostname der lokalen Platform Services Controller-Instanz verwendet werden.

Es muss ein durch zwei Buchstaben bezeichnetes Land angegeben werden, wie im folgenden Beispiel dargestellt.

```
#
# Template file for a CSR request
#

# Country is needed and has to be 2 characters
Country = US
Name = STS
Organization = ExampleInc
OrgUnit = ExampleInc Dev
State = Indiana
Locality = Indianapolis
IPAddress = 10.0.1.32
Email = chen@exampleinc.com
Hostname = homecenter.exampleinc.local
```

4 Generieren Sie den Schlüssel.

```
/usr/lib/vmware-vmca/bin/certool --server localhost --genkey --privkey=/root/newsts/
sts.key --pubkey=/root/newsts/sts.pub
```

5 Generieren Sie das Zertifikat.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=/root/newsts/newsts.cer --privkey=/root/
newsts/sts.key --config=/root/newsts/certool.cfg
```

6 Konvertieren Sie das Zertifikat in das PK12-Format.

```
openssl pkcs12 -export -in /root/newsts/newsts.cer -inkey /root/newsts/sts.key
-certfile /var/lib/vmware/vmca/root.cer -name "newstssigning" -passout pass:testpassword
-out newsts.p12
```

7 Fügen Sie das Zertifikat zum Java Keystore (JKS) hinzu.

```
/usr/java/jre-vmware/bin/keytool -v -importkeystore -srckeystore newsts.p12 -srcstoretype
pkcs12 -srcstorepass testpassword -srcalias newstssigning -destkeystore root-trust.jks
-deststoretype JKS -deststorepass testpassword -destkeypass testpassword

/usr/java/jre-vmware/bin/keytool -v -importcert -keystore root-trust.jks -deststoretype
JKS -storepass testpassword -keypass testpassword -file /var/lib/vmware/vmca/root.cer
-alias root-ca
```

Verwenden Sie `keytool -help`, um eine Liste aller verfügbaren Befehle zu erhalten.

8 Geben Sie bei der Aufforderung **Ja** ein, um das Zertifikat im Keystore zu akzeptieren.

### Nächste Schritte

Sie können das neue Zertifikat jetzt importieren. Weitere Informationen hierzu finden Sie unter Aktualisieren des Zertifikats für den Security Token Service.

## Generieren eines neuen STS-Signaturzertifikats in einer Windows-Installation von vCenter

Bei dem signierenden Zertifikat des vCenter Single Sign-On Security Token Service (STS) handelt es sich um ein internes VMware-Zertifikat. Ersetzen Sie es daher nicht, außer wenn Ihr Unternehmen Sie zum Ersatz interner Zertifikate anweist. Wenn Sie das standardmäßige STS-Signaturzertifikat ersetzen möchten, müssen Sie zuerst ein neues Zertifikat generieren und zum Java Keystore hinzufügen. In diesem Verfahren werden die Schritte in einer Windows-Installation beschrieben.

**Hinweis** Dieses Zertifikat ist zehn Jahre lang gültig und kein externes Zertifikat. Ersetzen Sie dieses Zertifikat nur, wenn die Sicherheitsrichtlinie des Unternehmens dies erfordert.

Wenn Sie eine virtuelle Appliance verwenden, ziehen Sie Generieren eines neuen STS-Signaturzertifikats auf der Appliance zurate.

### Verfahren

1 Erstellen Sie ein Verzeichnis zum Speichern des neuen Zertifikats.

```
cd C:\ProgramData\VMware\vCenterServer\cfg\sso\keys\
mkdir newsts
cd newsts
```

2 Erstellen Sie eine Kopie der Datei `certool.cfg` und speichern Sie sie im neuen Verzeichnis.

```
copy "C:\Program Files\VMware\vCenter Server\vmcad\certool.cfg" .
```

3 Öffnen Sie die Kopie der Datei `certool.cfg` und bearbeiten Sie sie so, dass die IP-Adresse und der Hostname der lokalen Platform Services Controller-Instanz verwendet werden.

   Das Land muss angegeben werden und aus zwei Buchstaben bestehen. Dies wird im folgenden Beispiel verdeutlicht.

```
#
# Template file for a CSR request
#

# Country is needed and has to be 2 characters
Country = US
Name = STS
Organization = ExampleInc
OrgUnit = ExampleInc Dev
State = Indiana
Locality = Indianapolis
IPAddress = 10.0.1.32
Email = chen@exampleinc.com
Hostname = homecenter.exampleinc.local
```

4 Generieren Sie den Schlüssel.

```
"C:\Program Files\VMware\vCenter Server\vmcad\certool.exe" --server localhost --genkey --
privkey=sts.key --pubkey=sts.pub
```

5 Generieren Sie das Zertifikat.

```
"C:\Program Files\VMware\vCenter Server\vmcad\certool.exe" --gencert --cert=newsts.cer --
privkey=sts.key --config=certool.cfg
```

6 Konvertieren Sie das Zertifikat in das PK12-Format.

```
"C:\Program Files\VMware\vCenter Server\openSSL\openssl.exe" pkcs12 -export -in newsts.cer
-inkey sts.key -certfile C:\ProgramData\VMware\vCenterServer\data\vmca\root.cer -name
"newstssigning" -passout pass:changeme -out newsts.p12
```

7 Fügen Sie das Zertifikat zum Java Keystore (JKS) hinzu.

```
"C:\Program Files\VMware\vCenter Server\jre\bin\keytool.exe" -v -importkeystore
-srckeystore newsts.p12 -srcstoretype pkcs12 -srcstorepass changeme -srcalias
newstssigning -destkeystore root-trust.jks -deststoretype JKS -deststorepass testpassword
-destkeypass testpassword
"C:\Program Files\VMware\vCenter Server\jre\bin\keytool.exe" -v -importcert -keystore
root-trust.jks -deststoretype JKS -storepass testpassword -keypass testpassword -file
C:\ProgramData\VMware\vCenterServer\data\vmca\root.cer -alias root-ca
```

### Nächste Schritte

Sie können das neue Zertifikat jetzt importieren. Weitere Informationen hierzu finden Sie unter Aktualisieren des Zertifikats für den Security Token Service.

## Ermitteln des Ablaufdatums eines LDAPS-SSL-Zertifikats

Wenn Sie eine LDAP-Identitätsquelle auswählen und LDAPS verwenden möchten, können Sie ein SSL-Zertifikat für den LDAP-Datenverkehr hochladen. SSL-Zertifikate werden nach einer vordefinierten Laufzeit ungültig. Wenn Sie das Ablaufdatum kennen, können Sie das Zertifikat vor dem Ende der Laufzeit ersetzen oder erneuern.

Sie sehen Daten zum Zertifikatsablauf nur, wenn Sie einen LDAP-Server und einen OpenLDAP-Server des Active Directory verwenden und eine `ldaps://`-URL für den Server angeben. Die Registerkarte „Identitätsquellen-**TrustStore**“ bleibt für andere Typen von Identitätsquellen oder für `ldap://`-Datenverkehr leer.

Verfahren

1. Melden Sie sich mit dem vSphere Web Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.
2. Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

   Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.
3. Navigieren Sie zur Benutzeroberfläche für die Konfiguration.
   a. Wählen Sie im Menü **Home** die Option **Verwaltung** aus.
   b. Klicken Sie unter **Single Sign-On** auf **Konfiguration**.
4. Klicken Sie auf die Registerkarte **Identitätsquellen**.
5. Wählen Sie im oberen Bereich des Bildschirms die Identitätsquelle aus, deren LDAPS-Zertifikat Sie anzeigen möchten.
6. Zeigen Sie im unteren Bereich des Bildschirms die Details des Zertifikats an und überprüfen Sie das Ablaufdatum im Feld **Gültig bis**.

   Sie sehen möglicherweise eine Warnung an der oberen Seite der Registerkarte, die anzeigt, dass ein Zertifikat bald abläuft.

# Verwalten der vCenter Single Sign On-Richtlinien

vCenter Single Sign On-Richtlinien erzwingen die Sicherheitsregeln in Ihrer Umgebung. Sie können die standardmäßige Kennwortrichtlinie, Sperrrichtlinie und Token-Richtlinie für vCenter Single Sign On anzeigen und bearbeiten.

## Bearbeiten der vCenter Single Sign On-Kennwortrichtlinie

Die vCenter Single Sign On-Kennwortrichtlinie bestimmt das Kennwortformat und den Kennwortablauf. Die Kennwortrichtlinie gilt nur für Benutzer in der vCenter Single Sign On-Domäne („vsphere.local“ oder „vmc.local“).

Standardmäßig laufen vCenter Single Sign On-Kennwörter nach 90 Tagen ab. Der vSphere Client erinnert Sie, wenn Ihr Kennwort nur noch wenige Tage gültig ist.

Weitere Informationen hierzu finden Sie unter Ändern des vCenter Single Sign On-Kennworts .

Verfahren

1 Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.

2 Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

   Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.

3 Navigieren Sie zur Benutzeroberfläche für die Konfiguration.

   a Wählen Sie im Menü **Home** die Option **Verwaltung** aus.

   b Klicken Sie unter **Single Sign-On** auf **Konfiguration**.

4 Klicken Sie auf **Richtlinien**, wählen Sie **Kennwortrichtlinie** aus und klicken Sie auf **Bearbeiten**.

5 Bearbeiten Sie die Kennwortrichtlinie.

| Option | Beschreibung |
|---|---|
| **Beschreibung** | Beschreibung der Kennwortrichtlinie. |
| **Maximale Lebensdauer** | Maximale Gültigkeitsdauer in Tagen für ein Kennwort, bevor der Benutzer es ändern muss. Die maximale Anzahl von Tagen, die Sie eingeben können, ist 999999999. Der Wert Null (0) bedeutet, dass das Kennwort nie abläuft. |
| **Wiederverwendung einschränken** | Anzahl der vorherigen Kennwörter, die nicht wiederverwendet werden können. Wenn Sie beispielsweise „6“ eingeben, kann der Benutzer die letzten sechs Kennwörter nicht wiederverwenden. |
| **Maximallänge** | Maximal zulässige Zeichenanzahl für das Kennwort. |
| **Mindestlänge** | Mindestens erforderliche Zeichenanzahl für das Kennwort. Die Mindestlänge darf nicht unter der Summe der erforderlichen Mindestanzahl von alphabetischen und numerischen Zeichen sowie Sonderzeichen liegen. |

| Option | Beschreibung |
|---|---|
| **Zeichenanforderungen** | Mindestens erforderliche Anzahl verschiedener Zeichenarten für das Kennwort. Die Anzahl der verschiedenen Zeichenarten können Sie wie folgt angeben:<br>■ Sonderzeichen: & # %<br>■ Buchstaben: A b c D<br>■ Großbuchstaben: A B C<br>■ Kleinbuchstaben: a b c<br>■ Zahlen: 1 2 3<br>Die Mindestanzahl alphabetischer Zeichen muss mindestens der Summe der Groß- und Kleinbuchstaben entsprechen.<br>In Kennwörtern werden Nicht-ASCII-Zeichen unterstützt. In älteren Versionen von vCenter Single Sign On existieren Beschränkungen in Bezug auf unterstützte Zeichen. |
| **Identische benachbarte Zeichen** | Maximal zulässige Anzahl identischer benachbarter Zeichen für das Kennwort. Wenn Sie beispielsweise 1 eingeben, ist das folgende Kennwort nicht zulässig: p@$$word.<br>Die Zahl muss größer als 0 sein. |

6 Klicken Sie auf **Speichern**.

## Bearbeiten der vCenter Single Sign On-Sperrrichtlinie

Wenn ein Benutzer versucht, sich mit falschen Anmeldedaten anzumelden, gibt eine vCenter Single Sign On-Sperrrichtlinie an, wann das vCenter Single Sign On-Konto des Benutzers gesperrt wird. Administratoren können die Sperrrichtlinie bearbeiten.

Wenn sich ein Benutzer bei „vsphere.local“ mehrmals mit dem falschen Kennwort anmeldet, wird er gesperrt. Über die Sperrrichtlinie können Administratoren die maximale Anzahl der fehlgeschlagenen Anmeldeversuche angeben und das Zeitintervall zwischen fehlgeschlagenen Versuchen festlegen. Mit der Richtlinie wird auch festgelegt, wie viel Zeit vergehen muss, bevor das Konto automatisch entsperrt wird.

**Hinweis** Die Sperrrichtlinie gilt für Benutzerkonten und nicht für Systemkonten wie „administrator@vsphere.local“.

### Verfahren

1 Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.

2 Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.

3 Navigieren Sie zur Benutzeroberfläche für die Konfiguration.

   a Wählen Sie im Menü **Home** die Option **Verwaltung** aus.

   b Klicken Sie unter **Single Sign-On** auf **Konfiguration**.

4 Wählen Sie **Sperrrichtlinie** aus und klicken Sie auf **Bearbeiten**.

5 Bearbeiten Sie die Parameter.

| Option | Beschreibung |
|---|---|
| **Beschreibung** | Optionale Beschreibung der Sperrrichtlinie |
| **Maximale Anzahl der fehlgeschlagenen Anmeldeversuche** | Maximal zulässige Anzahl fehlgeschlagener Anmeldeversuche, bevor das Konto gesperrt wird. |
| **Zeitintervall zwischen fehlgeschlagenen Versuchen** | Zeitraum, in dem fehlgeschlagene Anmeldeversuche vorkommen müssen, damit eine Sperrung ausgelöst wird. |
| **Entsperrzeit** | Die Zeitdauer, die das Konto gesperrt bleibt. Wenn Sie 0 eingeben, muss der Administrator das Konto explizit entsperren. |

6 Klicken Sie auf **Speichern**.

## Bearbeiten der vCenter Single Sign On-Token-Richtlinie

Die vCenter Single Sign On-Token-Richtlinie gibt die Token-Eigenschaften wie Zeittoleranz und Anzahl der Verlängerung an. Sie können die Token-Richtlinie bearbeiten, um sicherzustellen, dass die Token-Spezifikation den Sicherheitsstandards Ihres Unternehmens entspricht.

### Verfahren

1 Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.

2 Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

   Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.

3 Navigieren Sie zur Benutzeroberfläche für die Konfiguration.

   a Wählen Sie im Menü **Home** die Option **Verwaltung** aus.

   b Klicken Sie unter **Single Sign-On** auf **Konfiguration**.

4 Wählen Sie **Token-Richtlinie** aus und klicken Sie auf **Bearbeiten**.

5 Bearbeiten Sie die Konfigurationsparameter der Token-Richtlinie.

| Option | Beschreibung |
|---|---|
| **Zeittoleranz** | Der von vCenter Single Sign On tolerierte Zeitunterschied in Millisekunden zwischen einer Client-Uhr und der Uhr des Domänencontrollers. Ist der Zeitunterschied größer als der angegebene Wert, markiert vCenter Single Sign On das Token als ungültig. |
| **Maximalzahl der Token-Verlängerungen** | Die maximale Anzahl möglicher Verlängerungen für ein Token. Wenn die maximale Anzahl an Verlängerungsversuchen erreicht wurde, ist ein neues Sicherheitstoken erforderlich. |
| **Maximalzahl der Token-Delegierungen** | Token des Typs 'holder-of-key' können an Dienste in der vSphere-Umgebung delegiert werden. Ein Dienst, der ein delegiertes Token verwendet, führt den Dienst im Auftrag des Prinzipals aus, der das Token bereitgestellt hat. Eine Token-Anforderung gibt eine DelegateTo-Identität an. Der Wert für 'DelegateTo' kann entweder ein Lösungstoken oder eine Referenz auf ein Lösungstoken sein. Dieser Wert gibt an, wie oft ein einzelnes Token des Typs 'holder-of-key' delegiert werden kann. |
| **Maximale Lebensdauer für Bearer-Token** | Ein Bearer-Token bietet eine Authentifizierung, die nur auf dem Besitz des Tokens basiert. Bearer-Token sind für eine kurzzeitige Verwendung in einem einmaligen Vorgang ausgelegt. Ein Bearer-Token überprüft nicht die Identität des Benutzers oder Elements, von dem die Anforderung gesendet wird. Dieser Wert gibt den Wert für die Lebensdauer eines Bearer-Tokens an, bevor dieses neu ausgestellt werden muss. |
| **Maximale Lebensdauer für Token des Typs 'holder-of-key'** | Token des Typs 'holder-of-key' bieten eine Authentifizierung, die auf in das Token eingebetteten Sicherheitsartefakten basiert. Token des Typs 'holder-of-key' können delegiert werden. Ein Client kann ein Token des Typs 'holder-of-key' erhalten und dieses Token an ein anderes Element delegieren. Das Token enthält die Beanspruchungen zur Identifizierung des Urhebers und des Delegaten. In der vSphere-Umgebung ruft ein vCenter Server-System im Auftrag eines Benutzers delegierte Token ab und verwendet diese Token zum Ausführen von Vorgängen.<br>Dieser Wert gibt die Lebensdauer eines Tokens des Typs 'holder-of-key' an, bevor das Token als ungültig markiert wird. |

6 Klicken Sie auf **Speichern**.

## Bearbeiten der Benachrichtigungsfrist zum Kennwortablauf für Active Directory-Benutzer

Die Active Directory-Benachrichtigungsfrist zum Kennwortablauf wird getrennt vom vCenter Server SSO-Kennwortablauf gehandhabt. Die standardmäßige Benachrichtigungsfrist zum Kennwortablauf für einen Active Directory-Benutzer beträgt 30 Tage, die tatsächliche Kennwortablauffrist hängt jedoch von Ihrem Active Directory-System ab. Der vSphere Client und der vSphere Web Client steuern die Benachrichtigungsfrist zum Kennwortablauf. Sie können die standardmäßige Benachrichtigungsfrist zum Kennwortablauf so ändern, dass sie die Sicherheitsstandards in Ihrem Unternehmen erfüllt.

Verfahren

1 Melden Sie sich beim vCenter Server-System als Benutzer mit Administratorrechten an.

Der Standardbenutzer mit der Superadministratorrolle ist „root“.

2 Wechseln Sie zum Verzeichnis, in dem die `webclient.properties`-Datei abgelegt ist.

| Betriebssystem | Befehl |
| --- | --- |
| **Linux** | ■ vSphere Client:<br>`cd /etc/vmware/vsphere-ui`<br>■ vSphere Web Client:<br>`cd /etc/vmware/vsphere-client` |
| **Windows** | ■ vSphere Client:<br>`cd %ALLUSERSPROFILE%\VMware\vCenterServer\cfg\vsphere-ui`<br>■ vSphere Web Client:<br>`cd %ALLUSERSPROFILE%\VMware\vCenterServer\cfg\vsphere-client` |

3 Öffnen Sie die `webclient.properties`-Datei mit einem Texteditor.

4 Bearbeiten Sie die folgende Variable:

```
sso.pending.password.expiration.notification.days = 30
```

5 Starten Sie den Client neu.

| Betriebssystem | Befehl |
| --- | --- |
| **Linux** | ■ vSphere Client:<br>`service-control --stop vsphere-ui`<br>`service-control --start vsphere-ui`<br>■ vSphere Web Client:<br>`service-control --stop vsphere-client`<br>`service-control --start vsphere-client` |
| **Windows** | ■ vSphere Client:<br>`cd "C:\Program Files\VMware\vCenter Server\bin\"`<br>`service-control --stop vsphere-ui`<br>`service-control --start vsphere-ui`<br>■ vSphere Web Client:<br>`cd "C:\Program Files\VMware\vCenter Server\bin\"`<br>`service-control --stop vspherewebclientsvc`<br>`service-control --start vspherewebclientsvc` |

# Verwalten von vCenter Single Sign On-Benutzern und -Gruppen

Ein vCenter Single Sign On-Administratorbenutzer kann Benutzer und Gruppen in der Domäne „vsphere.local“ über den vSphere Client verwalten.

Der vCenter Single Sign On-Administratorbenutzer kann die folgenden Aufgaben ausführen.

- Hinzufügen von vCenter Single Sign On-Benutzern

  Benutzer, die im vSphere Client auf der Registerkarte **Benutzer** aufgeführt sind, sind intern für vCenter Single Sign On und gehören zur Domäne „vsphere.local“. Benutzer können über eine der vCenter Single Sign On-Verwaltungsschnittstellen zu dieser Domäne hinzugefügt werden.

- Aktivieren und Deaktivieren von vCenter Single Sign On-Benutzern

  Wenn ein vCenter Single Sign On-Benutzerkonto deaktiviert wird, kann sich der Benutzer so lange nicht beim vCenter Single Sign On-Server anmelden, bis ein Administrator das Konto aktiviert. Konten können über eine der vCenter Single Sign On-Verwaltungsschnittstellen deaktiviert und aktiviert werden.

- Löschen eines vCenter Single Sign On-Benutzers

  Sie können Benutzer in der Domäne „vsphere.local“ über eine vCenter Single Sign On-Verwaltungsschnittstelle löschen. Lokale Betriebssystembenutzer oder Benutzer in einer anderen Domäne können über eine vCenter Single Sign On-Verwaltungsschnittstelle nicht gelöscht werden.

- Bearbeiten eines vCenter Single Sign On-Benutzers

  Sie können das Kennwort oder andere Details eines vCenter Single Sign On-Benutzers über eine vCenter Single Sign On-Verwaltungsschnittstelle ändern. In der vsphere.local-Domäne können Sie keine Benutzer umbenennen. Das bedeutet, dass Sie „administrator@vsphere.local“ nicht umbenennen können.

- Hinzufügen einer vCenter Single Sign On-Gruppe

  Die vCenter Single Sign On-Registerkarte **Gruppen** enthält Gruppen in der lokalen Domäne (standardmäßig „vsphere.local“). Sie können Gruppen hinzufügen, wenn Sie einen Container für Gruppenmitglieder (Prinzipale) benötigen.

- Hinzufügen von Mitgliedern zu einer vCenter Single Sign On-Gruppe

  Bei den Mitgliedern einer vCenter Single Sign On-Gruppe kann es sich um Benutzer oder andere Gruppen aus einer oder mehreren Identitätsquellen handeln. Sie können neue Mitglieder aus dem vSphere Client hinzufügen.

- Entfernen von Mitgliedern aus einer vCenter Single Sign On-Gruppe

  Sie können Mitglieder aus einer vCenter Single Sign On-Gruppe mit dem vSphere Client entfernen. Wenn Sie ein Mitglied (Benutzer oder Gruppe) aus einer Gruppe entfernen, wird das Mitglied nicht aus dem System gelöscht.

- Löschen von vCenter Single Sign On-Lösungsbenutzern

  In vCenter Single Sign On werden die Lösungsbenutzer angezeigt. Ein Lösungsbenutzer ist eine Sammlung von Diensten. Mehrere vCenter Server-Lösungsbenutzer sind vordefiniert und werden bei vCenter Single Sign On im Rahmen der Installation authentifiziert. Wenn bei einer Fehlerbehebung beispielsweise eine Deinstallation nicht vollständig abgeschlossen werden konnte, können Sie einzelne Lösungsbenutzer aus dem vSphere Web Client löschen.

- Ändern des vCenter Single Sign On-Kennworts

  Benutzer in der lokalen Domäne (standardmäßig „vsphere.local“) können ihre vCenter Single Sign On-Kennwörter über eine Web-Benutzeroberfläche ändern. Benutzer in anderen Domänen ändern ihre Kennwörter gemäß den Regeln für diese Domäne.

## Hinzufügen von vCenter Single Sign On-Benutzern

Benutzer, die im vSphere Client auf der Registerkarte **Benutzer** aufgeführt sind, sind intern für vCenter Single Sign On und gehören zur Domäne „vsphere.local“. Benutzer können über eine der vCenter Single Sign On-Verwaltungsschnittstellen zu dieser Domäne hinzugefügt werden.

Sie können andere Domänen auswählen und Informationen zu den Benutzern in diesen Domänen anzeigen, aber Sie können von der vCenter Single Sign On-Verwaltungsschnittstelle aus keine Benutzer zu anderen Domänen hinzufügen.

### Verfahren

1 Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.

2 Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

   Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.

3 Navigieren Sie zur Benutzeroberfläche für die vCenter Single Sign-On-Benutzerkonfiguration.

   a Wählen Sie im Menü **Home** die Option **Verwaltung** aus.

   b Klicken Sie unter **Single Sign-On** auf **Benutzer und Gruppen**.

4 Wenn es sich bei der derzeit ausgewählten Domäne nicht um „vsphere.local“ handelt, wählen Sie sie im Dropdown-Menü aus.

   Sie können keine Benutzer zu anderen Domänen hinzufügen.

5 Klicken Sie auf der Registerkarte **Benutzer** auf **Benutzer hinzufügen**.

6 Geben Sie einen Benutzernamen und ein Kennwort für den neuen Benutzer ein.

   Sie können den Benutzernamen nicht ändern, nachdem Sie einen Benutzer angelegt haben. Das Kennwort muss die Anforderungen der Kennwortrichtlinie für das System erfüllen.

7 (Optional) Geben Sie den Vornamen und den Nachnamen des neuen Benutzers ein.

8 (Optional) Geben Sie eine E-Mail-Adresse und Beschreibung für den Benutzer ein.

9 Klicken Sie auf **Hinzufügen**.

#### Ergebnisse

Wenn Sie einen Benutzer hinzufügen, verfügt dieser Benutzer zunächst nicht über die entsprechenden Rechte, um Verwaltungsvorgänge auszuführen.

#### Nächste Schritte

Fügen Sie den Benutzer einer Gruppe in der Domäne „vsphere.local“ hinzu, beispielsweise der Benutzergruppe mit Administratorrechten für VMCA (CAAdmins) oder für vCenter Single Sign On (Administratoren). Weitere Informationen hierzu finden Sie unter Hinzufügen von Mitgliedern zu einer vCenter Single Sign On-Gruppe.

## Aktivieren und Deaktivieren von vCenter Single Sign On-Benutzern

Wenn ein vCenter Single Sign On-Benutzerkonto deaktiviert wird, kann sich der Benutzer so lange nicht beim vCenter Single Sign On-Server anmelden, bis ein Administrator das Konto aktiviert. Konten können über eine der vCenter Single Sign On-Verwaltungsschnittstellen deaktiviert und aktiviert werden.

Deaktivierte Benutzerkonten bleiben im vCenter Single Sign On-System verfügbar, aber der Benutzer kann sich nicht anmelden und keine Vorgänge auf dem Server durchführen. Benutzer mit Administratorrechten können Konten auf der vCenter-Seite **Benutzer und Gruppen** aktivieren und deaktivieren.

### Voraussetzungen

Sie müssen Mitglied der Administratorgruppe für vCenter Single Sign On sein, um vCenter Single Sign On-Benutzer aktivieren und deaktivieren zu können.

### Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.
2. Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

   Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.
3. Navigieren Sie zur Benutzeroberfläche für die vCenter Single Sign-On-Benutzerkonfiguration.
   a. Wählen Sie im Menü **Home** die Option **Verwaltung** aus.
   b. Klicken Sie unter **Single Sign-On** auf **Benutzer und Gruppen**.
4. Wählen Sie einen Benutzernamen aus, klicken Sie auf das Symbol mit den vertikalen Auslassungspunkten und anschließend auf **Deaktivieren**.
5. Klicken Sie auf **OK**.
6. Um den Benutzer erneut zu aktivieren, klicken Sie auf das Symbol mit den vertikalen Auslassungspunkten, anschließend auf **Aktivieren** und zum Schluss auf **OK**.

## Löschen eines vCenter Single Sign On-Benutzers

Sie können Benutzer in der Domäne „vsphere.local“ über eine vCenter Single Sign On-Verwaltungsschnittstelle löschen. Lokale Betriebssystembenutzer oder Benutzer in einer anderen Domäne können über eine vCenter Single Sign On-Verwaltungsschnittstelle nicht gelöscht werden.

**Vorsicht** Wenn Sie den Administratorbenutzer in der Domäne „vsphere.local“ löschen, können Sie sich nicht mehr bei vCenter Single Sign On anmelden. Installieren Sie vCenter Server und die zugehörigen Komponenten neu.

### Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.
2. Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

   Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.

3 Navigieren Sie zur Benutzeroberfläche für die vCenter Single Sign-On-Benutzerkonfiguration.
   a Wählen Sie im Menü **Home** die Option **Verwaltung** aus.
   b Klicken Sie unter **Single Sign-On** auf **Benutzer und Gruppen**.
4 Wählen Sie **Benutzer** und anschließend die Domäne „vsphere.local“ im Dropdown-Menü aus.
5 Wählen Sie in der Liste mit den Benutzern den Benutzer aus, den Sie löschen möchten, und klicken Sie auf das Symbol mit den vertikalen Auslassungspunkten.
6 Klicken Sie auf **Löschen**.

   Gehen Sie mit Bedacht vor. Diese Aktion kann nicht rückgängig gemacht werden.

## Bearbeiten eines vCenter Single Sign On-Benutzers

Sie können das Kennwort oder andere Details eines vCenter Single Sign On-Benutzers über eine vCenter Single Sign On-Verwaltungsschnittstelle ändern. In der vsphere.local-Domäne können Sie keine Benutzer umbenennen. Das bedeutet, dass Sie „administrator@vsphere.local“ nicht umbenennen können.

Sie können zusätzliche Benutzer mit den gleichen Berechtigungen wie administrator@vsphere.local erstellen.

vCenter Single Sign On-Benutzer werden in der vCenter Single Sign On-Domäne „vsphere.local“ gespeichert.

Sie können die vCenter Single Sign On-Kennwortrichtlinien im vSphere Client überprüfen. Melden Sie sich als administrator@vsphere.local an und wählen Sie im Menü **Administration** die Optionen **Konfiguration > Richtlinien > Kennwortrichtlinie**.

Siehe auch Bearbeiten der vCenter Single Sign On-Kennwortrichtlinie.

### Verfahren

1 Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.
2 Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

   Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.
3 Navigieren Sie zur Benutzeroberfläche für die vCenter Single Sign-On-Benutzerkonfiguration.
   a Wählen Sie im Menü **Home** die Option **Verwaltung** aus.
   b Klicken Sie unter **Single Sign-On** auf **Benutzer und Gruppen**.
4 Klicken Sie auf **Benutzer**.
5 Klicken Sie auf das Symbol mit den vertikalen Auslassungspunkten und wählen Sie **Bearbeiten** aus.

6 Bearbeiten Sie die Benutzerattribute.

Sie können den Benutzernamen des Benutzers nicht ändern.

Das Kennwort muss die Anforderungen der Kennwortrichtlinie für das System erfüllen.

7 Klicken Sie auf **OK**.

## Hinzufügen einer vCenter Single Sign On-Gruppe

Die vCenter Single Sign On-Registerkarte **Gruppen** enthält Gruppen in der lokalen Domäne (standardmäßig „vsphere.local“). Sie können Gruppen hinzufügen, wenn Sie einen Container für Gruppenmitglieder (Prinzipale) benötigen.

Sie können Gruppen über die vCenter Single Sign On-Registerkarte **Gruppen** nicht zu anderen Domänen hinzufügen (beispielsweise zur Active Directory-Domäne).

Wenn Sie keine Identitätsquelle zu vCenter Single Sign On hinzufügen, lässt sich die lokale Domäne durch das Erstellen von Gruppen und Hinzufügen von Benutzern besser organisieren.

### Verfahren

1 Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.

2 Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.

3 Navigieren Sie zur Benutzeroberfläche für die vCenter Single Sign-On-Benutzerkonfiguration.

a Wählen Sie im Menü **Home** die Option **Verwaltung** aus.

b Klicken Sie unter **Single Sign-On** auf **Benutzer und Gruppen**.

4 Wählen Sie **Gruppen** aus und klicken Sie auf **Gruppe hinzufügen**.

5 Geben Sie einen Namen und eine Beschreibung für die Gruppe ein.

Sie können den Gruppennamen nicht ändern, nachdem Sie die Gruppe angelegt haben.

6 Klicken Sie auf **Hinzufügen**.

### Nächste Schritte

- Fügen Sie dieser Gruppe Mitglieder hinzu.

## Hinzufügen von Mitgliedern zu einer vCenter Single Sign On-Gruppe

Bei den Mitgliedern einer vCenter Single Sign On-Gruppe kann es sich um Benutzer oder andere Gruppen aus einer oder mehreren Identitätsquellen handeln. Sie können neue Mitglieder aus dem vSphere Client hinzufügen.

Hintergrundinformationen finden Sie im VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/2095342.

Gruppen, die in der Webschnittstelle auf der Registerkarte **Gruppen** aufgeführt werden, sind Teil der Domäne „vsphere.local“. Weitere Informationen hierzu finden Sie unter Gruppen in der vCenter Single Sign On-Domäne.

Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.
2. Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

   Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.
3. Navigieren Sie zur Benutzeroberfläche für die vCenter Single Sign-On-Benutzerkonfiguration.
   a. Wählen Sie im Menü **Home** die Option **Verwaltung** aus.
   b. Klicken Sie unter **Single Sign-On** auf **Benutzer und Gruppen**.
4. Klicken Sie auf **Gruppen** und klicken Sie auf die Gruppe (z. B. „Administratoren“).
5. Klicken Sie im Bereich „Gruppenmitglieder“ auf **Mitglieder hinzufügen**.
6. Wählen Sie die Identitätsquelle, die das Mitglied enthält, das zur Gruppe hinzugefügt werden soll.
7. (Optional) Geben Sie einen Suchbegriff ein und klicken Sie auf **Suchen**.
8. Wählen Sie das Mitglied aus.

   Sie können mehrere Mitglieder hinzufügen.
9. Klicken Sie auf **OK**.

## Entfernen von Mitgliedern aus einer vCenter Single Sign On-Gruppe

Sie können Mitglieder aus einer vCenter Single Sign On-Gruppe mit dem vSphere Client entfernen. Wenn Sie ein Mitglied (Benutzer oder Gruppe) aus einer Gruppe entfernen, wird das Mitglied nicht aus dem System gelöscht.

Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.
2. Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

   Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.

3 Navigieren Sie zur Benutzeroberfläche für die vCenter Single Sign-On-Benutzerkonfiguration.
   a Wählen Sie im Menü **Home** die Option **Verwaltung** aus.
   b Klicken Sie unter **Single Sign-On** auf **Benutzer und Gruppen**.
4 Wählen Sie **Gruppen** aus und klicken Sie auf eine Gruppe.
5 Wählen Sie in der Liste der Gruppenmitglieder den Benutzer oder die Gruppe aus, den bzw. die Sie entfernen möchten, und klicken Sie auf das Symbol mit den vertikalen Auslassungspunkten.
6 Klicken Sie auf **Mitglied entfernen**.
7 Klicken Sie auf **Entfernen**.

#### Ergebnisse

Der Benutzer wird aus der Gruppe entfernt, ist aber noch im System vorhanden.

## Löschen von vCenter Single Sign On-Lösungsbenutzern

In vCenter Single Sign On werden die Lösungsbenutzer angezeigt. Ein Lösungsbenutzer ist eine Sammlung von Diensten. Mehrere vCenter Server-Lösungsbenutzer sind vordefiniert und werden bei vCenter Single Sign On im Rahmen der Installation authentifiziert. Wenn bei einer Fehlerbehebung beispielsweise eine Deinstallation nicht vollständig abgeschlossen werden konnte, können Sie einzelne Lösungsbenutzer aus dem vSphere Web Client löschen.

Wenn Sie einen Satz von Diensten eines vCenter Server-Lösungsbenutzers oder eines dritten Lösungsbenutzers aus Ihrer Umgebung entfernen, wird der Lösungsbenutzer im vSphere Web Client nicht mehr angezeigt. Wenn Sie das Entfernen einer Anwendung erzwingen oder das System in einen nicht behebbaren Zustand versetzt wird, während sich der Lösungsbenutzer noch im System befindet, können Sie ihn explizit aus dem vSphere Web Client entfernen.

**Wichtig** Die Dienste eines gelöschten Lösungsbenutzers können in vCenter Single Sign On nicht mehr authentifiziert werden.

#### Verfahren

1 Melden Sie sich mit dem vSphere Web Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.
2 Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

   Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.
3 Navigieren Sie zur Benutzeroberfläche für die vCenter Single Sign-On-Benutzerkonfiguration.
   a Wählen Sie im Menü **Home** die Option **Verwaltung** aus.
   b Klicken Sie unter **Single Sign-On** auf **Benutzer und Gruppen**.

4 Klicken Sie auf die Registerkarte **Lösungsbenutzer** und anschließend auf den Lösungsbenutzernamen.

5 Klicken Sie auf das Symbol **Lösungsbenutzer löschen**.

6 Klicken Sie auf **Ja**.

Ergebnisse

Die mit dem Lösungsbenutzer verknüpften Dienste haben keinen Zugriff auf vCenter Server mehr und können nicht mehr als vCenter Server-Dienste fungieren.

## Ändern des vCenter Single Sign On-Kennworts

Benutzer in der lokalen Domäne (standardmäßig „vsphere.local“) können ihre vCenter Single Sign On-Kennwörter über eine Web-Benutzeroberfläche ändern. Benutzer in anderen Domänen ändern ihre Kennwörter gemäß den Regeln für diese Domäne.

Die vCenter Single Sign On-Sperrrichtlinie bestimmt, wann Ihr Kennwort abläuft. Standardmäßig laufen Benutzerkennwörter für vCenter Single Sign On nach 90 Tagen ab. Administratorkennwörter wie das Kennwort für administrator@vsphere.local laufen jedoch nicht ab. vCenter Single Sign On-Verwaltungsschnittstellen zeigen eine Warnung an, wenn das Kennwort in Kürze abläuft.

**Hinweis** Sie können ein Kennwort nur ändern, wenn es nicht abgelaufen ist.

Wenn das Kennwort abgelaufen ist, kann der Administrator der lokalen Domäne (standardmäßig „administrator@vsphere.local“) das Kennwort unter Verwendung des Befehls `dir-cli password reset` zurücksetzen. Nur Mitglieder der Gruppe „Administrator“ für die vCenter Single Sign-On-Domäne können Kennwörter zurücksetzen.

Verfahren

1 Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.

2 Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

   Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.

3 Klicken Sie im oberen Navigationsbereich rechts neben dem Hilfemenü auf Ihren Benutzernamen, um das Pulldown-Menü zu öffnen.

   Alternativ können Sie auch **Single Sign-On > Benutzer und Gruppen** auswählen und dann im Menü mit den vertikalen Auslassungspunkten die Option **Benutzer bearbeiten** auswählen.

4 Wählen Sie die Option **Kennwort ändern** und geben Sie Ihr aktuelles Kennwort ein.

5 Geben Sie ein neues Kennwort ein und bestätigen Sie es.

   Das Kennwort muss der Kennwortrichtlinie entsprechen.

6 Klicken Sie auf **OK**.

# Empfohlene Vorgehensweisen für die Sicherheit von vCenter Single Sign On

Befolgen Sie im Zusammenhang mit vCenter Single Sign On die Best Practices für die Sicherheit, um Ihre vSphere-Umgebung effizient zu schützen.

Die Authentifizierungsinfrastruktur von vSphere sorgt für hohe Sicherheit in Ihrer vSphere-Umgebung. Um sicherzustellen, dass keine Sicherheitsrisiken in der Infrastruktur entstehen, befolgen Sie die empfohlenen Vorgehensweisen für vCenter Single Sign On.

### Prüfen des Kennwortablaufs

Die Standardkennwortrichtlinie für vCenter Single Sign On sieht vor, dass Kennwörter nach 90 Tagen ablaufen. Nach 90 Tagen läuft das Kennwort ab, und eine Anmeldung ist nicht mehr möglich. Überprüfen Sie das Ablaufdatum und aktualisieren Sie die Kennwörter rechtzeitig.

### Konfigurieren von NTP

Stellen Sie stets sicher, dass alle Systeme dieselbe relative Zeitquelle verwenden (dazu gehören auch Standortunterschiede) und diese sich auf einen vereinbarten Zeitstandard (etwa die koordinierte Weltzeit UTC) beziehen. Synchronisierte Systeme sind für die Gültigkeit der vCenter Single Sign On-Zertifikate und anderer vSphere-Zertifikate besonders wichtig.

NTP vereinfacht auch die Erkennung von Eindringungsversuchen in den Protokolldateien. Bei falschen Zeiteinstellungen kann es schwierig werden, Protokolldateien zur Suche nach Angriffen zu untersuchen und abzugleichen. Dies kann zu ungenauen Ergebnissen beim Audit führen.

# vSphere-Sicherheitszertifikate

3

vSphere bietet Sicherheit mithilfe von Zertifikaten zur Verschlüsselung der Kommunikation, Authentifizierung von Diensten und Signierung von Token.

vSphere verwendet Zertifikate zu folgenden Zwecken:

- Verschlüsseln der Kommunikationen zwischen zwei Knoten, wie z. B. vCenter Server und einem ESXi-Host.
- Authentifizieren von vSphere-Diensten.
- Durchführen interner Aktionen wie beispielsweise das Signieren von Token

Die interne Zertifizierungsstelle von vSphere, VMware Certificate Authority (VMCA), stellt alle für vCenter Server und ESXi erforderlichen Zertifikate zur Verfügung. VMCA wird auf jedem Platform Services Controller installiert und schützt die Lösung sofort und ohne weitere Änderung. Wenn die Standardkonfiguration beibehalten wird, ist der betriebliche Overhead für die Zertifikatverwaltung so gering wie möglich. vSphere bietet einen Mechanismus, durch den diese Zertifikate verlängert werden, wenn sie ablaufen.

Zudem bietet vSphere einen Mechanismus, um bestimmte Zertifikate durch Ihre eigenen Zertifikate zu ersetzen. Ersetzen Sie jedoch nur das SSL-Zertifikat, das die Verschlüsselung zwischen den Knoten bereitstellt, um den Overhead für die Zertifikatsverwaltung gering zu halten.

Die folgenden Optionen werden für die Verwaltung von Zertifikaten empfohlen.

Tabelle 3-1. Empfohlene Optionen zum Verwalten von Zertifikaten

| Modus | Beschreibung | Vorteile |
|---|---|---|
| VMCA-Standardzertifikate | VMCA stellt alle Zertifikate für vCenter Server- und ESXi-Hosts zur Verfügung. | Einfachster und geringster Overhead. VMCA kann den Zertifikat-Lebenszyklus für vCenter Server und ESXi-Hosts verwalten. |
| VMCA-Standardzertifikate mit externen SSL-Zertifikaten (Hybrid-Modus) | Sie ersetzen die SSL-Zertifikate des Platform Services Controllers und der vCenter Server Appliance und gestatten VMCA die Verwaltung von Zertifikaten für Lösungsbenutzer und ESXi-Hosts. Optional können Sie für Bereitstellungen, die auf hohe Sicherheit ausgelegt sind, auch die SSL-Zertifikate des ESXi-Hosts ersetzen. | Einfach und sicher. VMCA verwaltet interne Zertifikate. Sie können jedoch von der Verwendung Ihrer durch das Unternehmen genehmigten SSL-Zertifikate profitieren und diesen Zertifikaten in Ihren Browsern vertrauen lassen. |

VMware empfiehlt, weder Lösungsbenutzerzertifikate oder STS-Zertifikate zu ersetzen noch eine untergeordnete Zertifizierungsstelle anstelle der VMCA zu verwenden. Wenn Sie eine dieser Optionen auswählen, stoßen Sie ggf. auf erhebliche Komplexität und es besteht die Möglichkeit negativer Auswirkungen auf Ihre Sicherheit. Außerdem kann das operative Risiko unnötig ansteigen. Weitere Informationen zum Verwalten von Zertifikaten innerhalb einer vSphere-Umgebung finden Sie im Blogbeitrag mit dem Titel *New Product Walkthrough - Hybrid vSphere SSL Certificate Replacement* (Neuer Produktfunktionstest - Ersetzen von hybriden vSphere-SSL-Zertifikaten) unter http://vmware.com/go/hybridvmca.

Sie können die folgenden Optionen verwenden, um die vorhandenen Zertifikate zu ersetzen:

Tabelle 3-2. Unterschiedliche Methoden für die Zertifikatsersetzung

| Option | Informationen hierzu finden Sie unter |
|---|---|
| Verwenden Sie den vSphere Client. Ab vSphere 6.7 wird der Platform Services Controller über den vSphere Client verwaltet. | Verwalten von Zertifikaten mit dem vSphere Client |
| Mithilfe des Dienstprogramms vSphere Certificate Manager über die Befehlszeile | Verwalten von Zertifikaten mit dem Dienstprogramm vSphere Certificate Manager |
| Mithilfe von CLI-Befehlen für die manuelle Zertifikatsersetzung | Kapitel 4 Verwalten von Diensten und Zertifikaten mit CLI-Befehlen |

vSphere-Zertifikatsverwaltung (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_ejp3dqkt/uiConfId/49694343/)

Dieses Kapitel enthält die folgenden Themen:

- Zertifikatsanforderungen für unterschiedliche Lösungspfade
- Zertifikatsverwaltung – Übersicht

- Verwalten von Zertifikaten mit dem vSphere Client
- Verwalten von Zertifikaten mit dem vSphere Web Client
- Verwalten von Zertifikaten mit dem Dienstprogramm vSphere Certificate Manager
- Manuelle Zertifikatsersetzung

# Zertifikatsanforderungen für unterschiedliche Lösungspfade

Die Zertifikatsanforderungen sind abhängig davon, ob Sie VMCA als Zwischenzertifizierungsstelle oder aber benutzerdefinierte Zertifikate verwenden. Die Anforderungen variieren auch für Maschinen- und Lösungsbenutzerzertifikate.

Bevor Sie beginnen müssen Sie sicherstellen, dass für alle Knoten in Ihrer Umgebung die Uhrzeit synchronisiert ist.

## Anforderungen für alle importierten Zertifikate

- Schlüsselgröße: mindestens 2.048 Bit (PEM-kodiert)
- PEM-Format. VMware unterstützt PKCS8 und PKCS1 (RSA-Schlüssel). Schlüssel, die Sie zu VECS hinzufügen, werden in PKCS8 konvertiert.
- x509 Version 3
- „SubjectAltName“ muss DNS-Name=*Maschinen-FQDN* enthalten
- CRT-Format
- Enthält die folgenden Schlüsselverwendungen: digitale Signatur, Schlüsselverschlüsselung.
- Erweiterte Schlüsselverwendung kann entweder leer sein oder Serverauthentifizierung enthalten.

Die folgenden Zertifikate werden von vSphere nicht unterstützt.

- Zertifikate mit Platzhalterzeichen.
- Die Algorithmen md2WithRSAEncryption 1.2.840.113549.1.1.2, md5WithRSAEncryption 1.2.840.113549.1.1.4 und sha1WithRSAEncryption 1.2.840.113549.1.1.5 werden nicht empfohlen.
- Der Algorithmus RSASSA-PSS mit OID 1.2.840.113549.1.1.10 wird nicht unterstützt.

## Einhaltung von RFC 2253 bei Zertifikaten

Das Zertifikat muss RFC 2253 einhalten.

Wenn Sie Zertifikatssignieranforderungen (Certificate Signing Requests, CSRs) nicht mithilfe von Certificate Manager generieren, stellen Sie sicher, dass die CSR die folgenden Felder enthält.

| String | Attributtyp X.500 |
|---|---|
| CN | `commonName` |
| N | `localityName` |

| String | Attributtyp X.500 |
|---|---|
| ST | `stateOrProvinceName` |
| O | `organizationName` |
| OU | `organizationalUnitName` |
| C | `countryName` |
| STREET | `streetAddress` |
| DC | `domainComponent` |
| UID | `userid` |

Wenn Sie CSRs mithilfe von Certificate Manager generieren, werden Sie zur Eingabe der folgenden Informationen aufgefordert, und Certificate Manager fügt in der CSR-Datei die entsprechenden Felder hinzu.

- Das Kennwort für den Benutzer „administrator@vsphere.local“ oder für den Administrator der vCenter Single Sign On-Domäne, mit der Sie eine Verbindung herstellen.
- Wenn Sie eine Zertifikatssignieranforderung in einer Umgebung mit einem externen Platform Services Controller generieren, werden Sie zur Eingabe des Hostnamens oder der IP-Adresse für den Platform Services Controller aufgefordert.
- Informationen, die Certificate Manager in der Datei `certool.cfg` speichert. Für die meisten Felder können Sie den Standardwert übernehmen oder aber standortspezifische Werte eingeben. Der FQDN der Maschine ist erforderlich.
  - Kennwort für „administrator@vsphere.local“.
  - Aus zwei Buchstaben bestehender Ländercode
  - Name des Unternehmens
  - Organisationsname
  - Organisationseinheit
  - Zustand
  - Ort
  - IP-Adresse (optional)
  - E-Mail
  - Hostname, d. h., der vollqualifizierte Domänenname der Maschine, für die Sie das Zertifikat ersetzen möchten. Wenn der Hostname nicht mit dem FQDN übereinstimmt, wird die Zertifikatsersetzung nicht ordnungsgemäß abgeschlossen und Ihre Umgebung weist möglicherweise einen instabilen Status auf.
  - IP-Adresse des Platform Services Controller, wenn Sie den Befehl auf einem vCenter Server-Verwaltungsknoten ausführen.

# Anforderungen für die Verwendung von VMCA als Zwischenzertifizierungsstelle

Wenn Sie VMCA als Zwischenzertifizierungsstelle verwenden, müssen die Zertifikate die folgenden Anforderungen erfüllen.

| Zertifikatstyp | Zertifikatsanforderungen |
|---|---|
| Rootzertifikat | ■ Sie können vSphere Certificate Manager zum Generieren der CSR verwenden. Weitere Informationen hierzu finden Sie unter Generieren von CSRs mit vSphere Certificate Manager und Vorbereiten des Rootzertifikats (Zwischenzertifizierungsstelle).<br>■ Wenn Sie die CSR manuell erstellen möchten, muss das Zertifikat, das Sie zum Signieren senden, die folgenden Anforderungen erfüllen.<br>■ Schlüsselgröße: mindestens 2.048 Bit<br>■ PEM-Format. VMware unterstützt PKCS8 und PKCS1 (RSA-Schlüssel). Wenn Schlüssel zu VECS hinzugefügt werden, werden sie in PKCS8 konvertiert.<br>■ x509 Version 3<br>■ Wenn Sie benutzerdefinierte Zertifikate verwenden, muss die Zertifizierungsstellenerweiterung für Stammzertifikate auf „true“ festgelegt werden, und „cert sign“ muss in der Liste der Anforderungen vorhanden sein.<br>■ CRL-Signatur muss aktiviert sein.<br>■ Erweiterte Schlüsselverwendung kann entweder leer sein oder Serverauthentifizierung enthalten.<br>■ Keine explizite Beschränkung der Zertifikatskettenlänge. VMCA verwendet den OpenSSL-Standardwert von 10 Zertifikaten.<br>■ Zertifikate mit Platzhalterzeichen oder mehr als einem DNS-Namen werden nicht unterstützt.<br>■ Untergeordnete Zertifizierungsstellen von VMCA können nicht erstellt werden.<br>Im VMware-Knowledgebase-Artikel „Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.0“ unter http://kb.vmware.com/kb/2112009 finden Sie ein Beispiel für die Verwendung der Microsoft-Zertifizierungsstelle. |
| Maschinen-SSL-Zertifikat | Sie können die CSR mithilfe des vSphere Certificate Manager oder manuell erstellen.<br>Wenn Sie die CSR manuell erstellen, muss sie die weiter oben unter *Anforderungen für alle importierten Zertifikate* aufgeführten Anforderungen erfüllen. Darüber hinaus müssen Sie den FQDN für den Host angeben. |
| Lösungsbenutzerzertifikat | Sie können die CSR mithilfe des vSphere Certificate Manager oder manuell erstellen. |

| Zertifikatstyp | Zertifikatsanforderungen |
| --- | --- |
| | **Hinweis** Sie müssen für jeden Lösungsbenutzer einen eindeutigen Wert für den Namen verwenden. Wenn Sie das Zertifikat manuell generieren, wird es in Abhängigkeit vom verwendeten Tool möglicherweise unter **Betreff** als **CN** angezeigt.<br><br>Wenn Sie vSphere Certificate Manager verwenden, werden Sie für jeden Lösungsbenutzer zur Eingabe von Zertifikatinformationen aufgefordert. vSphere Certificate Manager speichert die Informationen in der Datei `certool.cfg`. Weitere Informationen hierzu finden Sie unter *Von Certificate Manager angeforderte Informationen*. |

## Anforderungen für benutzerdefinierte Zertifikate

Wenn Sie benutzerdefinierte Zertifikate verwenden möchten, müssen die Zertifikate die folgenden Anforderungen erfüllen.

| Zertifikatstyp | Zertifikatsanforderungen |
|---|---|
| Maschinen-SSL-Zertifikat | Für das Maschinen-SSL-Zertifikat auf jedem Knoten ist ein separates Zertifikat von Ihrer Drittanbieter- oder Unternehmenszertifizierungsstelle erforderlich.<br>■ Sie können die CSR mit vSphere Client oder vSphere Certificate Manager generieren oder aber manuell erstellen. Die CSR muss die weiter oben unter *Anforderungen für alle importierten Zertifikate* aufgeführten Anforderungen erfüllen.<br>■ Wenn Sie vSphere Certificate Manager verwenden, werden Sie für jeden Lösungsbenutzer zur Eingabe von Zertifikatinformationen aufgefordert. vSphere Certificate Manager speichert die Informationen in der Datei `certool.cfg`. Weitere Informationen hierzu finden Sie unter *Von Certificate Manager angeforderte Informationen*.<br>■ Für die meisten Felder können Sie den Standardwert übernehmen oder aber standortspezifische Werte eingeben. Der FQDN der Maschine ist erforderlich. |
| Lösungsbenutzerzertifikat | Für jeden Lösungsbenutzer auf jedem Knoten ist ein separates Zertifikat von Ihrer Drittanbieter- oder Unternehmenszertifizierungsstelle erforderlich.<br>■ Sie können die CSRs mit vSphere Certificate Manager generieren oder aber selbst erstellen. Wenn Sie die CSR manuell erstellen, muss sie die weiter oben unter *Anforderungen für alle importierten Zertifikate* aufgeführten Anforderungen erfüllen.<br>■ Wenn Sie vSphere Certificate Manager verwenden, werden Sie für jeden Lösungsbenutzer zur Eingabe von Zertifikatinformationen aufgefordert. vSphere Certificate Manager speichert die Informationen in der Datei `certool.cfg`. Weitere Informationen hierzu finden Sie unter *Von Certificate Manager angeforderte Informationen*.<br>**Hinweis** Sie müssen für jeden Lösungsbenutzer einen eindeutigen Wert für den Namen verwenden. Wenn Sie ein Zertifikat manuell generieren, wird es je nach dem verwendeten Tool möglicherweise unter **Betreff** als **CN** angezeigt.<br>Wenn Sie später Lösungsbenutzerzertifikate durch benutzerdefinierte Zertifikate ersetzen, geben Sie die vollständige Signaturzertifikatkette der Drittanbieterzertifizierungsstelle an. |

**Hinweis** CRL-Verteilungspunkte, Zugriff auf Zertifizierungsstelleninfos oder Zertifikatvorlageninformationen dürfen in benutzerdefinierten Zertifikaten nicht verwendet werden.

# Zertifikatsverwaltung – Übersicht

Die für das Einrichten oder Aktualisieren der Zertifikatinfrastruktur erforderliche Arbeit ist abhängig von den Anforderungen in Ihrer Umgebung. Dabei müssen Sie berücksichtigen, ob es sich um eine Neuinstallation oder ein Upgrade handelt und ob Sie ESXi oder vCenter Server verwenden möchten.

## Administratoren, die VMware-Zertifikate nicht ersetzen

VMCA kann die gesamte Zertifikatsverwaltung durchführen. VMCA stellt vCenter Server-Komponenten und ESXi-Hosts Zertifikate bereit, die VMCA als Root-Zertifizierungsstelle verwenden. Wenn Sie ein Upgrade auf vSphere 6 von einer früheren Version von vSphere durchführen, werden alle selbstsignierten Zertifikate durch Zertifikate ersetzt, die durch VMCA signiert wurden.

Wenn Sie derzeit keine VMware-Zertifikate ersetzen, verwendet Ihre Umgebung VMCA-signierte Zertifikate anstatt selbstsignerte Zertifikate.

## Administratoren, die VMware-Zertifikate durch benutzerdefinierte Zertifikate ersetzen

Wenn Ihre Firmenrichtlinie Zertifikate erfordert, die von einer Drittanbieter- oder Unternehmenszertifizierungsstelle signiert wurden oder für die benutzerdefinierte Zertifikatsinformationen erforderlich sind, stehen Ihnen zahlreiche Optionen für eine Neuinstallation zur Verfügung.

- Lassen Sie das VMCA-Root-Zertifikat von einer Drittanbieter- oder Unternehmenszertifizierungsstelle signieren. Ersetzen Sie das VMCA-Root-Zertifikat durch dieses signierte Zertifikat. In diesem Szenario handelt es sich beim VMCA-Zertifikat um ein Zwischenzertifikat. VMCA stellt vCenter Server-Komponenten und ESXi-Hosts Zertifikate bereit, die die vollständige Zertifikatskette beinhalten.
- Wenn Ihre Unternehmensrichtlinie keine Zwischenzertifikate in der Zertifikatskette zulässt, müssen Sie Zertifikate explizit ersetzen. Sie können den vSphere Client oder das Dienstprogramm vSphere Certificate Manager verwenden oder Zertifikate mithilfe der Zertifikatsverwaltungs-CLIs manuell ersetzen.

Beim Upgrade einer Umgebung, die benutzerdefinierte Zertifikate verwendet, können Sie einige Zertifikate beibehalten.

- ESXi-Hosts behalten ihre benutzerdefinierten Zertifikate während des Upgrades bei. Stellen Sie sicher, dass beim Upgrade von vCenter Server alle relevanten Root-Zertifikate zum TRUSTED_ROOTS-Speicher in VECS unter vCenter Server hinzugefügt werden.

  Nach dem Upgrade auf vSphere 6.0 oder höher können Sie den Zertifikatmodus auf **Benutzerdefiniert** festlegen. Wenn der Zertifikatsmodus „VMCA“ lautet (Standardwert) und der Benutzer über den vSphere Client ein Zertifikat aktualisiert, werden die benutzerdefinierten Zertifikate durch VMCA-signierte Zertifikate ersetzt.

- Die vorhandene Umgebung bestimmt, was bei vCenter Server-Komponenten passiert.
  - Bei einem Upgrade einer einfachen Installation auf einer eingebetteten Bereitstellung behält vCenter Server benutzerdefinierte Zertifikate bei. Die Funktionsweise der Umgebung ist nach dem Upgrade unverändert.
  - Bei einem Upgrade einer siteübergreifenden Bereitstellung kann sich vCenter Single Sign On auf einer anderen Maschine als andere vCenter ServerKomponenten befinden. In diesem Fall erstellt der Upgrade-Prozess eine Bereitstellung mit mehreren Knoten, die einen Platform Services Controller-Knoten und einen oder mehrere Verwaltungsknoten enthält.

    Bei diesem Szenario werden die bestehenden vCenter Server- und vCenter Single Sign On-Zertifikate beibehalten. Die Zertifikate dienen als Maschinen-SSL-Zertifikate.

    Darüber hinaus weist VMCA jedem Lösungsbenutzer ein VMCA-signiertes Zertifikat zu (Sammlung von vCenter-Diensten). Der Lösungsbenutzer verwendet dieses Zertifikat nur für die Authentifizierung bei vCenter Single Sign On. Häufig erfordern es die Unternehmensrichtlinien nicht, dass Lösungsbenutzerzertifikate ersetzt werden.

  Das Zertifikatersetzungs-Tool aus vSphere 5.5, das für vSphere 5.5-Installationen verfügbar war, kann nicht mehr verwendet werden, da die Dienste in der neuen Architektur anders verteilt und platziert werden. Ein neues Befehlszeilendienstprogramm, vSphere Certificate Manager, ist für die meisten Zertifikatsverwaltungsaufgaben verfügbar.

## vSphere-Zertifikatschnittstellen

Für vCenter Server können Sie Zertifikate mit den folgenden Tools und Schnittstellen anzeigen und ersetzen.

**Tabelle 3-3. Schnittstellen für die Verwaltung von vCenter Server-Zertifikaten**

| Schnittstelle | Verwenden |
|---|---|
| vSphere Client | Führen Sie gängige Zertifikataufgaben mit einer grafischen Benutzeroberfläche durch. |
| vSphere Certificate Manager-Dienstprogramm | Führen Sie gängige Zertifikatersetzungsaufgaben über die Befehlszeile der vCenter Server-Installation durch. |
| Zertifikatsverwaltungs-CLIs | Führen Sie alle Zertifikatsverwaltungsaufgaben mit `dir-cli`, `certool` und `vecs-cli` aus. |
| vSphere Web Client | Zeigen Sie Zertifikate einschließlich der Informationen zum Ablauf von Zertifikaten an. |

Für ESXi führen Sie die Zertifikatsverwaltung über den vSphere Client aus. VMCA stellt Zertifikate bereit und speichert sie lokal auf dem ESXi-Host. VMCA speichert ESXi-Hostzertifikate nicht in VMDIR oder in VECS. Informationen finden Sie in der Dokumentation *vSphere-Sicherheit*.

# Unterstützte vCenter-Zertifikate

Für vCenter Server, den Platform Services Controller und zugehörige Maschinen und Dienste werden die folgenden Zertifikate unterstützt:

- Zertifikate, die von VMware Certificate Authority (VMCA) generiert und signiert werden.
- Benutzerdefinierte Zertifikate.
  - Unternehmenszertifikate, die von Ihrer eigenen internen PKI generiert werden.
  - Von einer Zertifizierungsstelle eines Drittanbieters signierte Zertifikate, die von einer externen PKI wie etwa Verisign, GoDaddy usw. generiert werden.

Mithilfe von OpenSSL erstellte selbstsignierte Zertifikate, bei denen es keine Root-Zertifizierungsstelle gibt, werden nicht unterstützt.

# Übersicht Zertifikatsersetzung

Sie können je nach der Unternehmensrichtlinie und den Anforderungen für das System, das Sie konfigurieren, verschiedene Arten von Zertifikatsersetzungen ausführen. Sie können die Zertifikatersetzung über den Platform Services Controller mit dem Dienstprogramm „vSphere Certificate Manager“ oder manuell über die Befehlszeilenschnittstellen durchführen, die Teil Ihrer Installation sind.

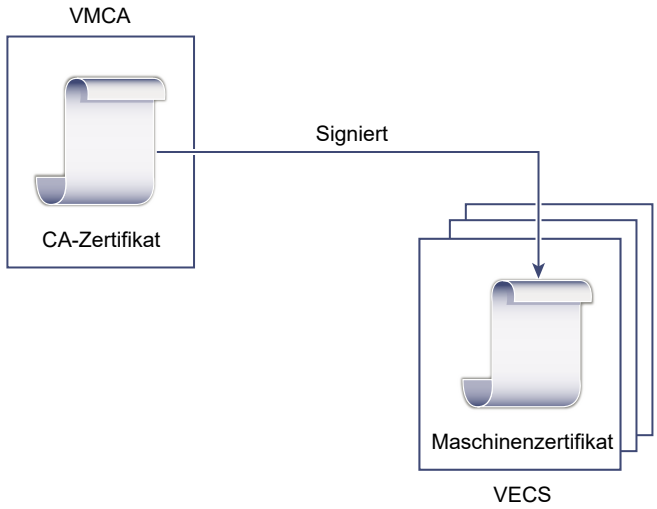
VMCA ist in jedem Platform Services Controller und in jeder eingebetteten Bereitstellung enthalten. VMCA stellt jedem Knoten, jedem vCenter Server-Lösungsbenutzer und jedem ESXi-Host ein Zertifikat zur Verfügung, das von VMCA als Zertifizierungsstelle signiert wurde. vCenter Server-Lösungsbenutzer sind Gruppen von vCenter Server-Diensten.

Sie können die Standardzertifikate ersetzen. Für vCenter Server-Komponenten können Sie einen Satz von Befehlszeilen-Tools verwenden, die bei Ihrer Installation enthalten sind. Es stehen mehrere Optionen zur Verfügung.

## Ersetzen durch von VMCA signierte Zertifikate

Wenn Ihr VMCA-Zertifikat abläuft oder wenn Sie es aus anderen Gründen ersetzen möchten, können Sie dazu die Befehlszeilenschnittstellen zur Zertifikatsverwaltung verwenden. Standardmäßig läuft das VMCA-Rootzertifikat nach zehn Jahren ab, und alle von VMCA signierten Zertifikate laufen gleichzeitig mit dem Rootzertifikat ab, also nach maximal zehn Jahren.

Abbildung 3-1. Von VMCA signierte Zertifikate werden in VECS gespeichert




Sie können die folgenden Optionen von vSphere Certificate Manager verwenden:

- Ersetzen des Maschinen-SSL-Zertifikats durch VMCA-Zertifikat
- Ersetzen des Lösungsbenutzerzertifikats durch VMCA-Zertifikat

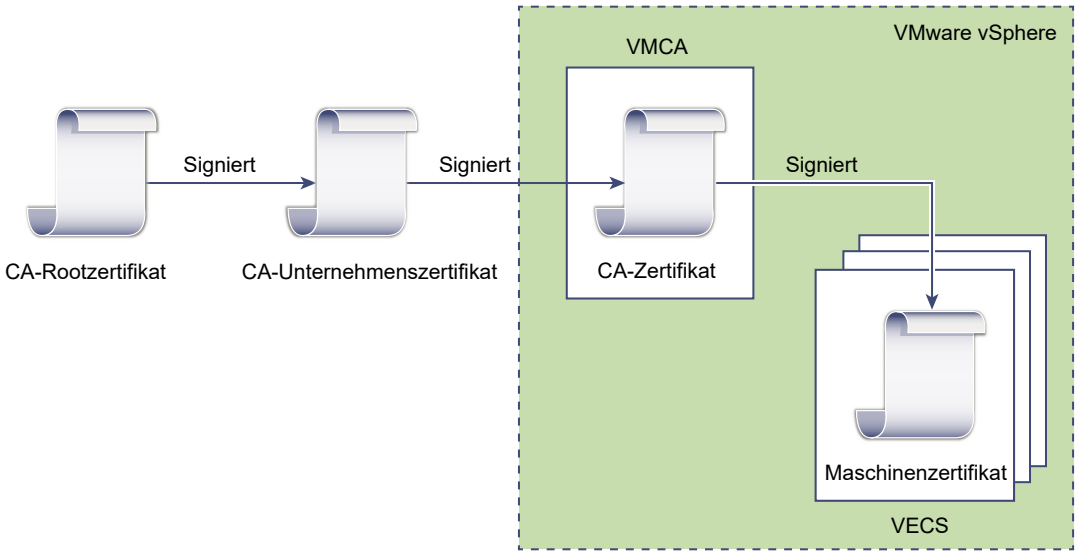
Informationen zur manuellen Zertifikatsersetzung finden Sie unter Ersetzen vorhandener VMCA-signierter Zertifikate durch neue VMCA-signierte Zertifikate.

## VMCA zu einer Zwischenzertifizierungsstelle machen

Sie können das VMCA-Rootzertifikat durch ein Zertifikat ersetzen, das durch eine Zertifizierungsstelle eines Unternehmens oder Drittanbieters signiert wurde. Die VMCA signiert das benutzerdefinierte Rootzertifikat immer, wenn sie Zertifikate zur Verfügung stellt, und macht so aus der VMCA eine Zwischenzertifizierungsstelle.

**Hinweis** Wenn Sie eine Neuinstallation mit einem externen Platform Services Controller durchführen, installieren Sie den Platform Services Controller zuerst und ersetzen Sie das VMCA-Rootzertifikat. Installieren Sie dann andere Dienste oder fügen Sie Ihrer Umgebung ESXi-Hosts hinzu. Wenn Sie eine Neuinstallation mit einem eingebetteten Platform Services Controller durchführen, ersetzen Sie das VMCA-Rootzertifikat vor dem Hinzufügen von ESXi-Hosts. In diesem Fall signiert VMCA die ganze Kette, und Sie brauchen keine neuen Zertifikate zu generieren.

**Abbildung 3-2. Zertifikate, die durch eine Zertifizierungsstelle eines Drittanbieters oder Unternehmens signiert wurden, verwenden VMCA als Zwischenzertifizierungsstelle**




Sie können die folgenden Optionen von vSphere Certificate Manager verwenden:

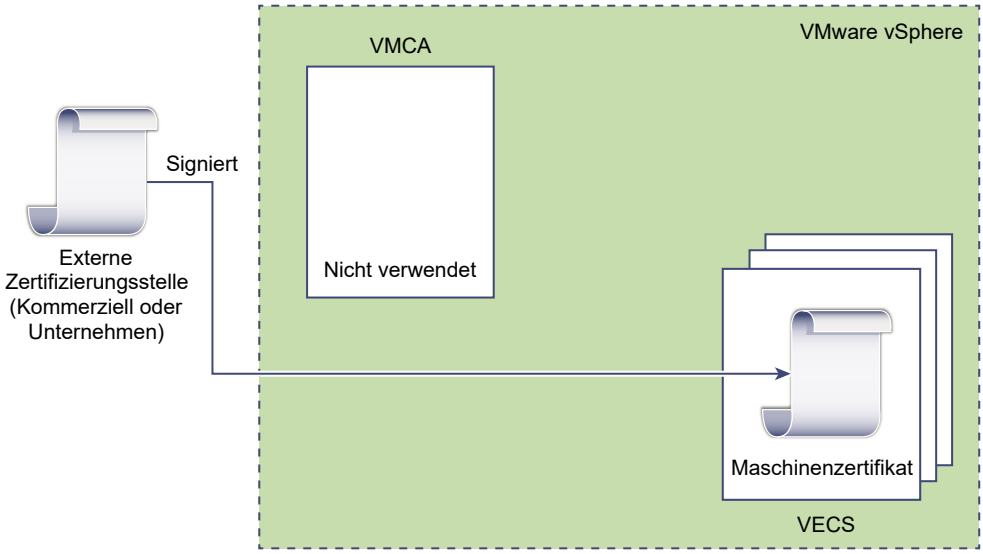
- Ersetzen des VMCA-Rootzertifikats durch ein benutzerdefiniertes Signaturzertifikat und Ersetzen aller Zertifikate
- Ersetzen des Maschinen-SSL-Zertifikats durch VMCA-Zertifikat (Mehrknoten-Bereitstellung)
- Ersetzen des Lösungsbenutzerzertifikats durch VMCA-Zertifikat (Mehrknoten-Bereitstellung)

Informationen zur manuellen Zertifikatsersetzung finden Sie unter Verwenden von VMCA als Zwischenzertifizierungsstelle.

## VMCA nicht verwenden, benutzerdefinierte Zertifikate zur Verfügung stellen

Sie können die vorhandenen VMCA-signierten Zertifikate durch benutzerdefinierte Zertifikate ersetzen. In diesem Fall sind Sie für die Bereitstellung und Überwachung aller Zertifikate verantwortlich.

Abbildung 3-3. Speichern externer Zertifikate direkt in VECS




Sie können die folgenden Optionen von vSphere Certificate Manager verwenden:

- Ersetzen des Maschinen-SSL-Zertifikats durch ein benutzerdefiniertes Zertifikat
- Ersetzen der Lösungsbenutzerzertifikate durch benutzerdefinierte Zertifikate

Informationen zur manuellen Zertifikatsersetzung finden Sie unter Verwenden benutzerdefinierter Zertifikate mit vSphere.

Sie können auch den vSphere Client verwenden, um eine CSR für ein Maschinen-SSL-Zertifikat (benutzerdefiniert) zu generieren und das Zertifikat, nachdem es von der Zertifizierungsstelle zurückgegeben wurde, ersetzen. Weitere Informationen hierzu finden Sie unter Generieren einer Zertifikatssignieranforderung (Certificate Signing Request, CSR) für ein Maschinen-SSL-Zertifikat mithilfe des vSphere Client (benutzerdefinierte Zertifikate).

## Hybrid-Bereitstellung

Sie können für bestimmte Teile Ihrer Infrastruktur VMCA-Zertifikate und für andere Teile Ihrer Infrastruktur benutzerdefinierte Zertifikate verwenden. Beispiel: Weil Lösungsbenutzerzertifikate nur zum Authentifizieren bei vCenter Single Sign On verwendet werden, empfiehlt es sich, diese Zertifikate durch VMCA bereitstellen zu lassen. Ersetzen Sie die Maschinen-SSL-Zertifikate durch benutzerdefinierte Zertifikate, um den ganzen SSL-Datenverkehr abzusichern.

Die Unternehmensrichtlinien lassen häufig keine Zwischenzertifizierungsstellen zu. In diesen Fällen ist die Hybrid-Bereitstellung eine geeignete Lösung. Hiermit wird die Anzahl der zu ersetzenden Zertifikate reduziert und der gesamte Verkehr gesichert. Bei der Hybrid-Bereitstellung kann lediglich interner Verkehr, d. h. Verkehr von Lösungsbenutzern, die VMCA-signierten Standardzertifikate verwenden.

### ESXi-Zertifikatsersetzung

Für ESXi-Hosts können Sie die Methode der Zertifikatsbereitstellung über den vSphere Client ändern. Weitere Informationen finden Sie in der Dokumentation *vSphere-Sicherheit*.

**Tabelle 3-4. ESXi Optionen zur Zertifikatersetzung**

| Option | Beschreibung |
|---|---|
| Modus „VMware Certificate Authority“ (Standard) | Wenn Sie Zertifikate über den vSphere Client erneuern, gibt VMCA die Zertifikate für die Hosts aus. Wenn Sie das VMCA-Rootzertifikat geändert haben, sodass eine Zertifikatskette enthalten ist, enthalten die Hostzertifikate die vollständige Kette. |
| Modus „Benutzerdefinierte Zertifizierungsstelle“ | Damit können Sie Zertifikate, die nicht von VMCA signiert oder ausgegeben wurden, manuell aktualisieren und verwenden. |
| Fingerabdruckmodus | Kann verwendet werden, um 5.5-Zertifikate beim Aktualisieren beizubehalten. Verwenden Sie diesen Modus nur vorübergehend in Debugging-Situationen. |

## Verwendung von Zertifikaten in vSphere

Ab vSphere 6.0 stellt die VMware Certificate Authority (VMCA) Zertifikate für Ihre Umgebung bereit. Zu den Zertifikaten zählen Maschinen-SSL-Zertifikate für sichere Verbindungen, Lösungsbenutzerzertifikate für die Authentifizierung von Diensten bei vCenter Single Sign On und Zertifikate für ESXi-Hosts.

Die folgenden Zertifikate werden verwendet.

**Tabelle 3-5. Zertifikate in vSphere 6.0 und höher**

| Zertifikat | Bereitgestellt | Anmerkungen |
|---|---|---|
| ESXi-Zertifikate | VMCA (Standard) | Lokal auf dem ESXi-Host gespeichert |
| Maschinen-SSL-Zertifikate | VMCA (Standard) | In VECS gespeichert |
| Lösungsbenutzerzertifikate | VMCA (Standard) | In VECS gespeichert |
| vCenter Single Sign On-SSL-Signaturzertifikat | Bereitgestellt während der Installation. | Verwalten Sie dieses Zertifikat über den vSphere Web Client.<br>**Hinweis** Dieses Zertifikat sollten Sie nicht im Dateisystem ändern, da dies zu unvorhersehbarem Verhalten führen kann. |
| SSL-Zertifikat für VMware Directory Service (VMDIR) | Bereitgestellt während der Installation. | Ab vSphere 6.5 wird das Maschinen-SSL-Zertifikat als vmdir-Zertifikat verwendet. |

## ESXi

ESXi-Zertifikate werden lokal auf jedem Host im Verzeichnis `/etc/vmware/ssl` gespeichert. ESXi-Zertifikate werden standardmäßig durch VMCA bereitgestellt, aber Sie können stattdessen benutzerdefinierte Zertifikate verwenden. ESXi-Zertifikate werden bereitgestellt, wenn der Host erstmalig zu vCenter Server hinzugefügt wird und wenn der Host erneut eine Verbindung herstellt.

## Maschinen-SSL-Zertifikate

Mit dem Maschinen-SSL-Zertifikat für jeden Knoten wird ein SSL-Socket auf der Serverseite erstellt. SSL-Clients stellen eine Verbindung zum SSL-Socket her. Dieses Zertifikat wird für die Serverüberprüfung und für die sichere Kommunikation (z. B. HTTPS oder LDAPS) verwendet.

Jeder Knoten verfügt über ein eigenes Maschinen-SSL-Zertifikat. Zu den Knoten gehören die vCenter Server-Instanz, die Platform Services Controller-Instanz oder die eingebettete Bereitstellungsinstanz. Alle Dienste, die auf einem Knoten ausgeführt werden, verwenden dieses Maschinen-SSL-Zertifikat, um die SSL-Endpoints verfügbar zu machen.

Die folgenden Dienste verwenden das Maschinen-SSL-Zertifikat:

- Der Reverse-Proxy-Dienst auf jedem Platform Services Controller-Knoten. SSL-Verbindungen zu einzelnen vCenter-Diensten werden stets an den Reverse-Proxy weitergeleitet. Der Datenverkehr wird nicht an die Dienste selbst weitergeleitet.
- Der vCenter-Dienst (vpxd) auf Verwaltungsknoten und eingebetteten Knoten.
- Der VMware Directory Service (vmdir) auf Infrastrukturknoten und eingebetteten Knoten.

VMware-Produkte verwenden X.509 Version 3 (X.509v3)-Standardzertifikate zur Verschlüsselung von Sitzungsinformationen. Die Sitzungsinformationen werden über SSL zwischen den Komponenten gesendet.

## Lösungsbenutzerzertifikate

Ein Lösungsbenutzer kapselt einen oder mehrere vCenter Server-Dienste. Jeder Lösungsbenutzer muss bei vCenter Single Sign On authentifiziert werden. Lösungsbenutzer verwenden Zertifikate zur Authentifizierung bei vCenter Single Sign On über den Austausch von SAML-Token.

Ein Lösungsbenutzer präsentiert vCenter Single Sign On das Zertifikat bei der erstmaligen Authentifizierung, nach einem Neustart sowie nach Ablauf einer Zeitüberschreitung. Die Zeitüberschreitung (Holder-of-Key-Zeitüberschreitung) kann über den vSphere Web Client festgelegt werden und ist standardmäßig auf 2592000 Sekunden (30 Tage) eingestellt.

Beispielsweise präsentiert der vpxd-Lösungsbenutzer vCenter Single Sign On sein Zertifikat, wenn die Verbindung zu vCenter Single Sign On hergestellt wird. Der vpxd-Lösungsbenutzer erhält von vCenter Single Sign On ein SAML-Token und kann sich dann damit bei anderen Lösungsbenutzern und Diensten authentifizieren.

Die folgenden Lösungsbenutzer-Zertifikatspeicher sind in VECS für jeden Verwaltungsknoten und für jede eingebettete Bereitstellung enthalten:

- `machine`: Wird vom Lizenzserver und vom Protokollierungsdienst verwendet.

  **Hinweis** Das Lösungsbenutzerzertifikat „machine“ hat nichts mit dem SSL-Zertifikat „machine“ zu tun. Das Lösungsbenutzerzertifikat „machine“ wird für den Austausch von SAML-Tokens verwendet. Das SSL-Zertifikat „machine“ wird für sichere SSL-Verbindungen für eine Maschine verwendet.

- `vpxd`: vCenter-Dienst-Daemon (vpxd)-Speicher für Verwaltungsknoten und eingebettete Bereitstellungen. vpxd verwendet das in diesem Speicher gespeicherte Lösungsbenutzerzertifikat für die Authentifizierung bei vCenter Single Sign On.
- `vpxd-extension`: vCenter-Erweiterungsspeicher. Enthält den Auto Deploy-Dienst, den Inventory Service und sonstige Dienste, die nicht Bestandteil anderer Lösungsbenutzer sind.
- `vsphere-webclient`: vSphere Web Client-Speicher. Enthält auch zusätzliche Dienste wie etwa den Leistungsdiagrammdienst.

Jeder Platform Services Controller-Knoten enthält ein `machine`-Zertifikat.

## Interne Zertifikate

vCenter Single Sign On-Zertifikate werden nicht in VECS gespeichert und werden nicht mit Zertifikatsverwaltungstools verwaltet. Im Allgemeinen gilt, dass keine Änderungen erforderlich sind, aber in speziellen Situationen können Sie diese Zertifikate ersetzen.

### vCenter Single Sign On-Signaturzertifikat

Der vCenter Single Sign On-Dienst enthält einen Identitätsanbieterdienst, der SAML-Token ausstellt, die in der gesamten vSphere-Umgebung zu Authentifizierungszwecken verwendet werden. Ein SAML-Token repräsentiert die Identität des Benutzers und enthält außerdem Gruppenmitgliedschaftsinformationen. Wenn vCenter Single Sign On SAML-Token ausstellt, wird jedes Token mit dem Signaturzertifikat signiert, damit Clients von vCenter Single Sign On sicherstellen können, dass das SAML-Token aus einer vertrauenswürdigen Quelle stammt.

vCenter Single Sign On stellt Lösungsbenutzern Holder-of-Key-SAML-Token sowie anderen Benutzern Bearer-Token aus, die sich mit einem Benutzernamen und einem Kennwort anmelden.

Dieses Zertifikat können Sie über den vSphere Web Client ersetzen. Weitere Informationen hierzu finden Sie unter Aktualisieren des Zertifikats für den Security Token Service.

### VMware Directory Service-SSL-Zertifikat

Ab vSphere 6.5 wird das Maschinen-SSL-Zertifikat als VMware-Verzeichniszertifikat verwendet. Informationen zu früheren Versionen von vSphere finden Sie in der entsprechenden Dokumentation.

### Verschlüsselungszertifikate der virtuellen vSphere-Maschine

Die Verschlüsselungslösung der virtuellen vSphere-Maschine stellt eine Verbindung zu einem externen Schlüsselmanagementserver (Key Management Server, KMS) her. Je nachdem, wie sich die Lösung beim KMS authentifiziert, generiert sie möglicherweise Zertifikate und speichert diese in VECS. Informationen finden Sie in der Dokumentation *vSphere-Sicherheit*.

## VMCA- und VMware-Kernidentitätsdienste

Kernidentitätsdienste sind Bestandteil jeder eingebetteten Bereitstellung und jedes Plattformdienstknotens. VMCA ist Bestandteil jeder VMware-Kernidentitätsdienste-Gruppe. Verwenden Sie Verwaltungs-Befehlszeilenschnittstellen (CLIs) sowie den vSphere Client für die Interaktion mit diesen Diensten.

Zu den VMware-Kernidentitätsdiensten zählen mehrere Komponenten.

**Tabelle 3-6. Kernidentitätsdienste**

| Dienst | Beschreibung | Bestandteil von |
|---|---|---|
| VMware Directory Service (vmdir) | Verwaltet SAML-Zertifikate für die Authentifizierung mit vCenter Single Sign On. | Platform Services Controller<br>Eingebettete Bereitstellung |
| VMware-Zertifizierungsstelle (VMCA) | Stellt Zertifikate für VMware-Lösungsbenutzer, Maschinenzertifikate für Maschinen, auf denen Dienste ausgeführt werden, sowie ESXi-Hostzertifikate aus. VMCA kann unverändert oder als Zwischenzertifizierungsstelle verwendet werden.<br>VMCA stellt Zertifikate nur für Clients aus, die sich bei vCenter Single Sign On in derselben Domäne authentifizieren können. | Platform Services Controller<br>Eingebettete Bereitstellung |
| VMware-Authentifizierungsframework-Daemon (VMAFD) | Enthält VMware Endpoint Certificate Store (VECS) und verschiedene weitere Authentifizierungsdienste. VMware-Administratoren interagieren mit VECS. Die anderen Dienste werden intern verwendet. | Platform Services Controller<br>vCenter Server<br>Eingebettete Bereitstellung |

## VMware Endpoint Certificate Store – Übersicht

VMware Endpoint Certificate Store (VECS) dient als lokales (clientseitiges) Repository für Zertifikate, private Schlüssel und sonstige Zertifikatinformationen, die in einem Keystore gespeichert werden können. Sie müssen VMCA nicht als Zertifizierungsstelle und Zertifikatssignaturgeber verwenden, aber Sie müssen VECS zum Speichern aller vCenter-Zertifikate, Schlüssel usw. verwenden. ESXi-Zertifikate werden lokal auf jedem Host und nicht in VECS gespeichert.

VECS wird als Komponente des VMware Authentication Framework Daemon (VMAFD) ausgeführt. VECS wird für jede eingebettete Bereitstellung, jeden Platform Services Controller-Knoten und jeden Verwaltungsknoten ausgeführt und enthält die Keystores mit den Zertifikaten und Schlüsseln.

VECS überprüft den VMware Directory Service (vmdir) in bestimmten Abständen auf Aktualisierungen für den vertrauenswürdigen Stammzertifikatspeicher. Zertifikate und Schlüssel können Sie in VECS auch explizit mithilfe der `vecs-cli`-Befehle verwalten. Weitere Informationen hierzu finden Sie unter Befehlsreferenz für vecs-cli.

VECS enthält die folgenden Speicher.

**Tabelle 3-7. Speicher in VECS**

| Speicher | Beschreibung |
|---|---|
| Maschinen-SSL-Speicher (MACHINE_SSL_CERT) | ■ Wird vom Reverse-Proxy-Dienst auf jedem vSphere-Knoten verwendet.<br>■ Wird vom VMware Directory Service (vmdir) für eingebettete Bereitstellungen und für jeden Platform Services Controller-Knoten verwendet.<br>Alle Dienste in vSphere 6.0 und höher kommunizieren über einen Reverse-Proxy, der das Maschinen-SSL-Zertifikat verwendet. Aus Gründen der Abwärtskompatibilität verwenden die 5.x-Dienste weiterhin bestimmte Ports. Deshalb ist für bestimmte Dienste wie etwa vpxd ein eigener Port geöffnet. |
| Vertrauenswürdiger Stammspeicher (TRUSTED_ROOTS) | Enthält alle vertrauenswürdigen Stammzertifikate. |

Tabelle 3-7. Speicher in VECS (Fortsetzung)

| Speicher | Beschreibung |
| --- | --- |
| Lösungsbenutzerspeicher<br>■ machine<br>■ vpxd<br>■ vpxd-extension<br>■ vsphere-webclient | VECS enthält einen Speicher für jeden Lösungsbenutzer. Das Objekt jedes Lösungsbenutzerzertifikats muss eindeutig sein. So darf z. B. das Maschinenzertifikat nicht das gleiche Objekt wie das vpxd-Zertifikat haben.<br>Lösungsbenutzerzertifikate werden für die Authentifizierung mit vCenter Single Sign On verwendet. vCenter Single Sign On überprüft, ob das Zertifikat gültig ist. Andere Zertifikatattribute werden jedoch nicht überprüft. Bei einer eingebetteten Bereitstellung befinden sich alle Lösungsbenutzerzertifikate im selben System.<br>Die folgenden Lösungsbenutzer-Zertifikatspeicher sind in VECS für jeden Verwaltungsknoten und für jede eingebettete Bereitstellung enthalten:<br>■ machine: Wird vom Lizenzserver und vom Protokollierungsdienst verwendet.<br>**Hinweis** Das Lösungsbenutzerzertifikat „machine“ hat nichts mit dem SSL-Zertifikat „machine“ zu tun. Das Lösungsbenutzerzertifikat „machine“ wird für den Austausch von SAML-Tokens verwendet. Das SSL-Zertifikat „machine“ wird für sichere SSL-Verbindungen für eine Maschine verwendet.<br>■ vpxd: vCenter-Dienst-Daemon (vpxd)-Speicher für Verwaltungsknoten und eingebettete Bereitstellungen. vpxd verwendet das in diesem Speicher gespeicherte Lösungsbenutzerzertifikat für die Authentifizierung bei vCenter Single Sign On.<br>■ vpxd-extension: vCenter-Erweiterungsspeicher. Enthält den Auto Deploy-Dienst, den Inventory Service und sonstige Dienste, die nicht Bestandteil anderer Lösungsbenutzer sind.<br>■ vsphere-webclient: vSphere Web Client-Speicher. Enthält auch zusätzliche Dienste wie etwa den Leistungsdiagrammdienst.<br>Jeder Platform Services Controller-Knoten enthält ein machine-Zertifikat. |

Tabelle 3-7. Speicher in VECS (Fortsetzung)

| Speicher | Beschreibung |
|---|---|
| vSphere Certificate Manager Utility-Backup-Speicher (BACKUP_STORE) | Wird von VMCA (VMware Certificate Manager) für die Unterstützung der Zertifikatwiederherstellung verwendet. Nur der letzte Status wird als Backup gespeichert und Sie können nur den letzten Schritt rückgängig machen. |
| Weitere Speicher | Weitere Speicher können durch Lösungen hinzugefügt werden. Beispielsweise fügt die Virtual Volumes-Lösung einen SMS-Speicher hinzu. Ändern Sie die Zertifikate in diesen Speichern nur, wenn Sie in der VMware-Dokumentation oder in einem VMware-Knowledgebase-Artikel dazu aufgefordert werden.<br>**Hinweis** Durch das Löschen des Speichers TRUSTED_ROOTS_CRLS kann die Zertifikatinfrastruktur beschädigt werden. Den TRUSTED_ROOTS_CRLS-Speicher sollten Sie weder löschen noch ändern. |

Der vCenter Single Sign On-Dienst speichert das Token-Signaturzertifikat und das SSL-Zertifikat auf Festplatte. Das Token-Signaturzertifikat können Sie über den vSphere Client ändern.

Bestimmte Zertifikate werden entweder temporär während des Starts oder dauerhaft im Dateisystem gespeichert. Die Zertifikate im Dateisystem sollten Sie nicht ändern. Verwenden Sie `vecs-cli`, um Vorgänge für in VECS gespeicherte Zertifikate auszuführen.

**Hinweis** Ändern Sie Zertifikatdateien auf Festplatte nur, wenn Sie in VMware-Dokumentation oder Knowledgebase-Artikeln dazu aufgefordert werden. Andernfalls könnte dies zu unvorhersehbarem Verhalten führen.

## Verwalten von Zertifikatswiderrufungen

Wenn Sie den Verdacht haben, dass eines Ihrer Zertifikate manipuliert wurde, ersetzen Sie alle vorhandenen Zertifikate, einschließlich des VMCA-Stammzertifikats.

vSphere 6.0 unterstützt das Ersetzen von Zertifikaten, aber der Zertifikatswiderruf wird für ESXi-Hosts oder für vCenter Server-Systeme nicht erzwungen.

Entfernen Sie widerrufene Zertifikate auf allen Knoten. Wenn Sie widerrufene Zertifikate nicht entfernen, könnten Manipulationen durch einen Man-in-the-Middle-Angriff in Form eines Identitätswechsels mit den Kontoanmeldedaten ermöglicht werden.

## Zertifikatsersetzung bei großen Bereitstellungen

Die Zertifikatersetzung bei Bereitstellungen, die mehrere Verwaltungsknoten und einen oder mehrere Platform Services Controller-Knoten enthalten, ist mit der Zertifikatersetzung bei eingebetteten Bereitstellungen vergleichbar. In beiden Fällen können Sie das Dienstprogramm vSphere Certificate Management verwenden oder die Zertifikate manuell ersetzen. Für die Zertifikatsersetzung gelten bestimmte Best Practices.

## Zertifikatsersetzung in High Availability-Umgebungen mit Lastausgleichsdienst

In Umgebungen mit weniger als acht vCenter Server-Systemen stellen Sie in der Regel eine einzige Platform Services Controller-Instanz und den zugehörigen vCenter Single Sign On-Dienst bereit. In größeren Umgebungen können Sie mehrere durch einen Netzwerk-Lastausgleichsdienst geschützte Platform Services Controller-Instanzen verwenden. Im Whitepaper *vCenter Server 6.0-Bereitstellungshandbuch* auf der VMware-Website wird diese Konfiguration behandelt.

## Ersetzen der Maschinen-SSL-Zertifikate in Umgebungen mit mehreren Verwaltungsknoten

Wenn Ihre Umgebung mehrere Verwaltungsknoten und eine einzige Platform Services Controller-Instanz aufweist, können Sie Zertifikate mit dem vSphere Client oder dem vSphere Certificate Manager-Dienstprogramm oder aber manuell mit vSphere-CLI-Befehlen ersetzen.

### vSphere Certificate Manager

vSphere Certificate Manager können Sie auf jeder Maschine ausführen. Auf Verwaltungsknoten werden Sie zur Eingabe der IP-Adresse des Platform Services Controller aufgefordert. In Abhängigkeit von der ausgeführten Aufgabe werden Sie auch zur Eingabe der Zertifikatinformationen aufgefordert.

### Manuelle Zertifikatsersetzung

Für die manuelle Zertifikatsersetzung führen Sie die Zertifikatsersetzungsbefehle auf jeder Maschine aus. Auf Verwaltungsknoten müssen Sie den Platform Services Controller mit dem Parameter `--server` angeben. Weitere Informationen finden Sie in den folgenden Themen:

- Ersetzen der Maschinen-SSL-Zertifikate durch VMCA-signierte Zertifikate
- Ersetzen der Maschinen-SSL-Zertifikate (Zwischenzertifizierungsstelle)
- Ersetzen der Maschinen-SSL-Zertifikate durch benutzerdefinierte Zertifikate

## Ersetzen der Lösungsbenutzerzertifikate in Umgebungen mit mehreren Verwaltungsknoten

Wenn Ihre Umgebung mehrere Verwaltungsknoten und eine einzige Platform Services Controller-Instanz aufweist, führen Sie für die Zertifikatsersetzung die folgenden Schritte aus.

**Hinweis** Wenn Sie Lösungsbenutzerzertifikate bei großen Bereitstellungen auflisten, enthält die Ausgabe von `dir-cli list` alle Lösungsbenutzer aus allen Knoten. Führen Sie `vmafd-cli get-machine-id --server-name localhost` aus, um für jeden Host nach der lokalen Maschinen-ID zu suchen. Jeder Lösungsbenutzername enthält die Maschinen-ID.

### vSphere Certificate Manager

vSphere Certificate Manager können Sie auf jeder Maschine ausführen. Auf Verwaltungsknoten werden Sie zur Eingabe der IP-Adresse des Platform Services Controller aufgefordert. In Abhängigkeit von der ausgeführten Aufgabe werden Sie auch zur Eingabe der Zertifikatinformationen aufgefordert.

**Manuelle Zertifikatsersetzung**

1. Generieren Sie ein Zertifikat oder fordern Sie ein Zertifikat an. Sie benötigen die folgenden Zertifikate:
   - Ein Zertifikat für den Lösungsbenutzer „machine“ auf dem Platform Services Controller.
   - Ein Zertifikat für den Lösungsbenutzer „machine“ auf jedem Verwaltungsknoten.
   - Ein Zertifikat für jeden der folgenden Lösungsbenutzer auf jedem Verwaltungsknoten:
     - Benutzer `vpxd solution`
     - Lösungsbenutzer `vpxd-extension`
     - Lösungsbenutzer `vsphere-webclient`
2. Ersetzen Sie die Zertifikate auf jedem Knoten. Die genaue Vorgehensweise hängt vom verwendeten Zertifikatsersetzungstyp ab. Weitere Informationen hierzu finden Sie unter Verwalten von Zertifikaten mit dem Dienstprogramm vSphere Certificate Manager.

Weitere Informationen finden Sie in den folgenden Themen:

- Ersetzen der Lösungsbenutzerzertifikate durch neue VMCA-signierte Stammzertifikate
- Ersetzen der Lösungsbenutzerzertifikate (Zwischenzertifizierungsstelle)
- Ersetzen der Lösungsbenutzerzertifikate durch benutzerdefinierte Zertifikate

## Zertifikatsersetzung in Umgebungen mit externen Lösungen

Einige Lösungen wie beispielsweise VMware vCenter Site Recovery Manager oder VMware vSphere Replication werden immer auf einem anderen Computer als das vCenter Server-System oder Platform Services Controller installiert. Beim Ersetzen des Standard-SSL-Zertifikats des Rechners auf dem vCenter Server-System oder dem Platform Services Controller, tritt ein Verbindungsfehler auf, falls die Lösung versucht, sich mit dem vCenter Server-System zu verbinden.

Sie können das Skript `ls_update_certs` ausführen, um das Problem zu beheben. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/2109074.

# Verwalten von Zertifikaten mit dem vSphere Client

Sie können Zertifikate mithilfe des vSphere Client anzeigen und überwachen. Sie können auch viele Zertifikatsverwaltungsaufgaben mit dem Dienstprogramm vSphere Certificate Manager durchführen.

Der vSphere Client ermöglicht Ihnen die Durchführung dieser Verwaltungsaufgaben.

- Zeigen Sie die vertrauenswürdigen Stammzertifikate und SSL-Zertifikate an.
- Verlängern vorhandener Zertifikate oder Ersetzen von Zertifikaten.
- Generieren Sie eine benutzerdefinierte Zertifikatsignieranforderung (CSR) für ein Maschinen-SSL-Zertifikat, und ersetzen Sie das Zertifikat, wenn es von der Zertifizierungsstelle zurückgegeben wird.

Die meisten Abschnitte der Workflows zur Zertifikatsersetzung werden vom vSphere Client vollständig unterstützt. Zum Generieren von CSRs für Maschinen-SSL-Zertifikate können Sie entweder den vSphere Client oder das Dienstprogramm „Certificate Manage“ verwenden.

## Unterstützte Workflows

Nach dem Installieren eines Platform Services Controller stellt die VMware Certificate Authority auf diesem Knoten allen anderen Knoten in der Umgebung standardmäßig Zertifikate bereit. Aktuelle Empfehlungen zum Verwalten von Zertifikaten finden Sie unter Kapitel 3 vSphere-Sicherheitszertifikate.

Zum Verlängern oder Ersetzen von Zertifikaten können Sie einen der folgenden Workflows verwenden.

### Zertifikate erneuern

Sie können SSL- und Lösungsbenutzerzertifikate in Ihrer Umgebung aus vSphere Client von VMCA erneuern lassen.

### VMCA zu einer Zwischenzertifizierungsstelle machen

Sie können eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) mit dem Dienstprogramm vSphere Certificate Manager generieren. Anschließend können Sie das Zertifikat der CSR bearbeiten, um VMCA zur Zertifikatskette hinzuzufügen, und anschließend die Zertifikatskette und den privaten Schlüssel zu Ihrer Umgebung hinzufügen. Wenn Sie anschließend alle Zertifikate verlängern, stellt VMCA für alle Maschinen und Lösungsbenutzer Zertifikate bereit, die von der vollständigen Zertifikatskette signiert sind.

### Zertifikate durch benutzerdefinierte Zertifikate ersetzen

Wenn Sie VMCA nicht verwenden möchten, können Sie CSRs für die zu ersetzenden Zertifikate generieren. Der Zertifizierungsstelle gibt für jede CSR ein Rootzertifikat und ein signiertes Zertifikat zurück. Sie können das Rootzertifikat und die benutzerdefinierten Zertifikate aus dem Platform Services Controller hochladen.

**Hinweis** Wenn Sie VMCA als Zwischenzertifizierungsstelle verwenden oder wenn Sie benutzerdefinierte Zertifikate verwenden, stoßen Sie möglicherweise auf erhebliche Komplexität und das Potenzial für Beeinträchtigungen Ihrer Sicherheit sowie einen unnötigen Anstieg Ihres Betriebsrisikos. Weitere Informationen zum Verwalten von Zertifikaten innerhalb einer vSphere-Umgebung finden Sie im Blogbeitrag mit dem Titel *New Product Walkthrough - Hybrid vSphere SSL Certificate Replacement* (Neuer Produktfunktionstest - Ersetzen von hybriden vSphere-SSL-Zertifikaten) unter http://vmware.com/go/hybridvmca.

In einer Umgebung im gemischten Modus können Sie das vCenter Single Sign On-Zertifikat nach dem Ersetzen der anderen Zertifikate mithilfe von CLI-Befehlen ersetzen. Weitere Informationen hierzu finden Sie unter Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus.

## Untersuchen der Zertifikatspeicher über den vSphere Client

Eine VMware Endpoint Certificate Store-Instanz (VECS-Instanz) ist in jedem Platform Services Controller-Knoten und in jedem vCenter Server-Knoten enthalten. Sie können die verschiedenen Zertifikatspeicher im VMware Endpoint Certificate Store (VECS) über den vSphere Client untersuchen.

Weitere Informationen zu den verschiedenen Zertifikatspeichern in VECS finden Sie unter VMware Endpoint Certificate Store – Übersicht.

### Voraussetzungen

Für die meisten Verwaltungsaufgaben benötigen Sie das Administratorkennwort für das lokale Domänenkonto, administrator@vsphere.local, oder für eine anderen Domäne, falls Sie während der Installation die Domäne geändert haben.

### Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.
2. Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

   Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.
3. Navigieren Sie zur Benutzeroberfläche für die Zertifikatsverwaltung.
   a. Wählen Sie im Menü **Home** die Option **Verwaltung** aus.
   b. Klicken Sie unter **Zertifikate** auf **Zertifikatsverwaltung**.

4 Geben Sie die Anmeldedaten für Ihren vCenter Server ein.

5 Untersuchen Sie die im VMware Endpoint Certificate Store (VECS) gespeicherten Zertifikate.

   Unter VMware Endpoint Certificate Store – Übersicht wird erläutert, was sich in den einzelnen Speichern befindet.

6 Um Details für ein Zertifikat anzuzeigen, wählen Sie das Zertifikat aus und klicken auf **Details anzeigen**.

7 Verwenden Sie das Menü **Aktionen** zum Verlängern oder Ersetzen von Zertifikaten.

   Wenn Sie beispielsweise das vorhandene Zertifikat ersetzen, können Sie später das alte Rootzertifikat entfernen. Entfernen Sie Zertifikate nur, wenn Sie sicher sind, dass sie nicht mehr verwendet werden.

## Festlegen des Schwellenwerts für Warnungen zum Ablauf von vCenter-Zertifikaten

Ab vSphere 6.0 überwacht vCenter Server alle Zertifikate in VMware Endpoint Certificate Store (VECS) und stellt einen Alarm aus, wenn ein Zertifikat in 30 oder weniger Tagen abläuft. Mithilfe der erweiterten Option `vpxd.cert.threshold` können Sie festlegen, wie früh Sie gewarnt werden.

### Verfahren

1 Melden Sie sich beim vSphere Client an.

2 Wählen Sie das vCenter Server-Objekt aus und klicken Sie auf **Konfigurieren**.

3 Klicken Sie auf **Erweiterte Einstellungen**.

4 Klicken Sie auf **Einstellungen bearbeiten** und filtern Sie nach dem **`Schwellenwert`**.

5 Ändern Sie die Einstellung von `vpxd.cert.threshold` auf den gewünschten Wert und klicken Sie auf **Speichern**.

## Ersetzen von Zertifikaten durch neue VMCA-signierte Zertifikate über den vSphere Client

Sie können alle VMCA-signierten Zertifikate durch neue VMCA-signierte Zertifikate ersetzen. Dieser Vorgang wird als Verlängern von Zertifikaten bezeichnet. Sie können einzelne Zertifikate oder alle Zertifikate in Ihrer Umgebung über den vSphere Client verlängern.

### Voraussetzungen

Für die Zertifikatsverwaltung müssen Sie das Kennwort des Administrators für die lokale Domäne angeben (standardmäßig administrator@vsphere.local). Wenn Sie Zertifikate für ein vCenter Server-System verlängern, müssen Sie auch die vCenter Single Sign On-Anmeldedaten eines Benutzers mit Administratorrechten für das vCenter Server-System eingeben.

Verfahren

1 Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.

2 Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

   Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.

3 Navigieren Sie zur Benutzeroberfläche für die Zertifikatsverwaltung.

   a Wählen Sie im Menü **Home** die Option **Verwaltung** aus.

   b Klicken Sie unter **Zertifikate** auf **Zertifikatsverwaltung**.

4 Geben Sie die Anmeldedaten für Ihren vCenter Server ein.

5 Verlängern Sie das Maschinen-SSL-Zertifikat für das lokale System.

   a Wählen Sie **Maschinen-SSL-Zertifikat** aus.

   b Klicken Sie auf **Aktionen > Verlängern**.

   c Klicken Sie auf **Verlängern**.

      Es wird eine Meldung angezeigt, dass das Zertifikat verlängert wird.

6 (Optional) Verlängern Sie die Lösungsbenutzerzertifikate für das lokale System.

   a Wählen Sie unter **Lösungszertifikate** ein Zertifikat aus.

   b Klicken Sie auf **Aktionen > Verlängern**, um einzelne ausgewählte Zertifikate zu verlängern, oder klicken Sie auf **Alle verlängern**, um alle Lösungsbenutzerzertifikate zu verlängern.

      Es wird eine Meldung angezeigt, dass das Zertifikat verlängert wird.

7 Wenn in Ihrer Umgebung ein externer Platform Services Controller vorhanden ist, können Sie die Zertifikate für jedes vCenter Server-System verlängern.

   a Klicken Sie im Bereich „Zertifikatsverwaltung“ auf die Schaltfläche **Abmelden**.

   b Geben Sie, wenn Sie dazu aufgefordert werden, die IP-Adresse oder den FQDN des vCenter Server-Systems und den Benutzernamen und das Kennwort eines vCenter Server-Administrators an, der sich bei vCenter Single Sign On authentifizieren kann.

   c Verlängern Sie das Maschinen-SSL-Zertifikat auf dem vCenter Server und optional jedes Lösungsbenutzerzertifikat.

   d Falls mehrere vCenter Server-Systeme in Ihrer Umgebung vorhanden sind, wiederholen Sie den Vorgang für jedes System.

#### Nächste Schritte

Starten Sie die Dienste auf dem Platform Services Controller neu. Sie können entweder den Platform Services Controller neu starten oder die folgenden Befehle über die Befehlszeile ausführen:

#### Windows

Unter Windows befindet sich der Befehl `service-control` unter *VCENTER_INSTALL_PATH*\bin.

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

#### vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

## Einrichten Ihres Systems für die Verwendung benutzerdefinierter Zertifikate des Platform Services Controller

Sie können den Platform Services Controller verwenden, um Ihre Umgebung für die Verwendung benutzerdefinierter Zertifikate einzurichten.

Mithilfe des Dienstprogramms Certificate Manager können Sie Zertifikatssignieranforderungen (Certificate Signing Requests, CSRs) für jede Maschine und für jeden Lösungsbenutzer generieren. Sie können auch CSRs für jede Maschine generieren und Zertifikate ersetzen, wenn Sie diese von der Drittanbieter-Zertifizierungsstelle erhalten. Verwenden Sie dafür den vSphere Client. Wenn Sie die CSRs an Ihre interne oder Drittanbieter-Zertifizierungsstelle übermitteln, gibt die Zertifizierungsstelle signierte Zertifikate und das Rootzertifikat zurück. Sie können sowohl das Rootzertifikat als auch die signierten Zertifikate aus der Platform Services Controller-Benutzerschnittstelle hochladen.

### Generieren einer Zertifikatssignieranforderung (Certificate Signing Request, CSR) für ein Maschinen-SSL-Zertifikat mithilfe des vSphere Client (benutzerdefinierte Zertifikate)

Das Maschinen-SSL-Zertifikat wird vom Reverse-Proxy-Dienst für jeden Verwaltungsknoten, Platform Services Controller und jede eingebettete Bereitstellung verwendet. Für jede Maschine ist ein Maschinen-SSL-Zertifikat für die sichere Kommunikation mit anderen Diensten erforderlich. Sie können den vSphere Client verwenden, um eine Zertifikatssignieranforderung für das Maschinen-SSL-Zertifikat zu generieren und das Zertifikat zu ersetzen, sobald es bereit ist.

### Voraussetzungen

Das Zertifikat muss die folgenden Anforderungen erfüllen:

- Schlüsselgröße: mindestens 2.048 Bit (PEM-kodiert)
- CRT-Format
- x509 Version 3
- „SubjectAltName“ muss DNS-Name=<Maschinen-FQDN> enthalten.
- Enthält die folgenden Schlüsselverwendungen: digitale Signatur, Schlüsselverschlüsselung

**Hinweis** CRL-Verteilungspunkte, Zugriff auf Zertifizierungsstelleninfos oder Zertifikatvorlageninformationen dürfen in benutzerdefinierten Zertifikaten nicht verwendet werden.

Das Generieren einer Zertifikatssignieranforderung für das Maschinen-SSL-Zertifikat wird nur auf der vCenter Server Appliance unterstützt. Es wird auf einer Windows-Installation von vCenter Server nicht unterstützt.

### Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.
2. Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

   Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.
3. Navigieren Sie zur Benutzeroberfläche für die Zertifikatsverwaltung.
   a. Wählen Sie im Menü **Home** die Option **Verwaltung** aus.
   b. Klicken Sie unter **Zertifikate** auf **Zertifikatsverwaltung**.
4. Geben Sie die Anmeldedaten für Ihren vCenter Server ein.
5. Generieren Sie die Zertifikatsignieranforderung (Certificate Signing Request, CSR).
   a. Klicken Sie unter **Maschinen-SSL-Zertifikat** für das zu ersetzende Zertifikat auf **Aktionen > Zertifikatssignieranforderung generieren**.
   b. Geben Sie die Zertifikatsinformationen ein und klicken Sie auf **Weiter**.
   c. Kopieren Sie die Zertifikatssignieranforderung oder laden Sie sie herunter.
   d. Klicken Sie auf **Beenden**.
   e. Übermitteln Sie die Zertifikatssignieranforderung an Ihre Zertifizierungsstelle.

### Nächste Schritte

Wenn das Zertifikat von der Zertifizierungsstelle zurückgegeben wird, ersetzen Sie das vorhandene Zertifikat im Zertifikatspeicher. Weitere Informationen hierzu finden Sie unter Hinzufügen benutzerdefinierter Zertifikate aus dem Platform Services Controller.

## Generieren von Zertifikatssignieranforderungen mit vSphere Certificate Manager (benutzerdefinierte Zertifikate)

Mithilfe von vSphere Certificate Manager können Sie Zertifikatssignieranforderungen (Certificate Signing Requests, CSRs) generieren, die Sie anschließend mit Ihrer Unternehmenszertifizierungsstelle verwenden oder an eine externe Zertifizierungsstelle senden können. Sie können die Zertifikate mit den unterschiedlichen unterstützten Ersetzungsvorgängen von Zertifikaten verwenden.

Sie können das Certificate Manager-Tool wie folgt über die Befehlszeile ausführen:

**Windows**

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

**Linux**

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

### Voraussetzungen

vSphere Certificate Manager fordert Sie zur Eingabe von Informationen auf. Die Eingabeaufforderungen sind abhängig von Ihrer Umgebung und vom Zertifikatstyp, den Sie ersetzen möchten.

- Beim Generieren von Zertifikatssignieranforderungen werden Sie generell aufgefordert, das Kennwort für den Benutzer „administrator@vsphere.local“ bzw. den Administrator für die vCenter Single Sign On-Domäne, mit der Sie eine Verbindung herstellen, einzugeben.
- Wenn Sie eine Zertifikatssignieranforderung in einer Umgebung mit einem externen Platform Services Controller generieren, werden Sie zur Eingabe des Hostnamens oder der IP-Adresse für den Platform Services Controller aufgefordert.
- Zum Generieren einer Zertifikatssignieranforderung für ein Maschinen-SSL-Zertifikat werden Sie zur Eingabe von Zertifikateigenschaften aufgefordert, die in der Datei `certool.cfg` gespeichert sind. Für die meisten Felder können Sie den Standardwert übernehmen oder aber standortspezifische Werte eingeben. Der FQDN der Maschine ist erforderlich.

### Verfahren

1. Starten Sie vSphere Certificate Manager auf jeder Maschine in Ihrer Umgebung und wählen Sie Option 1 aus.
2. Geben Sie, wenn Sie dazu aufgefordert werden, das Kennwort sowie die IP-Adresse oder den Hostnamen für den Platform Services Controller ein.

3 Wählen Sie Option 1 aus, um die Zertifikatssignieranforderung zu generieren, befolgen Sie die Anweisungen und beenden Sie Certificate Manager.

   Im Rahmen dieses Vorgangs müssen Sie ein Verzeichnis angeben. Certificate Manager speichert die Zertifikats- und Schlüsseldateien in dem Verzeichnis.

4 Wenn Sie alle Lösungsbenutzerzertifikate ersetzen möchten, starten Sie Certificate Manager neu.

5 Wählen Sie Option 5 aus.

6 Geben Sie, wenn Sie dazu aufgefordert werden, das Kennwort sowie die IP-Adresse oder den Hostnamen für den Platform Services Controller ein.

7 Wählen Sie Option 1 aus, um die Zertifikatssignieranforderungen zu generieren, befolgen Sie die Anweisungen und beenden Sie Certificate Manager.

   Im Rahmen dieses Vorgangs müssen Sie ein Verzeichnis angeben. Certificate Manager speichert die Zertifikats- und Schlüsseldateien in dem Verzeichnis.

   Certificate Manager generiert auf jedem Platform Services Controller-Knoten je ein Zertifikats- und Schlüsselpaar. Certificate Manager generiert auf jedem vCenter Server-Knoten je vier Zertifikats- und Schlüsselpaare.

#### Nächste Schritte

Führen Sie die Zertifikatsersetzung durch.

## Hinzufügen eines vertrauenswürdigen Rootzertifikats zum Zertifikatspeicher

Wenn Sie in Ihrer Umgebung Drittanbieterzertifikate verwenden möchten, müssen Sie ein vertrauenswürdiges Rootzertifikat zum Zertifikatspeicher hinzufügen.

#### Voraussetzungen

Beziehen Sie das benutzerdefinierte Rootzertifikat von Ihrer Drittanbieter- oder internen Zertifizierungsstelle.

#### Verfahren

1 Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.

2 Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

   Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.

3 Navigieren Sie zur Benutzeroberfläche für die Zertifikatsverwaltung.

   a Wählen Sie im Menü **Home** die Option **Verwaltung** aus.

   b Klicken Sie unter **Zertifikate** auf **Zertifikatsverwaltung**.

4 Geben Sie die Anmeldedaten für Ihren vCenter Server ein.

5 Klicken Sie unter **Vertrauenswürdige Stammzertifikate** auf **Hinzufügen**.

6 Klicken Sie auf **Durchsuchen** und wählen Sie den Speicherort der Zertifikatskette aus.

   Sie können Dateien des Typs CER, PEM oder CRT verwenden.

7 Klicken Sie auf **Hinzufügen**.

   Das Zertifikat wird zum Speicher hinzugefügt.

#### Nächste Schritte

Ersetzen Sie die Maschinen-SSL-Zertifikate und optional auch die Lösungsbenutzerzertifikate durch die Zertifikate, die von dieser Zertifizierungsstelle signiert wurden.

## Hinzufügen benutzerdefinierter Zertifikate aus dem Platform Services Controller

Sie können benutzerdefinierte Maschinen-SSL-Zertifikate und benutzerdefinierte Lösungsbenutzerzertifikate zum Zertifikatspeicher des Platform Services Controller hinzufügen.

In den meisten Fällen ist es ausreichend, das Maschinen-SSL-Zertifikat für jede Komponente zu ersetzen. Das Lösungsbenutzerzertifikat bleibt hinter einem Proxy-Server.

#### Voraussetzungen

Generieren Sie Zertifikatssignieranforderungen (Certificate Signing Requests, CSRs) für jedes zu ersetzende Zertifikat. Sie können die CSRs mit dem Dienstprogramm Certificate Manager generieren. Sie können auch eine CSR für ein Maschinen-SSL-Zertifikat mit dem vSphere Client generieren. Speichern Sie das Zertifikat und den privaten Schlüssel an einem Speicherort, auf den der Platform Services Controller zugreifen kann.

#### Verfahren

1 Melden Sie sich mit dem vSphere Client beim vCenter Server an, der mit dem Platform Services Controller verbunden ist.

2 Geben Sie den Benutzernamen und das Kennwort für „administrator@vsphere.local“ oder für ein anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an.

   Falls Sie eine andere Domäne während der Installation angegeben haben, melden Sie sich als administrator@*meinedomäne* an.

3 Navigieren Sie zur Benutzeroberfläche für die Zertifikatsverwaltung.

   a Wählen Sie im Menü **Home** die Option **Verwaltung** aus.

   b Klicken Sie unter **Zertifikate** auf **Zertifikatsverwaltung**.

4 Geben Sie die Anmeldedaten für Ihren vCenter Server ein.

5 Führen Sie diese Schritte durch, um ein Maschinen-SSL-Zertifikat zu ersetzen:

   a Klicken Sie unter **Maschinen-SSL-Zertifikat** für das Zertifikat, das Sie ersetzen möchten, auf **Aktionen > Ersetzen**.

   b Suchen Sie das Maschinen-SSL-Zertifikat (`.cer`-, `.pem`- oder `.crt`-Datei) und den privaten Schlüssel (`.key`-Datei).

   c Klicken Sie auf **Ersetzen**.

6 Befolgen Sie zum Ersetzen von Lösungsbenutzerzertifikaten diese Schritte:

   a Klicken Sie unter **Lösungszertifikate** für das erste der Zertifikate für eine Komponente, zum Beispiel **Rechner**, auf **Aktionen > Ersetzen**.

   b Klicken Sie auf **Durchsuchen**, um die Zertifikatskette zu ersetzen. Klicken Sie anschließend auf **Durchsuchen**, um den privaten Schlüssel zu ersetzen.

   c Klicken Sie auf **Ersetzen**.

   d Wiederholen Sie den Vorgang für die übrigen Zertifikate derselben Komponente.

#### Ergebnisse

Es wird eine Meldung angezeigt, dass das Zertifikat ersetzt wurde.

#### Nächste Schritte

Starten Sie die Dienste auf dem Platform Services Controller neu. Sie können entweder den Platform Services Controller neu starten oder die folgenden Befehle über die Befehlszeile ausführen:

**Windows**

Unter Windows befindet sich der Befehl `service-control` unter *`VCENTER_INSTALL_PATH`*`\bin`.

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

**vCenter Server Appliance**

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

# Verwalten von Zertifikaten mit dem vSphere Web Client

Sie können die Zertifikate von vSphere Web Client aus untersuchen. Führen Sie alle anderen Verwaltungsaufgaben über den vSphere Client aus.

Weitere Informationen hierzu finden Sie unter Verwalten von Zertifikaten mit dem vSphere Client.

## Anzeigen von vCenter-Zertifikaten mit dem vSphere Web Client

Sie können die der VMware-Zertifizierungsstelle (VMCA) bekannten Zertifikate anzeigen, um festzustellen, ob aktive Zertifikate demnächst ablaufen, um abgelaufene Zertifikate zu überprüfen und um den Status des Rootzertifikats anzuzeigen. Alle Zertifikatsverwaltungsaufgaben führen Sie mit den Zertifikatsverwaltungs-CLIs aus.

Sie zeigen Zertifikate für die VMCA-Instanz an, die in Ihrer eingebetteten Bereitstellung oder im Platform Services Controller enthalten ist. Zertifikatinformationen werden für die Instanzen des VMware-Verzeichnisdiensts (vmdir) repliziert.

Wenn Sie versuchen, Zertifikate im vSphere Web Client anzuzeigen, werden Sie zur Eingabe eines Benutzernamens und eines Kennworts aufgefordert. Geben Sie den Benutzernamen und das Kennwort eines Benutzers mit Rechten für die VMware-Zertifizierungsstelle an, d. h., eines Benutzers in der vCenter Single Sign On-Gruppe „CAAdmins“.

### Verfahren

1. Melden Sie sich mit dem vSphere Web Client beim vCenter Server als „administrator@vsphere.local“ oder als ein anderer Benutzer der vCenter Single Sign On-Gruppe „CAAdmins“ an.
2. Wählen Sie im Menü „Home“ die Option **Verwaltung** aus.
3. Klicken Sie auf **Bereitstellung > Systemkonfiguration**.
4. Klicken Sie auf **Knoten** und wählen Sie einen Host unter der Liste **Knoten** aus.
5. Klicken Sie auf die Registerkarte **Verwalten** und klicken Sie anschließend auf **Zertifizierungsstelle**.
6. Klicken Sie auf den Zertifikatstyp, für den Sie Zertifikatinformation anzeigen möchten.

| Option | Beschreibung |
|---|---|
| **Aktive Zertifikate** | Zeigt aktive Zertifikate einschließlich der Validierungsinformationen an. Das grüne Symbol „Gültig bis“ wird geändert, wenn das Zertifikat demnächst abläuft. |
| **Widerrufene Zertifikate** | Zeigt die Liste der widerrufenen Zertifikate an. Dies wird in dieser Version nicht unterstützt. |
| **Abgelaufene Zertifikate** | Listet abgelaufene Zertifikate auf. |
| **Rootzertifikate** | Zeigt die für diese Instanz der VMware-Zertifizierungsstelle verfügbaren Rootzertifikate an. |

7. Wählen Sie ein Zertifikat aus und klicken Sie auf die Schaltfläche **Zertifikatsdetails anzeigen**, um die Zertifikatsdetails anzuzeigen.

   Zu den Details gehören der Subjektname, der Aussteller, die Gültigkeit und der Algorithmus.

# Verwalten von Zertifikaten mit dem Dienstprogramm vSphere Certificate Manager

Mit dem Dienstprogramm vSphere Certificate Manager können Sie die meisten Zertifikatverwaltungsaufgaben interaktiv über die Befehlszeile ausführen. vSphere Certificate Manager fordert Sie zur Eingabe der auszuführenden Aufgabe, der Zertifikatspeicherorte und etwaiger sonstiger Informationen auf und beendet und startet dann Dienste und ersetzt Zertifikate.

Bei Verwendung von vSphere Certificate Manager müssen Sie die Zertifikate nicht in VECS (VMware Endpoint Certificate Store) platzieren und müssen die Dienste nicht starten und beenden.

Bevor Sie vSphere Certificate Manager ausführen, sollten Sie sich unbedingt mit dem Ersetzungsvorgang vertraut machen und die Zertifikate suchen, die Sie verwenden möchten.

**Vorsicht** Mit vSphere Certificate Manager kann nur eine Ausführungsebene rückgängig gemacht werden. Wenn Sie vSphere Certificate Manager zweimal ausführen und feststellen, dass Sie Ihre Umgebung versehentlich beschädigt haben, kann mit dem Tool die erste der beiden Ausführungsinstanzen nicht rückgängig gemacht werden.

## Speicherort des Dienstprogramms Certificate Manager

Sie können das Tool wie folgt in der Befehlszeile ausführen:

### Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

### Linux

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

### Verfahren

1 Certificate Manager-Optionen und die Workflows in diesem Dokument

   Die Certificate Manager-Optionen werden nacheinander ausgeführt, um einen Workflow abzuschließen. Verschiedene Optionen, wie beispielsweise das Generieren von CSRs, werden in unterschiedlichen Workflows verwendet.

2 Neugenerieren eines neuen VMCA-Rootzertifikats und Ersetzen aller Zertifikate

   Sie können das VMCA-Rootzertifikat neu generieren und das lokale Maschinen-SSL-Zertifikat sowie die lokalen Lösungsbenutzerzertifikate durch VMCA-signierte Zertifikate ersetzen. Bei Bereitstellungen mit mehreren Knoten führen Sie vSphere Certificate Manager mit dieser Option auf dem Platform Services Controller aus. Führen Sie anschließend das Dienstprogramm erneut auf allen anderen Knoten aus und wählen Sie `Replace Machine SSL certificate with VMCA Certificate` und `Replace Solution user certificates with VMCA certificates` aus.

3 Festlegen von VMCA als Zwischenzertifizierungsstelle (Certificate Manager)

   Sie können VMCA als Zwischenzertifizierungsstelle festlegen, indem Sie den Eingabeaufforderungen des Dienstprogramms Certificate Manager folgen. Nachdem Sie diesen Vorgang durchgeführt haben, signiert VMCA alle neuen Zertifikate mit der vollständigen Zertifikatskette. Wenn Sie möchten, können Sie Certificate Manager zum Ersetzen aller vorhandenen Zertifikate durch neue VMCA-signierte Zertifikate verwenden.

4 Ersetzen aller Zertifikate durch benutzerdefinierte Zertifikate (Certificate Manager)

   Sie können das Dienstprogramm vSphere Certificate Manager verwenden, um alle Zertifikate durch benutzerdefinierte Zertifikate zu ersetzen. Bevor Sie den Vorgang starten, müssen Sie Zertifikatssignieranforderungen (CSRs) an Ihre Zertifizierungsstelle (CA) senden. Sie können Certificate Manager zum Generieren der CSRs verwenden.

5 Rückgängigmachen des zuletzt ausgeführten Vorgangs durch die erneute Veröffentlichung alter Zertifikate

   Wenn Sie einen Zertifikatverwaltungsvorgang mithilfe von vSphere Certificate Manager durchführen, wird der aktuelle Zertifikatstatus im BACKUP_STORE-Speicher in VECS gespeichert, bevor Zertifikate ersetzt werden. Sie können den zuletzt ausgeführten Vorgang rückgängig machen und den vorherigen Status wiederherstellen.

6 Alle Zertifikate zurücksetzen

   Verwenden Sie die Option `Alle Zertifikate zurücksetzen`, wenn Sie alle vorhandenen vCenter-Zertifikate durch VMCA-signierte Zertifikate ersetzen möchten.

## Certificate Manager-Optionen und die Workflows in diesem Dokument

Die Certificate Manager-Optionen werden nacheinander ausgeführt, um einen Workflow abzuschließen. Verschiedene Optionen, wie beispielsweise das Generieren von CSRs, werden in unterschiedlichen Workflows verwendet.

### Ersetzen des VMCA-Rootzertifikats durch ein benutzerdefiniertes Signaturzertifikat und Ersetzen aller Zertifikate.

Dieser aus einer Option bestehende Workflow (Option 2) kann eigenständig oder im Zwischenzertifikat-Workflow verwendet werden. Weitere Informationen hierzu finden Sie unter Neugenerieren eines neuen VMCA-Rootzertifikats und Ersetzen aller Zertifikate.

## Festlegen von VMCA als Zwischenzertifizierungsstelle

Um VMCA als Zwischenzertifizierungsstelle festzulegen, müssen Sie Certificate Manager mehrmals ausführen. Der Workflow umfasst einen vollständigen Satz von Schritten zum Ersetzen von Maschinen-SSL-Zertifikaten und Lösungsbenutzerzertifikaten. Darin wird erläutert, wie in Umgebungen mit eingebettetem Platform Services Controller oder externem Platform Services Controller vorzugehen ist.

1 Zum Generieren einer CSR wählen Sie Option 2 aus: Ersetzen des VMCA-Rootzertifikats durch ein benutzerdefiniertes Signaturzertifikat und Ersetzen aller Zertifikate. Danach müssen Sie möglicherweise einige Informationen zum Zertifikat angeben. Wenn Sie erneut zur Angabe einer Option aufgefordert werden, wählen Sie Option 1 aus.

   Übermitteln Sie die CSR an die externe Zertifizierungsstelle oder die Unternehmenszertifizierungsstelle. Sie erhalten ein signiertes Zertifikat und ein Rootzertifikat von der Zertifizierungsstelle.

2 Kombinieren Sie das VMCA-Rootzertifikat mit dem Rootzertifikat der Zertifizierungsstelle und speichern Sie die Datei.

3 Wählen Sie Option 2 aus: Ersetzen des VMCA-Rootzertifikats durch ein benutzerdefiniertes Signaturzertifikat und Ersetzen aller Zertifikate. Mit diesem Verfahren werden alle Zertifikate auf der lokalen Maschine ersetzt.

4 In einer Bereitstellung mit mehreren Knoten müssen Sie Zertifikate auf jedem Knoten ersetzen.

   a Zuerst ersetzen Sie das Maschinen-SSL-Zertifikat durch das (neue) VMCA-Zertifikat (Option 3).

   b Anschließend ersetzen Sie die Lösungsbenutzerzertifikate durch das (neue) VMCA-Zertifikat (Option 6).

Weitere Informationen hierzu finden Sie unter Festlegen von VMCA als Zwischenzertifizierungsstelle (Certificate Manager).

## Ersetzen aller Zertifikate durch benutzerdefinierte Zertifikate

Um alle Zertifikate durch benutzerdefinierte Zertifikate zu ersetzen, müssen Sie Certificate Manager mehrmals ausführen. Der Workflow umfasst einen vollständigen Satz von Schritten zum Ersetzen von Maschinen-SSL-Zertifikaten und Lösungsbenutzerzertifikaten. Darin wird erläutert, wie in Umgebungen mit eingebettetem Platform Services Controller oder externem Platform Services Controller vorzugehen ist.

1 Zertifikatssignieranforderungen für das Maschinen-SSL-Zertifikat und die Lösungsbenutzerzertifikate werden auf jeder Maschine separat generiert.

   a Zum Generieren von CSRs für das Maschinen-SSL-Zertifikat wählen Sie Option 1 aus.

   b Wenn die Unternehmensrichtlinien das Ersetzen aller Zertifikate verlangen, wählen Sie außerdem Option 5 aus.

2 Nachdem Sie die signierten Zertifikate und das Rootzertifikat von Ihrer Zertifizierungsstelle erhalten haben, ersetzen Sie das Maschinen-SSL-Zertifikat auf jeder Maschine mithilfe von Option 1.

3 Falls auch die Lösungsbenutzerzertifikate ersetzt werden sollen, wählen Sie Option 5 aus.

4 In einer Bereitstellung mit mehreren Knoten müssen Sie den Vorgang anschließend auf jedem Knoten wiederholen.

Weitere Informationen hierzu finden Sie unter Ersetzen aller Zertifikate durch benutzerdefinierte Zertifikate (Certificate Manager).

**Hinweis** Beginnend mit vSphere 6.5 wird folgende Eingabeaufforderung angezeigt, wenn Sie das Zertifikatsmanager-Dienstprogramm ausführen:

```
Enter proper value for VMCA 'Name':
```

Reagieren Sie auf die Eingabeaufforderung, indem Sie den vollqualifizierten Domänennamen der Maschine, auf der die Zertifikatskonfiguration ausgeführt wird, eingeben.

## Neugenerieren eines neuen VMCA-Rootzertifikats und Ersetzen aller Zertifikate

Sie können das VMCA-Rootzertifikat neu generieren und das lokale Maschinen-SSL-Zertifikat sowie die lokalen Lösungsbenutzerzertifikate durch VMCA-signierte Zertifikate ersetzen. Bei Bereitstellungen mit mehreren Knoten führen Sie vSphere Certificate Manager mit dieser Option auf dem Platform Services Controller aus. Führen Sie anschließend das Dienstprogramm erneut auf allen anderen Knoten aus und wählen Sie `Replace Machine SSL certificate with VMCA Certificate` und `Replace Solution user certificates with VMCA certificates` aus.

Wenn Sie das vorhandene Maschinen-SSL-Zertifikat durch ein neues VMCA-signiertes Zertifikat ersetzen, werden Sie von vSphere Certificate Manager zur Eingabe von Informationen aufgefordert. vSphere Certificate Manager gibt alle Werte mit Ausnahme des Kennworts und der IP-Adresse des Platform Services Controller in die Datei `certool.cfg` ein.

- Kennwort für „administrator@vsphere.local“.
- Aus zwei Buchstaben bestehender Ländercode
- Name des Unternehmens
- Organisationsname
- Organisationseinheit
- Zustand
- Ort
- IP-Adresse (optional)
- E-Mail

- Hostname, d. h., der vollqualifizierte Domänenname der Maschine, für die Sie das Zertifikat ersetzen möchten. Wenn der Hostname nicht mit dem FQDN übereinstimmt, wird die Zertifikatsersetzung nicht ordnungsgemäß abgeschlossen und Ihre Umgebung weist möglicherweise einen instabilen Status auf.
- IP-Adresse des Platform Services Controllers, wenn Sie den Befehl auf einem Verwaltungsknoten ausführen.
- VMCA-Name, der der vollqualifizierte Domänenname der Maschine ist, auf der die Zertifikatskonfiguration ausgeführt wird.

### Voraussetzungen

Sie müssen die folgenden Informationen kennen, wenn Sie vSphere Certificate Manager mit dieser Option ausführen.

- Kennwort für „administrator@vsphere.local“.
- Der FQDN der Maschine, für die Sie ein neues VMCA-signiertes Zertifikat generieren möchten. Für alle anderen Eigenschaften werden standardmäßig die vordefinierten Werte verwendet, die Sie jedoch ändern können.

### Verfahren

1 Melden Sie sich bei vCenter Server in einer eingebetteten Bereitstellung oder auf einem Platform Services Controller an und starten Sie den vSphere Certificate Manager.

| Betriebssystem | Befehl |
|---|---|
| **Linux** | `/usr/lib/vmware-vmca/bin/certificate-manager` |
| **Windows** | `C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat` |

2 Wählen Sie Option 4 `Regenerate a new VMCA Root Certificate and replace all certificates` aus.

3 Beantworten Sie die Eingabeaufforderungen.

Certificate Manager generiert ein neues VMCA-Rootzertifikat basierend auf Ihrer Eingabe und ersetzt alle Zertifikate in dem System, in dem Certificate Manager ausgeführt wird. Wenn Sie eine eingebettete Bereitstellung verwenden, ist der Ersetzungsvorgang abgeschlossen, nachdem Certificate Manager die Dienste neu gestartet hat.

4 Falls Ihre Umgebung einen externen Platform Services Controller enthält, müssen Sie die Zertifikate in jedem vCenter Server-System ersetzen.

a Melden Sie sich beim vCenter Server-System an.

b Beenden Sie alle Dienste und starten Sie die Dienste für die Zertifikaterstellung, Weitergabe und Speicherung.

Die Dienstnamen sind unter Windows und bei der vCenter Server Appliance unterschiedlich.

**Windows**

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

**vCenter Server Appliance**

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

c Starten Sie alle Dienste neu.

```
service-control --start --all
```

d Führen Sie zum Ersetzen des SSL-Zertifikats der Maschine vSphere Certificate Manager mit Option 3, `Replace Machine SSL certificate with VMCA Certificate`, aus.

e Führen Sie zum Ersetzen der Lösungsbenutzerzertifikate Certificate Manager mit Option 6, `Replace Solution user certificates with VMCA certificates`, aus.

## Festlegen von VMCA als Zwischenzertifizierungsstelle (Certificate Manager)

Sie können VMCA als Zwischenzertifizierungsstelle festlegen, indem Sie den Eingabeaufforderungen des Dienstprogramms Certificate Manager folgen. Nachdem Sie diesen Vorgang durchgeführt haben, signiert VMCA alle neuen Zertifikate mit der vollständigen Zertifikatskette. Wenn Sie möchten, können Sie Certificate Manager zum Ersetzen aller vorhandenen Zertifikate durch neue VMCA-signierte Zertifikate verwenden.

Um VMCA als Zwischenzertifizierungsstelle festzulegen, müssen Sie Certificate Manager mehrmals ausführen. Der Workflow umfasst einen vollständigen Satz von Schritten zum Ersetzen von Maschinen-SSL-Zertifikaten und Lösungsbenutzerzertifikaten. Darin wird erläutert, wie in Umgebungen mit eingebettetem Platform Services Controller oder externem Platform Services Controller vorzugehen ist.

1 Zum Generieren einer CSR wählen Sie Option 1 aus: Ersetzen des Maschinen-SSL-Zertifikats durch ein benutzerdefiniertes Zertifikat.

   Sie erhalten ein signiertes Zertifikat und ein Rootzertifikat von der Zertifizierungsstelle.

2 Kombinieren Sie das VMCA-Rootzertifikat mit dem Rootzertifikat der Zertifizierungsstelle und speichern Sie die Datei.

3 Wählen Sie Option 2 aus: Ersetzen des VMCA-Rootzertifikats durch ein benutzerdefiniertes Signaturzertifikat und Ersetzen aller Zertifikate. Mit diesem Verfahren werden alle Zertifikate auf der lokalen Maschine ersetzt.

4 In einer Bereitstellung mit mehreren Knoten müssen Sie Zertifikate auf jedem Knoten ersetzen.

   a Zuerst ersetzen Sie das Maschinen-SSL-Zertifikat durch das (neue) VMCA-Zertifikat (Option 3).

   b Anschließend ersetzen Sie die Lösungsbenutzerzertifikate durch das (neue) VMCA-Zertifikat (Option 6).

### Verfahren

1 Generieren von CSRs mit vSphere Certificate Manager und Vorbereiten des Rootzertifikats (Zwischenzertifizierungsstelle)

   Mithilfe von vSphere Certificate Manager können Zertifikatssignieranforderungen (Certificate Signing Requests, CSRs) generiert werden. Übermitteln Sie diese CSRs zur Unterzeichnung an Ihre Unternehmenszertifizierungsstelle oder an eine externe Zertifizierungsstelle. Sie können die signierten Zertifikate mit den unterschiedlichen unterstützten Zertifikatsersetzungsvorgängen verwenden.

2 Ersetzen des VMCA-Rootzertifikats durch ein benutzerdefiniertes Signaturzertifikat und Ersetzen aller Zertifikate

   Sie können vSphere Certificate Manager zum Generieren eines CSR und zum Senden des CSR an eine Unternehmens- oder Drittanbieter-Zertifizierungsstelle zum Signieren verwenden. Anschließend können Sie das VMCA-Root-Zertifikat durch ein benutzerdefiniertes Signaturzertifikat und alle bestehenden Zertifikate durch von der Zertifizierungsstelle signierte Zertifikate ersetzen.

3 Ersetzen des Maschinen-SSL-Zertifikats durch ein VMCA-Zertifikat (Zwischenzertifizierungsstelle)

   In einer Bereitstellung mit mehreren Knoten, die VMCA als Zwischenzertifizierungsstelle verwendet, müssen Sie das Maschinen-SSL-Zertifikat explizit ersetzen. Zuerst ersetzen Sie das VMCA-Stammzertifikat auf dem Platform Services Controller-Knoten; dann können Sie die Zertifikate auf den vCenter Server-Knoten ersetzen, damit die Zertifikate in der gesamte Kette signiert sind. Sie können diese Option auch verwenden, um beschädigte oder in Kürze ablaufende Maschinen-SSL-Zertifikate zu ersetzen.

4 Ersetzen der Lösungsbenutzerzertifikate durch VMCA-Zertifikate (Zwischenzertifizierungsstelle)

   Bei einer Umgebung mit mehreren Knoten, in der VMCA als Zwischenzertifizierungsstelle verwendet wird, müssen Sie die Lösungsbenutzerzertifikate explizit ersetzen. Zuerst ersetzen Sie das VMCA-Stammzertifikat auf dem Platform Services Controller-Knoten; dann können Sie die Zertifikate auf den vCenter Server-Knoten ersetzen, damit die Zertifikate in der gesamte Kette signiert sind. Sie können diese Option auch verwenden, um Lösungsbenutzerzertifikate zu ersetzen, die beschädigt sind oder im Begriff sind abzulaufen.

## Generieren von CSRs mit vSphere Certificate Manager und Vorbereiten des Rootzertifikats (Zwischenzertifizierungsstelle)

Mithilfe von vSphere Certificate Manager können Zertifikatssignieranforderungen (Certificate Signing Requests, CSRs) generiert werden. Übermitteln Sie diese CSRs zur Unterzeichnung an Ihre Unternehmenszertifizierungsstelle oder an eine externe Zertifizierungsstelle. Sie können die signierten Zertifikate mit den unterschiedlichen unterstützten Zertifikatsersetzungsvorgängen verwenden.

- Sie können vSphere Certificate Manager zum Generieren der CSR verwenden.
- Wenn Sie die CSR manuell erstellen möchten, muss das Zertifikat, das Sie zum Signieren senden, die folgenden Anforderungen erfüllen.
  - Schlüsselgröße: mindestens 2.048 Bit
  - PEM-Format. VMware unterstützt PKCS8 und PKCS1 (RSA-Schlüssel). Wenn Schlüssel zu VECS hinzugefügt werden, werden sie in PKCS8 konvertiert.
  - x509 Version 3
  - Wenn Sie benutzerdefinierte Zertifikate verwenden, muss die Zertifizierungsstellenerweiterung für Stammzertifikate auf „true“ festgelegt werden, und „cert sign“ muss in der Liste der Anforderungen vorhanden sein.
  - CRL-Signatur muss aktiviert sein.
  - Erweiterte Schlüsselverwendung kann entweder leer sein oder Serverauthentifizierung enthalten.
  - Keine explizite Beschränkung der Zertifikatskettenlänge. VMCA verwendet den OpenSSL-Standardwert von 10 Zertifikaten.

- Zertifikate mit Platzhalterzeichen oder mehr als einem DNS-Namen werden nicht unterstützt.
- Untergeordnete Zertifizierungsstellen von VMCA können nicht erstellt werden.

  Im VMware-Knowledgebase-Artikel „Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.0“ unter http://kb.vmware.com/kb/2112009 finden Sie ein Beispiel für die Verwendung der Microsoft-Zertifizierungsstelle.

### Voraussetzungen

vSphere Certificate Manager fordert Sie zur Eingabe von Informationen auf. Die Eingabeaufforderungen sind abhängig von Ihrer Umgebung und vom Zertifikatstyp, den Sie ersetzen möchten.

Beim Generieren von Zertifikatssignieranforderungen werden Sie generell aufgefordert, das Kennwort für den Benutzer „administrator@vsphere.local“ bzw. den Administrator für die vCenter Single Sign On-Domäne, mit der Sie eine Verbindung herstellen, einzugeben.

### Verfahren

1 Führen Sie vSphere Certificate Manager aus.

| Betriebssystem | Befehl |
|---|---|
| Windows | `cd "C:\Program Files\VMware\vCenter Server\vmcad"`<br>`certificate-manager` |
| Linux | `/usr/lib/vmware-vmca/bin/certificate-manager` |

2 Wählen Sie Option 2 aus.

  Anfänglich verwenden Sie diese Option zum Generieren der CSR, nicht zum Ersetzen von Zertifikaten.

3 Geben Sie, wenn Sie dazu aufgefordert werden, das Kennwort sowie die IP-Adresse oder den Hostnamen für den Platform Services Controller ein.

4 Wählen Sie Option 1 aus, um die Zertifikatssignieranforderung zu generieren, und befolgen Sie die Anweisungen.

  Im Rahmen dieses Vorgangs müssen Sie ein Verzeichnis angeben. Certificate Manager fügt das zu signierende Zertifikat (`*.csr`-Datei) und die entsprechende Schlüsseldatei (`*.key`-Datei) in das Verzeichnis ein.

5 Geben Sie der Zertifikatssignieranforderung (CSR) den Namen `root_signing_cert.csr`.

6 Senden Sie die CSR zum Signieren an die Zertifizierungsstelle in Ihrem Unternehmen oder eine externe Zertifizierungsstelle und geben Sie dem resultierenden signierten Zertifikat den Namen `root_signing_cert.cer`.

7 Kombinieren Sie in einem Texteditor die Zertifikate wie folgt.

```
-----BEGIN CERTIFICATE-----
Signed VMCA root certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

8 Speichern Sie die Datei unter dem Namen `root_signing_chain.cer`.

#### Nächste Schritte

Ersetzen Sie das vorhandene Rootzertifikat durch das verkettete Rootzertifikat. Weitere Informationen hierzu finden Sie unter Ersetzen des VMCA-Rootzertifikats durch ein benutzerdefiniertes Signaturzertifikat und Ersetzen aller Zertifikate.

## Ersetzen des VMCA-Rootzertifikats durch ein benutzerdefiniertes Signaturzertifikat und Ersetzen aller Zertifikate

Sie können vSphere Certificate Manager zum Generieren eines CSR und zum Senden des CSR an eine Unternehmens- oder Drittanbieter-Zertifizierungsstelle zum Signieren verwenden. Anschließend können Sie das VMCA-Root-Zertifikat durch ein benutzerdefiniertes Signaturzertifikat und alle bestehenden Zertifikate durch von der Zertifizierungsstelle signierte Zertifikate ersetzen.

vSphere Certificate Manager führen Sie für eine eingebettete Installation oder einen externen Platform Services Controller aus, um das VMCA-Rootzertifikat durch ein benutzerdefiniertes Signaturzertifikat zu ersetzen.

#### Voraussetzungen

- Generieren Sie die Zertifikatskette.
  - Sie können die CSR mithilfe des vSphere Certificate Manager oder manuell erstellen.
  - Nachdem Sie das signierte Zertifikat von Ihrer Drittanbieter- oder Unternehmenszertifizierungsstelle erhalten haben, kombinieren Sie es mit dem anfänglichen VMCA-Stammzertifikat, um die vollständige Zertifikatskette zu erstellen.

    Zertifikatsanforderungen und das Verfahren zum Kombinieren der Zertifikate finden Sie unter Generieren von CSRs mit vSphere Certificate Manager und Vorbereiten des Rootzertifikats (Zwischenzertifizierungsstelle).
- Sammeln Sie die erforderlichen Informationen.
  - Kennwort für „administrator@vsphere.local“.
  - Gültiges benutzerdefiniertes Zertifikat für Root (`.crt`-Datei).
  - Gültiger benutzerdefinierter Schlüssel für Root (`.key`-Datei).

Verfahren

1. Starten Sie vSphere Certificate Manager in einer eingebetteten Installation oder auf einem externen Platform Services Controller und wählen Sie Option 2 aus.
2. Wählen Sie erneut Option 2 aus, um die Zertifikatsersetzung zu starten, und befolgen Sie die Anweisungen.
   a. Geben Sie, wenn Sie dazu aufgefordert werden, den vollständigen Pfad zum Stammzertifikat an.
   b. Falls Sie Zertifikate erstmalig ersetzen, werden Sie zur Eingabe von Informationen für das Maschinen-SSL-Zertifikat aufgefordert.

      Diese Informationen beinhalten den erforderlichen FQDN der Maschine und werden in der Datei `certool.cfg` gespeichert.
3. Falls Sie das Rootzertifikat in einer Bereitstellung mit mehreren Knoten auf dem Platform Services Controller ersetzen, führen Sie für jeden vCenter Server-Knoten die folgenden Schritte aus.
   a. Starten Sie die Dienste auf dem vCenter Server-Knoten neu.
   b. Generieren Sie alle Zertifikate auf der vCenter Server-Instanz neu, indem Sie die Optionen 3 (`Replace Machine SSL certificate with VMCA Certificate`) und 6 (`Replace Solution user certificates with VMCA certificates`) verwenden.

   Beim Ersetzen der Zertifikate signiert VMCA mit der vollständigen Zertifikatskette.

Nächste Schritte

Wenn Sie das Upgrade von einer vSphere 5.x-Umgebung aus vornehmen, müssen Sie möglicherweise das vCenter Single Sign On-Zertifikat innerhalb von vmdir ersetzen. Weitere Informationen hierzu finden Sie unter Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus.

## Ersetzen des Maschinen-SSL-Zertifikats durch ein VMCA-Zertifikat (Zwischenzertifizierungsstelle)

In einer Bereitstellung mit mehreren Knoten, die VMCA als Zwischenzertifizierungsstelle verwendet, müssen Sie das Maschinen-SSL-Zertifikat explizit ersetzen. Zuerst ersetzen Sie das VMCA-Stammzertifikat auf dem Platform Services Controller-Knoten; dann können Sie die Zertifikate auf den vCenter Server-Knoten ersetzen, damit die Zertifikate in der gesamte Kette signiert sind. Sie können diese Option auch verwenden, um beschädigte oder in Kürze ablaufende Maschinen-SSL-Zertifikate zu ersetzen.

Wenn Sie das vorhandene Maschinen-SSL-Zertifikat durch ein neues VMCA-signiertes Zertifikat ersetzen, werden Sie von vSphere Certificate Manager zur Eingabe von Informationen aufgefordert. vSphere Certificate Manager gibt alle Werte mit Ausnahme des Kennworts und der IP-Adresse des Platform Services Controller in die Datei `certool.cfg` ein.

- Kennwort für „administrator@vsphere.local“.

- Aus zwei Buchstaben bestehender Ländercode
- Name des Unternehmens
- Organisationsname
- Organisationseinheit
- Zustand
- Ort
- IP-Adresse (optional)
- E-Mail
- Hostname, d. h., der vollqualifizierte Domänenname der Maschine, für die Sie das Zertifikat ersetzen möchten. Wenn der Hostname nicht mit dem FQDN übereinstimmt, wird die Zertifikatsersetzung nicht ordnungsgemäß abgeschlossen und Ihre Umgebung weist möglicherweise einen instabilen Status auf.
- IP-Adresse des Platform Services Controllers, wenn Sie den Befehl auf einem Verwaltungsknoten ausführen.
- VMCA-Name, der der vollqualifizierte Domänenname der Maschine ist, auf der die Zertifikatskonfiguration ausgeführt wird.

**Voraussetzungen**

- Starten Sie alle vCenter Server-Knoten explizit neu, falls Sie das VMCA-Stammzertifikat in einer Bereitstellung mit mehreren Knoten ersetzt haben.
- Sie müssen die folgenden Informationen kennen, um den Zertifikatsmanager mit dieser Option auszuführen.
  - Kennwort für „administrator@vsphere.local“.
  - Der FQDN der Maschine, für die Sie ein neues VMCA-signiertes Zertifikat generieren möchten. Für alle anderen Eigenschaften werden standardmäßig die vordefinierten Werte verwendet, die Sie jedoch ändern können.
  - Hostname oder IP-Adresse des Platform Services Controller, falls Sie sich auf einem vCenter Server-System mit einem externen Platform Services Controller befinden.

**Verfahren**

1. Starten Sie vSphere Certificate Manager und wählen Sie Option 3 aus.
2. Beantworten Sie die Eingabeaufforderungen.

   Certificate Manager speichert die Informationen in der Datei `certool.cfg`.

**Ergebnisse**

vSphere Certificate Manager ersetzt das Maschinen-SSL-Zertifikat.

### Ersetzen der Lösungsbenutzerzertifikate durch VMCA-Zertifikate (Zwischenzertifizierungsstelle)

Bei einer Umgebung mit mehreren Knoten, in der VMCA als Zwischenzertifizierungsstelle verwendet wird, müssen Sie die Lösungsbenutzerzertifikate explizit ersetzen. Zuerst ersetzen Sie das VMCA-Stammzertifikat auf dem Platform Services Controller-Knoten; dann können Sie die Zertifikate auf den vCenter Server-Knoten ersetzen, damit die Zertifikate in der gesamte Kette signiert sind. Sie können diese Option auch verwenden, um Lösungsbenutzerzertifikate zu ersetzen, die beschädigt sind oder im Begriff sind abzulaufen.

#### Voraussetzungen

- Starten Sie alle vCenter Server-Knoten explizit neu, falls Sie das VMCA-Stammzertifikat in einer Bereitstellung mit mehreren Knoten ersetzt haben.
- Sie müssen die folgenden Informationen kennen, um den Zertifikatsmanager mit dieser Option auszuführen.
  - Kennwort für „administrator@vsphere.local“.
  - Hostname oder IP-Adresse des Platform Services Controller, falls Sie sich auf einem vCenter Server-System mit einem externen Platform Services Controller befinden.

#### Verfahren

1. Starten Sie vSphere Certificate Manager und wählen Sie Option 6 aus.
2. Beantworten Sie die Eingabeaufforderungen.

   Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/2112281.

#### Ergebnisse

vSphere Certificate Manager ersetzt alle Lösungsbenutzerzertifikate.

## Ersetzen aller Zertifikate durch benutzerdefinierte Zertifikate (Certificate Manager)

Sie können das Dienstprogramm vSphere Certificate Manager verwenden, um alle Zertifikate durch benutzerdefinierte Zertifikate zu ersetzen. Bevor Sie den Vorgang starten, müssen Sie Zertifikatssignieranforderungen (CSRs) an Ihre Zertifizierungsstelle (CA) senden. Sie können Certificate Manager zum Generieren der CSRs verwenden.

Eine Option besteht darin, nur das Maschinen-SSL-Zertifikat zu ersetzen und die durch VMCA bereitgestellten Lösungsbenutzerzertifikate zu verwenden. Lösungsbenutzerzertifikate werden nur für die Kommunikation zwischen vSphere-Komponenten verwendet.

Wenn Sie benutzerdefinierte Zertifikate verwenden, werden die VMCA-signierten Zertifikate durch benutzerdefinierte Zertifikate ersetzt. Sie können den vSphere Client, das vSphere Certificate Manager-Dienstprogramm oder CLIs zum manuellen Ersetzen von Zertifikaten verwenden. Zertifikate werden in VECS gespeichert.

Um alle Zertifikate durch benutzerdefinierte Zertifikate zu ersetzen, müssen Sie Certificate Manager mehrmals ausführen. Der Workflow umfasst einen vollständigen Satz von Schritten zum Ersetzen von Maschinen-SSL-Zertifikaten und Lösungsbenutzerzertifikaten. Darin wird erläutert, wie in Umgebungen mit eingebettetem Platform Services Controller oder externem Platform Services Controller vorzugehen ist.

1 Zertifikatssignieranforderungen für das Maschinen-SSL-Zertifikat und die Lösungsbenutzerzertifikate werden auf jeder Maschine separat generiert.
   a Zum Generieren von CSRs für das Maschinen-SSL-Zertifikat wählen Sie Option 1 aus.
   b Falls aufgrund einer Unternehmensrichtlinie keine Hybrid-Bereitstellung zulässig ist, wählen Sie Option 5 aus.
2 Nachdem Sie die signierten Zertifikate und das Rootzertifikat von Ihrer Zertifizierungsstelle erhalten haben, ersetzen Sie das Maschinen-SSL-Zertifikat auf jeder Maschine mithilfe von Option 1.
3 Falls auch die Lösungsbenutzerzertifikate ersetzt werden sollen, wählen Sie Option 5 aus.
4 In einer Bereitstellung mit mehreren Knoten müssen Sie den Vorgang anschließend auf jedem Knoten wiederholen.

### Verfahren

1 Generieren von Zertifikatssignieranforderungen mit vSphere Certificate Manager (benutzerdefinierte Zertifikate)

   Mithilfe von vSphere Certificate Manager können Sie Zertifikatssignieranforderungen (Certificate Signing Requests, CSRs) generieren, die Sie anschließend mit Ihrer Unternehmenszertifizierungsstelle verwenden oder an eine externe Zertifizierungsstelle senden können. Sie können die Zertifikate mit den unterschiedlichen unterstützten Ersetzungsvorgängen von Zertifikaten verwenden.

2 Ersetzen des Maschinen-SSL-Zertifikats durch ein benutzerdefiniertes Zertifikat

   Das Maschinen-SSL-Zertifikat wird vom Reverse-Proxy-Dienst für jeden Verwaltungsknoten, Platform Services Controller und jede eingebettete Bereitstellung verwendet. Für jede Maschine ist ein Maschinen-SSL-Zertifikat für die sichere Kommunikation mit anderen Diensten erforderlich. Sie können dieses Zertifikat für jeden Knoten durch ein benutzerdefiniertes Zertifikat ersetzen.

3 Ersetzen der Lösungsbenutzerzertifikate durch benutzerdefinierte Zertifikate

   Viele Unternehmen möchten lediglich Zertifikate zu Diensten ersetzen lassen, die extern zugänglich sind. Certificate Manager unterstützt jedoch auch das Ersetzen von Lösungsbenutzerzertifikaten. Lösungsbenutzer sind Sammlungen von Diensten, beispielsweise alle mit dem vSphere Client verbundenen Dienste. In Bereitstellungen mit mehreren Knoten ersetzen Sie das Geräte-Lösungsbenutzerzertifikat im Platform Services Controller sowie sämtliche Lösungsbenutzer auf allen Verwaltungsknoten.

## Generieren von Zertifikatssignieranforderungen mit vSphere Certificate Manager (benutzerdefinierte Zertifikate)

Mithilfe von vSphere Certificate Manager können Sie Zertifikatssignieranforderungen (Certificate Signing Requests, CSRs) generieren, die Sie anschließend mit Ihrer Unternehmenszertifizierungsstelle verwenden oder an eine externe Zertifizierungsstelle senden können. Sie können die Zertifikate mit den unterschiedlichen unterstützten Ersetzungsvorgängen von Zertifikaten verwenden.

Sie können das Certificate Manager-Tool wie folgt über die Befehlszeile ausführen:

**Windows**

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

**Linux**

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

#### Voraussetzungen

vSphere Certificate Manager fordert Sie zur Eingabe von Informationen auf. Die Eingabeaufforderungen sind abhängig von Ihrer Umgebung und vom Zertifikatstyp, den Sie ersetzen möchten.

- Beim Generieren von Zertifikatssignieranforderungen werden Sie generell aufgefordert, das Kennwort für den Benutzer „administrator@vsphere.local“ bzw. den Administrator für die vCenter Single Sign On-Domäne, mit der Sie eine Verbindung herstellen, einzugeben.
- Wenn Sie eine Zertifikatssignieranforderung in einer Umgebung mit einem externen Platform Services Controller generieren, werden Sie zur Eingabe des Hostnamens oder der IP-Adresse für den Platform Services Controller aufgefordert.
- Zum Generieren einer Zertifikatssignieranforderung für ein Maschinen-SSL-Zertifikat werden Sie zur Eingabe von Zertifikateigenschaften aufgefordert, die in der Datei `certool.cfg` gespeichert sind. Für die meisten Felder können Sie den Standardwert übernehmen oder aber standortspezifische Werte eingeben. Der FQDN der Maschine ist erforderlich.

#### Verfahren

1. Starten Sie vSphere Certificate Manager auf jeder Maschine in Ihrer Umgebung und wählen Sie Option 1 aus.
2. Geben Sie, wenn Sie dazu aufgefordert werden, das Kennwort sowie die IP-Adresse oder den Hostnamen für den Platform Services Controller ein.
3. Wählen Sie Option 1 aus, um die Zertifikatssignieranforderung zu generieren, befolgen Sie die Anweisungen und beenden Sie Certificate Manager.

   Im Rahmen dieses Vorgangs müssen Sie ein Verzeichnis angeben. Certificate Manager speichert die Zertifikats- und Schlüsseldateien in dem Verzeichnis.

4 Wenn Sie alle Lösungsbenutzerzertifikate ersetzen möchten, starten Sie Certificate Manager neu.

5 Wählen Sie Option 5 aus.

6 Geben Sie, wenn Sie dazu aufgefordert werden, das Kennwort sowie die IP-Adresse oder den Hostnamen für den Platform Services Controller ein.

7 Wählen Sie Option 1 aus, um die Zertifikatssignieranforderungen zu generieren, befolgen Sie die Anweisungen und beenden Sie Certificate Manager.

   Im Rahmen dieses Vorgangs müssen Sie ein Verzeichnis angeben. Certificate Manager speichert die Zertifikats- und Schlüsseldateien in dem Verzeichnis.

   Certificate Manager generiert auf jedem Platform Services Controller-Knoten je ein Zertifikats- und Schlüsselpaar. Certificate Manager generiert auf jedem vCenter Server-Knoten je vier Zertifikats- und Schlüsselpaare.

#### Nächste Schritte

Führen Sie die Zertifikatsersetzung durch.

## Ersetzen des Maschinen-SSL-Zertifikats durch ein benutzerdefiniertes Zertifikat

Das Maschinen-SSL-Zertifikat wird vom Reverse-Proxy-Dienst für jeden Verwaltungsknoten, Platform Services Controller und jede eingebettete Bereitstellung verwendet. Für jede Maschine ist ein Maschinen-SSL-Zertifikat für die sichere Kommunikation mit anderen Diensten erforderlich. Sie können dieses Zertifikat für jeden Knoten durch ein benutzerdefiniertes Zertifikat ersetzen.

#### Voraussetzungen

Bevor Sie beginnen, benötigen Sie eine Zertifikatssignieranforderung (CSR) für jede Maschine in Ihrer Umgebung. Sie können die CSR mit vSphere Certificate Manager oder explizit generieren.

1 Weitere Informationen zum Generieren einer CSR mit vSphere Certificate Manager finden Sie unter Generieren von Zertifikatssignieranforderungen mit vSphere Certificate Manager (benutzerdefinierte Zertifikate).

2 Um die CSR explizit zu generieren, fordern Sie für jede Maschine ein Zertifikat von Ihrer Drittanbieter- oder Unternehmenszertifizierungsstelle an. Das Zertifikat muss die folgenden Anforderungen erfüllen:

   - Schlüsselgröße: mindestens 2.048 Bit (PEM-kodiert)
   - CRT-Format
   - x509 Version 3
   - „SubjectAltName“ muss DNS-Name=<Maschinen-FQDN> enthalten.

- Enthält die folgenden Schlüsselverwendungen: digitale Signatur, Schlüsselverschlüsselung

**Hinweis** CRL-Verteilungspunkte, Zugriff auf Zertifizierungsstelleninfos oder Zertifikatvorlageninformationen dürfen in benutzerdefinierten Zertifikaten nicht verwendet werden.

Weitere Informationen finden Sie auch im VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/2112014, „Obtaining vSphere certificates from a Microsoft Certificate Authority“.

#### Verfahren

1. Starten Sie vSphere Certificate Manager und wählen Sie Option 1 aus.
2. Wählen Sie Option 2 aus, um die Zertifikatsersetzung zu starten, und befolgen Sie die Anweisungen.

   vSphere Certificate Manager fordert Sie zur Eingabe der folgenden Informationen auf:

   - Kennwort für „administrator@vsphere.local“.
   - Gültiges benutzerdefiniertes Maschinen-SSL-Zertifikat (`.crt`-Datei).
   - Gültiger benutzerdefinierter Maschinen-SSL-Schlüssel (`.key`-Datei).
   - Gültiges Signaturzertifikat für das benutzerdefinierte Maschinen-SSL-Zertifikat (`.crt`-Datei).
   - Die IP-Adresse des Platform Services Controller, wenn Sie den Befehl für einen Verwaltungsknoten in einer Bereitstellung mit mehreren Knoten ausführen.

#### Nächste Schritte

Wenn Sie das Upgrade von einer vSphere 5.x-Umgebung aus vornehmen, müssen Sie möglicherweise das vCenter Single Sign-On-Zertifikat innerhalb von `vmdir` ersetzen. Weitere Informationen hierzu finden Sie unter Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus.

## Ersetzen der Lösungsbenutzerzertifikate durch benutzerdefinierte Zertifikate

Viele Unternehmen möchten lediglich Zertifikate zu Diensten ersetzen lassen, die extern zugänglich sind. Certificate Manager unterstützt jedoch auch das Ersetzen von Lösungsbenutzerzertifikaten. Lösungsbenutzer sind Sammlungen von Diensten, beispielsweise alle mit dem vSphere Client verbundenen Dienste. In Bereitstellungen mit mehreren Knoten ersetzen Sie das Geräte-Lösungsbenutzerzertifikat im Platform Services Controller sowie sämtliche Lösungsbenutzer auf allen Verwaltungsknoten.

Wenn Sie zur Eingabe eines Lösungsbenutzerzertifikats aufgefordert werden, geben Sie die vollständige Signaturzertifikatkette der Drittanbieterzertifizierungsstelle an.

Das Format sollte so oder ähnlich aussehen:

```
-----BEGIN CERTIFICATE-----
Signing certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

### Voraussetzungen

Bevor Sie beginnen, benötigen Sie eine Zertifikatssignieranforderung (CSR) für jede Maschine in Ihrer Umgebung. Sie können die CSR mit vSphere Certificate Manager oder explizit generieren.

1 Weitere Informationen zum Generieren einer CSR mit vSphere Certificate Manager finden Sie unter Generieren von Zertifikatssignieranforderungen mit vSphere Certificate Manager (benutzerdefinierte Zertifikate).

2 Fordern Sie von Ihrer Drittanbieter- oder Unternehmenszertifizierungsstelle ein Zertifikat für jeden Benutzer der Lösung auf jedem Knoten an. Sie können die CSR mit vSphere Certificate Manager oder selbst generieren. Die CSR muss die folgenden Anforderungen erfüllen:

   - Schlüsselgröße: mindestens 2.048 Bit (PEM-kodiert)
   - CRT-Format
   - x509 Version 3
   - „SubjectAltName“ muss DNS-Name=<Maschinen-FQDN> enthalten.
   - Für jedes Lösungsbenutzerzertifikat ist ein unterschiedlicher Wert für `Subject` erforderlich. Geben Sie beispielsweise den Lösungsbenutzernamen (z. B. vpxd) oder einen anderen eindeutigen Bezeichner an.
   - Enthält die folgenden Schlüsselverwendungen: digitale Signatur, Schlüsselverschlüsselung

Weitere Informationen finden Sie auch im VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/2112014, „Obtaining vSphere certificates from a Microsoft Certificate Authority“.

### Verfahren

1 Starten Sie vSphere Certificate Manager und wählen Sie Option 5 aus.

2 Wählen Sie Option 2 aus, um die Zertifikatsersetzung zu starten, und befolgen Sie die Anweisungen.

   vSphere Certificate Manager fordert Sie zur Eingabe der folgenden Informationen auf:

   - Kennwort für „administrator@vsphere.local“.
   - Zertifikat und Schlüssel für Lösungsbenutzer „machine“.

- Wenn Sie vSphere Certificate Manager für einen Platform Services Controller-Knoten ausführen, werden Sie zur Eingabe des Zertifikats und des Schlüssels (`vpxd.crt` und `vpxd.key`) für den Lösungsbenutzer „machine“ aufgefordert.
- Wenn Sie vSphere Certificate Manager für einen Verwaltungsknoten oder eine eingebettete Bereitstellung ausführen, werden Sie zur Eingabe aller Zertifikate und Schlüssel (`vpxd.crt` und `vpxd.key`) für alle Lösungsbenutzer aufgefordert.

**Nächste Schritte**

Wenn Sie das Upgrade von einer vSphere 5.x-Umgebung aus vornehmen, müssen Sie möglicherweise das vCenter Single Sign On-Zertifikat innerhalb von vmdir ersetzen. Weitere Informationen hierzu finden Sie unter Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus.

## Rückgängigmachen des zuletzt ausgeführten Vorgangs durch die erneute Veröffentlichung alter Zertifikate

Wenn Sie einen Zertifikatverwaltungsvorgang mithilfe von vSphere Certificate Manager durchführen, wird der aktuelle Zertifikatstatus im BACKUP_STORE-Speicher in VECS gespeichert, bevor Zertifikate ersetzt werden. Sie können den zuletzt ausgeführten Vorgang rückgängig machen und den vorherigen Status wiederherstellen.

**Hinweis** Beim Rückgängigmachen wird der im BACKUP_STORE gespeicherte Status wiederhergestellt. Wenn Sie vSphere Certificate Manager für zwei unterschiedliche Optionen ausführen und rückgängig zu machen versuchen, wird nur der letzte Vorgang rückgängig gemacht.

## Alle Zertifikate zurücksetzen

Verwenden Sie die Option `Alle Zertifikate zurücksetzen`, wenn Sie alle vorhandenen vCenter-Zertifikate durch VMCA-signierte Zertifikate ersetzen möchten.

Bei Verwendung dieser Option werden alle benutzerdefinierten Zertifikate, die aktuell in VECS vorhanden sind, überschrieben.

- Auf einem Platform Services Controller-Knoten kann vSphere Certificate Manager das Stammzertifikat neu generieren und das Maschinen-SSL-Zertifikat („machine“) und das Lösungsbenutzerzertifikat „machine“ ersetzen.
- Auf einem Verwaltungsknoten kann vSphere Certificate Manager das Maschinen-SSL-Zertifikat und alle Lösungsbenutzerzertifikate ersetzen.
- Bei einer eingebetteten Bereitstellung kann vSphere Certificate Manager alle Zertifikate ersetzen.

Welche Zertifikate ersetzt werden, hängt von den von Ihnen ausgewählten Optionen ab.

# Manuelle Zertifikatsersetzung

Es kann vorkommen, dass Sie nur einen Lösungsbenutzerzertifikatstyp ersetzen möchten und deshalb nicht das Dienstprogramm vSphere Certificate Manager verwenden können. In diesem Fall verwenden Sie die Befehlszeilenschnittstellen (CLIs) Ihrer Installation zum Ersetzen von Zertifikaten.

## Grundlegendes zum Beenden und Starten von Diensten

Für bestimmte Bereiche der manuellen Zertifikatsersetzung müssen Sie alle Dienste beenden und dann nur jene Dienste starten, die die Zertifikatinfrastruktur verwalten. Wenn Sie Dienste nur bei Bedarf beenden, können Sie die Ausfallzeit minimieren.

Im Rahmen des Zertifikatsersetzungsvorgangs müssen Sie Dienste beenden und starten. Sie können den Befehl `service-control` zum Starten und Beenden von Diensten verwenden. Sie können alle oder einzelne Dienste starten und beenden. Weitere Informationen finden Sie in der Befehlszeilen-Hilfe.

- Wenn in Ihrer Umgebung ein eingebetteter Platform Services Controller verwendet wird, starten und beenden Sie alle Dienste wie im vorliegenden Dokument beschrieben.
- Wenn in Ihrer Umgebung ein externer Platform Services Controller verwendet wird, brauchen Sie VMware Directory Service (vmdird) und VMware Certificate Authority (vmcad) auf dem vCenter Server-Knoten nicht zu beenden und zu starten. Diese Dienste werden auf dem Platform Services Controller ausgeführt.

Befolgen Sie diese Richtlinien.

- Beenden Sie die Dienste nicht, um neue öffentliche/private Schlüsselpaare oder neue Zertifikate zu generieren.
- Wenn Sie der einzige Administrator sind, müssen Sie die Dienste beim Hinzufügen eines neuen Root-Zertifikats nicht beenden. Das alte Root-Zertifikat bleibt verfügbar, und alle Dienste können weiterhin mit diesem Zertifikat authentifiziert werden. Beenden Sie alle Dienste und starten Sie sie sofort neu, nachdem Sie das Root-Zertifikat hinzugefügt haben, um Probleme mit Ihren Hosts zu vermeiden.
- Wenn in Ihrer Umgebung mehrere Administratoren vorhanden sind, beenden Sie die Dienste, bevor Sie ein neues Root-Zertifikat hinzufügen, und starten Sie die Dienste neu, nachdem Sie ein neues Zertifikat hinzugefügt haben.
- Beenden Sie die Dienste, bevor Sie die folgenden Aufgaben ausführen:
  - Löschen Sie ein Maschinen-SSL-Zertifikat bzw. jedes Lösungsbenutzerzertifikat in VECS.
  - Ersetzen Sie ein Lösungsbenutzerzertifikat im VMware-Verzeichnisdienst (vmdir).

# Ersetzen vorhandener VMCA-signierter Zertifikate durch neue VMCA-signierte Zertifikate

Wenn das VMCA-Rootzertifikat in naher Zukunft abläuft oder wenn Sie es aus anderen Gründen ersetzen möchten, können Sie ein neues Rootzertifikat generieren und zum VMware-Verzeichnisdienst hinzufügen. Anschließend können Sie neue Maschinen-SSL-Zertifikate und Lösungsbenutzerzertifikate mithilfe des neuen Rootzertifikats generieren.

In den meisten Fällen können Sie das Dienstprogramm vSphere Certificate Manager zum Ersetzen von Zertifikaten verwenden.

Für die detailliertere Kontrolle finden Sie in diesem Szenario ausführliche schrittweise Anleitungen zum Ersetzen aller Zertifikate mithilfe von CLI-Befehlen. Mit der Vorgehensweise für die entsprechende Aufgabe können Sie stattdessen auch nur einzelne Zertifikate ersetzen.

### Voraussetzungen

Nur „administrator@vsphere.local“ oder andere Benutzer in der Gruppe „CAAdmins“ können Zertifikatverwaltungsaufgaben durchführen. Siehe Hinzufügen von Mitgliedern zu einer vCenter Single Sign On-Gruppe.

### Verfahren

1 Generieren eines neuen VMCA-signierten Stammzertifikats

   Sie generieren neue VMCA-signierte Zertifikate mit der `certool`-CLI oder dem vSphere Certificate Manager-Dienstprogramm und veröffentlichen die Zertifikate in vmdir.

2 Ersetzen der Maschinen-SSL-Zertifikate durch VMCA-signierte Zertifikate

   Nachdem Sie ein neues VMCA-signiertes Rootzertifikat generiert haben, können Sie alle Maschinen-SSL-Zertifikate in Ihrer Umgebung ersetzen.

3 Ersetzen der Lösungsbenutzerzertifikate durch neue VMCA-signierte Stammzertifikate

   Nachdem Sie die Maschinen-SSL-Zertifikate ersetzt haben, können Sie alle Lösungsbenutzerzertifikate ersetzen. Lösungsbenutzerzertifikate müssen gültig sein (also nicht abgelaufen), aber die anderen Informationen des Zertifikats werden nicht von der Zertifikatinfrastruktur verwendet.

4 Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus

   Während des Upgrades kann es vorkommen, dass in Ihrer Umgebung vorübergehend sowohl vCenter Single Sign On, Version 5.5, als auch vCenter Single Sign On, Version 6.x, vorhanden sind. Sie müssen in diesem Fall zusätzliche Schritte ausführen, um das SSL-Zertifikat des VMware Directory Service zu ersetzen, wenn Sie das SSL-Zertifikat des Knotens ersetzen, auf dem der vCenter Single Sign On-Dienst ausgeführt wird.

## Generieren eines neuen VMCA-signierten Stammzertifikats

Sie generieren neue VMCA-signierte Zertifikate mit der `certool`-CLI oder dem vSphere Certificate Manager-Dienstprogramm und veröffentlichen die Zertifikate in vmdir.

Bei einer Bereitstellung mit mehreren Knoten führen Sie Befehle zum Generieren von Root-Zertifikaten im Platform Services Controller aus.

**Verfahren**

1 Generieren Sie ein neues selbstsigniertes Zertifikat und einen privaten Schlüssel.

```
certool --genselfcacert --outprivkey <key_file_path> --outcert <cert_file_path> --config
<config_file>
```

2 Ersetzen Sie das vorhandene Root-Zertifikat durch das neue Zertifikat.

```
certool --rootca --cert <cert_file_path> --privkey <key_file_path>
```

Mit diesem Befehl wird das Zertifikat generiert und zu vmdir sowie zu VECS hinzugefügt.

3 Beenden Sie alle Dienste und starten Sie die Dienste für die Zertifikaterstellung, Weitergabe und Speicherung.

Die Dienstnamen sind unter Windows und bei der vCenter Server Appliance unterschiedlich.

**Hinweis** Wenn in Ihrer Umgebung ein externer Platform Services Controller verwendet wird, brauchen Sie VMware Directory Service (vmdird) und VMware Certificate Authority (vmcad) auf dem vCenter Server-Knoten nicht zu beenden und zu starten. Diese Dienste werden unter dem Platform Services Controller ausgeführt.

**Windows**

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

**vCenter Server Appliance**

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

4 (Optional) Veröffentlichen Sie das neue Root-Zertifikat in vmdir.

```
dir-cli trustedcert publish --cert newRoot.crt
```

Der Befehl aktualisiert alle vmdir-Instanzen sofort. Wenn Sie den Befehl nicht ausführen, kann die Weiterleitung des neuen Zertifikats an alle Knoten einige Zeit dauern.

5 Starten Sie alle Dienste neu.

```
service-control --start --all
```

### Beispiel: Generieren eines neuen VMCA-signierten Stammzertifikats

Das folgende Beispiel veranschaulicht alle Schritte, um die Informationen zur aktuellen Root-Zertifizierungsstelle zu überprüfen und das Root-Zertifikat neu zu generieren.

1 (Optional) Listen Sie das VMCA-Root-Zertifikat auf, um sicherzustellen, dass es sich im Zertifikatspeicher befindet.

- In einem Platform Services Controller-Knoten oder einer eingebetteten Installation:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca
```

- In einem Verwaltungsknoten (externe Installation):

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca --server=<psc-ip-or-fqdn>
```

Die Ausgabe sieht so oder ähnlich aus:

```
output:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cf:2d:ff:49:88:50:e5:af
    ...
```

2 (Optional) Listen Sie den VECS TRUSTED_ROOTS-Speicher auf und vergleichen Sie die Seriennummer des Zertifikats mit der Ausgabe aus Schritt 1.

Dieser Befehl kann sowohl für Platform Services Controller-Knoten als auch für Verwaltungsknoten verwendet werden, da VECS eine Abfrage für vmdir ausführt.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry list --store TRUSTED_ROOTS --text
```

Im einfachsten Fall mit nur einem Root-Zertifikat sieht die Ausgabe wie folgt aus:

```
Number of entries in store :    1
Alias : 960d43f31eb95211ba3a2487ac840645a02894bd
Entry type :    Trusted Cert
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cf:2d:ff:49:88:50:e5:af
```

3 Generieren Sie ein neues VMCA-Root-Zertifikat. Der Befehl fügt das Zertifikat zum TRUSTED_ROOTS-Speicher in VECS und in vmdir (VMware Directory Service) hinzu.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --selfca --config="C:\Program Files\VMware\vCenter Server\vmcad\certool.cfg"
```

Unter Windows ist `--config` optional, da der Befehl die Standarddatei `certool.cfg` verwendet.

## Ersetzen der Maschinen-SSL-Zertifikate durch VMCA-signierte Zertifikate

Nachdem Sie ein neues VMCA-signiertes Rootzertifikat generiert haben, können Sie alle Maschinen-SSL-Zertifikate in Ihrer Umgebung ersetzen.

Für jede Maschine ist ein Maschinen-SSL-Zertifikat für die sichere Kommunikation mit anderen Diensten erforderlich. Bei einer Bereitstellung mit mehreren Knoten müssen Sie die Befehle zum Generieren von Maschinen-SSL-Zertifikaten auf jedem Knoten ausführen. Verwenden Sie den Parameter `--server`, um von einem vCenter Server mit externem Platform Services Controller aus auf den Platform Services Controller zu verweisen.

### Voraussetzungen

Sie sollten darauf vorbereitet sein, alle Dienste zu beenden und die Dienste für die Weitergabe und Speicherung von Zertifikaten zu starten.

### Verfahren

1 Erstellen Sie eine Kopie von `certool.cfg` für jede Maschine, für die ein neues Zertifikat erforderlich ist.

`certool.cfg` finden Sie in den folgenden Speicherorten:

| Betriebssystem | Pfad |
|---|---|
| **Windows** | `C:\Program Files\VMware\vCenter Server\vmcad` |
| **Linux** | `/usr/lib/vmware-vmca/share/config/` |

2 Bearbeiten Sie die benutzerdefinierte Konfigurationsdatei für jede Maschine, um den FDQN dieser Maschine anzugeben.

Führen Sie `NSLookup` für die IP-Adresse der Maschine aus, um die DNS-Liste für den Namen anzuzeigen, und verwenden Sie diesen Namen für das Feld „Hostname“ in der Datei.

3 Generieren Sie für jede Datei ein öffentliches/privates Schlüsseldateipaar sowie ein Zertifikat und übergeben Sie die Konfigurationsdatei, die Sie soeben angepasst haben.

Beispiel:

```
certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certool --gencert --privkey=machine1.priv --cert machine1.crt --Name=Machine1_Cert --
config machine1.cfg
```

4 Beenden Sie alle Dienste und starten Sie die Dienste für die Zertifikaterstellung, Weitergabe und Speicherung.

Die Dienstnamen sind unter Windows und bei der vCenter Server Appliance unterschiedlich.

**Hinweis** Wenn in Ihrer Umgebung ein externer Platform Services Controller verwendet wird, brauchen Sie VMware Directory Service (vmdird) und VMware Certificate Authority (vmcad) auf dem vCenter Server-Knoten nicht zu beenden und zu starten. Diese Dienste werden unter dem Platform Services Controller ausgeführt.

**Windows**

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

**vCenter Server Appliance**

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 Fügen Sie VECS das neue Zertifikat hinzu.

Alle Maschinen benötigen das neue Zertifikat im lokalen Zertifikatspeicher für die Kommunikation über SSL. Zunächst löschen Sie den vorhanden Eintrag und fügen dann den neuen Eintrag hinzu.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.crt
 --key machine1.priv
```

6 Starten Sie alle Dienste neu.

```
service-control --start --all
```

### Beispiel: Ersetzen der Maschinenzertifikate durch VMCA-signierte Zertifikate

1 Erstellen Sie eine Konfigurationsdatei für das SSL-Zertifikat und speichern Sie sie unter dem Namen `ssl-config.cfg` im aktuellen Verzeichnis.

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = <my_company>
OrgUnit = <my_company Engineering>
State = <my_state>
Locality = <mytown>
Hostname = <FQDN>
```

2 Generieren Sie ein Schlüsselpaar für das Maschinen-SSL-Zertifikat. Führen Sie diesen Befehl auf jedem Verwaltungsknoten und Platform Services Controller-Knoten aus. Die Option `--server` ist dabei nicht erforderlich.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv
--pubkey=ssl-key.pub
```

Die Dateien `ssl-key.priv` und `ssl-key.pub` werden im aktuellen Verzeichnis erstellt.

3 Generieren Sie das neue Maschinen-SSL-Zertifikat. Dieses Zertifikat ist VMCA-signiert. Wenn Sie das VMCA-Rootzertifikat durch ein benutzerdefiniertes Zertifikat ersetzt haben, signiert VMCA alle Zertifikate mit der vollständigen Zertifikatskette.

- In einem Platform Services Controller-Knoten oder einer eingebetteten Installation:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- Auf einem vCenter Server (externe Installation):

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

Die Datei `new-vmca-ssl.crt` wird im aktuellen Verzeichnis erstellt.

4 (Optional) Listen Sie den Inhalt von VECS auf.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\" vecs-cli store list
```

- Beispiel-Ausgabe am Platform Services Controller:

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- Beispiel-Ausgabe am vCenter Server:

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vpxd
vpxd-extension
vsphere-webclient
sms
```

5 Ersetzen Sie das Maschinen-SSL-Zertifikat in VECS durch das neue Maschinen-SSL-Zertifikat. Die Werte `--store` und `--alias` müssen genau mit den Standardnamen übereinstimmen.

- Führen Sie auf dem Platform Services Controller den folgenden Befehl aus, um das Maschinen-SSL-Zertifikat im MACHINE_SSL_CERT-Speicher zu aktualisieren.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- Führen Sie auf jedem Verwaltungsknoten oder für jede eingebettete Bereitstellung den folgenden Befehl aus, um das Maschinen-SSL-Zertifikat im MACHINE_SSL_CERT-Speicher zu aktualisieren. Sie müssen das Zertifikat für jede Maschine separat aktualisieren, da jedes Zertifikat einen unterschiedlichen FQDN aufweist.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

**Nächste Schritte**

Sie können auch die Zertifikate für Ihre ESXi-Hosts ersetzen. Weitere Informationen finden Sie in der Dokumentation zu *vSphere-Sicherheit*.

Nach dem Ersetzen des Rootzertifikats bei einer Bereitstellung mit mehreren Knoten müssen Sie die Dienste für alle vCenter Server-Knoten mit externem Platform Services Controller neu starten.

## Ersetzen der Lösungsbenutzerzertifikate durch neue VMCA-signierte Stammzertifikate

Nachdem Sie die Maschinen-SSL-Zertifikate ersetzt haben, können Sie alle Lösungsbenutzerzertifikate ersetzen. Lösungsbenutzerzertifikate müssen gültig sein (also nicht abgelaufen), aber die anderen Informationen des Zertifikats werden nicht von der Zertifikatinfrastruktur verwendet.

Viele VMware-Kunden tauschen Lösungsbenutzerzertifikate nicht aus. Sie tauschen lediglich die Maschinen-SSL-Zertifikate gegen benutzerdefinierte Zertifikate aus. Mit dieser hybriden Herangehensweise werden die Anforderungen ihrer Sicherheitsteams erfüllt.

- Zertifikate befinden sich entweder hinter einem Proxy-Server oder stellen benutzerdefinierte Zertifikate dar.
- Es werden keine Zwischenzertifizierungsstellen verwendet.

Sie ersetzen das Lösungsbenutzerzertifikat „machine“ auf jedem Verwaltungsknoten und auf jedem Platform Services Controller-Knoten. Die anderen Lösungsbenutzerzertifikate ersetzen Sie nur auf jedem Verwaltungsknoten. Verwenden Sie den Parameter `--server`, um auf den Platform Services Controller zu verweisen, wenn Sie Befehle auf einem Verwaltungsknoten mit einem externen Platform Services Controller ausführen.

**Hinweis** Wenn Sie Lösungsbenutzerzertifikate bei großen Bereitstellungen auflisten, enthält die Ausgabe von `dir-cli list` alle Lösungsbenutzer aus allen Knoten. Führen Sie `vmafd-cli get-machine-id --server-name localhost` aus, um für jeden Host nach der lokalen Maschinen-ID zu suchen. Jeder Lösungsbenutzername enthält die Maschinen-ID.

### Voraussetzungen

Sie sollten darauf vorbereitet sein, alle Dienste zu beenden und die Dienste für die Weitergabe und Speicherung von Zertifikaten zu starten.

### Verfahren

1. Erstellen Sie eine Kopie von `certool.cfg`, entfernen Sie die Felder für den Namen, die IP-Adresse, den DNS-Namen und die E-Mail-Adresse und benennen Sie die Datei z. B. in `sol_usr.cfg` um.

   Sie können die Zertifikate im Rahmen des Generierungsvorgangs über die Befehlszeile benennen. Die restlichen Informationen sind für Lösungsbenutzer nicht erforderlich. Wenn Sie die Standardinformationen unverändert lassen, könnten die generierten Zertifikate für Verwirrung sorgen.

2. Generieren Sie für jeden Lösungsbenutzer ein öffentliches/privates Schlüsseldateipaar sowie ein Zertifikat und übergeben Sie die Konfigurationsdatei, die Sie soeben angepasst haben.

   Beispiel:

   ```
   certool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
   certool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
   ```

3. Suchen Sie den Namen für jeden Lösungsbenutzer.

   ```
   dir-cli service list
   ```

   Sie können die eindeutige ID verwenden, die beim Ersetzen der Zertifikate zurückgegeben wird. Die Ein- und Ausgabe könnte so oder ähnlich wie im Folgenden aussehen.

   ```
   C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
   Enter password for administrator@vsphere.local:
   1. machine-1d364500-4b45-11e4-96c2-020011c98db3
   2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
   3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
   4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
   ```

Wenn Sie Lösungsbenutzerzertifikate bei Bereitstellungen mit mehreren Knoten auflisten, enthält die Ausgabe von `dir-cli` alle Lösungsbenutzer aus allen Knoten. Führen Sie `vmafd-cli get-machine-id --server-name localhost` aus, um für jeden Host nach der lokalen Maschinen-ID zu suchen. Jeder Lösungsbenutzername enthält die Maschinen-ID.

4 Beenden Sie alle Dienste und starten Sie die Dienste für die Zertifikaterstellung, Weitergabe und Speicherung.

Die Dienstnamen sind unter Windows und bei der vCenter Server Appliance unterschiedlich.

**Hinweis** Wenn in Ihrer Umgebung ein externer Platform Services Controller verwendet wird, brauchen Sie VMware Directory Service (vmdird) und VMware Certificate Authority (vmcad) auf dem vCenter Server-Knoten nicht zu beenden und zu starten. Diese Dienste werden unter dem Platform Services Controller ausgeführt.

**Windows**

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

**vCenter Server Appliance**

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 Ersetzen Sie für jeden Lösungsbenutzer das vorhandene Zertifikat in vmdir und anschließend in VECS.

Das folgende Beispiel veranschaulicht, wie die Zertifikate für den vpxd-Dienst ersetzt werden.

```
dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --cert ./vpxd.crt
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
```

**Hinweis** Lösungsbenutzer können sich nur bei vCenter Single Sign On authentifizieren, wenn Sie das Zertifikat in vmdir ersetzen.

6 Starten Sie alle Dienste neu.

```
service-control --start --all
```

### Beispiel: Verwenden von VMCA-signierten Lösungsbenutzerzertifikaten

1 Generieren Sie für jeden Lösungsbenutzer ein öffentliches/privates Schlüsselpaar. Dies beinhaltet ein Schlüsselpaar für den Lösungsbenutzer „machine“ auf jedem Platform Services Controller und jedem Verwaltungsknoten sowie ein Schlüsselpaar für jeden zusätzlichen Lösungsbenutzer (vpxd, vpxd-extension, vsphere-webclient) auf jedem Verwaltungsknoten.

   a Generieren Sie für den Lösungsbenutzer „machine“ einer eingebetteten Bereitstellung oder für den Lösungsbenutzer „machine“ des Platform Services Controller ein Schlüsselpaar.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
   ```

   b (Optional) Generieren Sie für Bereitstellungen mit einem externen Platform Services Controller für den Lösungsbenutzer „machine“ ein Schlüsselpaar auf jedem Verwaltungsknoten.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
   ```

   c Generieren Sie für den vpxd-Lösungsbenutzer ein Schlüsselpaar auf jedem Verwaltungsknoten.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
   ```

   d Generieren Sie für den vpxd-extension-Lösungsbenutzer ein Schlüsselpaar auf jedem Verwaltungsknoten.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
   ```

   e Generieren Sie für den vsphere-webclient-Lösungsbenutzer ein Schlüsselpaar auf jedem Verwaltungsknoten.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
   ```

2 Generieren Sie vom neuen VMCA-Rootzertifikat signierte Lösungsbenutzerzertifikate für den Lösungsbenutzer „machine“ auf jedem Platform Services Controller und jedem Verwaltungsknoten sowie für jeden zusätzlichen Lösungsbenutzer (vpxd, vpxd-extension, vsphere-webclient) auf jedem Verwaltungsknoten.

**Hinweis** Der Parameter `--Name` muss eindeutig sein. Durch die Angabe des Namens des Lösungsbenutzerspeichers ist auf einfache Weise erkennbar, welches Zertifikat welchem Lösungsbenutzer zugeordnet ist. Dieses Beispiel umfasst in jedem Fall den Namen, z. B. `vpxd` oder `vpxd-extension`.

a Führen Sie den folgenden Befehl auf dem Platform Services Controller-Knoten aus, um für den Lösungsbenutzer „machine“ auf diesem Knoten ein Lösungsbenutzerzertifikat zu generieren.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-
machine.crt --privkey=machine-key.priv --Name=machine
```

b Generieren Sie für den Lösungsbenutzer „machine“ auf jedem Verwaltungsknoten ein Zertifikat.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-
machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

c Generieren Sie für den vpxd-Lösungsbenutzer auf jedem Verwaltungsknoten ein Zertifikat.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-
vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

d Generieren Sie für den vpxd-extensions-Lösungsbenutzer auf jedem Verwaltungsknoten ein Zertifikat.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd-
extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-
or-fqdn>
```

e Generieren Sie für den vsphere-webclient-Lösungsbenutzer auf jedem Verwaltungsknoten ein Zertifikat, indem Sie den folgenden Befehl ausführen.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-
vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --
server=<psc-ip-or-fqdn>
```

3 Ersetzen Sie die Lösungsbenutzerzertifikate in VECS durch die neuen Lösungsbenutzerzertifikate.

**Hinweis** Die Parameter `--store` und `--alias` müssen genau mit den Standardnamen für die Dienste übereinstimmen.

a Führen Sie auf dem Platform Services Controller-Knoten den folgenden Befehl aus, um das Lösungsbenutzerzertifikat „machine“ zu ersetzen:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
machine --alias machine --cert new-machine.crt --key machine-key.priv
```

b Ersetzen Sie das Lösungsbenutzerzertifikat „machine“ auf jedem Verwaltungsknoten:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

c Ersetzen Sie das vpxd-Lösungsbenutzerzertifikat auf jedem Verwaltungsknoten.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd
--alias vpxd
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd
--alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

d Ersetzen Sie das vpxd-extension-Lösungsbenutzerzertifikat auf jedem Verwaltungsknoten.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-
extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd-
extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-
key.priv
```

e Ersetzen Sie das vsphere-webclient-Lösungsbenutzerzertifikat auf jedem Verwaltungsknoten.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key
vsphere-webclient-key.priv
```

4 Aktualisieren Sie den VMware Directory Service (vmdir) mit den neuen Lösungsbenutzerzertifikaten. Sie werden Zur Eingabe eines vCenter Single Sign On-Administratorkennworts aufgefordert.

a Führen Sie `dir-cli service list` aus, um für jeden Lösungsbenutzer das eindeutige Dienst-ID-Suffix abzurufen. Sie können diesen Befehl auf einem Platform Services Controller oder für ein vCenter Server-System ausführen.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

**Hinweis** Wenn Sie Lösungsbenutzerzertifikate bei großen Bereitstellungen auflisten, enthält die Ausgabe von `dir-cli list` alle Lösungsbenutzer aus allen Knoten. Führen Sie `vmafd-cli get-machine-id --server-name localhost` aus, um für jeden Host nach der lokalen Maschinen-ID zu suchen. Jeder Lösungsbenutzername enthält die Maschinen-ID.

b Ersetzen Sie das Maschinenzertifikat in vmdir auf dem Platform Services Controller. Wenn beispielsweise „machine-29a45d00-60a7-11e4-96ff-00505689639a“ der Lösungsbenutzer „machine“ auf dem Platform Services Controller ist, führen Sie diesen Befehl aus:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

c Ersetzen Sie das Maschinenzertifikat in vmdir auf jedem Verwaltungsknoten. Wenn beispielsweise „machine-6fd7f140-60a9-11e4-9e28-005056895a69“ der Lösungsbenutzer „machine“ auf dem vCenter Server ist, führen Sie diesen Befehl aus:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

d Ersetzen Sie das vpxd-Lösungsbenutzerzertifikat in vmdir auf jedem Verwaltungsknoten. Wenn beispielsweise „vpxd-6fd7f140-60a9-11e4-9e28-005056895a69“ die vpxd-Lösungsbenutzer-ID ist, führen Sie diesen Befehl aus:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

e Ersetzen Sie das vpxd-extension-Lösungsbenutzerzertifikat in vmdir auf jedem Verwaltungsknoten. Wenn beispielsweise „vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69“ die vpxd-extension-Lösungsbenutzer-ID ist, führen Sie diesen Befehl aus:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

f Ersetzen Sie das vsphere-webclient-Lösungsbenutzerzertifikat auf jedem Verwaltungsknoten. Wenn beispielsweise „vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69“ die vsphere-webclient-Lösungsbenutzer-ID ist, führen Sie diesen Befehl aus:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

**Nächste Schritte**

Starten Sie alle Dienste auf jedem Platform Services Controller-Knoten und jedem Verwaltungsknoten neu.

## Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus

Während des Upgrades kann es vorkommen, dass in Ihrer Umgebung vorübergehend sowohl vCenter Single Sign On, Version 5.5, als auch vCenter Single Sign On, Version 6.x, vorhanden sind. Sie müssen in diesem Fall zusätzliche Schritte ausführen, um das SSL-Zertifikat des VMware Directory Service zu ersetzen, wenn Sie das SSL-Zertifikat des Knotens ersetzen, auf dem der vCenter Single Sign On-Dienst ausgeführt wird.

Das SSL-Zertifikat des VMware Directory Service wird von vmdir für Handshakes zwischen Platform Services Controller-Knoten verwendet, die die vCenter Single Sign On-Replizierung durchführen.

Diese Schritte sind für Umgebungen im gemischten Modus, die Knoten mit vSphere 6.0 und vSphere 6.5 enthalten, nicht erforderlich. Diese Schritte sind nur in folgenden Fällen erforderlich:

- In Ihrer Umgebung sind sowohl vCenter Single Sign On 5.5- als auch vCenter Single Sign On 6.x-Dienste vorhanden.
- Die vCenter Single Sign On-Dienste sind für die Replizierung von vmdir-Daten eingerichtet.
- Sie können die standardmäßigen VMCA-signierten Zertifikate für den Knoten, auf dem der vCenter Single Sign On 6.x-Dienst ausgeführt wird, durch benutzerdefinierte Zertifikate ersetzen.

**Hinweis** Es empfiehlt sich, vor dem Neustart der Dienste ein Upgrade der kompletten Umgebung durchzuführen. Vom Ersetzen des VMware Directory Service-Zertifikats wird in der Regel abgeraten.

Verfahren

1 Richten Sie auf dem Knoten, auf dem der vCenter Single Sign On 5.5-Dienst ausgeführt wird, die Umgebung so ein, dass der vCenter Single Sign On 6.x-Dienst bekannt ist.

   a Sichern Sie alle Dateien im Verzeichnis `C:\ProgramData\VMware\CIS\cfg\vmdird`.

   b Erstellen Sie eine Kopie der Datei `vmdircert.pem` auf dem Knoten der Version 6.x und benennen Sie sie in `<sso_node2.domain.com>.pem` um, wobei `<sso_node2.domain.com>` der FQDN des Knotens der Version 6.x ist.

   c Kopieren Sie das umbenannte Zertifikat in das Verzeichnis `C:\ProgramData\VMware\CIS\cfg\vmdird`, um das vorhandene Replizierungszertifikat zu ersetzen.

2 Starten Sie den VMware Directory Service auf allen Maschinen neu, auf denen Sie Zertifikate ersetzt haben.

   Sie können den Dienst über den vSphere Client oder mithilfe des Befehls `service-control` neu starten.

## Verwenden von VMCA als Zwischenzertifizierungsstelle

Das VMCA-Rootzertifikat können Sie durch ein von einer Zertifizierungsstelle (CA) signiertes Drittanbieterzertifikat ersetzen, das VMCA in der Zertifikatskette beinhaltet. In Zukunft beinhalten alle von VMCA generierten Zertifikate die Zertifikatskette. Vorhandene Zertifikate können Sie durch neu generierte Zertifikate ersetzen.

Verfahren

1 Ersetzen des Rootzertifikats (Zwischenzertifizierungsstelle)

   Der erste Schritt beim Ersetzen des VMCA-Zertifikats durch benutzerdefinierte Zertifikate besteht im Generieren einer Zertifikatsignieranforderung (Certificate Signing Request, CSR) und im Senden der zu signierenden CSR. Anschließend fügen Sie das signierte Zertifikat als Root-Zertifikat zu VMCA hinzu.

2 Ersetzen der Maschinen-SSL-Zertifikate (Zwischenzertifizierungsstelle)

   Nachdem Sie das signierte Zertifikat von der Zertifizierungsstelle erhalten und zum VMCA-Rootzertifikat gemacht haben, können Sie alle Maschinen-SSL-Zertifikate ersetzen.

3 Ersetzen der Lösungsbenutzerzertifikate (Zwischenzertifizierungsstelle)

   Nachdem Sie die Maschinen-SSL-Zertifikate ersetzt haben, können Sie die Lösungsbenutzerzertifikate ersetzen.

4 Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus

   Während des Upgrades kann es vorkommen, dass in Ihrer Umgebung vorübergehend sowohl vCenter Single Sign On, Version 5.5, als auch vCenter Single Sign On, Version 6.x, vorhanden sind. Sie müssen in diesem Fall zusätzliche Schritte ausführen, um das SSL-Zertifikat des VMware Directory Service zu ersetzen, wenn Sie das SSL-Zertifikat des Knotens ersetzen, auf dem der vCenter Single Sign On-Dienst ausgeführt wird.

## Ersetzen des Rootzertifikats (Zwischenzertifizierungsstelle)

Der erste Schritt beim Ersetzen des VMCA-Zertifikats durch benutzerdefinierte Zertifikate besteht im Generieren einer Zertifikatsignieranforderung (Certificate Signing Request, CSR) und im Senden der zu signierenden CSR. Anschließend fügen Sie das signierte Zertifikat als Root-Zertifikat zu VMCA hinzu.

Sie können das Certificate Manager-Dienstprogramm oder ein anderes Tool zum Generieren der Signaturanforderung verwenden. DIE CSR muss die folgenden Anforderungen erfüllen:

- Schlüsselgröße: mindestens 2.048 Bit
- PEM-Format. VMware unterstützt PKCS8 und PKCS1 (RSA-Schlüssel). Wenn Schlüssel zu VECS hinzugefügt werden, werden sie in PKCS8 konvertiert.
- x509 Version 3
- Wenn Sie benutzerdefinierte Zertifikate verwenden, muss die Zertifizierungsstellenerweiterung für Stammzertifikate auf „true“ festgelegt werden, und „cert sign“ muss in der Liste der Anforderungen vorhanden sein.
- CRL-Signatur muss aktiviert sein.
- Erweiterte Schlüsselverwendung kann entweder leer sein oder Serverauthentifizierung enthalten.
- Keine explizite Beschränkung der Zertifikatskettenlänge. VMCA verwendet den OpenSSL-Standardwert von 10 Zertifikaten.
- Zertifikate mit Platzhalterzeichen oder mehr als einem DNS-Namen werden nicht unterstützt.
- Untergeordnete Zertifizierungsstellen von VMCA können nicht erstellt werden.

  Im VMware-Knowledgebase-Artikel „Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.0“ unter http://kb.vmware.com/kb/2112009 finden Sie ein Beispiel für die Verwendung der Microsoft-Zertifizierungsstelle.

VMCA überprüft beim Ersetzen des Root-Zertifikats die folgenden Zertifikatattribute:

- Schlüsselgröße von mindestens 2.048 Bit
- Schlüsselverwendung: Cert Sign
- Basiseinschränkung: Betrefftyp Zertifizierungsstelle

### Verfahren

1 Generieren Sie eine Zertifikatsignieranforderung und senden Sie sie an Ihre Zertifizierungsstelle.

  Befolgen Sie die Anweisungen Ihrer Zertifizierungsstelle.

2 Bereiten Sie eine Zertifikatdatei vor, die das signierte VMCA-Zertifikat sowie die vollständige Zertifikatkette Ihrer Drittanbieter- oder Unternehmenszertifizierungsstelle enthält. Speichern Sie die Datei beispielsweise unter dem Namen `rootca1.crt`.

   Zu diesem Zweck können Sie alle Zertifizierungsstellenzertifikate im PEM-Format in eine einzige Datei kopieren. Sie beginnen mit dem VMCA-Root-Zertifikat und am Ende haben Sie das PEM-Zertifikat der Root-Zertifizierungsstelle. Beispiel:

```
-----BEGIN CERTIFICATE-----
<Certificate of VMCA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of intermediary CA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of Root CA>
-----END CERTIFICATE-----
```

3 Beenden Sie alle Dienste und starten Sie die Dienste für die Zertifikaterstellung, Weitergabe und Speicherung.

   Die Dienstnamen sind unter Windows und bei der vCenter Server Appliance unterschiedlich.

   **Hinweis** Wenn in Ihrer Umgebung ein externer Platform Services Controller verwendet wird, brauchen Sie VMware Directory Service (vmdird) und VMware Certificate Authority (vmcad) auf dem vCenter Server-Knoten nicht zu beenden und zu starten. Diese Dienste werden unter dem Platform Services Controller ausgeführt.

   **Windows**

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

   **vCenter Server Appliance**

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

4 Ersetzen Sie die vorhandene VMCA-Root-Zertifizierungsstelle.

```
certool --rootca --cert=rootca1.crt --privkey=root1.key
```

   Bei der Ausführung dieses Befehls passiert Folgendes:

   - Das neue benutzerdefinierte Root-Zertifikat wird dem Zertifikatspeicherort im Dateisystem hinzufügt.

- Das benutzerdefinierte Root-Zertifikat wird an den TRUSTED_ROOTS-Speicher in VECS angehängt (nach einer Verzögerung).
- Das benutzerdefinierte Root-Zertifikat wird zu vmdir hinzugefügt (nach einer Verzögerung).

5 (Optional) Zur Weitergabe der Änderung an alle Instanzen von vmdir (VMware Directory Service) veröffentlichen Sie das neue Root-Zertifikat in vmdir und geben Sie dabei für jede Datei den vollständigen Dateipfad an.

Beispiel:

```
dir-cli trustedcert publish --cert rootca1.crt
```

Die Replizierung zwischen vmdir-Knoten erfolgt alle 30 Sekunden. Sie müssen das Root-Zertifikat nicht explizit zu VECS hinzufügen, da vmdir von VECS alle fünf Minuten auf neue Root-Zertifikatsdateien überprüft wird.

6 (Optional) Bei Bedarf können Sie die Aktualisierung von VECS erzwingen.

```
vecs-cli force-refresh
```

7 Starten Sie alle Dienste neu.

```
service-control --start --all
```

### Beispiel: Ersetzen des Root-Zertifikats

Ersetzen Sie das VMCA-Root-Zertifikat durch das benutzerdefinierte Root-Zertifikat der Zertifizierungsstelle, indem Sie den certool-Befehl mit der Option `--rootca` verwenden.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\certool" --rootca --cert=C:\custom-certs\root.pem --privkey=C:\custom-certs\root.key
```

Bei der Ausführung dieses Befehls passiert Folgendes:

- Das neue benutzerdefinierte Root-Zertifikat wird dem Zertifikatspeicherort im Dateisystem hinzufügt.
- Das benutzerdefinierte Root-Zertifikat wird an den TRUSTED_ROOTS-Speicher in VECS angehängt.
- Das benutzerdefinierte Root-Zertifikat wird zu vmdir hinzugefügt.

#### Nächste Schritte

Sie können das ursprüngliche VMCA-Root-Zertifikat aus dem Zertifikatspeicher entfernen, wenn die Unternehmensrichtlinien dies verlangen. In diesem Fall müssen Sie das vCenter Single Sign-On-Signaturzertifikat ersetzen. Weitere Informationen hierzu finden Sie unter Aktualisieren des Zertifikats für den Security Token Service.

## Ersetzen der Maschinen-SSL-Zertifikate (Zwischenzertifizierungsstelle)

Nachdem Sie das signierte Zertifikat von der Zertifizierungsstelle erhalten und zum VMCA-Rootzertifikat gemacht haben, können Sie alle Maschinen-SSL-Zertifikate ersetzen.

Diese Schritte sind im Wesentlichen mit den Schritten zum Ersetzen durch ein Zertifikat, das VMCA als Zertifizierungsstelle verwendet, identisch. In diesem Fall signiert jedoch VMCA alle Zertifikate mit der vollständigen Zertifikatskette.

Für jede Maschine ist ein Maschinen-SSL-Zertifikat für die sichere Kommunikation mit anderen Diensten erforderlich. Bei einer Bereitstellung mit mehreren Knoten müssen Sie die Befehle zum Generieren von Maschinen-SSL-Zertifikaten auf jedem Knoten ausführen. Verwenden Sie den Parameter `--server`, um von einem vCenter Server mit externem Platform Services Controller aus auf den Platform Services Controller zu verweisen.

### Voraussetzungen

`SubjectAltName` muss für jedes Maschinen-SSL-Zertifikat `DNS Name=<Machine FQDN>` enthalten.

### Verfahren

1 Erstellen Sie eine Kopie von `certool.cfg` für jede Maschine, für die ein neues Zertifikat erforderlich ist.

`certool.cfg` finden Sie in den folgenden Speicherorten:

**Windows**

`C:\Program Files\VMware\vCenter Server\vmcad`

**Linux**

`/usr/lib/vmware-vmca/share/config/`

2 Bearbeiten Sie die benutzerdefinierte Konfigurationsdatei für jede Maschine, um den FDQN dieser Maschine anzugeben.

Führen Sie `NSLookup` für die IP-Adresse der Maschine aus, um die DNS-Liste für den Namen anzuzeigen, und verwenden Sie diesen Namen für das Feld „Hostname“ in der Datei.

3 Generieren Sie für jede Maschine ein öffentliches/privates Schlüsseldateipaar sowie ein Zertifikat und übergeben Sie die Konfigurationsdatei, die Sie soeben angepasst haben.

Beispiel:

```
certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certool --gencert --privkey=machine1.priv --cert machine42.crt --Name=Machine42_Cert --
config machine1.cfg
```

4 Beenden Sie alle Dienste und starten Sie die Dienste für die Zertifikaterstellung, Weitergabe und Speicherung.

Die Dienstnamen sind unter Windows und bei der vCenter Server Appliance unterschiedlich.

**Hinweis** Wenn in Ihrer Umgebung ein externer Platform Services Controller verwendet wird, brauchen Sie VMware Directory Service (vmdird) und VMware Certificate Authority (vmcad) auf dem vCenter Server-Knoten nicht zu beenden und zu starten. Diese Dienste werden unter dem Platform Services Controller ausgeführt.

**Windows**

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

**vCenter Server Appliance**

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 Fügen Sie VECS das neue Zertifikat hinzu.

Alle Maschinen benötigen das neue Zertifikat im lokalen Zertifikatspeicher für die Kommunikation über SSL. Zunächst löschen Sie den vorhanden Eintrag und fügen dann den neuen Eintrag hinzu.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.cert
--key machine1.priv
```

6 Starten Sie alle Dienste neu.

```
service-control --start --all
```

**Beispiel: Ersetzen der Maschinen-SSL-Zertifikate (VMCA ist die Zwischenzertifizierungsstelle)**

1 Erstellen Sie eine Konfigurationsdatei für das SSL-Zertifikat und speichern Sie sie unter dem Namen `ssl-config.cfg` im aktuellen Verzeichnis.

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = VMware
OrgUnit = VMware Engineering
State = California
Locality = Palo Alto
Hostname = <FQDN>
```

2 Generieren Sie ein Schlüsselpaar für das Maschinen-SSL-Zertifikat. Führen Sie diesen Befehl auf jedem Verwaltungsknoten und Platform Services Controller-Knoten aus. Die Option `--server` ist dabei nicht erforderlich.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv
--pubkey=ssl-key.pub
```

Die Dateien `ssl-key.priv` und `ssl-key.pub` werden im aktuellen Verzeichnis erstellt.

3 Generieren Sie das neue Maschinen-SSL-Zertifikat. Dieses Zertifikat ist VMCA-signiert. Wenn Sie das VMCA-Rootzertifikat durch ein benutzerdefiniertes Zertifikat ersetzt haben, signiert VMCA alle Zertifikate mit der vollständigen Zertifikatskette.

- In einem Platform Services Controller-Knoten oder einer eingebetteten Installation:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- Auf einem vCenter Server (externe Installation):

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

Die Datei `new-vmca-ssl.crt` wird im aktuellen Verzeichnis erstellt.

4 (Optional) Listen Sie den Inhalt von VECS auf.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\" vecs-cli store list
```

- Beispiel-Ausgabe am Platform Services Controller:

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- Beispiel-Ausgabe am vCenter Server:

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vpxd
vpxd-extension
vsphere-webclient
sms
```

5 Ersetzen Sie das Maschinen-SSL-Zertifikat in VECS durch das neue Maschinen-SSL-Zertifikat. Die Werte `--store` und `--alias` müssen genau mit den Standardnamen übereinstimmen.

- Führen Sie auf dem Platform Services Controller den folgenden Befehl aus, um das Maschinen-SSL-Zertifikat im MACHINE_SSL_CERT-Speicher zu aktualisieren.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- Führen Sie auf jedem Verwaltungsknoten oder für jede eingebettete Bereitstellung den folgenden Befehl aus, um das Maschinen-SSL-Zertifikat im MACHINE_SSL_CERT-Speicher zu aktualisieren. Sie müssen das Zertifikat für jede Maschine separat aktualisieren, da jedes Zertifikat einen unterschiedlichen FQDN aufweist.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

## Ersetzen der Lösungsbenutzerzertifikate (Zwischenzertifizierungsstelle)

Nachdem Sie die Maschinen-SSL-Zertifikate ersetzt haben, können Sie die Lösungsbenutzerzertifikate ersetzen.

Viele VMware-Kunden tauschen Lösungsbenutzerzertifikate nicht aus. Sie tauschen lediglich die Maschinen-SSL-Zertifikate gegen benutzerdefinierte Zertifikate aus. Mit dieser hybriden Herangehensweise werden die Anforderungen ihrer Sicherheitsteams erfüllt.

- Zertifikate befinden sich entweder hinter einem Proxy-Server oder stellen benutzerdefinierte Zertifikate dar.
- Es werden keine Zwischenzertifizierungsstellen verwendet.

Sie ersetzen das Lösungsbenutzerzertifikat „machine“ auf jedem Verwaltungsknoten und auf jedem Platform Services Controller-Knoten. Die anderen Lösungsbenutzerzertifikate ersetzen Sie nur auf jedem Verwaltungsknoten. Verwenden Sie den Parameter `--server`, um auf den Platform Services Controller zu verweisen, wenn Sie Befehle auf einem Verwaltungsknoten mit einem externen Platform Services Controller ausführen.

**Hinweis** Wenn Sie Lösungsbenutzerzertifikate bei großen Bereitstellungen auflisten, enthält die Ausgabe von `dir-cli list` alle Lösungsbenutzer aus allen Knoten. Führen Sie `vmafd-cli get-machine-id --server-name localhost` aus, um für jeden Host nach der lokalen Maschinen-ID zu suchen. Jeder Lösungsbenutzername enthält die Maschinen-ID.

### Voraussetzungen

Für jedes Lösungsbenutzerzertifikat ist ein unterschiedlicher Wert für `Subject` erforderlich. Geben Sie beispielsweise den Lösungsbenutzernamen (z. B. vpxd) oder einen anderen eindeutigen Bezeichner an.

**Hinweis** Der vpxd-Zertifikatspeicher existiert nur auf der vCenter Server Appliance, nicht auf dem Platform Services Controller.

### Verfahren

1 Erstellen Sie eine Kopie von `certool.cfg`, entfernen Sie die Felder für den Namen, die IP-Adresse, den DNS-Namen und die E-Mail-Adresse und benennen Sie die Datei z. B. in `sol_usr.cfg` um.

   Sie können die Zertifikate im Rahmen des Generierungsvorgangs über die Befehlszeile benennen. Die restlichen Informationen sind für Lösungsbenutzer nicht erforderlich. Wenn Sie die Standardinformationen unverändert lassen, könnten die generierten Zertifikate für Verwirrung sorgen.

2 Generieren Sie für jeden Lösungsbenutzer ein öffentliches/privates Schlüsseldateipaar sowie ein Zertifikat und übergeben Sie die Konfigurationsdatei, die Sie soeben angepasst haben.

   Beispiel:

```
certool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
certool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
```

3 Suchen Sie den Namen für jeden Lösungsbenutzer.

```
dir-cli service list
```

   Sie können die eindeutige ID verwenden, die beim Ersetzen der Zertifikate zurückgegeben wird. Die Ein- und Ausgabe könnte so oder ähnlich wie im Folgenden aussehen.

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

   Wenn Sie Lösungsbenutzerzertifikate bei Bereitstellungen mit mehreren Knoten auflisten, enthält die Ausgabe von `dir-cli` alle Lösungsbenutzer aus allen Knoten. Führen Sie `vmafd-cli get-machine-id --server-name localhost` aus, um für jeden Host nach der lokalen Maschinen-ID zu suchen. Jeder Lösungsbenutzername enthält die Maschinen-ID.

4 Beenden Sie alle Dienste und starten Sie die Dienste für die Zertifikaterstellung, Weitergabe und Speicherung.

Die Dienstnamen sind unter Windows und bei der vCenter Server Appliance unterschiedlich.

**Hinweis** Wenn in Ihrer Umgebung ein externer Platform Services Controller verwendet wird, brauchen Sie VMware Directory Service (vmdird) und VMware Certificate Authority (vmcad) auf dem vCenter Server-Knoten nicht zu beenden und zu starten. Diese Dienste werden unter dem Platform Services Controller ausgeführt.

**Windows**

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

**vCenter Server Appliance**

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 Ersetzen Sie das vorhandene Zertifikat in vmdir und anschließend in VECS.

Für Lösungsbenutzer müssen Sie die Zertifikate in dieser Reihenfolge hinzufügen. Beispiel:

```
dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --cert ./vpxd.crt
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
```

**Hinweis** Lösungsbenutzer können sich nur bei vCenter Single Sign-On anmelden, wenn Sie das Zertifikat in vmdir ersetzen.

6 Starten Sie alle Dienste neu.

```
service-control --start --all
```

### Beispiel: Ersetzen der Lösungsbenutzerzertifikate (Zwischenzertifizierungsstelle)

1 Generieren Sie für jeden Lösungsbenutzer ein öffentliches/privates Schlüsselpaar. Dies beinhaltet ein Schlüsselpaar für den Lösungsbenutzer „machine“ auf jedem Platform Services Controller und jedem Verwaltungsknoten sowie ein Schlüsselpaar für jeden zusätzlichen Lösungsbenutzer (vpxd, vpxd-extension, vsphere-webclient) auf jedem Verwaltungsknoten.

   a Generieren Sie für den Lösungsbenutzer „machine“ einer eingebetteten Bereitstellung oder für den Lösungsbenutzer „machine“ des Platform Services Controller ein Schlüsselpaar.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
   ```

   b (Optional) Generieren Sie für Bereitstellungen mit einem externen Platform Services Controller für den Lösungsbenutzer „machine“ ein Schlüsselpaar auf jedem Verwaltungsknoten.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
   ```

   c Generieren Sie für den vpxd-Lösungsbenutzer ein Schlüsselpaar auf jedem Verwaltungsknoten.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
   ```

   d Generieren Sie für den vpxd-extension-Lösungsbenutzer ein Schlüsselpaar auf jedem Verwaltungsknoten.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
   ```

   e Generieren Sie für den vsphere-webclient-Lösungsbenutzer ein Schlüsselpaar auf jedem Verwaltungsknoten.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
   ```

2 Generieren Sie vom neuen VMCA-Rootzertifikat signierte Lösungsbenutzerzertifikate für den Lösungsbenutzer „machine“ auf jedem Platform Services Controller und jedem Verwaltungsknoten sowie für jeden zusätzlichen Lösungsbenutzer (vpxd, vpxd-extension, vsphere-webclient) auf jedem Verwaltungsknoten.

**Hinweis** Der Parameter `--Name` muss eindeutig sein. Durch die Angabe des Namens des Lösungsbenutzerspeichers ist auf einfache Weise erkennbar, welches Zertifikat welchem Lösungsbenutzer zugeordnet ist. Dieses Beispiel umfasst in jedem Fall den Namen, z. B. `vpxd` oder `vpxd-extension`.

a Führen Sie den folgenden Befehl auf dem Platform Services Controller-Knoten aus, um für den Lösungsbenutzer „machine“ auf diesem Knoten ein Lösungsbenutzerzertifikat zu generieren.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-
machine.crt --privkey=machine-key.priv --Name=machine
```

b Generieren Sie für den Lösungsbenutzer „machine“ auf jedem Verwaltungsknoten ein Zertifikat.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-
machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

c Generieren Sie für den vpxd-Lösungsbenutzer auf jedem Verwaltungsknoten ein Zertifikat.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-
vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

d Generieren Sie für den vpxd-extensions-Lösungsbenutzer auf jedem Verwaltungsknoten ein Zertifikat.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd-
extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-
or-fqdn>
```

e Generieren Sie für den vsphere-webclient-Lösungsbenutzer auf jedem Verwaltungsknoten ein Zertifikat, indem Sie den folgenden Befehl ausführen.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-
vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --
server=<psc-ip-or-fqdn>
```

3 Ersetzen Sie die Lösungsbenutzerzertifikate in VECS durch die neuen Lösungsbenutzerzertifikate.

**Hinweis** Die Parameter `--store` und `--alias` müssen genau mit den Standardnamen für die Dienste übereinstimmen.

a Führen Sie auf dem Platform Services Controller-Knoten den folgenden Befehl aus, um das Lösungsbenutzerzertifikat „machine“ zu ersetzen:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
machine --alias machine --cert new-machine.crt --key machine-key.priv
```

b Ersetzen Sie das Lösungsbenutzerzertifikat „machine“ auf jedem Verwaltungsknoten:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

c Ersetzen Sie das vpxd-Lösungsbenutzerzertifikat auf jedem Verwaltungsknoten.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd
--alias vpxd
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd
--alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

d Ersetzen Sie das vpxd-extension-Lösungsbenutzerzertifikat auf jedem Verwaltungsknoten.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-
extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd-
extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-
key.priv
```

e Ersetzen Sie das vsphere-webclient-Lösungsbenutzerzertifikat auf jedem Verwaltungsknoten.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key
vsphere-webclient-key.priv
```

4 Aktualisieren Sie den VMware Directory Service (vmdir) mit den neuen Lösungsbenutzerzertifikaten. Sie werden Zur Eingabe eines vCenter Single Sign On-Administratorkennworts aufgefordert.

a Führen Sie `dir-cli service list` aus, um für jeden Lösungsbenutzer das eindeutige Dienst-ID-Suffix abzurufen. Sie können diesen Befehl auf einem Platform Services Controller oder für ein vCenter Server-System ausführen.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

**Hinweis** Wenn Sie Lösungsbenutzerzertifikate bei großen Bereitstellungen auflisten, enthält die Ausgabe von `dir-cli list` alle Lösungsbenutzer aus allen Knoten. Führen Sie `vmafd-cli get-machine-id --server-name localhost` aus, um für jeden Host nach der lokalen Maschinen-ID zu suchen. Jeder Lösungsbenutzername enthält die Maschinen-ID.

b Ersetzen Sie das Maschinenzertifikat in vmdir auf dem Platform Services Controller. Wenn beispielsweise „machine-29a45d00-60a7-11e4-96ff-00505689639a“ der Lösungsbenutzer „machine“ auf dem Platform Services Controller ist, führen Sie diesen Befehl aus:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

c Ersetzen Sie das Maschinenzertifikat in vmdir auf jedem Verwaltungsknoten. Wenn beispielsweise „machine-6fd7f140-60a9-11e4-9e28-005056895a69“ der Lösungsbenutzer „machine“ auf dem vCenter Server ist, führen Sie diesen Befehl aus:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

d Ersetzen Sie das vpxd-Lösungsbenutzerzertifikat in vmdir auf jedem Verwaltungsknoten. Wenn beispielsweise „vpxd-6fd7f140-60a9-11e4-9e28-005056895a69“ die vpxd-Lösungsbenutzer-ID ist, führen Sie diesen Befehl aus:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

e Ersetzen Sie das vpxd-extension-Lösungsbenutzerzertifikat in vmdir auf jedem Verwaltungsknoten. Wenn beispielsweise „vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69“ die vpxd-extension-Lösungsbenutzer-ID ist, führen Sie diesen Befehl aus:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

f Ersetzen Sie das vsphere-webclient-Lösungsbenutzerzertifikat auf jedem Verwaltungsknoten. Wenn beispielsweise „vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69“ die vsphere-webclient-Lösungsbenutzer-ID ist, führen Sie diesen Befehl aus:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

## Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus

Während des Upgrades kann es vorkommen, dass in Ihrer Umgebung vorübergehend sowohl vCenter Single Sign On, Version 5.5, als auch vCenter Single Sign On, Version 6.x, vorhanden sind. Sie müssen in diesem Fall zusätzliche Schritte ausführen, um das SSL-Zertifikat des VMware Directory Service zu ersetzen, wenn Sie das SSL-Zertifikat des Knotens ersetzen, auf dem der vCenter Single Sign On-Dienst ausgeführt wird.

Das SSL-Zertifikat des VMware Directory Service wird von vmdir für Handshakes zwischen Platform Services Controller-Knoten verwendet, die die vCenter Single Sign On-Replizierung durchführen.

Diese Schritte sind für Umgebungen im gemischten Modus, die Knoten mit vSphere 6.0 und vSphere 6.5 enthalten, nicht erforderlich. Diese Schritte sind nur in folgenden Fällen erforderlich:

- In Ihrer Umgebung sind sowohl vCenter Single Sign On 5.5- als auch vCenter Single Sign On 6.x-Dienste vorhanden.
- Die vCenter Single Sign On-Dienste sind für die Replizierung von vmdir-Daten eingerichtet.
- Sie können die standardmäßigen VMCA-signierten Zertifikate für den Knoten, auf dem der vCenter Single Sign On 6.x-Dienst ausgeführt wird, durch benutzerdefinierte Zertifikate ersetzen.

**Hinweis** Es empfiehlt sich, vor dem Neustart der Dienste ein Upgrade der kompletten Umgebung durchzuführen. Vom Ersetzen des VMware Directory Service-Zertifikats wird in der Regel abgeraten.

Verfahren

1 Richten Sie auf dem Knoten, auf dem der vCenter Single Sign On 5.5-Dienst ausgeführt wird, die Umgebung so ein, dass der vCenter Single Sign On 6.x-Dienst bekannt ist.

   a Sichern Sie alle Dateien im Verzeichnis `C:\ProgramData\VMware\CIS\cfg\vmdird`.

   b Erstellen Sie eine Kopie der Datei `vmdircert.pem` auf dem Knoten der Version 6.x und benennen Sie sie in `<sso_node2.domain.com>.pem` um, wobei `<sso_node2.domain.com>` der FQDN des Knotens der Version 6.x ist.

   c Kopieren Sie das umbenannte Zertifikat in das Verzeichnis `C:\ProgramData\VMware\CIS\cfg\vmdird`, um das vorhandene Replizierungszertifikat zu ersetzen.

2 Starten Sie den VMware Directory Service auf allen Maschinen neu, auf denen Sie Zertifikate ersetzt haben.

   Sie können den Dienst über den vSphere Client oder mithilfe des Befehls `service-control` neu starten.

## Verwenden benutzerdefinierter Zertifikate mit vSphere

Wenn es von einer Unternehmensrichtlinie verlangt wird, können Sie bestimmte oder alle in vSphere verwendeten Zertifikate durch Zertifikate ersetzen, die von einer Zertifizierungsstelle eines Drittanbieters oder Unternehmens signiert wurden. In diesem Fall ist VMCA in Ihrer Zertifikatskette nicht enthalten. Sie sind selbst für das Speichern aller vCenter-Zertifikate im VECS verantwortlich.

Sie können alle Zertifikate ersetzen oder eine Hybridlösung verwenden. Ersetzen Sie beispielsweise alle Zertifikate, die für Netzwerkdatenverkehr verwendet werden, und belassen Sie VMCA-signierte Lösungsbenutzerzertifikate. Lösungsbenutzerzertifikate werden nur für die Authentifizierung bei vCenter Single Sign On verwendet.

**Hinweis** Wenn Sie VMCA nicht verwenden möchten, müssen Sie selbst alle Zertifikate ersetzen, neue Komponenten mit Zertifikaten bereitstellen und den Ablauf von Zertifikaten nachverfolgen.

Auch wenn Sie benutzerdefinierte Zertifikate verwenden, können Sie den VMware Certificate Manager verwenden, um Zertifikate zu ersetzen. Weitere Informationen hierzu finden Sie unter Ersetzen aller Zertifikate durch benutzerdefinierte Zertifikate (Certificate Manager).

Falls nach dem Ersetzen von Zertifikaten Probleme mit vSphere Auto Deploy auftreten, erhalten Sie weitere Informationen im VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/2000988.

### Verfahren

1 Anfordern von Zertifikaten und Importieren eines benutzerdefinierten Rootzertifikats

   Sie können benutzerdefinierte Zertifikate von einer Unternehmens- oder Drittanbieter-Zertifizierungsstelle verwenden. Der erste Schritt besteht darin, die Zertifikate von der Zertifizierungsstelle anzufordern und die Stammzertifikate in den VMware Endpoint Certificate Store (VECS) zu importieren.

2 Ersetzen der Maschinen-SSL-Zertifikate durch benutzerdefinierte Zertifikate

   Nachdem Sie die benutzerdefinierten Zertifikate erhalten haben, können Sie jedes Maschinenzertifikat ersetzen.

3 Ersetzen der Lösungsbenutzerzertifikate durch benutzerdefinierte Zertifikate

   Nachdem Sie die Maschinen-SSL-Zertifikate ersetzt haben, können Sie die VMCA-signierten Lösungsbenutzerzertifikate durch Drittanbieter- oder Unternehmenszertifikate ersetzen.

4 Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus

   Während des Upgrades kann es vorkommen, dass in Ihrer Umgebung vorübergehend sowohl vCenter Single Sign On, Version 5.5, als auch vCenter Single Sign On, Version 6.x, vorhanden sind. Sie müssen in diesem Fall zusätzliche Schritte ausführen, um das SSL-Zertifikat des VMware Directory Service zu ersetzen, wenn Sie das SSL-Zertifikat des Knotens ersetzen, auf dem der vCenter Single Sign On-Dienst ausgeführt wird.

## Anfordern von Zertifikaten und Importieren eines benutzerdefinierten Rootzertifikats

Sie können benutzerdefinierte Zertifikate von einer Unternehmens- oder Drittanbieter-Zertifizierungsstelle verwenden. Der erste Schritt besteht darin, die Zertifikate von der Zertifizierungsstelle anzufordern und die Stammzertifikate in den VMware Endpoint Certificate Store (VECS) zu importieren.

#### Voraussetzungen

Das Zertifikat muss die folgenden Anforderungen erfüllen:

- Schlüsselgröße: mindestens 2.048 Bit (PEM-kodiert)
- PEM-Format. VMware unterstützt PKCS8 und PKCS1 (RSA-Schlüssel). Wenn Schlüssel zu VECS hinzugefügt werden, werden sie in PKCS8 konvertiert.
- x509 Version 3
- Für Stammzertifikate muss die Zertifizierungsstellenerweiterung auf „true“ festgelegt sein, und „cert sign“ muss in der Liste der Anforderungen vorhanden sein.
- „SubjectAltName“ muss DNS-Name=<Maschinen-FQDN> enthalten.

- CRT-Format
- Enthält die folgenden Schlüsselverwendungen: digitale Signatur, Schlüsselverschlüsselung
- Startzeit von einem Tag vor dem aktuellen Zeitpunkt.
- CN (und SubjectAltName) auf den Hostnamen (oder die IP-Adresse) festgelegt, den/die der ESXi-Host in der vCenter Server-Bestandsliste hat.

Verfahren

1 Senden Sie die Zertifikatsignieranforderungen (CSRs) für die folgenden Zertifikate an Ihren Unternehmens- oder Drittanbieter-Zertifikatanbieter.

   - Ein Maschinen-SSL-Zertifikat für jede Maschine. Für das Maschinen-SSL-Zertifikat muss das Feld „SubjectAltName“ den vollqualifizierten Domänennamen (DNS NAME=*Maschinen-FQDN*) enthalten.
   - Optional vier Lösungsbenutzerzertifikate für jedes eingebettete System bzw. jeden Verwaltungsknoten. Lösungsbenutzerzertifikate sollten keine IP-Adresse, keinen Hostnamen und keine E-Mail-Adresse enthalten. Für jedes Zertifikat ist ein unterschiedlicher Zertifikatantragsteller erforderlich.
   - Optional ein Lösungsbenutzerzertifikat „machine“ für externe Platform Services Controller-Instanzen. Dieses Zertifikat unterscheidet sich vom Maschinen-SSL-Zertifikat für den Platform Services Controller.

   Das Ergebnis sind in der Regel eine PEM-Datei für die Vertrauenskette sowie die signierten SSL-Zertifikate für jeden Platform Services Controller bzw. jeden Verwaltungsknoten.

2 Listen Sie die TRUSTED_ROOTS- und Maschinen-SSL-Speicher auf.

```
vecs-cli store list
```

   a Stellen Sie sicher, dass das aktuelle Rootzertifikat und alle Maschinen-SSL-Zertifikate von VMCA signiert wurden.

   b Notieren Sie sich den Inhalt der Felder „Seriennummer“, „Aussteller“ und „Subjektname“.

   c (Optional) Stellen Sie mithilfe eines Webbrowsers eine HTTPS-Verbindung zu einem Knoten her, auf dem das Zertifikat platziert werden soll. Überprüfen Sie die Zertifikatinformationen und stellen Sie sicher, dass sie mit dem Maschinen-SSL-Zertifikat übereinstimmen.

3 Beenden Sie alle Dienste und starten Sie die Dienste für die Zertifikaterstellung, Weitergabe und Speicherung.

Die Dienstnamen sind unter Windows und bei der vCenter Server Appliance unterschiedlich.

**Hinweis** Wenn in Ihrer Umgebung ein externer Platform Services Controller verwendet wird, brauchen Sie VMware Directory Service (vmdird) und VMware Certificate Authority (vmcad) auf dem vCenter Server-Knoten nicht zu beenden und zu starten. Diese Dienste werden unter dem Platform Services Controller ausgeführt.

**Windows**

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

**vCenter Server Appliance**

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

4 Veröffentlichen Sie das benutzerdefinierte Stammzertifikat.

```
dir-cli trustedcert publish --cert <my_custom_root>
```

Wenn Sie in der Befehlszeile keinen Benutzernamen und kein Kennwort eingeben, werden Sie zur Eingabe dieser Informationen aufgefordert.

5 Starten Sie alle Dienste neu.

```
service-control --start --all
```

**Nächste Schritte**

Sie können das ursprüngliche VMCA-Root-Zertifikat aus dem Zertifikatspeicher entfernen, wenn die Unternehmensrichtlinien dies verlangen. In diesem Fall müssen Sie das vCenter Single Sign-On-Zertifikat aktualisieren. Weitere Informationen hierzu finden Sie unter Aktualisieren des Zertifikats für den Security Token Service.

## Ersetzen der Maschinen-SSL-Zertifikate durch benutzerdefinierte Zertifikate

Nachdem Sie die benutzerdefinierten Zertifikate erhalten haben, können Sie jedes Maschinenzertifikat ersetzen.

Für jede Maschine ist ein Maschinen-SSL-Zertifikat für die sichere Kommunikation mit anderen Diensten erforderlich. Bei einer Bereitstellung mit mehreren Knoten müssen Sie die Befehle zum Generieren von Maschinen-SSL-Zertifikaten auf jedem Knoten ausführen. Verwenden Sie den Parameter `--server`, um von einem vCenter Server mit externem Platform Services Controller aus auf den Platform Services Controller zu verweisen.

Sie benötigen die folgenden Informationen, bevor Sie mit dem Ersetzen der Zertifikate beginnen können:

- Kennwort für „administrator@vsphere.local“.
- Gültiges benutzerdefiniertes Maschinen-SSL-Zertifikat (`.crt`-Datei).
- Gültiger benutzerdefinierter Maschinen-SSL-Schlüssel (`.key`-Datei).
- Gültiges benutzerdefiniertes Zertifikat für Root (`.crt`-Datei).
- Die IP-Adresse des Platform Services Controller, wenn Sie den Befehl für einen vCenter Server mit externem Platform Services Controller in einer Bereitstellung mit mehreren Knoten ausführen.

### Voraussetzungen

Sie müssen für jede Maschine ein Zertifikat von Ihrer Drittanbieter- oder Unternehmenszertifizierungsstelle erhalten haben.

- Schlüsselgröße: mindestens 2.048 Bit (PEM-kodiert)
- CRT-Format
- x509 Version 3
- „SubjectAltName“ muss DNS-Name=<Maschinen-FQDN> enthalten.
- Enthält die folgenden Schlüsselverwendungen: digitale Signatur, Schlüsselverschlüsselung

Verfahren

1 Beenden Sie alle Dienste und starten Sie die Dienste für die Zertifikaterstellung, Weitergabe und Speicherung.

Die Dienstnamen sind unter Windows und bei der vCenter Server Appliance unterschiedlich.

**Hinweis** Wenn in Ihrer Umgebung ein externer Platform Services Controller verwendet wird, brauchen Sie VMware Directory Service (vmdird) und VMware Certificate Authority (vmcad) auf dem vCenter Server-Knoten nicht zu beenden und zu starten. Diese Dienste werden unter dem Platform Services Controller ausgeführt.

**Windows**

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

**vCenter Server Appliance**

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

2 Melden Sie sich bei jedem Knoten an und fügen Sie die neuen Maschinenzertifikate, die Sie von der Zertifizierungsstelle erhalten haben, zu VECS hinzu.

Alle Maschinen benötigen das neue Zertifikat im lokalen Zertifikatspeicher für die Kommunikation über SSL.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert <cert-file-
path>
--key <key-file-path>
```

3 Starten Sie alle Dienste neu.

```
service-control --start --all
```

### Beispiel: Ersetzen der Maschinen-SSL-Zertifikate durch benutzerdefinierte Zertifikate

In diesem Beispiel wird die Vorgehensweise zum Ersetzen des Maschinen-SSL-Zertifikats durch ein benutzerdefiniertes Zertifikat in einer Windows-Installation gezeigt. Sie können das Maschinen-SSL-Zertifikat für jeden Knoten auf dieselbe Weise ersetzen.

1 Löschen Sie zunächst das vorhandene Zertifikat in VECS.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
```

2 Fügen Sie anschließend das Ersatzzertifikat hinzu.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert E:\custom-certs\ms-ca\signed-ssl\custom-w1-
vim-cat-dhcp-094.eng.vmware.com.crt --key E:\custom-certs\ms-ca\signed-ssl\custom-x3-vim-
cat-dhcp-1128.vmware.com.priv
```

## Ersetzen der Lösungsbenutzerzertifikate durch benutzerdefinierte Zertifikate

Nachdem Sie die Maschinen-SSL-Zertifikate ersetzt haben, können Sie die VMCA-signierten Lösungsbenutzerzertifikate durch Drittanbieter- oder Unternehmenszertifikate ersetzen.

Viele VMware-Kunden tauschen Lösungsbenutzerzertifikate nicht aus. Sie tauschen lediglich die Maschinen-SSL-Zertifikate gegen benutzerdefinierte Zertifikate aus. Mit dieser hybriden Herangehensweise werden die Anforderungen ihrer Sicherheitsteams erfüllt.

- Zertifikate befinden sich entweder hinter einem Proxy-Server oder stellen benutzerdefinierte Zertifikate dar.
- Es werden keine Zwischenzertifizierungsstellen verwendet.

Lösungsbenutzer verwenden Zertifikate für die Authentifizierung bei vCenter Single Sign On. Wenn das Zertifikat gültig ist, weist vCenter Single Sign On dem Lösungsbenutzer ein SAML-Token zu, und der Lösungsbenutzer verwendet das SAML-Token für die Authentifizierung bei anderen vCenter-Komponenten.

Sie ersetzen das Lösungsbenutzerzertifikat „machine“ auf jedem Verwaltungsknoten und auf jedem Platform Services Controller-Knoten. Die anderen Lösungsbenutzerzertifikate ersetzen Sie nur auf jedem Verwaltungsknoten. Verwenden Sie den Parameter `--server`, um auf den Platform Services Controller zu verweisen, wenn Sie Befehle auf einem Verwaltungsknoten mit einem externen Platform Services Controller ausführen.

**Hinweis** Wenn Sie Lösungsbenutzerzertifikate bei großen Bereitstellungen auflisten, enthält die Ausgabe von `dir-cli list` alle Lösungsbenutzer aus allen Knoten. Führen Sie `vmafd-cli get-machine-id --server-name localhost` aus, um für jeden Host nach der lokalen Maschinen-ID zu suchen. Jeder Lösungsbenutzername enthält die Maschinen-ID.

### Voraussetzungen

- Schlüsselgröße: mindestens 2.048 Bit (PEM-kodiert)
- CRT-Format
- x509 Version 3
- „SubjectAltName“ muss DNS-Name=<Maschinen-FQDN> enthalten.
- Für jedes Lösungsbenutzerzertifikat ist ein unterschiedlicher Wert für `Subject` erforderlich. Geben Sie beispielsweise den Lösungsbenutzernamen (z. B. vpxd) oder einen anderen eindeutigen Bezeichner an.
- Enthält die folgenden Schlüsselverwendungen: digitale Signatur, Schlüsselverschlüsselung

Verfahren

1 Beenden Sie alle Dienste und starten Sie die Dienste für die Zertifikaterstellung, Weitergabe und Speicherung.

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmca
```

2 Suchen Sie den Namen für jeden Lösungsbenutzer.

```
dir-cli service list
```

Sie können die eindeutige ID verwenden, die beim Ersetzen der Zertifikate zurückgegeben wird. Die Ein- und Ausgabe könnte so oder ähnlich wie im Folgenden aussehen.

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

Wenn Sie Lösungsbenutzerzertifikate bei Bereitstellungen mit mehreren Knoten auflisten, enthält die Ausgabe von `dir-cli` alle Lösungsbenutzer aus allen Knoten. Führen Sie `vmafd-cli get-machine-id --server-name localhost` aus, um für jeden Host nach der lokalen Maschinen-ID zu suchen. Jeder Lösungsbenutzername enthält die Maschinen-ID.

3 Ersetzen Sie für jeden Lösungsbenutzer das vorhandene Zertifikat in VECS und anschließend in vmdir.

Sie müssen die Zertifikate in dieser Reihenfolge hinzufügen.

```
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
dir-cli service update --name <vpxd-xxxx-xxx-xxxxxx> --cert vpxd.crt
```

**Hinweis** Lösungsbenutzer können sich nur bei vCenter Single Sign On authentifizieren, wenn Sie das Zertifikat in vmdir ersetzen.

4 Starten Sie alle Dienste neu.

```
service-control --start --all
```

## Ersetzen des VMware Directory Service-Zertifikats in Umgebungen im gemischten Modus

Während des Upgrades kann es vorkommen, dass in Ihrer Umgebung vorübergehend sowohl vCenter Single Sign On, Version 5.5, als auch vCenter Single Sign On, Version 6.x, vorhanden sind. Sie müssen in diesem Fall zusätzliche Schritte ausführen, um das SSL-Zertifikat des VMware Directory Service zu ersetzen, wenn Sie das SSL-Zertifikat des Knotens ersetzen, auf dem der vCenter Single Sign On-Dienst ausgeführt wird.

Das SSL-Zertifikat des VMware Directory Service wird von vmdir für Handshakes zwischen Platform Services Controller-Knoten verwendet, die die vCenter Single Sign On-Replizierung durchführen.

Diese Schritte sind für Umgebungen im gemischten Modus, die Knoten mit vSphere 6.0 und vSphere 6.5 enthalten, nicht erforderlich. Diese Schritte sind nur in folgenden Fällen erforderlich:

- In Ihrer Umgebung sind sowohl vCenter Single Sign On 5.5- als auch vCenter Single Sign On 6.x-Dienste vorhanden.
- Die vCenter Single Sign On-Dienste sind für die Replizierung von vmdir-Daten eingerichtet.
- Sie können die standardmäßigen VMCA-signierten Zertifikate für den Knoten, auf dem der vCenter Single Sign On 6.x-Dienst ausgeführt wird, durch benutzerdefinierte Zertifikate ersetzen.

**Hinweis** Es empfiehlt sich, vor dem Neustart der Dienste ein Upgrade der kompletten Umgebung durchzuführen. Vom Ersetzen des VMware Directory Service-Zertifikats wird in der Regel abgeraten.

### Verfahren

1. Richten Sie auf dem Knoten, auf dem der vCenter Single Sign On 5.5-Dienst ausgeführt wird, die Umgebung so ein, dass der vCenter Single Sign On 6.x-Dienst bekannt ist.
   a. Sichern Sie alle Dateien im Verzeichnis `C:\ProgramData\VMware\CIS\cfg\vmdird`.
   b. Erstellen Sie eine Kopie der Datei `vmdircert.pem` auf dem Knoten der Version 6.x und benennen Sie sie in `<sso_node2.domain.com>.pem` um, wobei `<sso_node2.domain.com>` der FQDN des Knotens der Version 6.x ist.
   c. Kopieren Sie das umbenannte Zertifikat in das Verzeichnis `C:\ProgramData\VMware\CIS\cfg\vmdird`, um das vorhandene Replizierungszertifikat zu ersetzen.
2. Starten Sie den VMware Directory Service auf allen Maschinen neu, auf denen Sie Zertifikate ersetzt haben.

   Sie können den Dienst über den vSphere Client oder mithilfe des Befehls `service-control` neu starten.

# Verwalten von Diensten und Zertifikaten mit CLI-Befehlen

4

Mit einer Reihe von Befehlszeilenschnittstellen (CLIs) können Sie VMCA (VMware Certificate Authority), VECS (VMware Endpoint Certificate Store) und den VMware Directory Service (vmdir) verwalten. Das Dienstprogramm vSphere Certificate Manager unterstützt zwar auch viele verwandte Aufgaben, für die manuelle Zertifikatverwaltung und für die Verwaltung von anderen Diensten sind jedoch Befehlszeilenschnittstellen erforderlich.

Normalerweise greifen Sie auf die CLI-Tools für die Verwaltung von Zertifikaten und zugehörigen Diensten zu, indem Sie über SSH eine Verbindung mit der Appliance-Shell herstellen. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/2100508.

Unter Manuelle Zertifikatsersetzung werden Beispiele zum Ersetzen von Zertifikaten mithilfe von CLI-Befehlen bereitgestellt.

**Tabelle 4-1. CLI-Tools für die Verwaltung von Zertifikaten und zugehörigen Diensten**

| Befehlszeilenschnittstelle | Beschreibung | Informationen hierzu unter |
|---|---|---|
| `certool` | Generieren und verwalten Sie Zertifikate und Schlüssel. Teil von VMCAD, dem VMware-Dienst für die Zertifikatverwaltung. | Befehlsreferenz für die certool-Initialisierung |
| `vecs-cli` | Verwalten Sie die Inhalte von VMware-Zertifikatspeicherinstanzen. Bestandteil von VMAFD. | Befehlsreferenz für vecs-cli |
| `dir-cli` | Erstellen und aktualisieren Sie Zertifikate im VMware Directory Service. Bestandteil von VMAFD. | Befehlsreferenz für dir-cli |
| `sso-config` | Teil der vCenter Single Sign-On-Konfiguration. In den meisten Fällen sollten Sie entweder den vSphere Web Client oder den vSphere Client verwenden. Verwenden Sie diesen Befehl für das Einrichten der zweistufigen Authentifizierung. | Befehlszeilenhilfe.<br>Grundlegendes zur zweistufigen vCenter Server-Authentifizierung |
| `service-control` | Starten oder beenden Sie Dienste, zum Beispiel als Teil eines Workflows zur Zertifikatsersetzung. | Führen Sie diesen Befehl aus, um Dienste anzuhalten, bevor Sie andere CLI-Befehle ausführen. |

# CLI-Speicherorte

Die CLIs finden Sie standardmäßig in den folgenden Speicherorten auf jedem Knoten.

**Windows**

`C:\Programme\VMware\vCenter Server\vmafdd\vecs-cli.exe`

`C:\Programme\VMware\vCenter Server\vmafdd\dir-cli.exe`

`C:\Programme\VMware\vCenter Server\vmcad\certool.exe`

`C:\Programme\VMware\VCenter server\VMware Identity Services\sso-config`

*VCENTER_INSTALL_PATH*`\bin\service-control`

**Linux**

`/usr/lib/vmware-vmafd/bin/vecs-cli`

`/usr/lib/vmware-vmafd/bin/dir-cli`

`/usr/lib/vmware-vmca/bin/certool`

`/opt/vmware/bin`

Unter Linux müssen Sie für den Befehl `service-control` den Pfad nicht angeben.

Wenn Sie Befehle auf einem vCenter Server-System mit einem externen Platform Services Controller durchführen, können Sie den Platform Services Controller mit dem Parameter `--server` angeben.

Dieses Kapitel enthält die folgenden Themen:

- Erforderliche Rechte für die Ausführung von CLIs
- Ändern der certool-Konfigurationsoptionen
- Befehlsreferenz für die certool-Initialisierung
- Befehlsreferenz für die certool-Verwaltung
- Befehlsreferenz für vecs-cli
- Befehlsreferenz für dir-cli

# Erforderliche Rechte für die Ausführung von CLIs

Die erforderlichen Rechte richten sich nach der von Ihnen verwendeten CLI und nach dem Befehl, den Sie ausführen möchten. Bei den meisten Vorgängen zur Zertifikatverwaltung müssen Sie beispielsweise ein Administrator für die lokale vCenter Single Sign-On-Domäne sein (standardmäßig „vsphere.local“). Manche Befehle sind für alle Benutzer verfügbar.

**dir-cli**

Zum Ausführen von `dir-cli`-Befehlen müssen Sie Mitglied der Gruppe „Administratoren“ in der lokalen Domäne sein (standardmäßig „vsphere.local“). Wenn Sie keinen Benutzernamen und kein Kennwort angeben, werden Sie zur Eingabe des Administratorkennworts für die lokale vCenter Single Sign-On-Domäne aufgefordert (standardmäßig „administrator@vsphere.local“).

**vecs-cli**

Anfänglich haben nur der Besitzer des Speichers und Benutzer mit pauschalen Zugriffsrechten Zugriff auf einen Speicher. Benutzer in der Gruppe „Administratoren“ unter Windows und Root-Benutzer unter Linux haben verdeckte Zugriffsrechte.

Bei den Speichern MACHINE_SSL_CERT und TRUSTED_ROOTS handelt es sich um spezielle Speicher. In Abhängigkeit vom Installationstyp hat nur der Rootbenutzer oder Administratorbenutzer vollständigen Zugriff.

**certool**

Für die meisten `certool`-Befehle muss der Benutzer der Gruppe „Administratoren“ angehören. Alle Benutzer können die folgenden Befehle ausführen.

- `genselfcacert`
- `initscr`
- `getdc`
- `waitVMDIR`
- `waitVMCA`
- `genkey`
- `viewcert`

# Ändern der certool-Konfigurationsoptionen

Wenn Sie `certool --gencert` oder bestimmte andere Zertifikatinitialisierungs- oder Verwaltungsbefehle ausführen, liest der Befehl alle Werte aus einer Konfigurationsdatei ein. Sie können die vorhandene Datei bearbeiten, die Standardkonfigurationsdatei (certool.cfg) mithilfe der Option `--config=<file name>` außer Kraft setzen oder verschiedene Werte in der Befehlszeile überschreiben.

Die Konfigurationsdatei `certool.cfg` befindet sich standardmäßig am folgenden Speicherort.

| Betriebssystem | Speicherort |
|---|---|
| Linux | `/usr/lib/vmware-vmca/share/config/` |
| Windows | `C:\Programme\VMware\vCenter Server\vmcad\` |

Die Datei weist mehrere Felder mit den folgenden Standardwerten auf:

```
Country = US
Name= Acme
Organization = AcmeOrg
OrgUnit = AcmeOrg Engineering
State = California
Locality = Palo Alto
IPAddress = 127.0.0.1
Email = email@acme.com
Hostname = server.acme.com
```

Sie können die Werte ändern, indem Sie in der Befehlszeile eine modifizierte Datei angeben oder indem Sie einzelne Werte wie folgt in der Befehlszeile überschreiben.

- Erstellen Sie eine Kopie der Konfigurationsdatei und bearbeiten Sie die Datei. Verwenden Sie die Befehlszeilenoption `--config`, um die Datei anzugeben. Geben Sie den vollständigen Pfad ein, um Probleme beim Pfadnamen zu vermeiden.
- ```
  certool --gencert --config C:\Temp\myconfig.cfg
  ```
- Überschreiben Sie einzelne Werte in der Befehlszeile. Führen Sie beispielsweise den folgenden Befehl aus, um „Locality“ zu überschreiben:

  ```
  certool --gencert --privkey=private.key --Locality="Mountain View"
  ```

Geben Sie `--Name` an, um das Feld „CN“ für den Objektnamen des Zertifikats zu ersetzen.

- Für Lösungsbenutzerzertifikate lautet der Name laut Konvention <Lösungsbenutzername>@<Domäne>. Sie können den Namen jedoch ändern, wenn in Ihrer Umgebung eine andere Konvention verwendet wird.
- Für Maschinen-SSL-Zertifikate wird der FQDN der Maschine verwendet.

  VMCA erlaubt nur einen einzigen DNSName-Wert (im Feld `Hostname`) und keine anderen Aliasoptionen. Wenn die IP-Adresse vom Benutzer angegeben wird, wird sie ebenfalls in „SubAltName“ gespeichert.

Verwenden Sie den Parameter `--Hostname`, um den DNSName-Wert für „SubAltName“ des Zertifikats anzugeben.

# Befehlsreferenz für die certool-Initialisierung

Mit den Befehlen zur `certool`-Initialisierung können Sie Zertifikatsignieranforderungen generieren, VMCA-signierte Zertifikate und Schlüssel anzeigen und generieren, Root-Zertifikate importieren und weitere Zertifikatsverwaltungsvorgänge durchführen.
  ```

In vielen Fällen übergeben Sie mit einem `certool`-Befehl eine Konfigurationsdatei. Weitere Informationen hierzu finden Sie unter Ändern der certool-Konfigurationsoptionen. Einige Beispiele für die Verwendung finden Sie unter Ersetzen vorhandener VMCA-signierter Zertifikate durch neue VMCA-signierte Zertifikate. In der Befehlszeilen-Hilfe finden Sie Details zu diesen Optionen.

## certool --initcsr

Generiert eine Zertifikatsignieranforderung (Certificate Signing Request, CSR). Der Befehl generiert eine PKCS10-Datei und einen privaten Schlüssel.

| Option | Beschreibung |
|---|---|
| `--gencsr` | Erforderlich zum Generieren von CSRs |
| `--privkey <key_file>` | Name der privaten Schlüsseldatei |
| `--pubkey <key_file>` | Name der öffentlichen Schlüsseldatei |
| `--csrfile <csr_file>` | Dateinamen der CSR-Datei, die an den Anbieter der Zertifizierungsstelle gesendet werden soll |
| `--config <config_file>` | Optionaler Name der Konfigurationsdatei. `certool.cfg` ist die Standardeinstellung. |

Beispiel:

```
certool --initcsr --privkey=<filename> --pubkey=<filename> --csrfile=<filename>
```

## certool --selfca

Erstellt ein selbstsigniertes Zertifikat und stattet den VMCA-Server mit einer selbstsignierten Stammzertifizierungsstelle aus. Diese Option ist eine der einfachsten Methoden zur Bereitstellung von Zertifikaten für den VMCA-Server. Sie können dem VMCA-Server auch ein Stammzertifikat eines Drittanbieters zur Verfügung stellen, wobei VMCA als Zwischenzertifizierungsstelle fungiert. Weitere Informationen hierzu finden Sie unter Verwenden von VMCA als Zwischenzertifizierungsstelle.

Dieser Befehl generiert ein um drei Tage rückdatiertes Zertifikat, um Zeitzonenkonflikte zu vermeiden.

| Option | Beschreibung |
|---|---|
| `--selfca` | Erforderlich zum Generieren eines selbstsignierten Zertifikats. |
| `--predate <number_of_minutes>` | Ermöglicht im Feld „Gültig nicht vor“ des Root-Zertifikats die Eingabe einer Anzahl von Minuten vor der aktuellen Uhrzeit. Mit dieser Option können Sie potenzielle Probleme aufgrund von Zeitverschiebungen vermeiden. Der Maximalwert beträgt drei Tage. |

| Option | Beschreibung |
| --- | --- |
| `--config <config_file>` | Optionaler Name der Konfigurationsdatei. `certool.cfg` ist die Standardeinstellung. |
| `--server <server>` | Optionaler Name des VMCA-Servers. Standardmäßig verwendet der Befehl „localhost“. |

Beispiel:

```
machine-70-59:/usr/lib/vmware-vmca/bin # ./certool --predate=2280  --selfca --server=
192.0.2.24 --srp-upn=administrator@vsphere.local
```

## certool --rootca

Importiert ein Stammzertifikat. Fügt das Zertifikat und den privaten Schlüssel der VMCA hinzu. VMCA verwendet zum Signieren stets das aktuellste Stammzertifikat, aber andere Zertifikate stehen nach wie vor zur Verfügung, es sei denn, Sie löschen sie manuell. Das bedeutet, dass Sie Ihre Infrastruktur schrittweise aktualisieren und zum Schluss alle nicht mehr benötigten Zertifikate löschen können.

| Option | Beschreibung |
| --- | --- |
| `--rootca` | Erforderlich zum Importieren einer Stammzertifizierungsstelle. |
| `--cert <certfile>` | Name der Zertifikatdatei. |
| `--privkey <key_file>` | Name der privaten Schlüsseldatei Die Datei muss im kodierten PEM-Format vorliegen. |
| `--server <server>` | Optionaler Name des VMCA-Servers. Standardmäßig verwendet der Befehl „localhost“. |

Beispiel:

```
certool --rootca --cert=root.cert --privkey=privatekey.pem
```

## certool --getdc

Gibt den Standarddomänennamen zurück, der vom vmdir verwendet wird.

| Option | Beschreibung |
| --- | --- |
| `--server <server>` | Optionaler Name des VMCA-Servers. Standardmäßig verwendet der Befehl „localhost“. |
| `--port <port_num>` | Optionale Portnummer. Die Standardeinstellung ist Port 389. |

Beispiel:

```
certool --getdc
```

## certool --waitVMDIR

Warten Sie, bis der VMware Directory Service ausgeführt wird oder die durch `--wait` angegebene Zeitüberschreitungsdauer abgelaufen ist. Verwenden Sie diese Option zusammen mit anderen Optionen zur Planung gewisser Aufgaben, z. B. der Rückgabe des Standarddomänennamens.

| Option | Beschreibung |
|---|---|
| `--wait` | Optionale Anzahl von Minuten, die gewartet werden soll. Die Standardeinstellung lautet 3. |
| `--server <server>` | Optionaler Name des VMCA-Servers. Standardmäßig verwendet der Befehl „localhost“. |
| `--port <port_num>` | Optionale Portnummer. Die Standardeinstellung ist Port 389. |

Beispiel:

```
certool --waitVMDIR --wait 5
```

## certool --waitVMCA

Warten Sie, bis der VMCA-Dienst ausgeführt wird oder die angegebene Zeitüberschreitungsdauer abgelaufen ist. Verwenden Sie diese Option zusammen mit anderen Optionen zur Planung gewisser Aufgaben, z. B. der Generierung von Zertifikaten.

| Option | Beschreibung |
|---|---|
| `--wait` | Optionale Anzahl von Minuten, die gewartet werden soll. Die Standardeinstellung lautet 3. |
| `--server <server>` | Optionaler Name des VMCA-Servers. Standardmäßig verwendet der Befehl „localhost“. |
| `--port <port_num>` | Optionale Portnummer. Die Standardeinstellung ist Port 389. |

Beispiel:

```
certool --waitVMCA --selfca
```

## certool --publish-roots

Erzwingt ein Update der Stammzertifikate. Für diesen Befehl sind Administratorrechte erforderlich.

| Option | Beschreibung |
|---|---|
| `--server <server>` | Optionaler Name des VMCA-Servers. Standardmäßig verwendet der Befehl „localhost“. |

Beispiel:

```
certool --publish-roots
```

# Befehlsreferenz für die certool-Verwaltung

Mit den `certool`-Verwaltungsbefehlen können Sie Zertifikate anzeigen, generieren und widerrufen sowie Informationen zu Zertifikaten anzeigen.

## certool --genkey

Erstellt ein privates und öffentliches Schlüsselpaar. Diese Dateien können dann zum Generieren eines Zertifikats verwendet werden, das durch VMCA signiert wird.

| Option | Beschreibung |
|---|---|
| `--genkey` | Ist zum Erstellen eines privaten und öffentlichen Schlüssels erforderlich. |
| `--privkey <keyfile>` | Name der privaten Schlüsseldatei |
| `--pubkey <keyfile>` | Name der öffentlichen Schlüsseldatei |
| `--server <server>` | Optionaler Name des VMCA-Servers. Standardmäßig verwendet der Befehl „localhost“. |

Beispiel:

```
certool --genkey --privkey=<filename> --pubkey=<filename>
```

## certool --gencert

Erstellt ein Zertifikat vom VMCA-Server. Dieser Befehl verwendet die Information in `certool.cfg` oder in der festgelegten Konfigurationsdatei. Sie können das Zertifikat zur Bereitstellung von Maschinenzertifikaten oder Lösungsbenutzerzertifikate verwenden.

| Option | Beschreibung |
|---|---|
| `--gencert` | Ist zum Erstellen eines Zertifikats erforderlich. |
| `--cert <certfile>` | Name der Zertifikatdatei. Die Datei muss im kodierten PEM-Format vorliegen. |
| `--privkey <keyfile>` | Name der privaten Schlüsseldatei Die Datei muss im kodierten PEM-Format vorliegen. |
| `--config <config_file>` | Optionaler Name der Konfigurationsdatei. `certool.cfg` ist die Standardeinstellung. |
| `--server <server>` | Optionaler Name des VMCA-Servers. Standardmäßig verwendet der Befehl „localhost“. |

Beispiel:

```
certool --gencert --privkey=<filename> --cert=<filename>
```

## certool --getrootca

Druckt das aktuelle Root-CA-Zertifikat in für Benutzer lesbarer Form. Wenn Sie diesen Befehl über einen Verwaltungsknoten ausführen, verwenden Sie den Maschinennamen des Platform Services Controller-Knotens zum Laden der Root-Zertifizierungsstelle. Diese Ausgabe ist nicht als Zertifikat nutzbar, sie wurde geändert, damit sie von Benutzern gelesen werden kann.

| Option | Beschreibung |
|---|---|
| `--getrootca` | Ist zum Drucken des Rootzertifikats erforderlich. |
| `--server <server>` | Optionaler Name des VMCA-Servers. Standardmäßig verwendet der Befehl „localhost“. |

Beispiel:

```
certool --getrootca --server=remoteserver
```

## certool --viewcert

Druckt alle Felder in einem Zertifikat in für Benutzer lesbarer Form.

| Option | Beschreibung |
|---|---|
| `--viewcert` | Ist zum Anzeigen eines Zertifikats erforderlich. |
| `--cert <certfile>` | Optionaler Name der Konfigurationsdatei. `certool.cfg` ist die Standardeinstellung. |

Beispiel:

```
 certool --viewcert --cert=<filename>
```

## certool --enumcert

Listet alle Zertifikate auf, die der VMCA-Server kennt. Mit der erforderlichen `filter`-Option können Sie alle Zertifikate oder nur widerrufene, aktive oder abgelaufene Zertifikate auflisten.

| Option | Beschreibung |
|---|---|
| `--enumcert` | Ist zum Auflisten aller Zertifikate erforderlich. |
| `--filter [all \| active]` | Erforderlicher Filter. Geben Sie „all“ oder „active“ an. Die Optionen „revoked“ und „expired“ werden derzeit nicht unterstützt. |

Beispiel:

```
certool --enumcert --filter=active
```

## certool --status

Sendet ein festgelegtes Zertifikat zum VMCA-Server, um zu prüfen, ob das Zertifikat widerrufen wurde. Gibt `Certificate: REVOKED` aus, wenn das Zertifikat widerrufen wird, und andernfalls `Certificate: ACTIVE`.

| Option | Beschreibung |
|---|---|
| `--status` | Ist zum Prüfen des Status eines Zertifikats erforderlich. |
| `--cert <certfile>` | Optionaler Name der Konfigurationsdatei. `certool.cfg` ist die Standardeinstellung. |
| `--server <server>` | Optionaler Name des VMCA-Servers. Standardmäßig verwendet der Befehl „localhost“. |

Beispiel:

```
certool --status --cert=<filename>
```

## certool --genselfcacert

Erstellt ein selbstsigniertes Zertifikat basierend auf den Werten in der Konfigurationsdatei. Dieser Befehl generiert ein um drei Tage rückdatiertes Zertifikat, um Zeitzonenkonflikte zu vermeiden.

| Option | Beschreibung |
|---|---|
| `--genselfcacert` | Erforderlich zum Generieren eines selbstsignierten Zertifikats. |
| `--outcert <cert_file>` | Name der Zertifikatdatei. Die Datei muss im kodierten PEM-Format vorliegen. |
| `--outprivkey <key_file>` | Name der privaten Schlüsseldatei Die Datei muss im kodierten PEM-Format vorliegen. |
| `--config <config_file>` | Optionaler Name der Konfigurationsdatei. `certool.cfg` ist die Standardeinstellung. |

Beispiel:

```
certool --genselfcert --privkey=<filename> --cert=<filename>
```

# Befehlsreferenz für vecs-cli

Mit dem Befehlssatz `vecs-cli` können Sie die Instanzen des VMware-Zertifikatspeichers (VMware Certificate Store, VECS) verwalten. Verwenden Sie diese Befehle zusammen mit `dir-cli` und

`certool`, um Ihre Zertifikatinfrastruktur und andere Platform Services Controller-Dienste zu verwalten.

## vecs-cli store create

Erstellt einen Zertifikatspeicher.

| Option | Beschreibung |
|---|---|
| `--name <name>` | Der Name des Zertifikatspeichers. |
| `--server <server-name>` | Wird verwendet, um einen Servernamen anzugeben, wenn Sie eine Verbindung zu einer VECS-Remote-Instanz herstellen. |
| `--upn <user-name>` | Benutzerprinzipalname, der zur Anmeldung bei der durch `--server <server-name>` angegebenen Serverinstanz verwendet wird. Wenn Sie einen Speicher erstellen, wird dieser im Kontext des aktuellen Benutzers erstellt. Daher ist der Besitzer des Speichers der aktuelle Benutzerkontext und nicht immer der Root-Benutzer. |

Beispiel:

```
vecs-cli store create --name <store>
```

## vecs-cli store delete

Löscht einen Zertifikatspeicher. Die Systemspeicher MACHINE_SSL_CERT, TRUSTED_ROOTS und TRUSTED_ROOT_CRLS können nicht gelöscht werden. Benutzer mit den erforderlichen Rechten können Lösungsbenutzerspeicher löschen.

| Option | Beschreibung |
|---|---|
| `--name <name>` | Name des zu löschenden Zertifikatspeichers. |
| `--server <server-name>` | Wird verwendet, um einen Servernamen anzugeben, wenn Sie eine Verbindung zu einer VECS-Remote-Instanz herstellen. |
| `--upn <user-name>` | Benutzerprinzipalname, der zur Anmeldung bei der durch `--server <server-name>` angegebenen Serverinstanz verwendet wird. Wenn Sie einen Speicher erstellen, wird dieser im Kontext des aktuellen Benutzers erstellt. Daher ist der Besitzer des Speichers der aktuelle Benutzerkontext und nicht immer der Root-Benutzer. |

Beispiel:

```
vecs-cli store delete --name <store>
```

# vecs-cli store list

Listet Zertifikatspeicher auf.

| Option | Beschreibung |
|---|---|
| `--server <server-name>` | Wird verwendet, um einen Servernamen anzugeben, wenn Sie eine Verbindung zu einer VECS-Remote-Instanz herstellen. |
| `--upn <user-name>` | Benutzerprinzipalname, der zur Anmeldung bei der durch `--server <server-name>` angegebenen Serverinstanz verwendet wird. Wenn Sie einen Speicher erstellen, wird dieser im Kontext des aktuellen Benutzers erstellt. Daher ist der Besitzer des Speichers der aktuelle Benutzerkontext und nicht immer der Root-Benutzer. |

VECS enthält die folgenden Speicher.

### Tabelle 4-2. Speicher in VECS

| Speicher | Beschreibung |
|---|---|
| Maschinen-SSL-Speicher (MACHINE_SSL_CERT) | ■ Wird vom Reverse-Proxy-Dienst auf jedem vSphere-Knoten verwendet.<br>■ Wird vom VMware Directory Service (vmdir) für eingebettete Bereitstellungen und für jeden Platform Services Controller-Knoten verwendet.<br>Alle Dienste in vSphere 6.0 und höher kommunizieren über einen Reverse-Proxy, der das Maschinen-SSL-Zertifikat verwendet. Aus Gründen der Abwärtskompatibilität verwenden die 5.x-Dienste weiterhin bestimmte Ports. Deshalb ist für bestimmte Dienste wie etwa vpxd ein eigener Port geöffnet. |
| Vertrauenswürdiger Stammspeicher (TRUSTED_ROOTS) | Enthält alle vertrauenswürdigen Stammzertifikate. |

Tabelle 4-2. Speicher in VECS (Fortsetzung)

| Speicher | Beschreibung |
| --- | --- |
| Lösungsbenutzerspeicher<br>■ machine<br>■ vpxd<br>■ vpxd-extension<br>■ vsphere-webclient | VECS enthält einen Speicher für jeden Lösungsbenutzer. Das Objekt jedes Lösungsbenutzerzertifikats muss eindeutig sein. So darf z. B. das Maschinenzertifikat nicht das gleiche Objekt wie das vpxd-Zertifikat haben.<br>Lösungsbenutzerzertifikate werden für die Authentifizierung mit vCenter Single Sign On verwendet. vCenter Single Sign On überprüft, ob das Zertifikat gültig ist. Andere Zertifikatattribute werden jedoch nicht überprüft. Bei einer eingebetteten Bereitstellung befinden sich alle Lösungsbenutzerzertifikate im selben System.<br>Die folgenden Lösungsbenutzer-Zertifikatspeicher sind in VECS für jeden Verwaltungsknoten und für jede eingebettete Bereitstellung enthalten:<br>■ machine: Wird vom Lizenzserver und vom Protokollierungsdienst verwendet.<br>**Hinweis** Das Lösungsbenutzerzertifikat „machine“ hat nichts mit dem SSL-Zertifikat „machine“ zu tun. Das Lösungsbenutzerzertifikat „machine“ wird für den Austausch von SAML-Tokens verwendet. Das SSL-Zertifikat „machine“ wird für sichere SSL-Verbindungen für eine Maschine verwendet.<br>■ vpxd: vCenter-Dienst-Daemon (vpxd)-Speicher für Verwaltungsknoten und eingebettete Bereitstellungen. vpxd verwendet das in diesem Speicher gespeicherte Lösungsbenutzerzertifikat für die Authentifizierung bei vCenter Single Sign On.<br>■ vpxd-extension: vCenter-Erweiterungsspeicher. Enthält den Auto Deploy-Dienst, den Inventory Service und sonstige Dienste, die nicht Bestandteil anderer Lösungsbenutzer sind.<br>■ vsphere-webclient: vSphere Web Client-Speicher. Enthält auch zusätzliche Dienste wie etwa den Leistungsdiagrammdienst.<br>Jeder Platform Services Controller-Knoten enthält ein machine-Zertifikat. |

Tabelle 4-2. Speicher in VECS (Fortsetzung)

| Speicher | Beschreibung |
|---|---|
| vSphere Certificate Manager Utility-Backup-Speicher (BACKUP_STORE) | Wird von VMCA (VMware Certificate Manager) für die Unterstützung der Zertifikatwiederherstellung verwendet. Nur der letzte Status wird als Backup gespeichert und Sie können nur den letzten Schritt rückgängig machen. |
| Weitere Speicher | Weitere Speicher können durch Lösungen hinzugefügt werden. Beispielsweise fügt die Virtual Volumes-Lösung einen SMS-Speicher hinzu. Ändern Sie die Zertifikate in diesen Speichern nur, wenn Sie in der VMware-Dokumentation oder in einem VMware-Knowledgebase-Artikel dazu aufgefordert werden.<br>**Hinweis** Durch das Löschen des Speichers TRUSTED_ROOTS_CRLS kann die Zertifikatinfrastruktur beschädigt werden. Den TRUSTED_ROOTS_CRLS-Speicher sollten Sie weder löschen noch ändern. |

Beispiel:

```
vecs-cli store list
```

## vecs-cli store permissions

Erteilt oder widerruft die Berechtigungen für den Speicher. Verwenden Sie entweder die Option `--grant` (erteilen) oder die Option `--revoke` (widerrufen).

Der Besitzer des Speichers kann alle Vorgänge ausführen. Dazu gehört auch das Recht zum Erteilen und Widerrufen von Berechtigungen. Der Administrator der lokalen vCenter Single Sign-On-Domäne (standardmäßig „administrator@vsphere.local“) verfügt über Rechte für alle Speicher. Dazu gehört auch das Recht zum Erteilen und Widerrufen von Berechtigungen.

Mit `vecs-cli get-permissions --name <store-name>` können Sie die aktuellen Einstellungen des Speichers abrufen.

| Option | Beschreibung |
|---|---|
| `--name <name>` | Der Name des Zertifikatspeichers. |
| `--user <username>` | Eindeutiger Name des Benutzers, dem Berechtigungen erteilt werden |
| `--grant [read\|write]` | Berechtigung, die erteilt wird: read (Lesen) oder write (Schreiben) |
| `--revoke [read\|write]` | Berechtigung, die widerrufen wird: read (Lesen) oder write (Schreiben). Wird derzeit nicht unterstützt. |

## vecs-cli store get-permissions

Ruft die aktuellen Berechtigungseinstellungen für den Speicher ab.

| Option | Beschreibung |
| --- | --- |
| `--name <name>` | Der Name des Zertifikatspeichers. |
| `--server <server-name>` | Wird verwendet, um einen Servernamen anzugeben, wenn Sie eine Verbindung zu einer VECS-Remote-Instanz herstellen. |
| `--upn <user-name>` | Benutzerprinzipalname, der zur Anmeldung bei der durch `--server <server-name>` angegebenen Serverinstanz verwendet wird. Wenn Sie einen Speicher erstellen, wird dieser im Kontext des aktuellen Benutzers erstellt. Daher ist der Besitzer des Speichers der aktuelle Benutzerkontext und nicht immer der Root-Benutzer. |

## vecs-cli entry create

Erstellt einen Eintrag in VECS. Verwenden Sie diesen Befehl, um einen privaten Schlüssel in ein Zertifikat oder einen Speicher einzufügen.

| Option | Beschreibung |
| --- | --- |
| `--store <NameOfStore>` | Der Name des Zertifikatspeichers. |
| `--alias <Alias>` | Der optionale Alias für das Zertifikat. Diese Option wird für den vertrauenswürdigen Stammzertifikatspeicher ignoriert. |
| `--cert <certificate_file_path>` | Der vollständige Pfad der Zertifikatsdatei. |
| `--key <key-file-path>` | Der vollständige Pfad des Schlüssels, der dem Zertifikat entspricht.<br>Optional. |
| `--password <password>` | Optionales Kennwort für die Verschlüsselung des privaten Schlüssels. |
| `--server <server-name>` | Wird verwendet, um einen Servernamen anzugeben, wenn Sie eine Verbindung zu einer VECS-Remote-Instanz herstellen. |
| `--upn <user-name>` | Benutzerprinzipalname, der zur Anmeldung bei der durch `--server <server-name>` angegebenen Serverinstanz verwendet wird. Wenn Sie einen Speicher erstellen, wird dieser im Kontext des aktuellen Benutzers erstellt. Daher ist der Besitzer des Speichers der aktuelle Benutzerkontext und nicht immer der Root-Benutzer. |

## vecs-cli entry list

Listet alle Einträge in einem angegebenen Speicher auf.

| Option | Beschreibung |
| --- | --- |
| `--store <NameOfStore>` | Der Name des Zertifikatspeichers. |

## vecs-cli entry getcert

Ruft ein Zertifikat aus dem VECS ab. Sie können das Zertifikat an eine Ausgabedatei senden oder als von Benutzern lesbaren Text anzeigen.

| Option | Beschreibung |
|---|---|
| `--store <NameOfStore>` | Der Name des Zertifikatspeichers. |
| `--alias <Alias>` | Alias des Zertifikats |
| `--output <output_file_path>` | Datei, in die das Zertifikat geschrieben wird. |
| `--text` | Zeigt eine von Benutzern lesbare Version des Zertifikats an. |
| `--server <server-name>` | Wird verwendet, um einen Servernamen anzugeben, wenn Sie eine Verbindung zu einer VECS-Remote-Instanz herstellen. |
| `--upn <user-name>` | Benutzerprinzipalname, der zur Anmeldung bei der durch `--server <server-name>` angegebenen Serverinstanz verwendet wird. Wenn Sie einen Speicher erstellen, wird dieser im Kontext des aktuellen Benutzers erstellt. Daher ist der Besitzer des Speichers der aktuelle Benutzerkontext und nicht immer der Root-Benutzer. |

## vecs-cli entry getkey

Ruft einen im VECS gespeicherten Schlüssel ab. Sie können den Schlüssel an eine Ausgabedatei senden oder als von Benutzern lesbaren Text anzeigen.

| Option | Beschreibung |
|---|---|
| `--store <NameOfStore>` | Der Name des Zertifikatspeichers. |
| `--alias <Alias>` | Alias des Schlüssels |
| `--output <output_file_path>` | Ausgabedatei, in die der Schlüssel geschrieben wird. |
| `--text` | Zeigt eine von Benutzern lesbare Version des Schlüssels an. |
| `--server <server-name>` | Wird verwendet, um einen Servernamen anzugeben, wenn Sie eine Verbindung zu einer VECS-Remote-Instanz herstellen. |
| `--upn <user-name>` | Benutzerprinzipalname, der zur Anmeldung bei der durch `--server <server-name>` angegebenen Serverinstanz verwendet wird. Wenn Sie einen Speicher erstellen, wird dieser im Kontext des aktuellen Benutzers erstellt. Daher ist der Besitzer des Speichers der aktuelle Benutzerkontext und nicht immer der Root-Benutzer. |

## vecs-cli entry delete

Löscht einen Eintrag in einem Zertifikatspeicher. Wenn ein Eintrag aus dem VECS gelöscht wird, wird er dauerhaft aus dem VECS entfernt. Die einzige Ausnahme ist das aktuelle Stammzertifikat. VECS ruft ein Rootzertifikat aus vmdir ab.

| Option | Beschreibung |
|---|---|
| `--store <NameOfStore>` | Der Name des Zertifikatspeichers. |
| `--alias <Alias>` | Alias des Eintrags, der gelöscht werden soll |
| `--server <server-name>` | Wird verwendet, um einen Servernamen anzugeben, wenn Sie eine Verbindung zu einer VECS-Remote-Instanz herstellen. |
| `--upn <user-name>` | Benutzerprinzipalname, der zur Anmeldung bei der durch `--server <server-name>` angegebenen Serverinstanz verwendet wird. Wenn Sie einen Speicher erstellen, wird dieser im Kontext des aktuellen Benutzers erstellt. Daher ist der Besitzer des Speichers der aktuelle Benutzerkontext und nicht immer der Root-Benutzer. |
| `-y` | Unterdrückt die Bestätigungsaufforderung. Nur für fortgeschrittene Benutzer. |

## vecs-cli force-refresh

Erzwingt die Aktualisierung von VECS. Standardmäßig sieht der VECS alle 5 Minuten im vmdir nach, ob ein neues Stammzertifikat vorliegt. Mit diesem Befehl wird der VECS sofort aus dem vmdir aktualisiert.

| Option | Beschreibung |
|---|---|
| `--server <server-name>` | Wird verwendet, um einen Servernamen anzugeben, wenn Sie eine Verbindung zu einer VECS-Remote-Instanz herstellen. |
| `--upn <user-name>` | Benutzerprinzipalname, der zur Anmeldung bei der durch `--server <server-name>` angegebenen Serverinstanz verwendet wird. Wenn Sie einen Speicher erstellen, wird dieser im Kontext des aktuellen Benutzers erstellt. Daher ist der Besitzer des Speichers der aktuelle Benutzerkontext und nicht immer der Root-Benutzer. |

# Befehlsreferenz für dir-cli

Mit dem Dienstprogramm `dir-cli` können Sie Lösungsbenutzer erstellen und aktualisieren, Benutzerkonten verwalten und Zertifikate und Kennwörter in vmdir (VMware Directory Service) verwalten. Sie können auch `dir-cli` zum Verwalten und Abfragen der Domänenfunktionsebene von Platform Services Controller-Instanzen verwenden.

## dir-cli nodes list

Listet alle vCenter Server-Systeme für die angegebene Platform Services Controller-Instanz auf.

| Option | Beschreibung |
|---|---|
| `--login <admin_user_id>` | Der Administrator der lokalen vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“. |
| `--password <admin_password>` | Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert. |
| `--server <psc_ip_or_fqdn>` | Verwenden Sie diese Option, wenn der zugewiesene Platform Services Controller nicht als Ziel verwendet werden soll. Geben Sie die IP-Adresse oder den FQDN des Platform Services Controller an. |

## dir-cli computer password-reset

Mit diesem Befehl können Sie das Kennwort des Maschinenkontos in der Domäne zurücksetzen. Diese Option ist hilfreich, wenn Sie eine Platform Services Controller-Instanz wiederherstellen müssen.

| Option | Beschreibung |
|---|---|
| `--login <admin_user_id>` | Der Administrator der lokalen vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“. |
| `--password <admin_password>` | Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert. |
| `--live-dc-hostname <server name>` | Aktueller Name der Platform Services Controller-Instanz. |

## dir-cli service create

Erstellt einen Lösungsbenutzer. Wird hauptsächlich für Lösungen von Drittanbietern verwendet.

| Option | Beschreibung |
|---|---|
| `--name <name>` | Name des zu erstellenden Lösungsbenutzers. |
| `--cert <cert file>` | Pfad zur Zertifikatdatei. Dies kann ein von VMCA signiertes Zertifikat oder ein Drittanbieterzertifikat sein. |
| `--ssogroups <comma-separated-groupnames>` | Macht den Lösungsbenutzer zu einem Mitglied der angegebenen Gruppen. |
| `--wstrustrole <ActAsUser>` | Macht den Lösungsbenutzer zu einem Mitglied der integrierten Administratoren- oder Benutzergruppe. In anderen Worten: bestimmt, ob der Lösungsbenutzer über Administrationsrechte verfügt. |
| `--ssoadminrole <Administrator/User>` | Macht den Lösungsbenutzer zu einem Mitglied der ActAsUser-Gruppe. Mit der ActAsUser-Rolle können Benutzer im Namen anderer Benutzer agieren. |

| Option | Beschreibung |
| --- | --- |
| `--login <admin_user_id>` | Der Administrator der lokalen vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“. |
| `--password <admin_password>` | Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert. |

## dir-cli service list

Listet die Lösungsbenutzer auf, die `dir-cli` bekannt sind.

| Option | Beschreibung |
| --- | --- |
| `--login <admin_user_id>` | Der Administrator der lokalen vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“. |
| `--password <admin_password>` | Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert. |

## dir-cli service delete

Löscht einen Lösungsbenutzer in vmdir. Wenn Sie den Lösungsbenutzer löschen, sind alle zugehörigen Dienste für alle Verwaltungsknoten, die diese vmdir-Instanz verwenden, nicht mehr verfügbar.

| Option | Beschreibung |
| --- | --- |
| `--name` | Name des zu löschenden Lösungsbenutzers. |
| `--login <admin_user_id>` | Der Administrator der lokalen vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“. |
| `--password <admin_password>` | Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert. |

## dir-cli service update

Aktualisiert das Zertifikat für einen angegebenen Lösungsbenutzer, d. h. eine Sammlung von Diensten. Nach Ausführen dieses Befehls übernimmt VECS die Änderung nach 5 Minuten, oder Sie können `vecs-cli force-refresh` verwenden, um eine Aktualisierung zu erzwingen.

| Option | Beschreibung |
| --- | --- |
| `--name <name>` | Name des zu aktualisierenden Lösungsbenutzers. |
| `--cert <cert_file>` | Name des Zertifikats, das dem Dienst zugewiesen wird. |
| `--login <admin_user_id>` | Der Administrator der lokalen vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“. |
| `--password <admin_password>` | Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert. |

## dir-cli user create

Erstellt einen regulären Benutzer innerhalb von vmdir. Dieser Befehl kann für Personen verwendet werden, die sich bei vCenter Single Sign On mit einem Benutzernamen und Kennwort authentifizieren. Verwenden Sie diesen Befehl beim Erstellen von Prototypen.

| Option | Beschreibung |
|---|---|
| `--account <name>` | Name des zu erstellenden vCenter Single Sign On-Benutzers. |
| `--user-password <password>` | Anfängliches Kennwort des Benutzers. |
| `--first-name <name>` | Vorname des Benutzers. |
| `--last-name <name>` | Nachname des Benutzers. |
| `--login <admin_user_id>` | Der Administrator der lokalen vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“. |
| `--password <admin_password>` | Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert. |

## dir-cli user modify

Ändert den angegebenen Benutzer innerhalb von vmdir.

| Option | Beschreibung |
|---|---|
| `--account <name>` | Name des zu ändernden vCenter Single Sign On-Benutzers. |
| `--password-never-expires` | Legen Sie diese Option auf „true“ fest, wenn Sie ein Benutzerkonto für automatisierte Aufgaben erstellen, die beim Platform Services Controller authentifiziert werden müssen, und Sie sicherstellen möchten, dass die Aufgaben bei Kennwortablauf trotzdem ausgeführt werden.<br>Verwenden Sie diese Option mit Vorsicht. |
| `--password-expires` | Legen Sie diese Option auf „true“ fest, wenn Sie die `--password-never-expires`-Option wiederherstellen möchten. |
| `--login <admin_user_id>` | Der Administrator der lokalen vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“. |
| `--password <admin_password>` | Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert. |

## dir-cli user delete

Löscht den angegebenen Benutzer in vmdir.

| Option | Beschreibung |
|---|---|
| `--account <name>` | Name des zu löschenden vCenter Single Sign On-Benutzers. |
| `--login <admin_user_id>` | Der Administrator der lokalen vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“. |
| `--password <admin_password>` | Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert. |

## dir-cli user find-by-name

Sucht einen Benutzer innerhalb von vmdir anhand des Namens. Die von diesem Befehl zurückgegebenen Informationen richten sich danach, was Sie für die Option `--level` angeben.

| Option | Beschreibung |
|---|---|
| `--account <name>` | Name des zu löschenden vCenter Single Sign On-Benutzers. |
| `--level <info level 0\|1\|2>` | Gibt die folgenden Informationen zurück:<br>■ Ebene 0 – Konto und UPN<br>■ Ebene 1 – Ebene 0-Info + Vor- und Nachname<br>■ Ebene 2 : Ebene 0 + Flag „Konto deaktiviert“, Flag „Konto gesperrt“, Flag „Kennwort läuft nie ab“, Flag „Kennwort abgelaufen“ und Flag „Kennwortablauf“.<br>Die Standardebene ist 0. |
| `--login <admin_user_id>` | Der Administrator der lokalen vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“. |
| `--password <admin_password>` | Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert. |

## dir-cli group modify

Fügt einer vorhandenen Gruppe einen Benutzer oder eine Gruppe hinzu.

| Option | Beschreibung |
|---|---|
| `--name <name>` | Name der Gruppe in vmdir. |
| `--add <user_or_group_name>` | Name des hinzuzufügenden Benutzers oder der Gruppe. |
| `--login <admin_user_id>` | Der Administrator der lokalen vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“. |
| `--password <admin_password>` | Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert. |

## dir-cli group list

Listet eine angegebene vmdir-Gruppe auf.

| Option | Beschreibung |
| --- | --- |
| `--name <name>` | Optionaler Name der Gruppe in vmdir. Mit dieser Option können Sie prüfen, ob eine bestimmte Gruppe vorhanden ist. |
| `--login <admin_user_id>` | Der Administrator der lokalen vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“. |
| `--password <admin_password>` | Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert. |

## dir-cli ssogroup create

Erstellt eine Gruppe innerhalb der lokalen Domäne (standardmäßig „vsphere.local“).

Verwenden Sie diesen Befehl, wenn Sie Gruppen zum Verwalten von Benutzerberechtigungen für die vCenter Single Sign-On-Domäne erstellen möchten. Wenn Sie zum Beispiel eine Gruppe erstellen und diese dann zur Gruppe „Administratoren“ der vCenter Single Sign-On-Domäne hinzufügen, haben alle zu dieser Gruppe hinzugefügten Benutzer Administratorrechte für die Domäne.

Gruppen in der vCenter Single Sign-On-Domäne können auch Berechtigungen für vCenter-Bestandslistenobjekte erteilt werden. Informationen finden Sie in der Dokumentation *vSphere-Sicherheit*.

| Option | Beschreibung |
| --- | --- |
| `--name <name>` | Name der Gruppe in vmdir. Die maximale Länge beträgt 487 Zeichen. |
| `--description <description>` | Optionale Beschreibung für die Gruppe. |
| `--login <admin_user_id>` | Der Administrator der lokalen vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“. |
| `--password <admin_password>` | Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert. |

## dir-cli trustedcert publish

Veröffentlicht ein vertrauenswürdiges Root-Zertifikat in vmdir.

| Option | Beschreibung |
| --- | --- |
| `--cert <file>` | Pfad zur Zertifikatdatei. |
| `--crl <file>` | Diese Option wird von VMCA nicht unterstützt. |
| `--login <admin_user_id>` | Der Administrator der lokalen vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“. |

| Option | Beschreibung |
| --- | --- |
| `--password <admin_password>` | Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert. |
| `--chain` | Geben Sie diese Option an, wenn Sie ein verkettetes Zertifikat veröffentlichen. Es ist kein Optionswert erforderlich. |

## dir-cli trustedcert publish

Veröffentlicht ein vertrauenswürdiges Root-Zertifikat in vmdir.

| Option | Beschreibung |
| --- | --- |
| `--cert <file>` | Pfad zur Zertifikatdatei. |
| `--crl <file>` | Diese Option wird von VMCA nicht unterstützt. |
| `--login <admin_user_id>` | Der Administrator der lokalen vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“. |
| `--password <admin_password>` | Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert. |
| `--chain` | Geben Sie diese Option an, wenn Sie ein verkettetes Zertifikat veröffentlichen. Es ist kein Optionswert erforderlich. |

## dir-cli trustedcert unpublish

Hebt die Veröffentlichung eines vertrauenswürdigen Root-Zertifikats in vmdir auf. Verwenden Sie diesen Befehl beispielsweise, wenn Sie ein anderes Root-Zertifikat zu vmdir hinzugefügt haben, das jetzt das Root-Zertifikat für alle anderen Zertifikate in der Umgebung ist. Das Aufheben der Veröffentlichung von nicht mehr verwendeten Zertifikaten ist Bestandteil der Sicherung Ihrer Umgebung.

| Option | Beschreibung |
| --- | --- |
| `--cert-file <file>` | Pfad zur Zertifikatdatei, deren Veröffentlichung aufgehoben werden soll. |
| `--login <admin_user_id>` | Der Administrator der lokalen vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“. |
| `--password <admin_password>` | Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert. |

## dir-cli trustedcert list

Listet alle vertrauenswürdigen Root-Zertifikate und deren IDs auf. Sie benötigen die Zertifikat-IDs, um ein Zertifikat mit `dir-cli trustedcert get` abzurufen.

| Option | Beschreibung |
| --- | --- |
| `--login <admin_user_id>` | Der Administrator der lokalen vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“. |
| `--password <admin_password>` | Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert. |

## dir-cli trustedcert get

Ruft ein vertrauenswürdiges Root-Zertifikat aus vmdir ab und schreibt es in eine angegebene Datei.

| Option | Beschreibung |
| --- | --- |
| `--id <cert_ID>` | ID des abzurufenden Zertifikats. Der Befehl `dir-cli trustedcert list` zeigt die ID an. |
| `--outcert <path>` | Pfad, in den die Zertifikatdatei geschrieben wird. |
| `--outcrl <path>` | Pfad, in den die CRL-Datei geschrieben wird. Wird derzeit nicht verwendet. |
| `--login <admin_user_id>` | Der Administrator der lokalen vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“. |
| `--password <admin_password>` | Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert. |

## dir-cli password create

Erstellt ein zufälliges Kennwort, das die Kennwortanforderungen erfüllt. Dieser Befehl kann von Benutzern von Drittanbieterlösungen verwendet werden.

| Option | Beschreibung |
| --- | --- |
| `--login <admin_user_id>` | Der Administrator der lokalen vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“. |
| `--password <admin_password>` | Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert. |

## dir-cli password reset

Damit kann ein Administrator ein Benutzerkennwort zurücksetzen. Wenn Sie kein Administratorbenutzer sind und ein Kennwort zurücksetzen möchten, verwenden Sie stattdessen `dir-cli password change`.

| Option | Beschreibung |
| --- | --- |
| `--account` | Name des Kontos, dem ein neues Kennwort zugewiesen werden soll. |
| `--new` | Neues Kennwort für den angegebenen Benutzer. |

| Option | Beschreibung |
| --- | --- |
| `--login <admin_user_id>` | Der Administrator der lokalen vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“. |
| `--password <admin_password>` | Das Kennwort des Administrators. Wenn Sie kein Kennwort angeben, werden Sie zur Eingabe aufgefordert. |

## dir-cli password change

Damit kann ein Benutzer sein Kennwort ändern. Sie können diese Änderung nur vornehmen, wenn Sie der Besitzer des Benutzerkontos sind. Administratoren können jedes beliebige Kennwort mit `dir-cli password reset` zurücksetzen.

| Option | Beschreibung |
| --- | --- |
| `--account` | Kontoname. |
| `--current` | Aktuelles Kennwort des Benutzers, der Besitzer des Kontos ist. |
| `--new` | Neues Kennwort des Benutzers, der Besitzer des Kontos ist. |

# Fehlerbehebung für Platform Services Controller

5

Die folgenden Themen bieten einen guten Einstieg in die Fehlerbehebung für Platform Services Controller. Zusätzliche Pointer finden Sie in diesem Dokumentationscenter und im VMware-Knowledgebase-System.

Dieses Kapitel enthält die folgenden Themen:



## Ermitteln der Ursache eines Lookup Service-Fehlers

vCenter Single Sign On-Installation zeigt einen Fehler in vCenter Server, vSphere Client oder vSphere Web Client an.

### Problem

Die Installationsprogramme von vCenter Server und Web Client zeigen folgenden Fehler an: `Could not contact Lookup Service. Please check VM_ssoreg.log....`

### Ursache

Dieses Problem kann mehrere Ursachen haben. Dazu zählen nicht synchronisierte Uhren auf den Hostmaschinen, Firewall-Blockierung und nicht gestartete Dienste.

### Lösung

1. Vergewissern Sie sich, dass die Uhren auf den Hostmaschinen synchronisiert sind, auf denen vCenter Single Sign On, vCenter Server und Web Client ausgeführt werden.
2. Zeigen Sie die in der Fehlermeldung angegebene Protokolldatei an.

   „Temporärer Systemordner“ in der Meldung bezieht sich auf `%TEMP%`.

3 Suchen Sie in der Protokolldatei nach den folgenden Meldungen.

Die Protokolldatei enthält die Ausgaben aller Installationsversuche. Suchen Sie die letzte Meldung mit folgendem Inhalt: `Initializing registration provider...`

| Meldung | Ursache und Lösung |
|---|---|
| **`java.net.ConnectException: Connection timed out: connect`** | Die IP-Adresse ist falsch, eine Firewall blockiert den Zugriff auf vCenter Single Sign On oder vCenter Single Sign On ist überlastet.<br>Stellen Sie sicher, dass der vCenter Single Sign-On-Port (standardmäßig 7444) nicht von einer Firewall blockiert wird. Stellen Sie außerdem sicher, dass die Maschine, auf der vCenter Single Sign On installiert ist, über entsprechende freie CPU-, E/A- und RAM-Kapazitäten verfügt. |
| **`java.net.ConnectException: Connection refused: connect`** | Die IP-Adresse oder der FQDN ist falsch und der vCenter Single Sign On-Dienst wurde nicht oder innerhalb der letzten Minute gestartet.<br>Vergewissern Sie sich, dass vCenter Single Sign On ausgeführt wird, indem Sie den Status des vCenter Single Sign On-Diensts (Windows) bzw. des vmware-sso-Daemons (Linux) prüfen.<br>Starten Sie den Dienst neu. Wenn das Problem durch einen Neustart nicht behoben wird, finden Sie weitere Informationen im *Handbuch für vSphere-Fehlerbehebung*, im Abschnitt zur Wiederherstellung. |
| **`Unexpected status code: 404. SSO Server failed during initialization`** | Starten Sie vCenter Single Sign On neu. Wenn das Problem durch einen Neustart nicht behoben wird, finden Sie weitere Informationen im *Handbuch für vSphere-Fehlerbehebung*, im Abschnitt zur Wiederherstellung. |
| **Die in der Benutzeroberfläche angezeigte Fehlermeldung beginnt mit `Could not connect to vCenter Single Sign-On`** | Außerdem wird der Rückgabecode `SslHandshakeFailed` angezeigt. Diese Fehler gibt an, dass die bereitgestellte IP-Adresse oder der bereitgestellte FQDN, die bzw. der in den vCenter Single Sign On-Host aufgelöst wird, nicht mit der bei der Installation von vCenter Single Sign-On verwendeten Adresse übereinstimmt.<br>Suchen Sie in `%TEMP%\VM_ssoreg.log` die Zeile, die die folgende Meldung enthält.<br>`host name in certificate did not match: <install-configured FQDN or IP> != <A> or <B> or <C>`. Dabei ist A der während der Installation von vCenter Single Sign-On eingegebene FQDN, und B und C sind systemgenerierte zulässige Alternativen.<br>Korrigieren Sie die Konfiguration so, dass der auf der rechten Seite des Ungleichheitszeichens (`!=`) in der Protokolldatei angegebene FQDN verwendet wird. In den meisten Fällen können Sie den während der Installation von vCenter Single Sign On angegebenen FQDN verwenden.<br>Wenn keine der Alternativen in Ihrer Netzwerkkonfiguration verwendet werden kann, stellen Sie Ihre SSL-Konfiguration von vCenter Single Sign On wieder her. |

# Anmelden unter Verwendung der Active Directory-Domänenauthentifizierung nicht möglich

Sie melden sich bei einer vCenter Server-Komponente über den vSphere Client oder den vSphere Web Client an. Sie verwenden Ihren Benutzernamen und Ihr Kennwort von Active Directory. Authentifizierung schlägt fehl.

### Problem

Sie fügen eine Active Directory-Identitätsquelle zu vCenter Single Sign On hinzu, aber die Benutzer können sich nicht bei vCenter Server anmelden.

### Ursache

Benutzer verwenden ihren Benutzernamen und ihr Kennwort, um sich bei der Standarddomäne anzumelden. Für alle anderen Domänen müssen Benutzer den Domänennamen angeben (user@domain oder DOMÄNE\Benutzer).

Wenn Sie die vCenter Server Appliance verwenden, liegen möglicherweise andere Probleme vor.

### Lösung

Sie können die standardmäßige Identitätsquelle für alle vCenter Single Sign On-Bereitstellungen ändern. Benutzer können sich nach dieser Änderung nur mit dem Benutzernamen und Kennwort bei der Standard-Identitätsquelle anmelden.

Informationen zur Konfiguration der Identitätsquelle für integrierte Windows-Authentifizierung mit einer untergeordneten Domäne in der Active Directory-Gesamtstruktur finden Sie im VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/2070433. Standardmäßig verwendet die integrierte Windows-Authentifizierung die Rootdomäne Ihrer Active Directory-Gesamtstruktur.

Wenn Sie die vCenter Server Appliance verwenden und eine Änderung der standardmäßigen Identitätsquelle das Problem nicht behebt, führen Sie die folgenden zusätzlichen Schritte zur Fehlerbehebung durch:

1 Synchronisieren Sie die Uhren zwischen der vCenter Server Appliance und den Active Directory-Domänencontrollern.

2 Stellen Sie sicher, dass jeder Domänencontroller über einen Pointer Record (PTR) im DNS-Dienst der Active Directory-Domäne verfügt.

   Stellen Sie sicher, dass die PTR-Informationen mit dem DNS-Namen des Controllers übereinstimmen. Wenn Sie die vCenter Server Appliance verwenden, führen Sie die folgenden Befehle aus, um die Aufgabe durchzuführen:

   a Führen Sie den folgenden Befehl aus, um die Domänencontroller aufzulisten:

   ```
   # dig SRV _ldap._tcp.my-ad.com
   ```

   Die relevanten Adressen befinden sich, wie im folgenden Beispiel, im Antwort-Bereich:

   ```
   ;; ANSWER SECTION:
   _ldap._tcp.my-ad.com. (...) my-controller.my-ad.com
   ...
   ```

   b Stellen Sie die Forward- und Reverse-Auflösung für jeden Domänencontroller fest, indem Sie den folgenden Befehl ausführen:

   ```
   # dig my-controller.my-ad.com
   ```

Die relevanten Adressen befinden sich, wie im folgenden Beispiel, im Antwort-Bereich:

```
;; ANSWER SECTION:
my-controller.my-ad.com (...) IN A IP-Adresse des Controllers
...
```

```
# dig -x <controller IP address>
```

Die relevanten Adressen befinden sich, wie im folgenden Beispiel, im Antwort-Bereich:

```
;; ANSWER SECTION:
IP-in-reverse.in-addr.arpa. (...) IN PTR my-controller.my-ad.com
...
```

3 Wenn das Problem dadurch nicht gelöst wird, entfernen Sie die vCenter Server Appliance aus der Active Directory-Domäne und treten anschließend der Domäne wieder bei. Informationen finden Sie in der Dokumentation *vCenter Server Appliance-Konfiguration*.

4 Schließen Sie alle mit der vCenter Server Appliance verbundenen Browsersitzungen und starten Sie alle Dienste neu.

```
/bin/service-control --restart --all
```

# vCenter Server-Anmeldung schlägt aufgrund des gesperrten Benutzerkontos fehl

Wenn Sie sich von der vSphere Client- oder der vSphere Web Client-Anmeldeseite aus bei vCenter Server anmelden, zeigt eine Fehlermeldung an, dass das Benutzerkonto gesperrt ist.

### Problem

Nach mehreren fehlgeschlagenen Versuchen können Sie sich nicht mehr mithilfe von vCenter Single Sign On bei vSphere Client oder vSphere Web Client anmelden. Sie erhalten die Meldung, dass Ihr Konto gesperrt ist.

### Ursache

Sie haben die maximale Anzahl an fehlgeschlagenen Anmeldeversuchen überschritten.

### Lösung

- Wenn Sie sich als Benutzer der Systemdomäne (standardmäßig „vsphere.local“) anmelden, bitten Sie Ihren vCenter Single Sign On-Administrator, Ihr Konto zu entsperren. Sie können warten, bis Ihr Konto entsperrt wird, wenn in den Kennwortrichtlinien eine Frist für den Ablauf der Sperre eingestellt ist. vCenter Single Sign On-Administratoren können mit CLI-Befehlen Ihr Konto entsperren.
- Wenn Sie sich als Benutzer von Active Directory oder der LDAP-Domäne anmelden, bitten Sie Ihren Active Directory- bzw. LDAP-Administrator, Ihr Konto zu entsperren.

# Replizierung des VMware-Verzeichnisdiensts kann lange dauern

Wenn in Ihrer Umgebung mehrere Platform Services Controller-Instanzen vorhanden sind und eine der Platform Services Controller-Instanzen nicht mehr verfügbar ist, kann Ihre Umgebung weiterhin verwendet werden. Sobald der Platform Services Controller wieder verfügbar ist, werden Benutzerdaten und sonstige Informationen in der Regel innerhalb von 60 Sekunden repliziert. Unter bestimmten Umständen kann die Replizierung jedoch lange dauern.

### Problem

In bestimmten Situationen wird die Replizierung für die VMware-Verzeichnisdienst-Instanzen nicht sofort angezeigt. Beispielsweise, wenn in Ihrer Umgebung mehrere Platform Services Controller-Instanzen an unterschiedlichen Orten vorhanden sind und Sie umfangreiche Änderungen vornehmen, während ein Platform Services Controller nicht verfügbar ist. Beispielsweise wird ein neuer Benutzer, der zu einer verfügbaren Platform Services Controller-Instanz hinzugefügt wurde, erst nach Abschluss der Replizierung in der anderen Instanz angezeigt.

### Ursache

Im regulären Betrieb werden Änderungen an einer Instanz des VMware-Verzeichnisdiensts (vmdir) in einer Platform Services Controller-Instanz (Knoten) für den direkten Replizierungspartner innerhalb von etwa 60 Sekunden angezeigt. In Abhängigkeit von der Replizierungstopologie müssen Änderungen an einem Knoten möglicherweise über Zwischenknoten weitergegeben werden, bevor sie für jede vmdir-Instanz in jedem Knoten angezeigt werden. Zu den replizierten Informationen zählen Benutzerinformationen, Zertifikatinformationen, Lizenzinformationen für virtuelle Maschinen, die mit VMware vMotion erstellt, geklont oder migriert werden, usw.

Wenn die Replizierungsverbindung unterbrochen wird, beispielsweise aufgrund eines Netzwerkausfalls oder weil ein Knoten nicht mehr verfügbar ist, werden Änderungen im Verbund nicht vereinheitlicht. Nach der Wiederherstellung des nicht verfügbaren Knotens versucht jeder Knoten, alle Änderungen zu übernehmen. Letztlich weisen alle vmdir-Instanzen einen einheitlichen Status auf. Es kann jedoch eine Weile dauern, um diesen Status zu erreichen, wenn viele Änderungen vorgenommen wurden, während ein Knoten nicht verfügbar war.

### Lösung

Ihre Umgebung kann während der Replizierung wie gewohnt verwendet werden. Nehmen Sie nur dann eine Fehlerbehebung vor, wenn der Vorgang länger als eine Stunde dauert.

# Exportieren eines Platform Services Controller-Support-Pakets

Sie können ein Support-Paket exportieren, das die Protokolldateien für Platform Services Controller-Dienste enthält. Nach dem Export können Sie die Protokolle lokal durchsuchen oder das Paket an den VMware-Support senden.

### Voraussetzungen

Stellen Sie sicher, dass die virtuelle Platform Services Controller-Appliance erfolgreich bereitgestellt wurde und ausgeführt wird.

### Verfahren

1. Stellen Sie über einen Webbrowser eine Verbindung zur Platform Services Controller-Verwaltungsschnittstelle unter https://*platform_services_controller_ip*:5480 her.
2. Melden Sie sich als Root-Benutzer für die virtuelle Appliance an.
3. Wählen Sie im Menü **Aktionen** die Option **Support-Paket erstellen** aus.
4. Wenn Ihre Browsereinstellungen einen sofortigen Download nicht verhindern, wird das Support-Paket auf Ihrer lokalen Maschine gespeichert.

# Platform Services Controller-Dienstprotokolle – Referenz

Die Platform Services Controller-Dienste verwenden Syslog zur Protokollierung. Sie können die Protokolldateien prüfen, um die Ursache von Fehlern zu ermitteln.

Die folgende Tabelle zeigt den Speicherort der Protokolle für die vCenter Server Appliance. Für Windows-Bereitstellungen befinden sich die meisten Protokolle im Verzeichnis `C:\ProgramData\VMware\vCenterServer\logs`.

**Tabelle 5-1. Dienstprotokolle**

| Dienst | Beschreibung |
|---|---|
| VMware Directory Service | Die vmdir-Protokolle werden standardmäßig im Verzeichnis `/var/log/messages` oder `/var/log/vmware/vmdird/` gespeichert.<br>Bei Problemen während der Bereitstellung enthält das Verzeichnis `/var/log/vmware/vmdir/vmafdvmdirclient.log` möglicherweise ebenfalls hilfreiche Fehlerbehebungsdaten. |
| VMware Single Sign-On | vCenter Single Sign-On-Protokolle werden im Verzeichnis `/var/log/vmware/sso/` gespeichert. |
| VMware Certificate Authority (VMCA) | Das VMCA-Dienstprotokoll befindet sich im Verzeichnis `/var/log/vmware/vmcad/vmcad-syslog.log`. |
| VMware Endpoint Certificate Store (VECS) | Das VECS-Dienstprotokoll befindet sich im Verzeichnis `/var/log/vmware/vmafdd/vmafdd-syslog.log`. |
| VMware Lookup Service | Das Lookup Service-Protokoll befindet sich im Verzeichnis `/var/log/vmware/sso/lookupServer.log`. |