vSphere-Authentifizierung

Update 3
Geändert am 30. November 2022
VMware vSphere 7.0
VMware ESXi 7.0
vCenter Server 7.0

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 *vSphere-Authentifizierung*

Die *vSphere-Authentifizierung*-Dokumentation enthält Informationen, die Ihnen bei der Durchführung allgemeiner Aufgaben wie der Zertifikatsverwaltung und der Konfiguration von vCenter Single Sign On helfen.

Wir bei VMware legen Wert auf die Verwendung neutraler Sprache. Um dieses Prinzip bei unseren Kunden und Partnern sowie innerhalb der internen Community zu fördern, erstellen wir Inhalte mit neutraler Sprache.

vSphere-Authentifizierung erläutert, wie Sie Zertifikate für vCenter Server und zugehörige Dienste verwalten und die Authentifizierung mit vCenter Single Sign On einrichten können.

Tabelle 1-1. *vSphere-Authentifizierung* – Schwerpunkte

Themen	Inhaltliche Schwerpunkte
Erste Schritte mit der Authentifizierung	■ Verwalten von Authentifizierungsdiensten ■ Verwalten von vCenter Server über die vCenter Server-Verwaltungsschnittstelle
vSphere-Sicherheitszertifikate	■ Zertifikatmodell und Optionen für das Ersetzen von Zertifikaten. ■ Ersetzen von Zertifikaten über die Benutzeroberfläche (einfache Fälle). ■ Ersetzen von Zertifikaten mit dem Dienstprogramm Certificate Manager. ■ Ersetzen von Zertifikaten mithilfe der CLI (komplexe Situationen). ■ Referenz zur Zertifikatsverwaltungs-CLI.
vSphere-Authentifizierung mit vCenter Single Sign-On	■ Architektur des Authentifizierungsprozesses. ■ Informationen zum Hinzufügen von Identitätsquellen, sodass sich Benutzer in Ihrer Domäne authentifizieren können. ■ Zwei-Faktor-Authentifizierung. ■ Verwalten von Benutzern, Gruppen und Richtlinien. ■ vCenter Server-Identitätsanbieterverbund

Was ist mit Platform Services Controller (PSC) geschehen?

Ab vSphere 7.0 muss für die Bereitstellung einer neuen Version von vCenter Server oder das Upgrade auf vCenter Server 7.0 die vCenter Server Appliance verwendet werden. Dies ist eine vorkonfigurierte virtuelle Maschine, die für die Ausführung von vCenter Server optimiert ist. Der neue vCenter Server enthält alle Platform Services Controller-Dienste, wobei die Funktionen

und Workflows – darunter Authentifizierung, Zertifikatsverwaltung, Tags und Lizenzierung – beibehalten wurden. Es ist nicht mehr erforderlich und auch nicht mehr möglich, eine externe Platform Services Controller-Instanz bereitzustellen und zu verwenden. Alle Platform Services Controller-Dienste sind in vCenter Server konsolidiert, sodass die Bereitstellung und Verwaltung vereinfacht werden.

Da diese Dienste jetzt zu vCenter Server gehören, werden sie nicht mehr als Teil von Platform Services Controller beschrieben. In vSphere 7.0 wurde die Dokumentation *Platform Services Controller-Verwaltung* durch die Dokumentation *vSphere-Authentifizierung* ersetzt. Die neue Publikation enthält vollständige Informationen zur Authentifizierung und Zertifikatsverwaltung. Informationen dazu, wie Sie für vSphere 6.5- und 6.7-Bereitstellungen mithilfe einer vorhandenen externen Platform Services Controller-Instanz und der vCenter Server Appliance ein Upgrade auf bzw. eine Migration zu vSphere 7.0 durchführen, finden Sie in der Dokumentation *vSphere-Upgrade*.

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 *vSphere Security Configuration Guide* (früher bekannt als *Hardening Guide*) für jede vSphere-Version, die unter https://core.vmware.com/security verfügbar ist. 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 die Authentifizierung von vCenter Server konfigurieren sowie Zertifikate verwalten möchten. Die Informationen sind für erfahrene Linux-Systemadministratoren bestimmt, die mit der VM-Technologie und Datencenteroperationen vertraut sind.

Aktualisierte Informationen

Dieses *vSphere-Authentifizierung*-Dokument wird mit jeder Produktversion oder bei Bedarf aktualisiert.

Diese Tabelle enthält den Update-Verlauf für die Dokumentation *vSphere-Authentifizierung*.

Revision	Beschreibung
30. NOV. 2022	■ Geringfügiges Update für Verwalten von vCenter Server über die Verwaltungsschnittstelle. ■ Geringfügiges Update für Befehlsreferenz für dir-cli.
01. NOV. 2022	■ Geringfügiges Update für Einstellungen der Active Directory-Identitätsquelle über LDAP-Server und OpenLDAP-Server.
11. OKT. 2022	■ Geringfügiges Update für Ersetzen der Lösungsbenutzerzertifikate durch neue VMCA-signierte Zertifikate.
27. JUL 2022	■ Geringfügiges Update für Zertifikatsanforderungen für unterschiedliche Lösungspfade. ■ Im Abschnitt Verwendung von Zertifikaten in vSphere wurden Informationen zu selbstsignierten SMS-Zertifikaten hinzugefügt.
06. Mai 2022	■ Geringfügiges Update für Zertifikatsverwaltung – Übersicht. ■ Geringfügiges Update für Neugenerieren eines neuen VMCA-Rootzertifikats und Ersetzen aller Zertifikate.
21. Jan. 2022	■ Einschränkungen und Interoperabilität des vCenter Server-Identitätsanbieterverbunds und Konfigurieren des vCenter Server-Identitätsanbieterverbunds für AD FS wurden mit zusätzlichen Informationen aktualisiert.
17. Dez. 2021	■ Geringfügiges Update für Zertifikatsanforderungen für unterschiedliche Lösungspfade. ■ Geringfügiges Update für Festlegen von VMCA als Zwischenzertifizierungsstelle (Certificate Manager).
05. OKT. 2021	Erstversion.

Erste Schritte mit der Zertifikatsverwaltung und -Authentifizierung

1

vCenter Server bietet gemeinsame Infrastrukturdienste für die vSphere-Umgebung, einschließlich der Zertifikatsverwaltung und -Authentifizierung mit vCenter Single Sign On.

Dieses Kapitel enthält die folgenden Themen:

Übersicht über die Verwaltung und Authentifizierung von vSphere-Zertifikaten

vSphere stellt Dienste bereit, mit denen Sie Zertifikatsverwaltungsaufgaben für vCenter Server- und ESXi-Komponenten durchführen und Authentifizierung über vCenter Single Sign On konfigurieren können.

vSphere-Zertifikatsverwaltung – Übersicht

vSphere bietet standardmäßig die Möglichkeit, vCenter Server-Komponenten und ESXi-Hosts mit VMCA-Zertifikaten (VMware Certificate Authority) bereitzustellen. Sie können auch benutzerdefinierte Zertifikate verwenden, die im VMware Endpoint Certificate Store (VECS) gespeichert sind.

Übersicht über vCenter Single Sign-On

vCenter Single Sign On ermöglicht vSphere-Komponenten, über einen sicheren Token-Mechanismus miteinander zu kommunizieren. vCenter Single Sign On verwendet bestimmte Begriffe und Definitionen, mit denen Sie sich vertraut machen müssen.

Tabelle 1-1. vCenter Single Sign On-Glossar

Begriff	Definition
Prinzipal	Ein Element, das authentifiziert werden kann, z. B. ein Benutzer.
Identitätsanbieter	Ein Dienst, der Identitätsquellen verwaltet und Prinzipale authentifiziert. Beispiele: Microsoft Active Directory Federation Services (AD FS) und vCenter Single Sign On.
Identitätsquelle (Verzeichnisdienst)	Speichert und verwaltet Prinzipale. Prinzipale bestehen aus einer Sammlung von Attributen über ein Benutzer- oder Dienstkonto, wie z. B. Name, Adresse, E-Mail und Gruppenmitgliedschaft. Beispiele: Microsoft Active Directory und VMware Directory Service (vmdir).
Authentifizierung	Eine Möglichkeit sicherzustellen, ob jemand oder etwas der bzw. das ist, was er bzw. es vorgibt zu sein. Benutzer werden authentifiziert, wenn sie ihre Anmeldedaten eingeben, wie z. B. Smartcards, Benutzername, korrektes Kennwort usw.
Autorisierung	Der Prozess zur Überprüfung der Objekte, auf die Prinzipale Zugriff haben.
Token	Eine signierte Datensammlung, die die Identitätsinformationen für einen bestimmten Prinzipal enthält. Ein Token enthält unter Umständen nicht nur grundlegende Informationen zum Prinzipal, wie z. B. E-Mail-Adresse und vollständiger Name, sondern je nach Token-Typ auch die Gruppen und Rollen des Prinzipals.
vmdir	VMware Directory Service Das interne (lokale) LDAP-Repository in vCenter Server, das Benutzeridentitäten, Gruppen und Konfigurationsdaten enthält.
OpenID Connect (OIDC)	Auf OAuth2 basierendes Authentifizierungsprotokoll. vCenter Server verwendet OIDC-Funktionen bei der Interaktion mit Active Directory Federation Services (AD FS).

vCenter Single Sign On-Authentifizierungstypen

vCenter Single Sign On verwendet verschiedene Authentifizierungstypen, je nachdem, ob der integrierte vCenter Server-Identitätsanbieter oder ein externer Identitätsanbieter beteiligt ist.

Tabelle 1-2. vCenter Single Sign On-Authentifizierungstypen

Authentifizierungstyp	Was fungiert als Identitätsanbieter?	Verarbeitet vCenter Server das Kennwort?	Beschreibung
Token-basierte Authentifizierung	Externer Identitätsanbieter. Beispiel: AD FS.	Nein	vCenter Server kontaktiert den externen Identitätsanbieter über ein bestimmtes Protokoll und ruft ein Token ab, das eine bestimmte Benutzeridentität darstellt.
Einfache Authentifizierung	vCenter Server	Ja	Der Benutzername und das Kennwort werden direkt an vCenter Server übergeben, der die Anmeldedaten mithilfe der zugehörigen Identitätsquellen überprüft.

Verwalten von Zertifikaten

Sie verwalten Zertifikate über den vSphere Client oder mithilfe einer API, Skripts oder CLIs.

Sie können Zertifikate mit unterschiedlichen Schnittstellen verwalten.

Tabelle 1-3. Schnittstellen für die Verwaltung von Zertifikaten

Schnittstelle	Beschreibung
vSphere Client	Web-Benutzeroberfläche (HTML5-basierter Client). Weitere Informationen hierzu finden Sie unter Verwalten von Zertifikaten mit dem vSphere Client.
vSphere Automation-API	Weitere Informationen finden Sie im *Programmierhandbuch zu den VMware vSphere Automation SDKs*.
Dienstprogramm für die Zertifikatsverwaltung	Befehlszeilenprogramm, das die CSR-Generierung (Certificate Signing Request) und die Zertifikatsersetzung unterstützt. Weitere Informationen hierzu finden Sie unter Verwalten von Zertifikaten mit dem Dienstprogramm vSphere Certificate Manager.
Befehlszeilenschnittstellen für die Verwaltung von Zertifikat- und Verzeichnisdiensten	Befehlssatz für die Verwaltung von Zertifikaten, der VMware Endpoint Certificate Store (VECS) und VMware Directory Service (vmdir). Weitere Informationen hierzu finden Sie unter Kapitel 3 Verwalten von Diensten und Zertifikaten mit CLI-Befehlen.

Verwalten von Zertifikaten über den vSphere Client

Sie können die Zertifikate von vSphere Client aus verwalten.

Verfahren

1 Melden Sie sich bei einem vCenter Server als Benutzer mit Administratorrechten in der lokalen vCenter Single Sign-On-Domäne an.

   Die Standarddomäne lautet „vsphere.local“.

2 Wählen Sie **Verwaltung** aus.

3 Klicken Sie unter **Zertifikate** auf **Zertifikatsverwaltung**.

   Es werden Zertifikatsbereiche für die verschiedenen Zertifikatstypen angezeigt.

4 Führen Sie Zertifikatsaufgaben aus, z. B. das Anzeigen von Zertifikatsdetails, das Verlängern des Maschinen-SSL-Zertifikats und das Hinzufügen eines vertrauenswürdigen Root-Zertifikats.

Verwalten von Zertifikaten mithilfe von Skripts

vCenter Server enthält Skripts zum Generieren von CSRs (Certificate Signing Requests) und zum Verwalten von Zertifikaten und Diensten.

Zum Generieren von CSRs und zum Ersetzen von Zertifikaten können Sie z. B. das Dienstprogramm `certool` verwenden. Weitere Informationen hierzu finden Sie unter Verwalten von Zertifikaten mit dem Dienstprogramm vSphere Certificate Manager.

Verwenden Sie die CLIs für Verwaltungsaufgaben, die der vSphere Client 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 der VMware Certificate Authority (VMCA).	Befehlsreferenz für die certool-Initialisierung
`vecs-cli`	Verwalten Sie die Inhalte von VMware-Zertifikatspeicherinstanzen. Bestandteil des VMware-Authentifizierungsframework-Daemon (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`	Aktualisiert Security Token Service (STS)-Zertifikate.	Ersetzen eines vCenter Server-STS-Zertifikats über die Befehlszeile
`service-control`	Befehl zum Starten, Anhalten und Auflisten von Diensten.	Führen Sie diesen Befehl aus, um Dienste anzuhalten, bevor Sie andere CLI-Befehle ausführen.

Voraussetzungen

Aktivieren Sie die SSH-Anmeldung bei vCenter Server. Weitere Informationen hierzu finden Sie unter Verwalten von vCenter Server über die Verwaltungsschnittstelle.

Verfahren

1 Melden Sie sich bei der vCenter Server-Shell an.

   In der Regel 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. Manchmal werden Sie zweimal zur Eingabe des Kennworts aufgefordert, um vertrauliche Informationen zu schützen.

```
/usr/lib/vmware-vmafd/bin/vecs-cli
/usr/lib/vmware-vmafd/bin/dir-cli
/usr/lib/vmware-vmca/bin/certool
/opt/vmware/bin
/opt/vmware/bin/sso-config.sh
```

   Für den Befehl `service-control` müssen Sie den Pfad nicht eingeben.

Verwalten von Authentifizierungsdiensten

Sie verwalten Authentifizierungsdienste über den vSphere Client oder über die Befehlszeilenschnittstelle. Sie können den Konfigurationsvorgang für den vCenter Server-Identitätsanbieterverbund auch mithilfe einer API verwalten.

Sie können Authentifizierung mithilfe unterschiedlicher Schnittstellen verwalten.

Tabelle 1-5. Schnittstellen für die Verwaltung von Authentifizierungsdiensten

Schnittstelle	Beschreibung
vSphere Client	Webschnittstelle (HTML5-basierter Client).
API	Verwalten Sie den Konfigurationsprozess des vCenter Server-Identitätsanbieterverbunds.
`sso-config`	Befehlszeilendienstprogramm zum Konfigurieren des in vCenter Server integrierten Identitätsanbieters.

Verwalten von Authentifizierungsdiensten über vSphere Client

Sie können vCenter Server-Authentifizierungsdienste über den vSphere Client verwalten.

Verfahren

1 Melden Sie sich bei einem vCenter Server als Benutzer mit Administratorrechten in der lokalen vCenter Single Sign-On-Domäne an.

   Die Standarddomäne lautet „vsphere.local“.

2 Wählen Sie **Verwaltung** aus.

3 Klicken Sie unter **Single Sign-On** auf **Konfiguration**, um Identitätsanbieter zu verwalten und Kennwort- und Sperrrichtlinien zu konfigurieren.

Verwalten von Authentifizierungsdiensten mithilfe von Skripts

vCenter Server enthält ein Dienstprogramm (`sso-config`) für die Verwaltung von Authentifizierungsdiensten.

Verwenden Sie das `sso-config`-Dienstprogramm für Verwaltungsaufgaben, die vom vSphere Client nicht unterstützt werden, oder zum Erstellen von benutzerdefinierten Skripts für Ihre Umgebung.

Tabelle 1-6. Befehlszeilenschnittstellen für die Verwaltung von Authentifizierung und zugehörigen Diensten

Befehlszeilenschnittstelle	Beschreibung	Links
`sso-config`	Befehlszeilendienstprogramm zum Konfigurieren des in vCenter Server integrierten Identitätsanbieters.	Beispiele für die Verwendung erhalten Sie, indem Sie die `sso-config`-Hilfe durch Ausführung von `sso-config.sh -help` aufrufen oder den VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/67304 lesen.
`service-control`	Befehl zum Starten, Anhalten und Auflisten von Diensten.	Führen Sie diesen Befehl aus, um Dienste anzuhalten, bevor Sie andere CLI-Befehle ausführen.

Voraussetzungen

Aktivieren Sie die SSH-Anmeldung bei vCenter Server. Weitere Informationen hierzu finden Sie unter Verwalten von vCenter Server über die Verwaltungsschnittstelle.

Verfahren

1 Melden Sie sich bei der vCenter Server-Shell an.

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

2 Greifen Sie auf das `sso-config`-Dienstprogramm in folgendem Standardverzeichnis zu.

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

   ```
   /opt/vmware/bin/sso-config.sh
   ```

   Für den Befehl `service-control` müssen Sie den Pfad nicht angeben.

Verwalten von vCenter Server

Sie können vCenter Server über die vCenter Server-Verwaltungsschnittstelle oder über die vCenter Server-Shell verwalten.

Weitere Informationen zur Verwaltung von vCenter Server finden Sie unter *vCenter Server-Konfiguration*.

Tabelle 1-7. Schnittstellen für die Verwaltung von vCenter Server

Schnittstelle	Beschreibung
vCenter Server-Verwaltungsschnittstelle	Über diese Schnittstelle können Sie die Systemeinstellungen neu konfigurieren. Weitere Informationen hierzu finden Sie unter Verwalten von vCenter Server über die Verwaltungsschnittstelle.
vCenter Server-Shell	Verwenden Sie diese Befehlszeilenschnittstelle, um Dienstverwaltungsvorgänge für VMCA, VECS und VMDIR durchzuführen. Weitere Informationen hierzu finden Sie unter Verwalten von Zertifikaten mit dem Dienstprogramm vSphere Certificate Manager und Kapitel 3 Verwalten von Diensten und Zertifikaten mit CLI-Befehlen.

Verwalten von vCenter Server über die Verwaltungsschnittstelle

Über die vCenter Server-Verwaltungsschnittstelle können Sie die 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.

Hinweis Im Bereich **Netzwerk** ist die virtuelle Netzwerkkarte 0 für den Verwaltungsdatenverkehr reserviert. Sie können den Datenverkehr von Netzwerkkarte 0 nicht einer anderen Netzwerkkarte neu zuweisen. Wenn Sie VCHA verwenden, verwendet dieser Datenverkehr die Netzwerkkarte 1. Sie können Netzwerkkarten zu vCenter Server Appliance hinzufügen. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/article/2147155.

Verfahren

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

   Das standardmäßige Root-Kennwort ist das Root-Kennwort, das Sie bei der Bereitstellung von vCenter Server festlegen.

Ergebnisse

Die Seite „Übersicht“ der vCenter Server-Verwaltungsschnittstelle wird angezeigt.

Verwalten von vCenter Server über die vCenter Server-Shell

Sie können Dienstverwaltungsprogramme und CLIs in der vCenter Server-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://*vcenter_server_ip*:5480 bei der vCenter Server-Verwaltungsschnittstelle 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 vCenter Server können Sie dieselben Schritte ausführen.
2. Rufen Sie die Shell auf.
   - Wenn Sie Direktzugriff auf die vCenter Server-Konsole haben, wählen Sie **Anmelden** aus und drücken Sie die Eingabetaste.
   - Wenn Sie eine Remoteverbindung herstellen möchten, verwenden Sie SSH oder eine andere Remote-Konsolenverbindung, um eine Sitzung mit vCenter Server zu starten.
3. Melden Sie sich als Root-Benutzer mit dem Kennwort an, das Sie bei der erstmaligen Bereitstellung von vCenter Server verwendet haben.

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

Hinzufügen von vCenter Server zu einer Active Directory-Domäne

Wenn Sie vCenter Server eine Active Directory-Identitätsquelle hinzufügen möchten, müssen Sie vCenter Server mit einer Active Directory-Domäne verbinden.

Wenn Sie den vCenter Server-Identitätsanbieterverbund oder Active Directory über LDAPS nicht verwenden können, unterstützt vCenter Server die integrierte Windows-Authentifizierung (IWA). Um IWA verwenden zu können, müssen Sie den vCenter Server zu Ihrer Active Directory-Domäne hinzufügen.

Verfahren

1. Melden Sie sich mithilfe von vSphere Client als Benutzer mit Administratorrechten bei vCenter Server 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 der Registerkarte **Identitätsanbieter** auf **Active Directory-Domäne**.
5. Klicken Sie auf **AD beitreten**, geben Sie die Domäne, die optionale Organisationseinheit sowie den Benutzernamen und das Kennwort ein und klicken Sie auf **Beitreten**.
6. Starten Sie vCenter Server neu.

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-Sicherheitszertifikate

2

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. einem 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 vCenter Server-Host 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 2-1. 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 Lebenszyklus des Zertifikats für vCenter Server- und ESXi-Hosts verwalten.
VMCA-Standardzertifikate mit externen SSL-Zertifikaten (Hybrid-Modus)	Sie ersetzen die SSL-Zertifikate des vCenter Server 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 2-2. Unterschiedliche Methoden für die Zertifikatsersetzung

Option	Informationen hierzu finden Sie unter
Verwenden Sie den vSphere Client.	Verwalten von Zertifikaten mit dem vSphere Client
Verwenden Sie die vSphere Automation-API, um den Lebenszyklus von Zertifikaten zu verwalten.	*Programmierhandbuch zu den VMware vSphere Automation SDKs*
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 3 Verwalten von Diensten und Zertifikaten mit CLI-Befehlen

Dieses Kapitel enthält die folgenden Themen:

- Zertifikatsanforderungen für unterschiedliche Lösungspfade
- Zertifikatsverwaltung – Übersicht
- Verwalten von Zertifikaten mit dem vSphere 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. Außerdem unterscheiden sich die Anforderungen für Maschinenzertifikate.

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

Hinweis vSphere stellt nur RSA-Zertifikate für die Serverauthentifizierung bereit und unterstützt nicht das Generieren von ECDSA-Zertifikaten. vSphere überprüft ECDSA-Zertifikate, die von anderen Servern bereitgestellt werden. Wenn beispielsweise vSphere eine Verbindung mit einem Syslog-Server herstellt und der Syslog-Server über ein ECDSA-Zertifikat verfügt, unterstützt vSphere die Überprüfung dieses Zertifikats.

Anforderungen für alle importierten Zertifikate

- Schlüsselgröße: 2048 Bit (Minimum) bis 16384 Bit (Maximum) (PEM-codiert)
- 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.
- Wenn eine Ausnahme für das Benutzerzertifikat der vpxd-extension-Lösung geschaffen wird, kann die erweiterte Schlüsselverwendung entweder leer sein oder eine Serverauthentifizierung enthalten.

Die folgenden Zertifikate werden von vSphere nicht unterstützt.

- Zertifikate mit Platzhalterzeichen.
- Die Algorithmen md2WithRSAEncryption, md5WithRSAEncryption, RSASSA-PSS, dsaWithSHA1, ecdsa_with_SHA1 und sha1WithRSAEncryption werden 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.
- 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 vCenter Server-Knotens, auf dem Sie Certificate Manager 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).
	■ Wenn Sie die CSR manuell erstellen möchten, muss das Zertifikat, das Sie zum Signieren senden, die folgenden Anforderungen erfüllen.
	■ Schlüsselgröße: 2048 Bit (Minimum) bis 16384 Bit (Maximum) (PEM-codiert)
	■ PEM-Format. VMware unterstützt PKCS8 und PKCS1 (RSA-Schlüssel). Wenn Schlüssel zu VECS hinzugefügt werden, werden sie in PKCS8 konvertiert.
	■ x509 Version 3
	■ Die Zertifizierungsstellenerweiterung muss für Stammzertifikate auf „true“ festgelegt werden und „cert sign“ muss in der Liste der Anforderungen vorhanden sein. Beispiel:
	`basicConstraints = critical,CA:true`
	`keyUsage = critical,digitalSignature,keyCertSign`
	■ 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.x“ 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. 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. 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*. Für den Lösungsbenutzer „vpxd-extension“ können Sie „Erweiterte Schlüsselnutzung“ leer lassen oder „TLS-WWW-Clientauthentifizierung“ verwenden.

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. ■ 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. ■ 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. ■ 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. ■ 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*. **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. Wenn Sie später Lösungsbenutzerzertifikate durch benutzerdefinierte Zertifikate ersetzen, geben Sie die vollständige Signaturzertifikatkette der Drittanbieterzertifizierungsstelle an. Für den Lösungsbenutzer „vpxd-extension“ können Sie „Erweiterte Schlüsselnutzung“ leer lassen oder „TLS-WWW-Clientauthentifizierung“ verwenden.

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.
- Bei einem Upgrade einer einfachen vCenter Server-Installation auf einer eingebetteten Bereitstellung behält vCenter Server benutzerdefinierte Zertifikate bei. Die Funktionsweise der Umgebung ist nach dem Upgrade unverändert. Die vorhandenen vCenter Server- und vCenter Single Sign On-Zertifikate werden 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.

Sie können das Befehlszeilendienstprogramm, vSphere Certificate Manager, für die meisten Aufgaben der Zertifikatsverwaltung verwenden.

vSphere-Zertifikatschnittstellen

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

Tabelle 2-3. Schnittstellen für die Verwaltung von vCenter Server-Zertifikaten

Schnittstelle	Verwenden
vSphere Client	Führen Sie gängige Zertifikataufgaben mit einer grafischen Benutzeroberfläche durch.
vSphere Automation-API	Weitere Informationen finden Sie im *Programmierhandbuch zu den VMware vSphere Automation SDKs*.
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.
`sso-config`-Dienstprogramm	Führen Sie STS-Zertifikatsverwaltung über die Befehlszeile der vCenter Server-Installation durch.
PowerCLI 12.4 (vSphere 7.0 oder höher erforderlich)	Führen Sie die Verwaltung vertrauenswürdiger Zertifikatspeicher durch, verwalten Sie vCenter Server-Maschinen-SSL-Zertifikate und verwalten Sie ESXi-Maschinen-SSL-Zertifikate.

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 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 vCenter Server mit dem Dienstprogramm vSphere Certificate Manager oder manuell über die Befehlszeilenschnittstellen durchführen, die Teil Ihrer Installation sind.

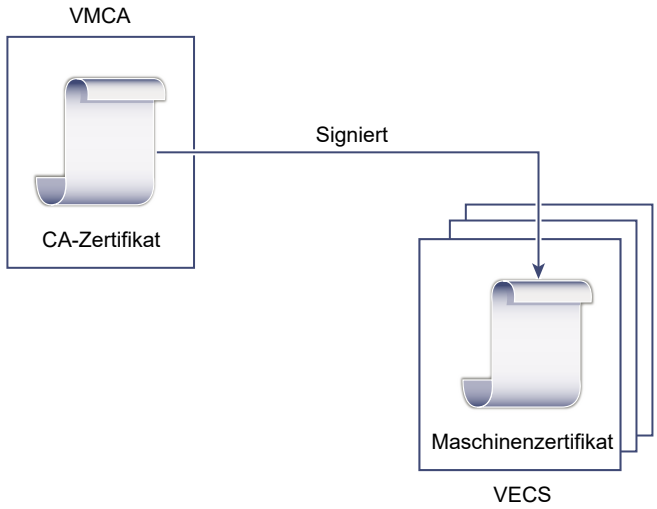
VMCA ist in jeder vCenter Server-Bereitstellung enthalten. VMCA stellt jeden Knoten, jeden vCenter Server-Lösungsbenutzer und jeden ESXi-Host mit einem Zertifikat bereit, das von VMCA als Zertifizierungsstelle signiert wurde.

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 2-1. 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

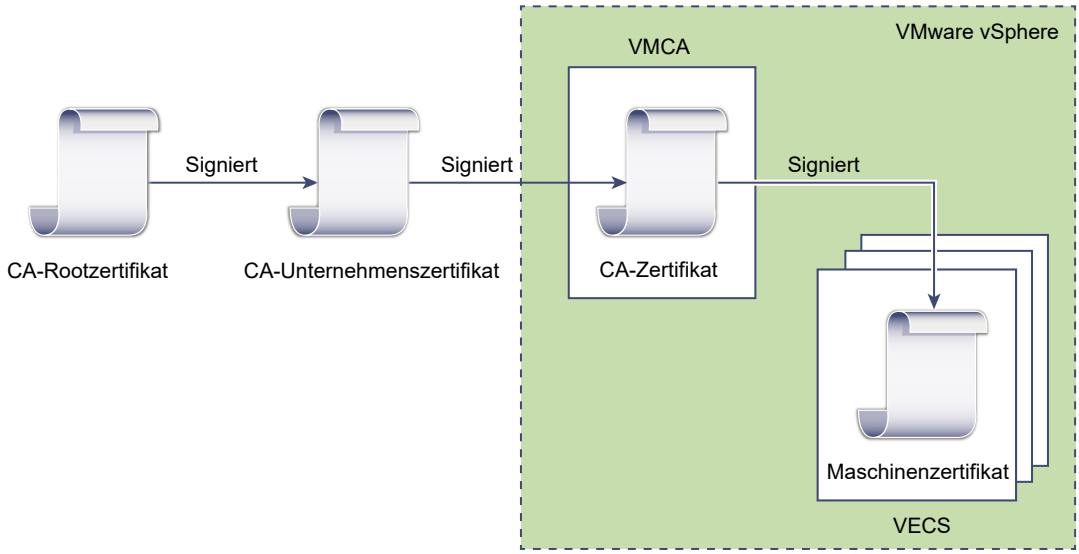
Informationen zur manuellen Zertifikatsersetzung finden Sie unter Ersetzen vorhandener VMCA-signierter Zertifikate durch neue VMCA-signierte Zertifikate.

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 vCenter Server durchführen, ersetzen Sie vor dem Hinzufügen von ESXi-Hosts das VMCA-Rootzertifikat. In diesem Fall signiert VMCA die ganze Kette, und Sie brauchen keine neuen Zertifikate zu generieren.

Abbildung 2-2. 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:

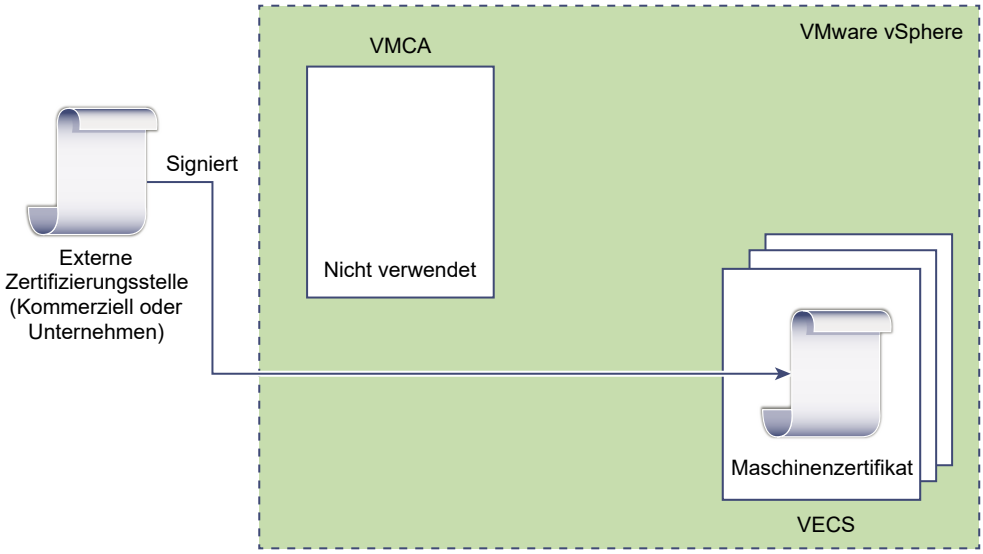
- Ersetzen des VMCA-Rootzertifikats durch ein benutzerdefiniertes Signaturzertifikat und Ersetzen aller Zertifikate
- Ersetzen des Maschinen-SSL-Zertifikats durch das VMCA-Zertifikat (Bereitstellung mit mehreren Knoten im erweiterten verknüpften Modus)
- Ersetzen des Lösungsbenutzerzertifikats durch das VMCA-Zertifikat (Bereitstellung mit mehreren Knoten im erweiterten verknüpften Modus)

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 2-3. 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 von benutzerdefinierten Zertifikaten 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 2-4. 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

VMware Certificate Authority (VMCA, die VMware-Zertifizierungsstelle) stellt in Ihrer Umgebung Zertifikate 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 2-5. Zertifikate in vSphere

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 die Befehlszeile. **Hinweis** Dieses Zertifikat sollten Sie nicht im Dateisystem ändern, da dies zu unvorhersehbarem Verhalten führen kann.

Tabelle 2-5. Zertifikate in vSphere (Fortsetzung)

Zertifikat	Bereitgestellt	Anmerkungen
SSL-Zertifikat für VMware Directory Service (VMDIR)	Bereitgestellt während der Installation.	Ab vSphere 6.5 wird das Maschinen-SSL-Zertifikat als vmdir-Zertifikat verwendet.
Selbstsignierte SMS-Zertifikate	Bereitgestellt während der Registrierung des IOFilter-Anbieters.	In vSphere 7.0 und höher werden selbstsignierte SMS-Zertifikate in `/etc/vmware/ssl/iofiltervp_castore.pem` gespeichert. In älteren Versionen als vSphere 7.0 werden selbstsignierte SMS-Zertifikate in `/etc/vmware/ssl/castore.pem` gespeichert. Darüber hinaus kann der SMS Store auch selbstsignierte Zertifikate des VVOL-VASA-Anbieters (Version 4.0 und früher) speichern, wenn retainVasaProviderCertificate=True.

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 vCenter Server-Knoten verfügt über ein eigenes Maschinen-SSL-Zertifikat. Alle Dienste, die auf einem vCenter Server-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. SSL-Verbindungen zu einzelnen vCenter-Diensten werden stets an den Reverse-Proxy weitergeleitet. Der Datenverkehr wird nicht an die Dienste selbst weitergeleitet.
- Der vCenter Server-Dienst (vpxd).
- Der VMware Directory Service (vmdir).

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 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 Speicher für Lösungsbenutzerzertifikate sind in VECS 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-Speicher (vpxd). vpxd verwendet das in diesem Speicher abgelegte Lösungsbenutzerzertifikat, um sich bei vCenter Single Sign On zu authentifizieren.
- `vpxd-extension`: vCenter-Erweiterungsspeicher. Enthält den Auto Deploy-Dienst, den Inventory Service und sonstige Dienste, die nicht Bestandteil anderer Lösungsbenutzer sind.
- `vsphere-webclient`: vSphere Client-Speicher. Enthält auch zusätzliche Dienste wie etwa den Leistungsdiagrammdienst.
- `wcp`: VMware vSphere® mit VMware Tanzu™-Speicher.

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.

Dieses Zertifikat können Sie über die Befehlszeilenschnittstelle ersetzen. Weitere Informationen hierzu finden Sie unter Ersetzen eines vCenter Server-STS-Zertifikats über die Befehlszeile.

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

Die Kernidentitätsdienste sind Bestandteil jedes vCenter Server-Systems. 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 2-6. Kernidentitätsdienste

Dienst	Beschreibung
VMware Directory Service (vmdir)	Identitätsquelle, die die SAML-Zertifikatsverwaltung für die Authentifizierung mit vCenter Single Sign On verarbeitet.
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. VMCA stellt Zertifikate nur für Clients aus, die sich bei vCenter Single Sign On in derselben Domäne authentifizieren können.
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.

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 auf jedem vCenter Server-Knoten 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 2-7. Speicher in VECS

Speicher	Beschreibung
Maschinen-SSL-Speicher (MACHINE_SSL_CERT)	■ Wird vom Reverse-Proxy-Dienst auf jedem vSphere-Knoten verwendet. ■ Wird vom VMware Directory Service (vmdir) für jeden vCenter Server-Knoten verwendet. 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.
Lösungsbenutzerspeicher ■ `machine` ■ `vpxd` ■ `vpxd-extension` ■ `vsphere-webclient` ■ `wcp`	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. Lösungsbenutzerzertifikate werden für die Authentifizierung mit vCenter Single Sign On verwendet. vCenter Single Sign On überprüft, ob das Zertifikat gültig ist. Andere Zertifikatsattribute werden jedoch nicht überprüft. Die folgenden Speicher für Lösungsbenutzerzertifikate sind in VECS 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-Speicher (vpxd). vpxd verwendet das in diesem Speicher abgelegte Lösungsbenutzerzertifikat, um sich bei vCenter Single Sign On zu authentifizieren. ■ `vpxd-extension`: vCenter-Erweiterungsspeicher. Enthält den Auto Deploy-Dienst, den Inventory Service und sonstige Dienste, die nicht Bestandteil anderer Lösungsbenutzer sind. ■ `vsphere-webclient`: vSphere Client-Speicher. Enthält auch zusätzliche Dienste wie etwa den Leistungsdiagrammdienst. ■ `wcp`: VMware vSphere® mit VMware Tanzu™-Speicher. Jeder vCenter Server-Knoten enthält ein `machine`-Zertifikat.
Vertrauenswürdiger Stammspeicher (TRUSTED_ROOTS)	Enthält alle vertrauenswürdigen Stammzertifikate.

Tabelle 2-7. 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. **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 die CLI ändern.

Bestimmte Zertifikate werden entweder temporär während des Starts oder dauerhaft im Dateisystem gespeichert. Die Zertifikate im Dateisystem sollten Sie nicht ändern.

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-Root-Zertifikats.

vSphere 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

Wenn Sie Zertifikate in Bereitstellungen mit vielen vCenter Server-Hosts ersetzen, können Sie das vSphere Certificate Manager-Dienstprogramm verwenden oder Zertifikate manuell ersetzen. Das von Ihnen ausgewählte Verfahren wird von einigen Best Practices begleitet.

Ersetzen der Maschinen-SSL-Zertifikate in Umgebungen mit mehreren vCenter Server-Knoten

Wenn Ihre Umgebung mehrere vCenter Server-Knoten enthält, können Sie Zertifikate mit dem vSphere Client, dem vSphere Certificate Manager-Dienstprogramm oder manuell mithilfe von ESXCLI-Befehlen ersetzen.

vSphere Certificate Manager

vSphere Certificate Manager können Sie auf jeder Maschine ausführen. 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. 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 von Lösungsbenutzerzertifikaten in Umgebungen mit mehreren vCenter Server-Systemen im erweiterten verknüpften Modus

Wenn Ihre Umgebung mehrere vCenter Server-Systeme im erweiterten verknüpften Modus enthält, führen Sie die folgenden Schritte für die Zertifikatsersetzung 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. 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 jedem vCenter Server.
   - Ein Zertifikat für jeden der folgenden Lösungsbenutzer auf allen Knoten:
     - Lösungsbenutzer `vpxd`
     - Lösungsbenutzer `vpxd-extension`

- Lösungsbenutzer `vsphere-webclient`
- Lösungsbenutzer `wcp`

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 Zertifikate
- Ersetzen der Lösungsbenutzerzertifikate (Zwischenzertifizierungsstelle)
- Ersetzen der Lösungsbenutzerzertifikate durch benutzerdefinierte Zertifikate

Zertifikatsersetzung in Umgebungen mit externen Lösungen

Bestimmte Lösungen, wie z. B. VMware vCenter Site Recovery Manager oder VMware vSphere Replication, werden immer auf einer anderen Maschine als das vCenter Server-System installiert. Beim Ersetzen des standardmäßigen Maschinen-SSL-Zertifikats auf dem vCenter Server-System, tritt ein Verbindungsfehler auf, wenn die Lösung versuchsweise eine Verbindung zum vCenter Server-System herstellt.

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 Maschinen-SSL-, vertrauenswürdigen Root- und Security Token Service (STS)-Zertifikate der Maschine an.
- Fügen Sie neue vertrauenswürdige Root-Zertifikate hinzu und erneuern oder ersetzen Sie vorhandene Maschinen-SSL- und STS-Zertifikate.
- 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 vCenter Server 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 2 vSphere-Sicherheitszertifikate.

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

Zertifikate erneuern

Sie können die Maschinen-SSL-, Lösungsbenutzer- und STS-Zertifikate in Ihrer Umgebung aus dem 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. Danach 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 vCenter Server hochladen.

Hinweis Wenn Sie VMCA als Zwischenzertifizierungsstelle verwenden oder wenn Sie benutzerdefinierte Zertifikate verwenden, bringt dies möglicherweise eine erhebliche Komplexität und das Potenzial für Beeinträchtigungen Ihrer Sicherheit sowie einen unnötigen Anstieg Ihres Betriebsrisikos mit sich. 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.

Untersuchen der Zertifikatspeicher über den vSphere Client

Eine VMware Endpoint Certificate Store-Instanz (VECS-Instanz) ist in jedem vCenter Server-Knoten enthalten. Sie können die verschiedenen Speicher innerhalb des VMware Endpoint Certificate Store vom vSphere Client aus durchsuchen, einschließlich Maschinen-SSL- und vertrauenswürdigen Stammzertifikaten.

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 vSphere Client bei vCenter Server an.
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. Wenn Sie vom System aufgefordert werden, geben Sie die Anmeldedaten Ihres 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

vCenter Server Überwacht alle Zertifikate im VMware Endpoint Certificate Store (VECS) und gibt 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**.

Verlängern von VMCA-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 vSphere Client bei vCenter Server an.

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 Wenn Sie vom System aufgefordert werden, geben Sie die Anmeldedaten Ihres vCenter Server ein.

5 Verlängern Sie das VMCA-signierte 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**.

      vCenter Server-Dienste werden automatisch neu gestartet. Sie müssen sich erneut anmelden, da durch einen Neustart der Dienste die UI-Sitzung beendet wird.

Einrichten des Systems für die Verwendung von benutzerdefinierten Zertifikaten

Sie können Ihre Umgebung für die Verwendung benutzerdefinierter Zertifikate einrichten.

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 vCenter Server-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 auf jedem vCenter Server-Knoten 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: 2048 Bit (Minimum) bis 16384 Bit (Maximum) (PEM-codiert)
- CRT-Format
- x509 Version 3
- „SubjectAltName“ muss DNS-Name=<Maschinen-FQDN> enthalten.
- Enthält die folgenden Schlüsselverwendungen: digitale Signatur, Schlüsselverschlüsselung

Verfahren

1. Melden Sie sich mit vSphere Client bei vCenter Server an.
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 für das zu ersetzende Zertifikat unter **Maschinen-SSL-Zertifikat** auf **Aktionen > Zertifikatssignierungsanforderung (Certificate Signing Request, CSR) generieren**.

b Geben Sie die Zertifikatsinformationen ein und klicken Sie auf **Weiter**.

Hinweis Wenn Sie vCenter Server zum Erzeugen einer Zertifikatssignieranforderung mit einer Schlüsselgröße von 16384 Bit verwenden, nimmt dieser Vorgang aufgrund der hohen CPU-Auslastung einige Zeit in Anspruch.

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 von benutzerdefinierten Zertifikaten.

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:

```
/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.
- Sie werden zur Eingabe des Hostnamens oder der IP-Adresse des vCenter Server 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 vCenter Server 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 vCenter Server 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.

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 vSphere Client bei vCenter Server an.

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 Wenn Sie vom System aufgefordert werden, geben Sie die Anmeldedaten Ihres 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.

Hinzufügen von benutzerdefinierten Zertifikaten

Sie können benutzerdefinierte Maschinen-SSL-Zertifikate zum Zertifikatspeicher hinzufügen.

In den meisten Fällen ist es ausreichend, das Maschinen-SSL-Zertifikat für jede Komponente zu ersetzen.

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 vCenter Server zugreifen kann.

Verfahren

1 Melden Sie sich mit vSphere Client bei vCenter Server an.

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 Wenn Sie vom System aufgefordert werden, geben Sie die Anmeldedaten Ihres vCenter Server ein.

5 Klicken Sie unter **Maschinen-SSL-Zertifikat** für das Zertifikat, das Sie ersetzen möchten, auf **Aktionen > Zertifikat importieren und ersetzen**.

6 Klicken Sie auf die entsprechende Option zum Ersetzen des Zertifikats und dann auf **Weiter**.

Option	Beschreibung
Durch VMCA ersetzen	Erstellt eine VMCA-generierte CSR, um das aktuelle Zertifikat zu ersetzen.
Durch ein von vCenter Server erzeugtes Zertifikat ersetzen	Verwenden Sie ein Zertifikat, das mit einer vCenter Server generierten CSR signiert wurde, um das aktuelle Zertifikat zu ersetzen.
Durch externes CA-Zertifikat ersetzen (privater Schlüssel erforderlich)	Verwenden Sie ein Zertifikat, das von einer externen Zertifizierungsstelle signiert wurde, um das aktuelle Zertifikat zu ersetzen.

7 Geben Sie die CSR-Informationen ein oder laden Sie die entsprechenden Zertifikate hoch.

8 Klicken Sie auf **Ersetzen**.

vCenter Server-Dienste werden automatisch neu gestartet.

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:

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

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 an Schritten zum Ersetzen von Maschinen-SSL- und Lösungsbenutzerzertifikaten.

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 Wenn mehrere vCenter Server-Instanzen in der Konfiguration des erweiterten verknüpften Modus verbunden sind, 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 an Schritten zum Ersetzen von Maschinen-SSL- und Lösungsbenutzerzertifikaten.

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 Wenn schließlich mehrere vCenter Server-Instanzen in der Konfiguration des erweiterten verknüpften Modus verbunden sind, müssen Sie den Vorgang auf jedem Knoten wiederholen.

Weitere Informationen hierzu finden Sie unter Ersetzen aller Zertifikate durch benutzerdefinierte Zertifikate (Certificate Manager).

Hinweis Die folgende Eingabeaufforderung wird angezeigt, wenn Sie das Certificate Manager-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. Wenn mehrere vCenter Server-Instanzen in der Konfiguration des erweiterten verknüpften Modus verbunden sind, müssen Sie Zertifikate auf jedem vCenter Server 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 vCenter Server 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 von vCenter Server.
- 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 beim vCenter Server an und starten Sie den vSphere Certificate Manager.

   ```
   /usr/lib/vmware-vmca/bin/certificate-manager
   ```

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. Der Ersetzungsvorgang ist abgeschlossen, nachdem Certificate Manager die Dienste neu gestartet hat.
4. Führen Sie zum Ersetzen des SSL-Zertifikats der Maschine vSphere Certificate Manager mit Option 3, `Replace Machine SSL certificate with VMCA Certificate`, aus.
5. 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.

VMware empfiehlt nicht, VMCA als untergeordnete oder Zwischenzertifizierungsstelle zu betreiben. Wenn Sie diese 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.

Um VMCA als Zwischenzertifizierungsstelle festzulegen, müssen Sie Certificate Manager mehrmals ausführen. Der Workflow umfasst den vollständigen Satz von Schritten zum Ersetzen von Maschinen-SSL-Zertifikaten.

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.

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: 2048 Bit (Minimum) bis 16384 Bit (Maximum) (PEM-codiert)
  - PEM-Format. VMware unterstützt PKCS8 und PKCS1 (RSA-Schlüssel). Wenn Schlüssel zu VECS hinzugefügt werden, werden sie in PKCS8 konvertiert.

- x509 Version 3
- Die Zertifizierungsstellenerweiterung muss für Stammzertifikate auf „true“ festgelegt werden und „cert sign“ muss in der Liste der Anforderungen vorhanden sein. Beispiel:

```
basicConstraints        = critical,CA:true
keyUsage                = critical,digitalSignature,keyCertSign
```

- 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.x“ 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.

```
/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 vCenter Server 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 vCenter Server aus, um das VMCA-Root-Zertifikat 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 auf dem vCenter Server-Host 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.

Ersetzen des Maschinen-SSL-Zertifikats durch ein VMCA-Zertifikat (Zwischenzertifizierungsstelle)

Wenn Sie VMCA als Zwischenzertifizierungsstelle verwenden, können Sie das Maschinen-SSL-Zertifikat explizit ersetzen. Zuerst ersetzen Sie das VMCA-Root-Zertifikat auf dem vCenter Server. Anschließend können Sie das Maschinen-SSL-Zertifikat ersetzen, das vom neuen Root der VMCA signiert wird. 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 vCenter Server 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 von vCenter Server.
- VMCA-Name, der der vollqualifizierte Domänenname der Maschine ist, auf der die Zertifikatskonfiguration ausgeführt wird.

Voraussetzungen

- 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 vCenter Server-Systems.

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)

Wenn Sie VMCA als Zwischenzertifizierungsstelle verwenden, können Sie das Lösungsbenutzerzertifikat explizit ersetzen. Zuerst ersetzen Sie das VMCA-Root-Zertifikat auf dem vCenter Server. Anschließend können Sie das Lösungsbenutzerzertifikat ersetzen, das vom neuen Root der VMCA signiert wird. Sie können diese Option auch verwenden, um Lösungszertifikate zu ersetzen, die beschädigt sind oder im Begriff sind abzulaufen.

Voraussetzungen

- Starten Sie alle vCenter Server-Knoten explizit neu, wenn Sie das VMCA-Root-Zertifikat in einer Bereitstellung ersetzt haben, die aus mehreren Instanzen von vCenter Server in der Konfiguration des erweiterten verknüpften Modus besteht.
- Sie müssen die folgenden Informationen kennen, um den Zertifikatsmanager mit dieser Option auszuführen.
  - Kennwort für „administrator@vsphere.local“
  - Hostname oder IP-Adresse des vCenter Server-Systems

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 an Schritten zum Ersetzen von Maschinen-SSL- und Lösungsbenutzerzertifikaten.

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 Wenn schließlich mehrere vCenter Server-Instanzen in der Konfiguration des erweiterten verknüpften Modus verbunden sind, müssen Sie den Vorgang auf jedem Knoten wiederholen.

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:

```
/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.
- Sie werden zur Eingabe des Hostnamens oder der IP-Adresse des vCenter Server 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 vCenter Server 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 vCenter Server 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.

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 auf jedem vCenter Server-Knoten 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: 2048 Bit (Minimum) bis 16384 Bit (Maximum) (PEM-codiert)
   - CRT-Format
   - x509 Version 3
   - „SubjectAltName“ muss DNS-Name=<Maschinen-FQDN> enthalten.
   - 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 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)
   - IP-Adresse des vCenter Server

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, z. B. alle Dienste, die mit dem vSphere Client verknüpft sind.

Wenn Sie zur Eingabe eines Lösungsbenutzerzertifikats aufgefordert werden, geben Sie die vollständige Signaturzertifikatkette der Drittanbieterzertifizierungsstelle an.

Das Format sieht so oder ähnlich aus:

```
-----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: 2048 Bit (Minimum) bis 16384 Bit (Maximum) (PEM-codiert)
   - 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“
   - Zertifikat und Schlüssel (`vpxd.crt` und `vpxd.key`) für den Lösungsbenutzer „machine“
   - Vollständiger Satz an Zertifikaten und Schlüsseln (`vpxd.crt` und `vpxd.key`) für alle Lösungsbenutzer

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 `Reset All Certificates`, um alle vorhandenen vCenter-Zertifikate durch VMCA-signierte Zertifikate zu ersetzen.

Bei Verwendung dieser Option werden alle benutzerdefinierten Zertifikate, die aktuell in VECS vorhanden sind, überschrieben.

vSphere Certificate Manager kann alle Zertifikate ersetzen. Welche Zertifikate ersetzt werden, hängt von den von Ihnen ausgewählten Optionen ab.

Manuelle Zertifikatsersetzung

Das vSphere Certificate Manager-Dienstprogramm kann bei bestimmten Zertifikatsersetzungen nicht verwendet werden. Stattdessen können Sie die Befehlszeilenschnittstellen (CLIs) Ihrer Installation zum Ersetzen von Zertifikaten verwenden.

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.

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 kurz vor dem Löschen eines Maschinen-SSL-Zertifikats in VECS.

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. Weitere Informationen hierzu finden Sie unter Hinzufügen von Mitgliedern zu einer vCenter Single Sign On-Gruppe.

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.

Verfahren

1 Generieren Sie auf dem vCenter Server 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.

```
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 in Anspruch nehmen.

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 auf dem vCenter Server das VMCA-Root-Zertifikat auf, um sicherzustellen, dass es sich im Zertifikatspeicher befindet.

```
/usr/lib/vmware-vmca/bin/certool --getrootca
```

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.

```
/usr/lib/vmware-vmafd/bin/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.

```
/usr/lib/vmware-vmca/bin/certool --selfca --config=/usr/lib/vmware-vmca/share/config/
certool.cfg
```

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. Wenn mehrere vCenter Server-Instanzen in der Konfiguration des erweiterten verknüpften Modus verbunden sind, müssen Sie die Befehle zum Generieren von Maschinen-SSL-Zertifikaten auf jedem Knoten ausführen.

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.

   Sie finden die Datei `certool.cfg` im Verzeichnis `/usr/lib/vmware-vmca/share/config/`.

2. Bearbeiten Sie die benutzerdefinierte Konfigurationsdatei für jede Maschine, um den FQDN 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.

   ```
   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-<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 vCenter Server-Knoten in einer Bereitstellung mit mehreren vCenter Server-Instanzen aus, die in der Konfiguration des erweiterten verknüpften Modus verbunden sind.

```
/usr/lib/vmware-vmca/bin/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.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv
--config=ssl-config.cfg
```

Die Datei `new-vmca-ssl.crt` wird im aktuellen Verzeichnis erstellt.

4 (Optional) Listen Sie den Inhalt von VECS auf.

```
/usr/lib/vmware-vmafd/bin/vecs-cli store list
```

- Beispiel-Ausgabe am vCenter Server:

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vsphere-webclient
vpxd
vpxd-extension
hvc
data-encipherment
```

```
APPLMGMT_PASSWORD
SMS
wcp
KMS_ENCRYPTION
```

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 jedem vCenter Server die folgenden Befehle 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.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store MACHINE_SSL_CERT --alias
__MACHINE_CERT
/usr/lib/vmware-vmafd/bin/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*.

Ersetzen der Lösungsbenutzerzertifikate durch neue VMCA-signierte Zertifikate

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 der Maschine und das Lösungsbenutzerzertifikat auf jedem vCenter Server-System.

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.

```
dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

   Bei einer Bereitstellung mehrerer vCenter Server-Instanzen, die in der Konfiguration des erweiterten verknüpften Modus verbunden sind, enthält die Ausgabe von `dir-cli service 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.

4 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 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 ein öffentliches/privates Schlüsselpaar für alle Lösungsbenutzer auf sämtlichen vCenter Server-Knoten in einer Konfiguration des erweiterten verknüpften Modus. Hierzu gehören ein Paar für die Maschinenlösung und ein Paar für jeden zusätzlichen Lösungsbenutzer (vpxd, vpxd-extension, vsphere-webclient, wcp).

a Generieren Sie ein Schlüsselpaar für den Lösungsbenutzer „machine“.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

b Generieren Sie ein Schlüsselpaar für den Lösungsbenutzer „vpxd“ auf jedem Knoten.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

c Generieren Sie ein Schlüsselpaar für den Lösungsbenutzer „vpxd-extension“ auf jedem Knoten.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
```

d Generieren Sie ein Schlüsselpaar für den Lösungsbenutzer „vsphere-webclient“ auf jedem Knoten.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vsphere-webclient-key.priv --
pubkey=vsphere-webclient-key.pub
```

e Generieren Sie ein Schlüsselpaar für den Lösungsbenutzer „wcp“ auf jedem Knoten.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=wcp-key.priv --pubkey=wcp-key.pub
```

2 Generieren Sie vom neuen VMCA-Stammzertifikat signierte Lösungsbenutzerzertifikate für den Lösungsbenutzer „machine“ und für jeden zusätzlichen Lösungsbenutzer (vpxd, vpxd-extension, vsphere-webclient, wcp) auf allen vCenter Server-Knoten.

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 aus, um für den Lösungsbenutzer „machine“ auf diesem Knoten ein Lösungsbenutzerzertifikat zu generieren.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-
key.priv --Name=machine
```

b Generieren Sie ein Zertifikat für den Lösungsbenutzer „machine“ auf jedem Knoten.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-
key.priv --Name=machine
```

c Generieren Sie ein Zertifikat für den Lösungsbenutzer „vpxd“ auf jedem Knoten.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv
--Name=vpxd
```

d Generieren Sie ein Zertifikat für den Lösungsbenutzer „vpxd-extension“ auf jedem Knoten.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd-extension.crt --
privkey=vpxd-extension-key.priv --Name=vpxd-extension
```

e Generieren Sie ein Zertifikat für den Lösungsbenutzer „vsphere-webclient“ auf jedem Verwaltungsknoten, indem Sie folgenden Befehl ausführen.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vsphere-webclient.crt --
privkey=vsphere-webclient-key.priv --Name=vsphere-webclient
```

f Generieren Sie ein Zertifikat für den Lösungsbenutzer „wcp“ auf jedem Knoten, indem Sie folgende Befehle ausführen.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-wcp.crt --privkey=wcp-key.priv --
Name=wcp
```

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 Ersetzen Sie das Lösungsbenutzerzertifikat „machine“ auf jedem Verwaltungsknoten:

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store machine --alias machine
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store machine --alias machine --cert
new-machine.crt --key machine-key.priv
```

b Ersetzen Sie das Lösungsbenutzerzertifikat „vpxd“ auf jedem Knoten.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd --alias vpxd
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd --alias vpxd --cert new-
vpxd.crt --key vpxd-key.priv
```

c Ersetzen Sie das Lösungsbenutzerzertifikat „vpxd-extension“ auf jedem Knoten.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd-extension --alias vpxd-
extension
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd-extension --alias vpxd-
extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

d Ersetzen Sie das Lösungsbenutzerzertifikat „vsphere-webclient“ auf jedem Knoten.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vsphere-webclient --alias
vsphere-webclient
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vsphere-webclient --alias
vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

e Ersetzen Sie das Lösungsbenutzerzertifikat „wcp“ auf jedem Knoten.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store wcp --alias wcp
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store wcp --alias wcp --cert new-
wcp.crt --key wcp-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 führen diesen Befehl auf einem vCenter Server-System aus.

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
output:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

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 Zertifikat „machine“ im VM-Verzeichnis auf jedem vCenter Server-Knoten. Wenn beispielsweise „machine-6fd7f140-60a9-11e4-9e28-005056895a69“ der Lösungsbenutzer „machine“ auf dem vCenter Server ist, führen Sie diesen Befehl aus:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine.crt
```

c Ersetzen Sie das Lösungsbenutzerzertifikat „vpxd“ im VM-Verzeichnis auf jedem Knoten. Wenn beispielsweise „vpxd-6fd7f140-60a9-11e4-9e28-005056895a69“ die vpxd-Lösungsbenutzer-ID ist, führen Sie diesen Befehl aus:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

d Ersetzen Sie das Lösungsbenutzerzertifikat „vpxd-extension“ im VM-Verzeichnis auf jedem Knoten. Wenn beispielsweise „vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69“ die vpxd-extension-Lösungsbenutzer-ID ist, führen Sie diesen Befehl aus:

```
/usr/lib/vmware-vmafd/bin/dir-cli update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

e Ersetzen Sie das Lösungsbenutzerzertifikat „vsphere-webclient“ auf jedem Knoten. Wenn beispielsweise „vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69“ die vsphere-webclient-Lösungsbenutzer-ID ist, führen Sie diesen Befehl aus:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name vsphere-
webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

f Ersetzen Sie das Lösungsbenutzerzertifikat „wcp“ auf jedem Knoten. Wenn beispielsweise wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e die ID des Lösungsbenutzers „wcp“ ist, führen Sie folgenden Befehl aus:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name wcp-1cbe0a40-e4ce-4378-
b5e7-9460e2b8200e --cert new-wcp.crt
```

Nächste Schritte

Starten Sie alle Dienste auf sämtlichen vCenter Server-Knoten neu.

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.

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.

Ersetzen des Rootzertifikats (Zwischenzertifizierungsstelle)

Der erste Schritt beim Ersetzen des VMCA-Zertifikats durch benutzerdefinierte Zertifikate besteht im Generieren einer Zertifikatsignieranforderung (Certificate Signing Request, CSR) sowie 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: 2048 Bit (Minimum) bis 16384 Bit (Maximum) (PEM-codiert)
- PEM-Format. VMware unterstützt PKCS8 und PKCS1 (RSA-Schlüssel). Wenn Schlüssel zu VECS hinzugefügt werden, werden sie in PKCS8 konvertiert.
- x509 Version 3
- Die Zertifizierungsstellenerweiterung muss für Stammzertifikate auf „true“ festgelegt werden und „cert sign“ muss in der Liste der Anforderungen vorhanden sein. Beispiel:

```
basicConstraints        = critical,CA:true
keyUsage                = critical,digitalSignature,keyCertSign
```

- 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.x“ 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: 2048 Bit (Minimum) bis 16384 Bit (Maximum)
- 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.

   ```
   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: Wenn das Zertifikat nur über ein Zertifikat in der Kette verfügt:

```
dir-cli trustedcert publish --cert rootca1.crt
```

Wenn das Zertifikat über mehrere Zertifikate in der Kette verfügt:

```
dir-cli trustedcert publish --cert rootcal.crt --chain
```

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 Befehl `certool` mit der Option `--rootca` verwenden.

```
/usr/lib/vmware-vmca/bin/certool --rootca --cert=<path>/root.pem --privkey=<path>/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 Ersetzen eines vCenter Server-STS-Zertifikats über die Befehlszeile.

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. Wenn mehrere vCenter Server-Instanzen in der Konfiguration des erweiterten verknüpften Modus verbunden sind, müssen Sie die Befehle zum Generieren von Maschinen-SSL-Zertifikaten auf jedem Knoten ausführen.

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.

   Die Datei `certool.cfg` befindet sich im Verzeichnis `/usr/lib/vmware-vmca/share/config/`.

2. Bearbeiten Sie die benutzerdefinierte Konfigurationsdatei für jede Maschine, um den FQDN 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.

```
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-<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 vCenter Server-Knoten in einer Bereitstellung mit mehreren vCenter Server-Instanzen aus, die in der Konfiguration des erweiterten verknüpften Modus verbunden sind.

```
/usr/lib/vmware-vmca/bin/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.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv
--config=ssl-config.cfg
```

Die Datei `new-vmca-ssl.crt` wird im aktuellen Verzeichnis erstellt.

4 (Optional) Listen Sie den Inhalt von VECS auf.

```
/usr/lib/vmware-vmafd/bin/vecs-cli store list
```

- Beispiel-Ausgabe am vCenter Server:

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vsphere-webclient
vpxd
vpxd-extension
hvc
data-encipherment
APPLMGMT_PASSWORD
SMS
wcp
KMS_ENCRYPTION
```

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 jedem vCenter Server die folgenden Befehle 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.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store MACHINE_SSL_CERT --alias
__MACHINE_CERT
/usr/lib/vmware-vmafd/bin/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 der Maschine und das Lösungsbenutzerzertifikat auf jedem vCenter Server-System.

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.

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.

   ```
   dir-cli service list
   Enter password for administrator@vsphere.local:
   ```

```
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

Bei einer Bereitstellung mehrerer vCenter Server-Instanzen, die in der Konfiguration des erweiterten verknüpften Modus verbunden sind, enthält die Ausgabe von `dir-cli service 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.

4 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 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 ein öffentliches/privates Schlüsselpaar für alle Lösungsbenutzer auf sämtlichen vCenter Server-Knoten in einer Konfiguration des erweiterten verknüpften Modus. Hierzu gehören ein Paar für die Maschinenlösung und ein Paar für jeden zusätzlichen Lösungsbenutzer (vpxd, vpxd-extension, vsphere-webclient, wcp).

a Generieren Sie ein Schlüsselpaar für den Lösungsbenutzer „machine“.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

b Generieren Sie ein Schlüsselpaar für den Lösungsbenutzer „vpxd“ auf jedem Knoten.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

c Generieren Sie ein Schlüsselpaar für den Lösungsbenutzer „vpxd-extension“ auf jedem Knoten.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-extension-key.priv --
pubkey=vpxd-extension-key.pub
```

d Generieren Sie ein Schlüsselpaar für den Lösungsbenutzer „vsphere-webclient“ auf jedem Knoten.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vsphere-webclient-key.priv --
pubkey=vsphere-webclient-key.pub
```

e Generieren Sie ein Schlüsselpaar für den Lösungsbenutzer „wcp“ auf jedem Knoten.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=wcp-key.priv --pubkey=wcp-key.pub
```

2 Generieren Sie vom neuen VMCA-Stammzertifikat signierte Lösungsbenutzerzertifikate für den Lösungsbenutzer „machine“ und für jeden zusätzlichen Lösungsbenutzer (vpxd, vpxd-extension, vsphere-webclient, wcp) auf allen vCenter Server-Knoten.

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 aus, um für den Lösungsbenutzer „machine“ auf diesem Knoten ein Lösungsbenutzerzertifikat zu generieren.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-
key.priv --Name=machine
```

b Generieren Sie ein Zertifikat für den Lösungsbenutzer „machine“ auf jedem Knoten.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-
key.priv --Name=machine
```

c Generieren Sie ein Zertifikat für den Lösungsbenutzer „vpxd“ auf jedem Knoten.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv
--Name=vpxd
```

d Generieren Sie ein Zertifikat für den Lösungsbenutzer „vpxd-extension“ auf jedem Knoten.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd-extension.crt --
privkey=vpxd-extension-key.priv --Name=vpxd-extension
```

e Generieren Sie ein Zertifikat für den Lösungsbenutzer „vsphere-webclient“ auf jedem Verwaltungsknoten, indem Sie folgenden Befehl ausführen.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vsphere-webclient.crt --
privkey=vsphere-webclient-key.priv --Name=vsphere-webclient
```

f Generieren Sie ein Zertifikat für den Lösungsbenutzer „wcp“ auf jedem Knoten, indem Sie folgende Befehle ausführen.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-wcp.crt --privkey=wcp-key.priv --
Name=wcp
```

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 Ersetzen Sie das Lösungsbenutzerzertifikat „machine“ auf jedem Verwaltungsknoten:

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store machine --alias machine
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store machine --alias machine --cert
new-machine.crt --key machine-key.priv
```

b Ersetzen Sie das Lösungsbenutzerzertifikat „vpxd“ auf jedem Knoten.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd --alias vpxd
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd --alias vpxd --cert new-
vpxd.crt --key vpxd-key.priv
```

c Ersetzen Sie das Lösungsbenutzerzertifikat „vpxd-extension“ auf jedem Knoten.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd-extension --alias vpxd-
extension
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd-extension --alias vpxd-
extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

d Ersetzen Sie das Lösungsbenutzerzertifikat „vsphere-webclient“ auf jedem Knoten.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vsphere-webclient --alias
vsphere-webclient
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vsphere-webclient --alias
vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

e Ersetzen Sie das Lösungsbenutzerzertifikat „wcp“ auf jedem Knoten.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store wcp --alias wcp
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store wcp --alias wcp --cert new-
wcp.crt --key wcp-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 führen diesen Befehl auf einem vCenter Server-System aus.

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
output:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

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 Zertifikat „machine“ im VM-Verzeichnis auf jedem vCenter Server-Knoten. Wenn beispielsweise „machine-6fd7f140-60a9-11e4-9e28-005056895a69“ der Lösungsbenutzer „machine“ auf dem vCenter Server ist, führen Sie diesen Befehl aus:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine.crt
```

c Ersetzen Sie das Lösungsbenutzerzertifikat „vpxd“ im VM-Verzeichnis auf jedem Knoten. Wenn beispielsweise „vpxd-6fd7f140-60a9-11e4-9e28-005056895a69“ die vpxd-Lösungsbenutzer-ID ist, führen Sie diesen Befehl aus:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

d Ersetzen Sie das Lösungsbenutzerzertifikat „vpxd-extension“ im VM-Verzeichnis auf jedem Knoten. Wenn beispielsweise „vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69“ die vpxd-extension-Lösungsbenutzer-ID ist, führen Sie diesen Befehl aus:

```
/usr/lib/vmware-vmafd/bin/dir-cli update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

e Ersetzen Sie das Lösungsbenutzerzertifikat „vsphere-webclient“ auf jedem Knoten. Wenn beispielsweise „vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69“ die vsphere-webclient-Lösungsbenutzer-ID ist, führen Sie diesen Befehl aus:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name vsphere-
webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

f Ersetzen Sie das Lösungsbenutzerzertifikat „wcp“ auf jedem Knoten. Wenn beispielsweise wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e die ID des Lösungsbenutzers „wcp“ ist, führen Sie folgenden Befehl aus:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name wcp-1cbe0a40-e4ce-4378-
b5e7-9460e2b8200e --cert new-wcp.crt
```

Verwenden von benutzerdefinierten Zertifikaten mit vSphere

Wenn es von Ihrer 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. vCenter Server verwendet Lösungsbenutzerzertifikate nur für die interne Kommunikation. Lösungsbenutzerzertifikate werden nicht für die externe Kommunikation 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.

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: 2048 Bit (Minimum) bis 16384 Bit (Maximum) (PEM-codiert)
- 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 Zertifikatssignieranforderungen (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 fünf Lösungsbenutzerzertifikate für jeden Knoten. Lösungsbenutzerzertifikate müssen keine IP-Adresse, keinen Hostnamen und keine E-Mail-Adresse enthalten. Für jedes Zertifikat ist ein unterschiedlicher Zertifikatantragsteller erforderlich.

   Das Ergebnis ist in der Regel eine PEM-Datei für die Vertrauenskette, einschließlich der signierten SSL-Zertifikate für jeden vCenter Server-Knoten.
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 ersetzt werden soll. Sehen Sie sich die Zertifikatsinformationen an 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.

   ```
   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 Ersetzen eines vCenter Server-STS-Zertifikats über die Befehlszeile.

Ersetzen der Maschinen-SSL-Zertifikate durch benutzerdefinierte Zertifikate

Nachdem Sie die benutzerdefinierten Zertifikate erhalten haben, können Sie jedes Maschinenzertifikat ersetzen.

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)

Voraussetzungen

Sie müssen für jede Maschine ein Zertifikat von Ihrer Drittanbieter- oder Unternehmenszertifizierungsstelle erhalten haben.

- Schlüsselgröße: 2048 Bit (Minimum) bis 16384 Bit (Maximum) (PEM-codiert)
- 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.

```
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 Aktualisieren Sie den Endpoint für die Lookup Service-Registrierung.

```
/usr/lib/vmware-lookupsvc/tools/ls_update_certs.py --url https://<vCenterServer_FQDN>/
lookupservice/sdk --certfile <cert-file-path> --user 'administrator@vsphere.local' --
password '<password>' --fingerprint <SHA1_hash_of_the_old_certificate_to_replace>
```

4 Starten Sie alle Dienste neu.

```
service-control --start --all
```

Verwalten von Diensten und Zertifikaten mit CLI-Befehlen

3

Sie können Zertifikate von VMCA (VMware Certificate Authority), VECS (VMware Endpoint Certificate Store), VMware Directory Service (vmdir) und Security Token Service (STS) mithilfe eines Satzes von CLIs 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 3-1. 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 des VMware-Authentifizierungsframework-Daemon (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`	Verwalten Sie STS-Zertifikate.	Befehlszeilenhilfe.
`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.

```
/usr/lib/vmware-vmafd/bin/vecs-cli
/usr/lib/vmware-vmafd/bin/dir-cli
/usr/lib/vmware-vmca/bin/certool
/opt/vmware/bin/sso-config.sh
```

Hinweis Für den Befehl `service-control` müssen Sie den Pfad nicht angeben.

Dieses Kapitel enthält die folgenden Themen:

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 Administratorengruppe verfügen über pauschale 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 im Verzeichnis `/usr/lib/vmware-vmca/share/config/`.

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.
- ```
  /usr/lib/vmware-vmca/bin/certool --gencert --config /tmp/myconfig.cfg
  ```
  ```

- Überschreiben Sie einzelne Werte in der Befehlszeile. Führen Sie beispielsweise den folgenden Befehl aus, um „Locality“ zu überschreiben:

```
/usr/lib/vmware-vmca/bin/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 --gencsr --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.
`--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.

Option	Beschreibung
`--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 mit anderen Optionen zur Planung bestimmter Aufgaben, wie z. B. der Rückgabe des Namens der Standarddomäne.

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

Option	Beschreibung
`--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. 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 Zertifikatsinfrastruktur und Authentifizierungsdienste 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 3-2. Speicher in VECS

Speicher	Beschreibung
Maschinen-SSL-Speicher (MACHINE_SSL_CERT)	■ Wird vom Reverse-Proxy-Dienst auf jedem vSphere-Knoten verwendet. ■ Wird vom VMware Directory Service (vmdir) für jeden vCenter Server-Knoten verwendet. 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.
Lösungsbenutzerspeicher ■ `machine` ■ `vpxd` ■ `vpxd-extension` ■ `vsphere-webclient` ■ `wcp`	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. Lösungsbenutzerzertifikate werden für die Authentifizierung mit vCenter Single Sign On verwendet. vCenter Single Sign On überprüft, ob das Zertifikat gültig ist. Andere Zertifikatsattribute werden jedoch nicht überprüft. Die folgenden Speicher für Lösungsbenutzerzertifikate sind in VECS 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-Speicher (vpxd). vpxd verwendet das in diesem Speicher abgelegte Lösungsbenutzerzertifikat, um sich bei vCenter Single Sign On zu authentifizieren. ■ `vpxd-extension`: vCenter-Erweiterungsspeicher. Enthält den Auto Deploy-Dienst, den Inventory Service und sonstige Dienste, die nicht Bestandteil anderer Lösungsbenutzer sind. ■ `vsphere-webclient`: vSphere Client-Speicher. Enthält auch zusätzliche Dienste wie etwa den Leistungsdiagrammdienst. ■ `wcp`: VMware vSphere® mit VMware Tanzu™-Speicher. Jeder vCenter Server-Knoten enthält ein `machine`-Zertifikat.
Vertrauenswürdiger Stammspeicher (TRUSTED_ROOTS)	Enthält alle vertrauenswürdigen Stammzertifikate.

Tabelle 3-2. 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. **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.

Hinweis Verwenden Sie diesen Befehl nicht, um dem TRUSTED_ROOTS-Speicher Stammzertifikate hinzuzufügen. Verwenden Sie stattdessen den Befehl `dir-cli`, um Stammzertifikate zu veröffentlichen.

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. 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.

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-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 `dir-cli` verwenden, um die Domänenfunktionsebene von vCenter Server-Instanzen zu verwalten und abzufragen.

dir-cli nodes list

Listet alle über den erweiterten verknüpften Modus verbundenen vCenter Server-Systeme 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, um eine Verbindung zu einem anderen vCenter Server herzustellen und dessen Replizierungspartner anzuzeigen.

dir-cli computer password-reset

Mit diesem Befehl können Sie das Kennwort des Maschinenkontos in der Domäne zurücksetzen.

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 vCenter Server-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.
`--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. Aktualisieren Sie nach dem Ausführen dieses Befehls den Eintrag des Lösungsbenutzerzertifikats in VECS, indem Sie den Befehl `vecs-cli entry create` ausführen. Weitere Informationen finden Sie unter Befehlsreferenz für vecs-cli.

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 ändern, die beim vCenter Server authentifiziert werden müssen, und Sie sicherstellen möchten, dass die Aufgaben bei Kennwortablauf weiterhin ausgeführt werden. 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: ■ Ebene 0 – Konto und UPN ■ Ebene 1 – Ebene 0-Info + Vor- und Nachname ■ Ebene 2 : Ebene 0 + Flag „Konto deaktiviert“, Flag „Konto gesperrt“, Flag „Kennwort läuft nie ab“, Flag „Kennwort abgelaufen“ und Flag „Kennwortablauf“. Die Standardebene ist 0.

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 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. Nach der Ausführung dieses Befehls übernimmt VECS die Zertifikatsänderung nach einer Minute. Alternativ können Sie den Befehl `vecs-cli force-refresh` ausführen, um das Zertifikat sofort zu synchronisieren.

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.
`--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.

vSphere-Authentifizierung mit vCenter Single Sign On

4

vCenter Single Sign On ist ein Authentifizierungs-Broker und eine Austauschinfrastruktur für Sicherheitstoken. vCenter Single Sign On gibt ein Token aus, wenn sich ein Benutzer authentifiziert. Mit dem Token kann sich der Benutzer bei vCenter Server-Diensten authentifizieren. 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.

Benutzer und Dienstkonten authentifizieren sich mit einem Token oder mit einem Benutzernamen und Kennwort. Lösungsbenutzer authentifizieren sich mit einem Zertifikat. Informationen zum Ersetzen von Lösungsbenutzerzertifikaten finden Sie unter Kapitel 2 vSphere-Sicherheitszertifikate.

Im nächsten Schritt autorisieren Sie die Benutzer, die die Durchführung bestimmter Aufgaben authentifizieren können. In der Regel weisen Sie vCenter Server-Berechtigungen zu, indem Sie den Benutzer einer Gruppe mit einer Rolle zuweisen. vSphere beinhaltet weitere Berechtigungsmodelle, wie zum Beispiel globale Berechtigungen. Informationen finden Sie in der Dokumentation *vSphere-Sicherheit*.

Dieses Kapitel enthält die folgenden Themen:

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.

- Authentifizierung von Benutzern über einen externen Identitätsanbieterverbund oder den integrierten vCenter Server-Identitätsanbieter. Der integrierte Identitätsanbieter unterstützt lokale Konten, Active Directory oder OpenLDAP, integrierte Windows-Authentifizierung (IWA) sowie verschiedene Authentifizierungsmechanismen (Smartcard, RSA SecurID und Windows-Sitzungsauthentifizierung).
- Authentifizierung von Lösungsbenutzern über Zertifikate.
- Security Token Service (STS).
- SSL für sicheren Datenverkehr.

Übersicht über Identitätsanbieter

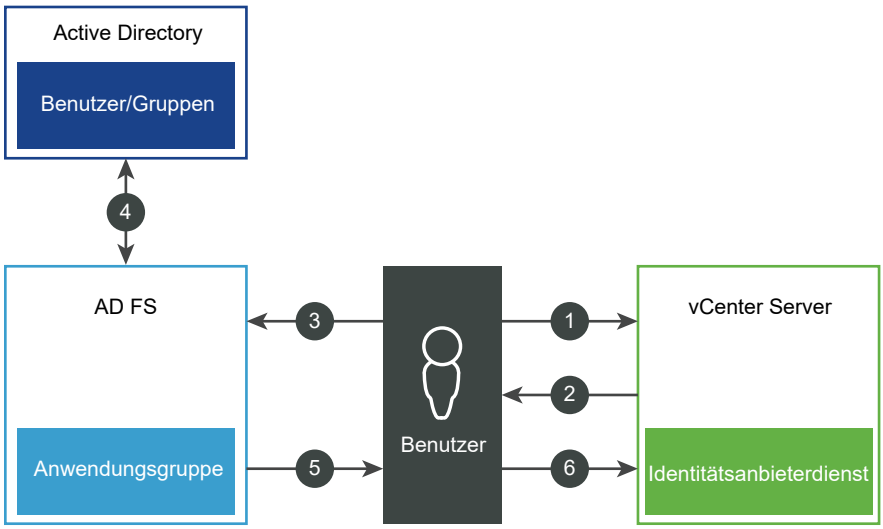
Vor vSphere 7.0 enthält vCenter Server einen integrierten Identitätsanbieter. Standardmäßig verwendet vCenter Server die Domäne „vsphere.local“ als Identitätsquelle (diese kann jedoch während der Installation geändert werden). Sie können den in vCenter Server integrierten Identitätsanbieter konfigurieren, um Active Directory (AD) als Identitätsquelle mithilfe von LDAP/S, OpenLDAP/S und der integrierten Windows-Authentifizierung (IWA) zu verwenden. Aufgrund dieser Konfigurationen können sich Kunden mithilfe ihrer AD-Konten bei vCenter Server anmelden.

Ab vSphere 7.0 können Sie vCenter Server für einen externen Identitätsanbieter mithilfe der Verbundauthentifizierung konfigurieren. In einer solchen Konfiguration ersetzen Sie vCenter Server als Identitätsanbieter. Aktuell bietet vSphere Unterstützung für Active Directory Federation Services (AD FS) als externen Identitätsanbieter. In dieser Konfiguration interagiert AD FS im Auftrag von vCenter Server mit den Identitätsquellen.

Benutzeranmeldung mit Identitätsanbieter-Verbundauthentifizierung in vCenter Server

Die folgende Abbildung zeigt den Ablauf der Benutzeranmeldung für den vCenter Server-Identitätsanbieterverbund.

Abbildung 4-1. Benutzeranmeldung beim vCenter Server-Identitätsanbieterverbund



vCenter Server, AD FS und Active Directory interagieren wie folgt:

1 Der Benutzer beginnt auf der vCenter Server-Startseite mit der Eingabe eines Benutzernamens.

2 Wenn der Benutzername für eine Verbunddomäne gilt, leitet vCenter Server die Authentifizierungsanforderung an AD FS um.

3 Bei Bedarf fordert AD FS den Benutzer auf, sich mit den Active Directory-Anmeldedaten anzumelden.

4 AD FS authentifiziert den Benutzer mit Active Directory.

5 AD FS gibt ein Sicherheitstoken mit Active Directory-Gruppeninformationen aus.

6 vCenter Server verwendet das Token, um den Benutzer anzumelden.

Der Benutzer ist jetzt authentifiziert und kann alle Objekte anzeigen und ändern, für die die Benutzerrolle über die entsprechenden Berechtigungen verfügt.

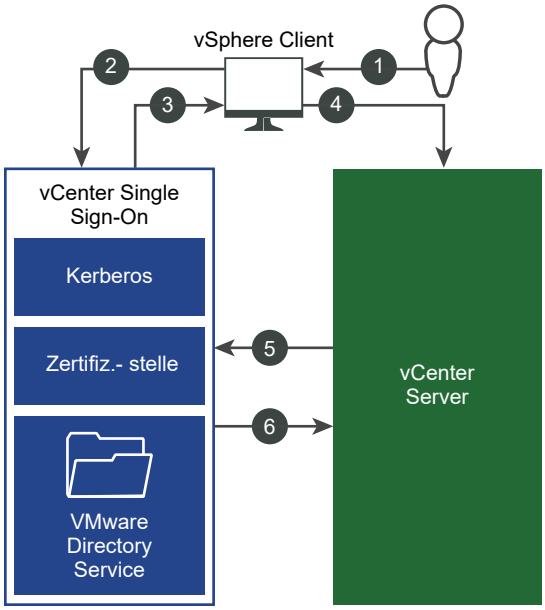
Hinweis Zu Beginn wird jedem Benutzer die Rolle „Kein Zugriff“ zugewiesen. Ein vCenter Server-Administrator muss dem jeweiligen Benutzer mindestens die Rolle für den Zugriff „Nur Lesen“ zuweisen, bevor sich der Benutzer anmelden kann. Informationen finden Sie in der Dokumentation *vSphere-Sicherheit*.

Wenn der externe Identitätsanbieter nicht erreichbar ist, wird der Anmeldevorgang an die vCenter Server-Startseite zurückgeleitet, auf der eine entsprechende Informationsmeldung angezeigt wird. Benutzer können sich weiterhin mit ihren lokalen Konten in der vsphere.local-Identitätsquelle anmelden.

Benutzeranmeldung mit dem in vCenter Server integrierten Identitätsanbieter

Die folgende Abbildung zeigt den Ablauf der Benutzeranmeldung, wenn vCenter Server als Identitätsanbieter fungiert.

Abbildung 4-2. Benutzeranmeldung mit dem in vCenter Server integrierten Identitätsanbieter



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.

   Wenn integrierte Windows-Authentifizierung (IWA) konfiguriert wurde, können sich Benutzer auch ohne erneute Eingabe des Windows-Kennworts anmelden, indem sie 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 ist jetzt authentifiziert und kann 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*.

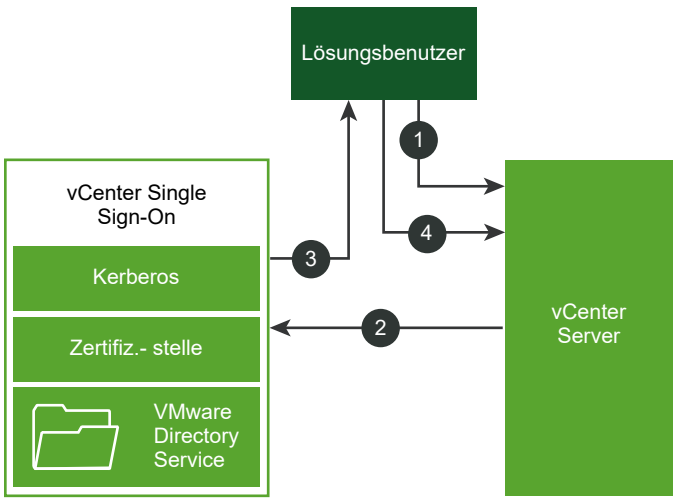
Anmeldung für Lösungsbenutzer

Bei Lösungsbenutzern handelt es sich um Sätze von Diensten, die in der vCenter Server-Infrastruktur verwendet werden, wie z. B. vCenter Server-Erweiterungen. VMware-Erweiterungen und eventuell Erweiterungen von Drittanbietern können sich ebenfalls bei vCenter Single Sign On authentifizieren.

Hinweis vCenter Server verwendet Lösungsbenutzerzertifikate ausschließlich für die interne Kommunikation. Lösungsbenutzerzertifikate werden nicht für die externe Kommunikation verwendet.

Die folgende Abbildung zeigt den Ablauf der Anmeldung für Lösungsbenutzer.

Abbildung 4-3. Anmeldung für Lösungsbenutzer



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

   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 laut 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 von benutzerdefinierten Zertifikaten 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.

Sie wirkt sich auch immer dann auf die Sicherheit aus, wenn ein ESXi-Host oder vCenter Server zu Active Directory hinzugefügt wird.

Grundlegendes zum vCenter Server-Identitätsanbieterverbund

Ab vSphere 7.0 bietet vCenter Server Unterstützung für Verbundauthentifizierung zum Anmelden bei vCenter Server.

Um Verbundauthentifizierung für vCenter Server zu aktivieren, konfigurieren Sie eine Verbindung mit einem externen Identitätsanbieter. Die von Ihnen konfigurierte Identitätsanbieterinstanz ersetzt vCenter Server als Identitätsanbieter. Derzeit unterstützt vCenter Server nur Active Directory Federation Services (AD FS) als externen Identitätsanbieter.

Hinweis VMware empfiehlt Ihnen, Verbundauthentifizierung zu verwenden, da in vSphere künftig tokenbasierte Authentifizierung verwendet wird. vCenter Server verwendet weiterhin lokale Konten für Administratorzugriff und Fehlerbehebung.

Funktionsweise des vCenter Server-Identitätsanbieterverbunds

Mit dem vCenter Server-Identitätsanbieterverbund können Sie einen externen Identitätsanbieter für Verbundauthentifizierung konfigurieren. In dieser Konfiguration interagiert der externe Identitätsanbieter im Auftrag von vCenter Server mit der Identitätsquelle.

Grundlegendes zum vCenter Server-Identitätsanbieterverbund

Ab vSphere 7.0 bietet vCenter Server Unterstützung für Verbundauthentifizierung. Wenn sich in diesem Szenario ein Benutzer bei vCenter Server anmeldet, leitet vCenter Server die Benutzeranmeldung an den externen Identitätsanbieter weiter. Die Benutzeranmeldedaten werden vCenter Server nicht mehr direkt bereitgestellt. Stattdessen werden dem externen Identitätsanbieter die Anmeldedaten vom Benutzer zur Verfügung gestellt. vCenter Server stuft den externen Identitätsanbieter als vertrauenswürdig für die Durchführung der Authentifizierung ein. Im Verbundmodell werden Anmeldedaten niemals direkt vom Benutzer an einen Dienst oder eine Anwendung, sondern ausschließlich an den Identitätsanbieter übergeben. Folglich können Ihre Anwendungen und Dienste, wie z. B. vCenter Server, einen Verbund mit dem Identitätsanbieter eingehen.

Vorteile des vCenter Server-Identitätsanbieterverbunds

Der vCenter Server-Identitätsanbieterverbund bietet die folgenden Vorteile.

- Sie können Single Sign-On mit der vorhandenen Verbundinfrastruktur und vorhandenen Anwendungen verwenden.
- Sie können die Sicherheit des Datencenters verbessern, da die Benutzeranmeldedaten niemals von vCenter Server verarbeitet werden.
- Sie können die Authentifizierungsmechanismen (wie z. B. Multifaktor-Authentifizierung) verwenden, die vom externen Identitätsanbieter unterstützt werden.

Komponenten des vCenter Server-Identitätsanbieterverbunds

Die Konfiguration eines vCenter Server-Identitätsanbieterverbunds, die Microsoft Active Directory Federation Services (AD FS) verwendet, setzt sich aus folgenden Komponenten zusammen:

- Einem vCenter Server
- Einem auf dem vCenter Server konfigurierten Identitätsanbieterdienst
- Einem AD FS-Server und der zugehörigen Microsoft Active Directory-Domäne
- Einer AD FS-Anwendungsgruppe
- Active Directory-Gruppen und -Benutzer, die vCenter Server-Gruppen und -Benutzern zugeordnet sind

Hinweis Aktuell unterstützt vCenter Server nur AD FS als externen Identitätsanbieter.

Architektur des vCenter Server-Identitätsanbieterverbunds

Im vCenter Server-Identitätsanbieterverbund verwendet vCenter Server das OpenID Connect OIDC-Protokoll (OpenID Connect), um ein Identitätstoken zu erhalten, das den Benutzer bei vCenter Server authentifiziert.

Zum Einrichten einer Vertrauensstellung der vertrauenden Seite zwischen vCenter Server und einem Identitätsanbieter müssen Sie Identifzierungsinformationen und einen gemeinsamen geheimen Schlüssel zwischen ihnen festlegen. In AD FS erstellen Sie hierzu eine als Anwendungsgruppe bezeichnete OIDC-Konfiguration, die aus einer Serveranwendung und einer Webschnittstelle besteht. Die beiden Komponenten enthalten die Informationen, die von vCenter Server zum Herstellen von Vertrauen und zur Kommunikation mit dem AD FS-Server verwendet werden. Sie können auch einen entsprechenden Identitätsanbieter in vCenter Server erstellen. Schließlich konfigurieren Sie Gruppenmitgliedschaften in vCenter Server, um Anmeldungen von Benutzern in der AD FS-Domäne zu autorisieren.

Der AD FS-Administrator muss die folgenden Informationen bereitstellen, um die Konfiguration des vCenter Server-Identitätsanbieters zu erstellen:

- Client-ID: Die vom Assistenten für die AD FS-Anwendungsgruppe erzeugte UUID-Zeichenfolge, die die Anwendungsgruppe angibt.
- Gemeinsamer geheimer Schlüssel: Der vom Assistenten für die AD FS-Anwendungsgruppe erzeugte Schlüssel, der zur Authentifizierung von vCenter Server mit AD FS verwendet wird.
- OpenID-Adresse: Die OpenID Provider Discovery-Endpoint-URL des AD FS-Servers, die eine bekannte Adresse angibt, bei der es sich in der Regel um den mit dem Pfad „`/.well-known/openid-configuration`“ verketteten Aussteller-Endpoint handelt. Beispiel: `https://webserver.example.com/adfs/.well-known/openid-configuration`.

vCenter Server-Identitätsanbieterverbund und erweiterter verknüpfter Modus

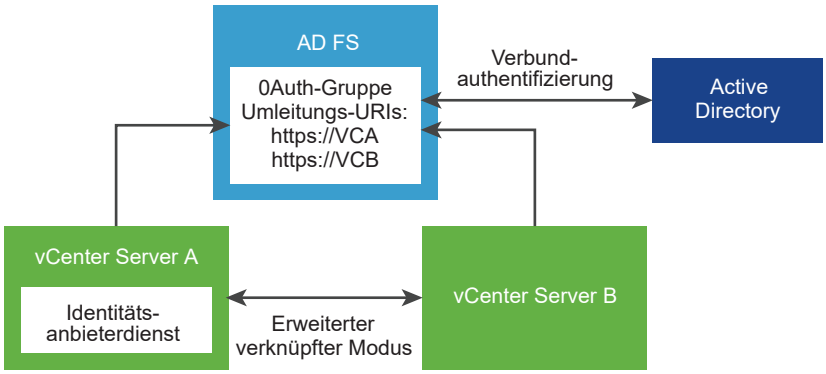
Wenn Sie einen Identitätsanbieterverbund in vCenter Server-Umgebungen aktivieren, die den erweiterten verknüpften Modus verwenden, werden Authentifizierung und Workflows unverändert ausgeführt.

Beachten Sie bei Verwendung der Konfiguration des erweiterten verknüpften Modus Folgendes, wenn Sie sich mithilfe von Verbundauthentifizierung bei vCenter Server anmelden.

- Benutzern wird weiterhin dieselbe Bestandsliste angezeigt und sie können dieselben Aktionen basierend auf dem Modell der vCenter Server-Berechtigungen und -rollen durchführen.
- vCenter Server-Hosts im erweiterten verknüpften Modus müssen keinen Zugriff auf die Identitätsanbieter der anderen Hosts haben. Beispiel: Stellen Sie sich zwei vCenter Server-Systeme A und B vor, die den erweiterten verknüpften Modus verwenden. Nachdem vCenter Server a einen Benutzer autorisiert hat, wird der Benutzer ebenfalls auf vCenter Server B autorisiert.

Die folgende Abbildung zeigt den Authentifizierungs-Workflow mit dem erweiterten verknüpften Modus und dem vCenter Server-Identitätsanbieterverbund.

Abbildung 4-4. Erweiterter verknüpfter Modus und vCenter Server-Identitätsanbieterverbund



1 Zwei vCenter Server-Knoten werden in der Konfiguration des erweiterten verknüpften Modus bereitgestellt.

2 Das AD FS-Setup wurde auf vCenter Server A mithilfe des Assistenten zum Ändern des Identitätsanbieters im vSphere Client konfiguriert. Gruppenmitgliedschaften und -berechtigungen wurden ebenfalls für AD FS-Benutzer oder -Gruppen eingerichtet.

3 vCenter Server A repliziert die AD FS-Konfiguration auf vCenter Server B.

4 Alle Umleitungs-URIs für beide vCenter Server-Knoten werden der OAuth-Anwendungsgruppe in AD FS hinzugefügt. Nur eine OAuth-Anwendungsgruppe wird erstellt.

5 Wenn sich ein Benutzer bei vCenter Server A anmeldet und autorisiert wird, gilt diese Autorisierung auch für vCenter Server B. Wenn sich der Benutzer zuerst bei vCenter Server B anmeldet, gilt dasselbe.

Der erweiterte verknüpfte vCenter Server-Modus unterstützt die folgenden Konfigurationsszenarien für den Identitätsanbieterverbund. Die Begriffe „AD FS-Einstellungen“ und „AD FS-Konfiguration“ in diesem Abschnitt beziehen sich auf die Einstellungen, die Sie im vSphere Client mithilfe des Assistenten zum Ändern von Identitätsanbietern konfiguriert haben, sowie auf alle Gruppenmitgliedschaften oder -berechtigungen, die Sie für AD FS-Benutzer oder -Gruppen eingerichtet haben.

Aktivieren von AD FS in einer vorhandenen Konfiguration des erweiterten verknüpften Modus

Allgemeine Schritte:

1 Stellen Sie N vCenter Server-Knoten in der Konfiguration des erweiterten verknüpften Modus bereit.

2 Konfigurieren Sie AD FS auf einem der verknüpften vCenter Server-Knoten.

3 Die AD FS-Konfiguration wird auf alle anderen (N-1) vCenter Server-Knoten repliziert.

4 Fügen Sie alle Umleitungs-URIs für alle N vCenter Server-Knoten zur konfigurierten OAuth-Anwendungsgruppe in AD FS hinzu.

Verknüpfen eines neuen vCenter Server mit einer vorhandenen AD FS-Konfiguration des erweiterten verknüpften Modus

Allgemeine Schritte:

1 (Voraussetzung) Richten Sie AD FS auf einem vCenter Server mit N Knoten in einer Konfiguration des erweiterten verknüpften Modus ein.

2 Stellen Sie einen neuen unabhängigen vCenter Server-Knoten bereit.

3 Verweisen Sie den neuen vCenter Server auf die AD FS-Domäne mit N Knoten im erweiterten verknüpften Modus, indem Sie einen der *N* Knoten als Replizierungspartner verwenden.

4 Alle AD FS-Einstellungen in der vorhandenen Konfiguration des erweiterten verknüpften Modus werden auf den neuen vCenter Server repliziert.

   Die AD FS-Einstellungen, die sich in der aus N-Knoten bestehenden AD FS-Domäne des erweiterten verknüpften Modus befinden, überschreiben alle vorhandenen AD FS-Einstellungen auf dem neu verknüpften vCenter Server.

5 Fügen Sie alle Umleitungs-URIs für den neuen vCenter Server zur vorhandenen konfigurierten OAuth-Anwendungsgruppe in AD FS hinzu.

Aufheben der Verknüpfung eines vCenter Server mit einer AD FS-Konfiguration des erweiterten verknüpften Modus

Allgemeine Schritte:

1 (Voraussetzung) Richten Sie AD FS in einer aus N-Knoten bestehenden Konfiguration des erweiterten verknüpften Modus für vCenter Server ein.

2 Heben Sie die Registrierung eines der vCenter Server-Hosts in der aus N-Knoten bestehenden Konfiguration auf und verweisen Sie ihn an eine neue Domäne, um die Verknüpfung mit der aus N-Knoten bestehenden Konfiguration aufzuheben.

3 Beim Neuverweisen der Domäne werden SSO-Einstellungen nicht beibehalten, sodass alle AD FS-Einstellungen auf dem nicht verknüpften vCenter Server-Knoten zurückgesetzt werden und verloren gehen. Zur weiteren Verwendung von AD FS auf diesem nicht verknüpften vCenter Server-Knoten müssen Sie AD FS von Grund auf neu konfigurieren oder den vCenter Server erneut mit einer Konfiguration des erweiterten verknüpften Modus verknüpfen, in der AD FS bereits eingerichtet ist.

Einschränkungen und Interoperabilität des vCenter Server-Identitätsanbieterverbunds

Der vCenter Server-Identitätsanbieterverbund kann mit vielen anderen VMware-Funktionen zusammenarbeiten.

Beachten Sie beim Planen Ihrer Strategie für den vCenter Server-Identitätsanbieterverbund mögliche Beschränkungen bei der Interoperabilität.

Authentifizierungsmechanismen

In einer Konfiguration für vCenter Server-Identitätsanbieterverbund verarbeitet der externe Identitätsanbieter die Authentifizierungsmechanismen (Kennwörter, MFA, Biometrie usw.).

Unterstützung für eine einzelne Active Directory-Domäne

Wenn Sie denvCenter Server-Identitätsanbieterverbund konfigurieren, werden Sie vom Assistenten „Hauptidentitätsanbieter konfigurieren“ aufgefordert, LDAP-Informationen für die AD-Domäne einzugeben, die die Benutzer und Gruppen enthält, die auf vCenter Server zugreifen sollen. vCenter Server leitet die AD-Domäne, die zur Autorisierung und für Berechtigungen verwendet wird, vom Benutzer-Basis-DN ab, den Sie im Assistenten angeben. Sie können Berechtigungen für vSphere-Objekte nur für Benutzer und Gruppen aus dieser AD-Domäne hinzufügen. Benutzer oder Gruppen aus untergeordneten AD-Domänen oder anderen Domänen in der AD-Gesamtstruktur werden vom vCenter Server-Identitätsanbieterverbund nicht unterstützt.

vCenter Server-Richtlinien

Wenn vCenter Server als Identitätsanbieter fungiert, steuern Sie Kennwort-, Sperrungs- und Token-Richtlinien von vCenter Server für die Domäne „vsphere.local“. Wenn Sie die Verbundauthentifizierung mit vCenter Server verwenden, steuert der externe Identitätsanbieter die Kennwort-, Sperrungs- und Token-Richtlinien für die in der Identitätsquelle gespeicherten Konten, wie z. B. Active Directory.

Audits und Konformität

Wenn Sie vCenter Server-Identitätsanbieterverbund verwenden, erstellt vCenter Server weiterhin Protokolleinträge für erfolgreiche Benutzeranmeldungen. Der externe Identitätsanbieter ist jedoch für die Verfolgung und Protokollierung von Aktionen wie fehlgeschlagenen Versuchen zur Kennworteingabe und die Sperrung von Benutzerkonten verantwortlich. vCenter Server protokolliert solche Ereignisse nicht, da sie für vCenter Server nicht mehr sichtbar sind. Wenn beispielsweise AD FS der Identitätsanbieter ist, werden Fehler für Verbundanmeldungen von AD FS nachverfolgt und protokolliert. Wenn vCenter Server der Identifizierungsanbieter für lokale Anmeldungen ist, werden Fehler für lokale Anmeldungen von vCenter Server nachverfolgt und protokolliert. In einer Verbundkonfiguration protokolliert vCenter Server weiterhin Benutzeraktionen nach der Anmeldung.

Integration vorhandener VMware-Produkte

VMware-Produkte, die in vCenter Server integriert sind (z. B. vROps, vSAN, NSX usw.), funktionieren weiterhin wie bisher.

Produkte, die nach der Anmeldung integriert werden

Produkte, die nach der Anmeldung integriert werden (also keine separate Anmeldung benötigten), funktionieren weiterhin wie bisher.

Einfache Authentifizierung für API-, SDK- und CLI-Zugriff

Vorhandene Skripts, Produkte und andere Funktionen, die auf API-, SDK- oder CLI-Befehlen basieren, die eine einfache Authentifizierung (Benutzername und Kennwort) verwenden, funktionieren weiterhin wie zuvor. Intern erfolgt die Authentifizierung durch Übergabe des Benutzernamens und des Kennworts. Diese Weitergabe des Benutzernamens und des Kennworts beeinträchtigt einige der Vorteile der Verwendung des Identitätsverbunds, da das Kennwort für vCenter Server und Ihre Skripts verfügbar gemacht werden. Migrieren Sie nach Möglichkeit zu einer token-basierten Authentifizierung.

vCenter Server-Verwaltungsschnittstelle

Wenn der Benutzer ein Mitglied der Administratorgruppe ist, wird der Zugriff auf die vCenter Server-Verwaltungsschnittstelle (früher als vCenter Server Appliance-Verwaltungsschnittstelle oder VAMI bezeichnet) unterstützt.

Eingeben von Benutzernamentext auf der AD FS-Anmeldeseite

Die AD FS-Anmeldeseite unterstützt keine Übergabe von Text, um das Textfeld „Benutzername“ vorab auszufüllen. Infolgedessen müssen Sie bei Verbundanmeldungen mit AD FS nach der Eingabe Ihres Benutzernamens auf der vCenter Server-Startseite und der Umleitung auf die AD FS-Anmeldeseite Ihren Benutzernamen auf der AD FS-Anmeldeseite erneut eingeben. Der Benutzername, den Sie auf der vCenter Server-Startseite eingeben, wird benötigt, um die Anmeldung an den entsprechenden Identitätsanbieter umzuleiten, und der Benutzername auf der AD FS-Anmeldeseite ist für die Authentifizierung bei AD FS erforderlich. Diese Unfähigkeit, den Benutzernamen an die AD FS-Anmeldeseite zu übergeben, ist eine Einschränkung von AD FS. Sie können dieses Verhalten nicht direkt über vCenter Server konfigurieren oder ändern.

vCenter Server-Identitätsanbieterverbund-Lebenszyklus

Bei der Verwaltung des Lebenszyklus des vCenter Server-Identitätsanbieterverbunds gelten einige besondere Überlegungen.

Sie können den Lebenszyklus Ihres vCenter Server-Identitätsanbieterverbunds auf folgende Arten verwalten.

Migrieren von der Verwendung von Active Directory zu AD FS

Wenn Sie Active Directory als Identitätsquelle für vCenter Server verwenden, ist die Migration zur Verwendung von AD FS komplikationslos. Wenn Ihre Active Directory-Gruppen und -Rollen mit Ihren AD FS-Gruppen und -Rollen übereinstimmen, müssen Sie keine zusätzlichen Maßnahmen ergreifen. Wenn die Gruppen und Rollen nicht übereinstimmen, müssen Sie zusätzliche Aufgaben durchführen. Wenn der vCenter Server ein Domänenmitglied ist, sollten Sie ihn aus der Domäne entfernen, da er für den Identitätsverbund nicht benötigt oder verwendet wird.

Domänenübergreifendes Neuverweisen und Migration

Der vCenter Server-Identitätsanbieterverbund unterstützt die domänenübergreifende Neuverweisung, das heißt, das Verschieben eines vCenter Server von einer vSphere SSO-Domäne in eine andere. Der neu verwiesene vCenter Server erhält die replizierte AD FS-Konfiguration von den vCenter Server-Systemen, auf die er zuvor verwies.

Im Allgemeinen müssen Sie keine zusätzliche AD FS-Neukonfiguration für eine domänenübergreifende Neuverweisung durchführen, es sei denn, eine der folgenden Bedingungen ist erfüllt.

1 Die AD FS-Konfiguration des neu verwiesenen vCenter Server unterscheidet sich von der AD FS-Konfiguration des vCenter Server, auf den zuvor verwiesen wurde.

2 Dies ist das erste Mal, dass der neu verwiesene vCenter Server eine AD FS-Konfiguration erhält.

In diesen Fällen müssen Sie die Umleitungs-URIs des vCenter Server-Systems zur entsprechenden Anwendungsgruppe auf dem AD FS-Server hinzufügen. Wenn beispielsweise vCenter Server 1 mit AD FS-Anwendungsgruppe A (oder ohne AD FS-Konfiguration) neu auf vCenter Server 2 mit AD FS-Anwendungsgruppe B verwiesen wird, müssen Sie die Umleitungs-URIs von vCenter Server 1 zu Anwendungsgruppe B hinzufügen.

Konfigurieren des vCenter Server-Identitätsanbieterverbunds

Nachdem Sie vCenter Server anfänglich bereitgestellt haben, können Sie einen externen Identitätsanbieter für die Verbundauthentifizierung konfigurieren.

Sie konfigurieren den vCenter Server-Identitätsanbieterverbund über den vSphere Client oder die API. Sie müssen auch einige Konfigurationsschritte auf Ihrem externen Identitätsanbieter durchführen. Um vCenter Server-Identitätsanbieterverbund 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.

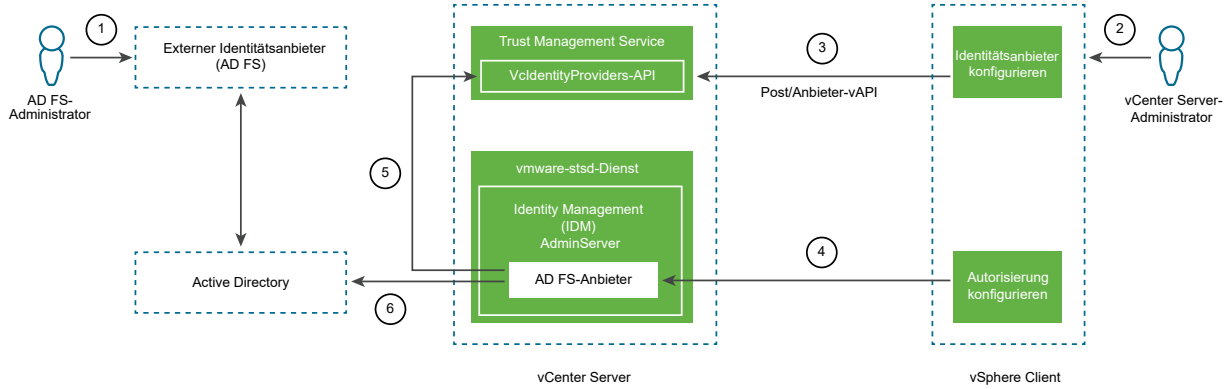
Prozessablauf bei der Konfiguration des vCenter Server-Identitätsanbieterverbunds

Zur wirksamen Konfiguration eines vCenter Server-Identitätsanbieterverbunds müssen Sie sich mit den stattfindenden Kommunikationsabläufen vertraut machen.

Prozessablauf bei der Konfiguration des vCenter Server-Identitätsanbieterverbunds

Die folgende Abbildung zeigt den Prozessablauf beim Konfigurieren eines vCenter Server-Identitätsanbieterverbunds.

Abbildung 4-5. Prozessablauf bei der Konfiguration des vCenter Server-Identitätsanbieterverbunds



vCenter Server, AD FS und Active Directory interagieren folgendermaßen.

1 Der AD FS-Administrator konfiguriert eine AD FS-OAuth-Anwendung für vCenter Server.

2 Der vCenter Server-Administrator meldet sich mit dem vSphere Client bei vCenter Server an.

3 Der vCenter Server-Administrator fügt einen AD FS-Identitätsanbieter zu vCenter Server hinzu und gibt zusätzlich Informationen zur Active Directory-Domäne ein.

   vCenter Server benötigt diese Informationen, um eine LDAP-Verbindung zur Active Directory-Domäne des AD FS-Servers herzustellen. Mit dieser Verbindung sucht vCenter Server nach Benutzern und Gruppen und fügt sie im nächsten Schritt zu lokalen vCenter Server-Gruppen hinzu. Weitere Informationen finden Sie in folgendem Abschnitt mit dem Titel „Durchsuchen der Active Directory-Domäne“.

4 Der vCenter Server-Administrator konfiguriert Autorisierungsberechtigungen in vCenter Server für AD FS-Benutzer.

5 Der AD FS-Anbieter fragt die VcIdentityProviders-API ab, um die LDAP-Verbindungsinformationen für die Active Directory-Quelle zu erhalten.

6 Der AD FS-Anbieter durchsucht Active Directory nach den abgefragten Benutzern oder Gruppen, um die Autorisierungskonfiguration abzuschließen.

Durchsuchen der Active Directory-Domäne

Sie konfigurieren AD FS als externen Identitätsanbieter in vCenter Server, indem Sie den Assistenten zum Konfigurieren des Hauptidentitätsanbieters im vSphere Client verwenden. Im Rahmen des Konfigurationsprozesses müssen Sie Informationen zur Active Directory-Domäne eingeben, einschließlich Informationen zum DN (Distinguished Name) des Benutzers und der Gruppe. Wenn Sie AD FS für die Authentifizierung konfigurieren, müssen Sie Informationen zu dieser Active Directory-Verbindung angeben. Diese Verbindung ist erforderlich, um nach Active Directory-Benutzernamen und -Gruppen zu suchen und diese Rollen und Berechtigungen in vCenter Server zuzuordnen, während AD FS für die Authentifizierung des Benutzers verwendet

wird. In diesem Schritt des Assistenten zum Konfigurieren des Hauptidentitätsanbieters wird keine Active Directory über LDAP-Identitätsquelle erstellt. Stattdessen verwendet vCenter Server diese Informationen, um eine gültige durchsuchbare Verbindung mit Ihrer Active Directory-Domäne herzustellen, in der nach Benutzern und Gruppen gesucht werden kann.

Überlegen Sie sich ein Beispiel, in dem die folgenden DN-Einträge verwendet werden:

- Basis-DN (Distinguished Name) für Benutzer: cn=Users,dc=corp,dc=local
- Basis-DN (Distinguished Name) für Gruppen: dc=corp,dc=local
- Benutzername: cn=Administrator,cn=Users,dc=corp,dc=local

Wenn der Benutzer „AdfsUser@corp.local“ ein Mitglied der Gruppe „ADGroup@corp.local“ ist, kann ein vCenter Server-Administrator durch Eingabe dieser Informationen im Assistenten nach der Gruppe „ADGroup@corp.local“ suchen und sie zur vCenter Server-Gruppe „Administrators@vsphere.local“ hinzufügen. Folglich werden dem Benutzer „AdfsUser@corp.local“ bei der Anmeldung Administratorrechte in vCenter Server eingeräumt.

vCenter Server verwendet diesen Suchlauf auch, wenn Sie globale Berechtigungen für Active Directory-Benutzer und -Gruppen konfigurieren. In beiden Fällen – entweder beim Konfigurieren globaler Berechtigungen oder beim Hinzufügen eines Benutzers oder einer Gruppe – wählen Sie im Dropdown-Menü **Domäne** die Domäne aus, die Sie für Ihren AD FS-Identitätsanbieter eingegeben haben, um nach Benutzern und Gruppen in Ihrer Active Directory-Domäne zu suchen und diese auszuwählen.

Verwenden des Speichers für vertrauenswürdige Root-Zertifikate anstelle des JRE-Truststore

Wenn Sie ein CA-Root-Zertifikat, das von Ihre eigenen internen Zertifizierungsstelle ausgestellt wurde, in vSphere 7.0 in den JRE-Truststore importiert haben, können Sie ab vSphere 7.0 Update 1 das Zertifikat im Speicher für vertrauenswürdige Root-Zertifikate registrieren.

Um vCenter Server-Identitätsanbieterverbund in vSphere 7.0 mit einem Stamm-CA-Zertifikat zu konfigurieren, das von Ihrer eigenen internen Zertifizierungsstelle ausgestellt wurde, mussten Sie es in den JRE-Truststore importieren. Ab vSphere 7.0 Update 1 können Sie das Zertifikat im Speicher für vertrauenswürdige Root-Zertifikate registrieren. Diese Änderung bedeutet, dass Sie das CA-Root-Zertifikat, das von Ihrer eigenen internen Zertifizierungsstelle ausgestellt wurde, dem Speicher für vertrauenswürdige Root-Zertifikate hinzufügen sollten (auch als VMware Endpoint Certificate Store bzw. VECS bezeichnet). Zertifikate im JRE-Truststore funktionieren zwar weiterhin, vCenter Server wird aber für die Verwendung des Speichers für vertrauenswürdige Root-Zertifikate standardisiert.

Verfahren

1. Melden Sie sich mit vSphere Client bei vCenter Server an.
2. Navigieren Sie zu **Verwaltung > Zertifikate > Zertifikatsverwaltung**.
3. Klicken Sie unter **Vertrauenswürdige Root-Zertifikate** auf **Hinzufügen**.

4 Suchen Sie nach dem AD FS-Root-Zertifikat und klicken Sie auf **Hinzufügen**.

Das Zertifikat wird in einem Bereich unter **Vertrauenswürdige Root-Zertifikate** hinzugefügt.

Konfigurieren des vCenter Server-Identitätsanbieterverbunds für AD FS

Nach der Installation oder dem Upgrade auf vSphere 7.0 oder höher können Sie den vCenter Server-Identitätsanbieterverbund konfigurieren.

vCenter Server unterstützt nur einen konfigurierten externen Identitätsanbieter (eine Quelle) und die Identitätsquelle „vsphere.local“. Sie können nicht mehrere externe Identitätsanbieter verwenden. Der vCenter Server-Identitätsanbieterverbund verwendet OpenID Connect (OIDC) für die Benutzeranmeldung bei vCenter Server.

In dieser Aufgabe wird das Hinzufügen einer AD FS-Gruppe zur vSphere-Administratorengruppe als Möglichkeit zur Steuerung von Berechtigungen beschrieben. Sie können Berechtigungen auch mithilfe von AD FS-Autorisierung über globale oder Objektberechtigungen in vCenter Server konfigurieren. Weitere Informationen zum Hinzufügen von Berechtigungen finden Sie in der *vSphere-Sicherheit*-Dokumentation.

Vorsicht Wenn Sie eine Identitätsquelle von Active Directory verwenden, die Sie zuvor vCenter Server für Ihre AD FS hinzugefügt haben, löschen Sie diese vorhandene Identitätsquelle nicht von vCenter Server. Dies führt zu einer Regression mit zuvor zugewiesenen Rollen und Gruppenmitgliedschaften. Sowohl der AD FS-Benutzer mit globalen Berechtigungen als auch die Benutzer, die der Administratorgruppe hinzugefügt wurden, werden sich nicht anmelden können.

Problemumgehung: Wenn Sie die zuvor zugewiesenen Rollen und Gruppenmitgliedschaften nicht benötigen und die vorherige Identitätsquelle für Active Directory entfernen möchten, entfernen Sie die Identitätsquelle, bevor Sie den AD FS-Anbieter erstellen, und konfigurieren Sie Gruppenmitgliedschaften in vCenter Server.

Voraussetzungen

Anforderungen der Active Directory Federation Services (AD FS):

- AD FS für Windows Server 2016 oder höher muss bereits bereitgestellt worden sein.
- AD FS muss mit Active Directory verbunden sein.
- Eine Anwendungsgruppe für vCenter Server muss im Rahmen des Konfigurationsvorgangs in AD FS erstellt werden. Informationen finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/78029.
- Ein AD FS-Root-CA-Zertifikat, das zum Speicher vertrauenswürdiger Stammzertifikate (auch als VMware-Zertifikatspeicher bezeichnet) hinzugefügt wird.
- Sie haben eine vCenter Server-Administratorengruppe in AD FS erstellt, die die Benutzer enthält, denen vCenter Server-Administratorrechte zugewiesen werden sollen.

Weitere Informationen zum Konfigurieren von AD FS finden Sie in der Microsoft-Dokumentation.

vCenter Server und sonstige Anforderungen:

- vSphere 7.0 oder höher
- vCenter Server muss in der Lage sein, eine Verbindung mit dem Ermittlungs-Endpoint für AD FS sowie der Autorisierung, dem Token, der Abmeldung, JWKS und allen anderen Endpoints, die in den Metadaten des Ermittlungs-Endpoints angegeben wurden, herzustellen.
- Sie benötigen das Recht **VcIdentityProviders.Verwalten** zum Erstellen, Aktualisieren oder Löschen eines vCenter Server-Identitätsanbieters, der für die Verbundauthentifizierung erforderlich ist. Um die Rechte eines Benutzers auf die Ansicht der Konfigurationsinformationen für den Identitätsanbieter zu beschränken, weisen Sie ihm das Recht **VcIdentityProviders.Lesen** zu.

Verfahren

1. Melden Sie sich mit vSphere Client bei vCenter Server an.
2. Fügen Sie dem vertrauenswürdigen Stammzertifikatspeicher Ihr AD FS-Root-CA-Zertifikat hinzu.
   a. Navigieren Sie zu **Verwaltung > Zertifikate > Zertifikatsverwaltung**.
   b. Klicken Sie neben **Vertrauenswürdiger Stammspeicher** auf **Hinzufügen**.
   c. Suchen Sie nach dem AD FS-Root-Zertifikat und klicken Sie auf **Hinzufügen**.

      Das Zertifikat wird in einem Bereich unter **Vertrauenswürdige Root-Zertifikate** hinzugefügt.
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 die Registerkarte **Identitätsanbieter** aus und erhalten Sie die Umleitungs-URIs.
   a. Klicken Sie auf das **Symbol** „i“ neben dem Link „Identitätsanbieter ändern“.

      Im Pop-up-Fenster werden zwei Umleitungs-URIs angezeigt.
   b. Kopieren Sie beide URIs in eine-Datei oder notieren Sie sie zur späteren Verwendung in den nachfolgenden Schritten, um den AD FS-Server zu konfigurieren.
   c. Schließen Sie das Pop-up-Fenster.
5. Erstellen Sie eine OpenID Connect-Konfiguration in AD FS und konfigurieren Sie sie für vCenter Server.

   Zum Einrichten einer Vertrauensstellung der vertrauenden Seite zwischen vCenter Server und einem Identitätsanbieter müssen Sie Identifzierungsinformationen und einen gemeinsamen geheimen Schlüssel zwischen ihnen festlegen. In AD FS erstellen Sie hierzu eine als Anwendungsgruppe bezeichnete OpenID Connect-Konfiguration, die aus einer Serveranwendung und einer Web-API besteht. Die beiden Komponenten enthalten die

Informationen, die von vCenter Server zum Herstellen von Vertrauen und zur Kommunikation mit dem AD FS-Server verwendet werden. Informationen zum Aktivieren von OpenID Connect in AD FS finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/78029.

Beachten Sie Folgendes, wenn Sie die Anwendungsgruppe AD FS erstellen.

- Für die Umleitung benötigen Sie die beiden URIs, die Sie erhalten und im vorherigen Schritt gespeichert haben.
- Kopieren Sie die folgenden Informationen in eine Datei oder notieren Sie sie für die Verwendung bei der Konfiguration des vCenter Server-Identitätsanbieters im nächsten Schritt.
  - Clientbezeichner
  - Gemeinsamer geheimer Schlüssel
  - OpenID-Adresse des AD FS-Servers

6 Erstellen Sie einen Identitätsanbieter auf vCenter Server.

a Kehren Sie zur Registerkarte **Identitätsanbieter** in vSphere Client zurück.

b Klicken Sie auf den Link „Identitätsanbieter ändern“.

Der Assistent „Hauptidentitätsanbieter konfigurieren“ wird geöffnet.

c Wählen Sie **Microsoft ADFS** aus und klicken Sie auf **Weiter**.

Geben Sie die Informationen ein, die Sie zuvor für die folgenden Textfelder gesammelt haben:

- Clientbezeichner
- Gemeinsamer geheimer Schlüssel
- OpenID-Adresse des AD FS-Servers

d Klicken Sie auf **Weiter**.

e Geben Sie die Benutzer- und Gruppeninformationen für die Verbindung mit Active Directory über LDAP ein, um nach Benutzern und Gruppen zu suchen.

vCenter Server leitet die AD-Domäne, die für Autorisierung und Berechtigungen verwendet werden soll, aus dem Basis-DN für Benutzer ab. Sie können Berechtigungen für vSphere-Objekte nur für Benutzer und Gruppen aus dieser AD-Domäne hinzufügen. Benutzer oder Gruppen aus untergeordneten AD-Domänen oder anderen Domänen in der AD-Gesamtstruktur werden vom vCenter Server-Identitätsanbieterverbund nicht unterstützt.

Option	Beschreibung
Basis-DN für Benutzer	Basis-DN (Distinguished Name) für Benutzer.
Basis-DN für Gruppen	Der Basis-DN (Distinguished Name) für Gruppen.
Benutzername	ID eines Benutzers in der Domäne, der über einen minimalen Base-DN-Zugriff (nur Lesen) für Benutzer und Gruppen verfügt
Kennwort	ID eines Benutzers in der Domäne, der über einen minimalen Base-DN-Zugriff (nur Lesen) für Benutzer und Gruppen verfügt
URL des primären Servers:	LDAP-Server des primären Domänencontrollers für die Domäne. Verwenden Sie das Format **`ldap://hostname:port`** oder **`ldaps://hostname: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. 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`**.

f Klicken Sie zum Überprüfen der Informationen auf **Weiter** und dann auf **Beenden**.

7 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**.

8 Konfigurieren Sie den vCenter Server der Gruppenmitgliedschaft für AD FS-Autorisierung.

a Klicken Sie auf die Registerkarte **Gruppen**.

b Klicken Sie auf die Gruppe **Administratoren** und klicken Sie auf **Mitglieder hinzufügen**.

c Wählen Sie die Domäne im Dropdown-Menü aus.

d Geben Sie im Textfeld unterhalb des Dropdown-Menü die ersten Zeichen der hinzuzufügenden AD FS-Gruppe ein und warten Sie dann, bis die Dropdown-Auswahl angezeigt wird.

   Es kann einige Sekunden dauern, bis die Auswahl angezeigt wird, da vCenter Server die Verbindung mit Active Directory herstellt und dieses durchsucht.

e Wählen Sie die AD FS-Gruppe aus und fügen Sie sie zur Administratorengruppe hinzu.

f Klicken Sie auf **Speichern**.

9 Überprüfen Sie die Anmeldung bei vCenter Server mit einem Active Directory-Benutzer.

Grundlegendes zu vCenter Single Sign On

Wenn Sie keinen externen Identitätsanbieter verwenden, müssen Sie die zugrunde liegende Architektur des integrierten Identitätsanbieters vCenter Single Sign On und deren Auswirkungen auf die Installation und Upgrades verstehen.

Komponenten für vCenter Single Sign On

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

Während der Installation werden die folgenden Komponenten als Teil einer vCenter Server-Bereitstellung 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 Server unterstützten Identitätsquellentypen dar. Die SAML-Token ermöglichen interaktiven, Skript- und Dienstbenutzern (einschließlich Lösungsbenutzern), die sich erfolgreich bei vCenter Single Sign On authentifizieren, alle von vCenter Single Sign On unterstützten vCenter-Dienste 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 Client verwalten. Anfänglich hat nur der Benutzer „administrator@*ihr_domänenname*“ diese Berechtigungen. Sie können die vSphere-Domäne bei der Installation von vCenter Server ändern. Benennen Sie die Domäne nicht mit Ihrem Microsoft Active Directory- oder OpenLDAP-Domänennamen.

VMware Directory Service (vmdir)

Ein VMware-Verzeichnisdienst (vmdir) ist der während der Installation angegebenen Domäne zugeordnet und wird in jede vCenter Server-Bereitstellung eingeschlossen. Bei diesem Dienst handelt es sich um einen mehrmandantenfähigen Verzeichnisdienst mit Peer-Replikation, der ein LDAP-Verzeichnis auf Port 389 zur Verfügung stellt. Darüber hinaus werden mithilfe dieses Diensts vCenter Single Sign On-Benutzerkonten und -Kennwörter gespeichert und verwaltet, die mit dem SHA-512-Hashing-Algorithmus gesichert werden.

Wenn in Ihrer Umgebung mehrere Instanzen von vCenter Server im verknüpften Modus konfiguriert sind, wird eine Aktualisierung des vmdir-Inhalts in einer vmdir-Instanz an alle anderen Instanzen von vmdir weitergegeben.

Der VMware Directory Service speichert nicht nur vCenter Single Sign On-Informationen, sondern auch Zertifikatsinformationen.

Identitäts-Verwaltungsdienst

Bearbeitete Identitätsquellen und STS-Authentifizierungsanforderungen.

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 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. 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.

vCenter Single Sign On-Administratorbenutzer

Die vCenter Single Sign On-Verwaltungsschnittstelle ist vom vSphere Client aus 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.

Andere Benutzerkonten

Die folgenden Benutzerkonten werden automatisch innerhalb von vCenter Server in der vsphere.local.domain (oder der Standarddomäne, die Sie bei der Installation erstellt haben) erstellt. Bei diesen Benutzerkonten handelt es sich um Shell-Konten. Die vCenter Single Sign On-Kennwortrichtlinie gilt nicht für diese Konten.

Tabelle 4-1. Andere vSphere-Benutzerkonten

Konto	Beschreibung
K/M	Für die Kerberos-Schlüsselverwaltung.
krbtgt/VSPHERE.LOCAL	Für die Kompatibilität mit integrierter Windows-Authentifizierung.
waiter-*random_string*	Für Auto Deploy.

ESXi-Benutzer

Eigenständige ESXi-Hosts sind nicht in vCenter Single Sign On 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, ESXCLI 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 zu vSphere 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.

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. 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.

Vorsicht 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 4-2. Gruppen in der Domäne „vsphere.local“

Recht	Beschreibung
Benutzer	Benutzer in der vCenter Single Sign On-Domäne (standardmäßig „vsphere.local“).
SolutionUsers	Gruppe der Lösungsbenutzer für vCenter-Dienste. 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. **Hinweis** Verwalten Sie den Domänencontroller nicht direkt. Verwenden Sie für die entsprechenden Aufgaben stattdessen die `vmdir`-CLI oder den vSphere Client.
SystemConfiguration.BashShellAdministrators	Ein Benutzer in dieser Gruppe kann den Zugriff auf die BASH-Shell aktivieren und deaktivieren. Standardmäßig können Benutzer, die sich über SSH mit dem vCenter Server verbinden, nur Befehle in der eingeschränkten Shell verwenden. Benutzer in dieser Gruppe haben hingegen Zugriff auf die BASH-Shell.

Tabelle 4-2. Gruppen in der Domäne „vsphere.local“ (Fortsetzung)

Recht	Beschreibung
ActAsUsers	Mitglieder der Gruppe „Act-As Users“ dürfen Act-As-Token aus vCenter Single Sign On abrufen.
ExternalIDPUsers	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. **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.
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.
TrustedAdmins	Mitglieder dieser Gruppe können Konfigurations- und Verwaltungsaufgaben in VMware® vSphere Trust Authority™ durchführen. Standardmäßig enthält diese Gruppe keine Mitglieder. Sie müssen dieser Gruppe ein Mitglied hinzufügen, damit Sie vSphere-Trust Authority-Aufgaben durchführen können.
AutoUpdate	Diese Gruppe wird intern für das vCenter Cloud-Gateway verwendet.
SyncUsers	Diese Gruppe wird intern für das vCenter Cloud-Gateway verwendet.
vSphereClientSolutionUsers	Diese Gruppe wird intern für den vSphere Client verwendet.
ServiceProviderUsers	Mitglieder dieser Gruppe können die Infrastruktur von vSphere with Tanzu und VMware Cloud on AWS verwalten.
NsxAdministrators	Diese Gruppe wird für NSX verwendet.
WorkloadStorage	Arbeitslastspeichergruppe.
RegistryAdministrators	Mitglieder dieser Gruppe können die Registrierung verwalten.
NsxAuditors	Diese Gruppe wird für NSX verwendet.
NsxViAdministrators	Diese Gruppe wird für NSX verwendet.

Tabelle 4-2. Gruppen in der Domäne „vsphere.local“ (Fortsetzung)

Recht	Beschreibung
SystemConfiguration.SupportUsers	Mitglieder der Gruppe „SystemConfiguration.SupportUsers“ können auf die API des Support-Pakets zugreifen.
SystemConfiguration.ReadOnly	Mitglieder dieser Gruppe können auf schreibgeschützte Vorgänge der vCenter Server Appliance zugreifen.

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.

Hinweis Ab vSphere 7.0 Update 2 können Sie FIPS auf dem vCenter Server aktivieren. Informationen finden Sie in der Dokumentation *vSphere-Sicherheit*. AD über LDAP und IWA werden nicht unterstützt, wenn FIPS aktiviert ist. Verwenden Sie einen externen Identitätsanbieterverbund im FIPS-Modus. Weitere Informationen hierzu finden Sie unter Konfigurieren des vCenter Server-Identitätsanbieterverbunds.

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 verfügt jede Instanz von vCenter Single Sign On über die Identitätsquelle *your_domain_name*, z. B. „vsphere.local“. Diese Identitätsquelle befindet sich innerhalb von vCenter Single Sign On.

Hinweis Es ist jeweils immer nur eine Standarddomäne vorhanden. Wenn sich ein Benutzer aus einer Nicht-Standarddomäne anmeldet, muss dieser Benutzer den Domänennamen hinzufügen, um erfolgreich authentifiziert zu werden. Der Domänenname weist die folgende Form auf:

```
DOMAIN\user
```

Die folgenden Identitätsquellen sind verfügbar.

- Active Directory über LDAP. vCenter Single Sign On unterstützt mehrere Active Directory-über LDAP-Identitätsquellen.
- Active Directory (Integrierte Windows-Authentifizierung Authentication) 2003 und höher. Mithilfe von 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.
- OpenLDAP Version 2.4 und höher. vCenter Single Sign On unterstützt mehrere OpenLDAP-Identitätsquellen.

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.

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 vSphere Client bei vCenter Server an.
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 der Registerkarte **Identitätsanbieter** auf **Identitätsquellen**, wählen Sie eine Identitätsquelle aus und klicken Sie auf **Als Standard festlegen**.
5. Klicken Sie auf **OK**.

   In der Domänenansicht wird „(Standard)“ in der Spalte „Typ“ 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 Active Directory über LDAP, eine native Active Directory-Domäne (Integrierte Windows-Authentifizierung) oder ein OpenLDAP-Verzeichnisdienst sein. Weitere Informationen hierzu finden Sie unter Identitätsquellen für vCenter Server mit vCenter Single Sign On.

Unmittelbar nach der Installation ist die Domäne „vsphere.local“ (oder die Domäne, die Sie während der Installation angegeben haben) mit den internen vCenter Single Sign On-Benutzern verfügbar.

Hinweis Wenn Sie Ihr Active Directory-SSL-Zertifikat aktualisiert oder ersetzt haben, müssen Sie die Identitätsquelle entfernen und erneut in vCenter Server hinzufügen.

Voraussetzungen

Wenn Sie eine Active Directory-Identitätsquelle (Integrierte Windows-Authentifizierung) hinzufügen, muss sich der vCenter Server in der Active Directory-Domäne befinden. Weitere Informationen hierzu finden Sie unter Hinzufügen von vCenter Server zu einer Active Directory-Domäne.

Verfahren

1. Melden Sie sich mit vSphere Client bei vCenter Server an.
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 der Registerkarte **Identitätsanbieter** auf **Identitätsquellen** und dann auf **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. Weitere Informationen hierzu finden Sie unter Einstellungen der Active Directory-Identitätsquelle.
Active Directory über LDAP	Diese Option setzt voraus, dass Sie den Domänencontroller und andere Informationen angeben. Weitere Informationen hierzu finden Sie unter Einstellungen der Active Directory-Identitätsquelle über 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 über LDAP-Server und OpenLDAP-Server.

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

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*.

Einstellungen der Active Directory-Identitätsquelle über 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 4-3. Einstellungen für Active Directory über LDAP und OpenLDAP

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.
Domänenalias	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. 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: ■ UPN (user@domain.com) ■ NetBIOS (DOMAIN\user) ■ DN (cn=user,cn=Users,dc=domain,dc=com) 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 4-3. Einstellungen für Active Directory über LDAP und OpenLDAP (Fortsetzung)

Option	Beschreibung
URL des primären Servers	LDAP-Server des primären Domänencontrollers für die Domäne. Sie können entweder den Hostnamen oder die IP-Adresse verwenden. 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. 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. Sie können entweder den Hostnamen oder die IP-Adresse verwenden.
Zertifikate (für LDAPS)	Wenn Sie LDAPS mit Ihrer Active Directory LDAP-Server- oder OpenLDAP-Serveridentitätsquelle verwenden möchten, klicken Sie auf **`Durchsuchen`** und wählen Sie ein Zertifikat aus, das aus dem in der LDAPS-URL angegebenen Domänencontroller exportiert wurde. (Beachten Sie, dass es sich bei dem hier verwendeten Zertifikat nicht um ein Stamm-CA-Zertifikat handelt.) Informationen zum Exportieren des Zertifikats aus Active Directory finden Sie in der Microsoft-Dokumentation.

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 (Integrierte Windows-Authentifizierung)

Sie können vCenter Single Sign On so einrichten, dass nur dann eine Active Directory-Identitätsquelle (Integrierte Windows-Authentifizierung) verwendet wird, wenn diese Identitätsquelle verfügbar ist. Folgen Sie den Anweisungen in der Dokumentation zur *vCenter Server-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.

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 4-4. 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.
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.

Tabelle 4-4. Hinzufügen von Einstellungen der Identitätsquelle (Fortsetzung)

Textfeld	Beschreibung
SPN (Dienstprinzipalname)	Der SPN, mit dem Kerberos den Active Directory-Dienst identifiziert. Schließen Sie die Domäne in den Namen ein. Beispiel: „`STS/example.com`“. Der SPN muss innerhalb der Domäne eindeutig sein. Durch Ausführen des Befehls `setspn -S` wird sichergestellt, dass keine Duplikate erstellt werden. Weitere Informationen zu `setspn` finden Sie in der Microsoft-Dokumentation.
UPN (Benutzerprinzipalname) **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.

Hinzufügen oder Entfernen einer Identitätsquelle mithilfe der CLI

Sie können das Dienstprogramm `sso-config` verwenden, um eine Identitätsquelle hinzuzufügen oder zu entfernen.

Bei einer Identitätsquelle kann es sich um eine native Active Directory-Domäne (integrierte Windows-Authentifizierung), AD über LDAP, AD über LDAP unter Verwendung von LDAPS (LDAP über SSL) oder OpenLDAP handeln. Weitere Informationen hierzu finden Sie unter Identitätsquellen für vCenter Server mit vCenter Single Sign On. Sie können auch das Dienstprogramm `sso-config` verwenden, um die Smartcard- und RSA SecurID-Authentifizierung einzurichten.

Voraussetzungen

Wenn Sie eine Active Directory-Identitätsquelle hinzufügen, muss sich der vCenter Server in der Active Directory-Domäne befinden. Weitere Informationen hierzu finden Sie unter Hinzufügen von vCenter Server zu einer Active Directory-Domäne.

Aktivieren Sie die SSH-Anmeldung. Weitere Informationen hierzu finden Sie unter Verwalten von vCenter Server über die vCenter Server-Shell.

Verfahren

1. Verwenden Sie SSH oder eine andere Remotekonsolenverbindung, um eine Sitzung auf dem vCenter Server-System zu starten.
2. Melden Sie sich als „root“ an.
3. Wechseln Sie in das Verzeichnis, in dem sich das Dienstprogramm `sso-config` befindet.

```
cd /opt/vmware/bin
```

4 Beispiele für die Verwendung erhalten Sie, indem Sie die `sso-config`-Hilfe durch Ausführung von `sso-config.sh -help` aufrufen oder den VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/67304 lesen.

Verwenden von vCenter Single Sign On mit Windows-Sitzungsauthentifizierung

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

Voraussetzungen

- Hinzufügen von vCenter Server zu einer Active Directory-Domäne Weitere Informationen hierzu finden Sie unter Hinzufügen von vCenter Server 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.
- Stellen Sie sicher, dass das erweiterte Authentifizierungs-Plug-In installiert ist. Siehe *Installation und Einrichtung von vCenter Server*.

Hinweis Wenn Sie vCenter Server für die Verwendung der Verbundauthentifizierung mit Active Directory Federation Services konfigurieren, gilt das Plug-In für erweiterte Authentifizierung nur für Konfigurationen, bei denen vCenter Server der Identitätsanbieter ist (Konfigurationen mit Active Directory über LDAP, integrierter Windows-Authentifizierung und OpenLDAP).

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“.

Verwalten des vCenter Server-Security Token Service

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

Als Token-Aussteller verwendet der Security Token Service einen privaten Schlüssel zum Signieren von Token und veröffentlicht die öffentlichen Zertifikate für Dienste, um die Token-Signatur zu überprüfen. Der vCenter Server verwaltet die STS-Signaturzertifikate und speichert sie im VMware Directory Service (vmdir). Token können eine beträchtliche Lebensdauer haben und historisch gesehen mit einem beliebigen von mehreren Schlüsseln signiert worden sein.

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

Lösungsbenutzer

Gültiges Zertifikat.

Andere Benutzer

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

STS authentifiziert den Benutzer anhand der primären Anmeldedaten und erstellt ein SAML-Token mit Benutzerattributen.

Standardmäßig generiert VMware Certificate Authority (VMCA) das STS-Signaturzertifikat. Sie können das STS-Signaturzertifikat mit einem neuen VMCA-Zertifikat aktualisieren. Sie können das standardmäßige STS-Signaturzertifikat auch durch ein benutzerdefiniertes oder von Einem Drittanbieter generiertes STS-Signaturzertifikat importieren und ersetzen. Ersetzen Sie das STS-Signaturzertifikat nur dann, wenn die Sicherheitsrichtlinien Ihres Unternehmens das Ersetzen aller Zertifikate erfordern.

Mithilfe des vSphere Client können Sie folgende Aktionen ausführen:

- STS-Zertifikate aktualisieren
- Benutzerdefinierte STS-Zertifikate und von Drittanbietern generierte STS-Zertifikate importieren und ersetzen
- Details zu STS-Zertifikaten anzeigen, z. B. das Ablaufdatum

Sie können auch die Befehlszeile verwenden, um benutzerdefinierte und von Drittanbietern generierte STS-Zertifikate zu ersetzen.

STS-Zertifikatslaufzeit und -ablauf

Bei einer Neuinstallation von vSphere 7.0 Update 1 und höher wird ein STS-Signaturzertifikat mit einer Laufzeit von 10 Jahren erstellt. Wenn ein STS-Signaturzertifikat kurz vor dem Ablauf steht, werden Sie durch einen Alarm ab 90 Tagen vor Ablauf einmal pro Woche und ab 7 Tagen vor Ablauf täglich gewarnt.

Hinweis Unter bestimmten Umständen kann das Ersetzen Ihrer STS-Signaturzertifikate die Dauer der Zertifikate ändern. Achten Sie bei der Zertifikatsersetzung auf die Ausstellungs- und Ablaufdaten.

Aktualisieren eines vCenter Server-STS-Zertifikats mithilfe des vSphere Client

Sie können Ihre vCenter Server-STS-Signaturzertifikate mithilfe des vSphere Client aktualisieren. Der VMware Certificate Authority (VMCA) stellt ein neues Zertifikat aus und ersetzt das aktuelle Zertifikat.

Wenn Sie STS-Signaturzertifikate aktualisieren, stellt VMware Certificate Authority (VMCA) ein neues Zertifikat aus und ersetzt das aktuelle Zertifikat im VMware Directory Service (vmdir). STS beginnt, das neue Zertifikat zu verwenden, damit neue Token ausgegeben werden. Bei einer Konfiguration mit dem erweiterten verknüpften Modus lädt vmdir das neue Zertifikat vom ausstellenden vCenter Server-System auf alle verknüpften vCenter Server-Systeme hoch. Wenn Sie STS-Signaturzertifikate aktualisieren, müssen Sie das vCenter Server-System und alle anderen vCenter Server-Systeme neu starten, die Teil einer Konfiguration mit dem erweiterten verknüpften Modus sind.

Falls Sie ein benutzerdefiniertes generiertes STS-Signaturzertifikat oder ein STS-Signaturzertifikat eines Drittanbieters verwenden, wird dieses Zertifikat bei der Aktualisierung mit einem von VMCA ausgestellten Zertifikat überschrieben. Um benutzerdefinierte generierte STS-Signaturzertifikate oder STS-Signaturzertifikate von Drittanbietern zu aktualisieren, verwenden Sie die Option zum Importieren und Ersetzen. Weitere Informationen finden Sie unter Importieren und Ersetzen eines vCenter Server-STS-Zertifikats mithilfe des vSphere Client.

Das von VMCA ausgestellte STS-Signaturzertifikat ist 10 Jahre lang gültig und ist kein externes Zertifikat. Ersetzen Sie dieses Zertifikat nur dann, wenn die Sicherheitsrichtlinien Ihres Unternehmens dies erfordern.

Voraussetzungen

Für die Zertifikatsverwaltung müssen Sie das Kennwort des Administrators für die lokale Domäne angeben (standardmäßig administrator@vsphere.local). Beim Verlängern von Zertifikaten 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 vSphere Client bei vCenter Server an.
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. Wenn Sie vom System aufgefordert werden, geben Sie die Anmeldedaten Ihres vCenter Server ein.

5 Klicken Sie unter **STS-Signaturzertifikat** auf **Aktionen > Mit vCenter-Zertifikat aktualisieren**.

Falls Sie ein benutzerdefiniertes generiertes STS-Signaturzertifikat oder ein STS-Signaturzertifikat eines Drittanbieters verwenden, wird dieses Zertifikat bei der Aktualisierung mit einem von VMCA generierten Zertifikat überschrieben.

Hinweis Wenn Sie aus Konformitätsgründen Zertifikate von Drittanbietern verwendet haben, kann die Aktualisierung dazu führen, dass Ihre vCenter Server-Systeme anschließend nicht mehr konform sind. Darüber hinaus nutzt der Security Token Service, wenn Sie ein benutzerdefiniertes generiertes STS-Signaturzertifikat oder ein STS-Signaturzertifikat eines Drittanbieters verwenden, dieses benutzerdefinierte oder Drittanbieterzertifikat nicht mehr für die Tokensignierung.

6 Klicken Sie auf **Aktualisieren**.

VMCA aktualisiert das STS-Signaturzertifikat auf diesem vCenter Server-System und auf allen verknüpften vCenter Server-Systemen.

7 (Optional) Wenn die Schaltfläche **Aktualisierung erzwingen** angezeigt wird, hat vCenter Single Sign On ein Problem erkannt. Bevor Sie auf **Aktualisierung erzwingen** klicken, sollten Sie die folgenden potenziellen Ergebnisse berücksichtigen, die dies nach sich ziehen kann.

- Die Zertifikataktualisierung wird nur unterstützt, wenn alle betroffenen vCenter Server-Systeme mindestens über vSphere 7.0 Update 3 verfügen.
- Wenn Sie **Aktualisierung erzwingen** auswählen, müssen Sie alle vCenter Server-Systeme neu starten. Andernfalls kann die Auswahl dieser Option dazu führen, dass diese Systeme nicht mehr funktionsfähig sind.

a Falls Sie sich im Hinblick auf die Auswirkungen nicht sicher sind, klicken Sie auf **Abbrechen** und untersuchen Sie Ihre Umgebung.

b Wenn Sie wissen, mit welchen Auswirkungen zu rechnen ist, klicken Sie auf **Aktualisierung erzwingen**, um mit der Aktualisierung fortzufahren. Starten Sie dann Ihre vCenter Server-Systeme manuell neu.

Nächste Schritte

Um sicherzustellen, dass alle STS-Dienste in einer Konfiguration mit dem erweiterten verknüpften Modus die neuen Token validieren, müssen Sie die verknüpften vCenter Server-Systeme neu starten. Weitere Informationen zum Neustart des vCenter Server finden Sie in der Dokumentation *vCenter Server-Konfiguration*.

Importieren und Ersetzen eines vCenter Server-STS-Zertifikats mithilfe des vSphere Client

Sie können das vCenter Server-STS-Zertifikat mithilfe des vSphere Client importieren und durch ein benutzerdefiniertes generiertes Zertifikat oder ein Drittanbieterzertifikat ersetzen.

Um das standardmäßige STS-Signaturzertifikat zu importieren und zu ersetzen, müssen Sie zuerst ein neues Zertifikat generieren. Wenn Sie STS-Signaturzertifikate importieren und ersetzen, lädt der VMware Directory Service (vmdir) das neue Zertifikat vom ausstellenden vCenter Server-System auf alle verknüpften vCenter Server-Systeme hoch.

Das STS-Zertifikat ist kein externes Zertifikat. Ersetzen Sie dieses Zertifikat nur dann, wenn die Sicherheitsrichtlinien Ihres Unternehmens dies erfordern.

Voraussetzungen

Für die Zertifikatsverwaltung müssen Sie das Kennwort des Administrators für die lokale Domäne angeben (standardmäßig administrator@vsphere.local). Darüber hinaus müssen Sie die vCenter Single Sign On-Anmeldedaten eines Benutzers mit Administratorrechten für das vCenter Server-System eingeben.

Verfahren

1. Melden Sie sich mit vSphere Client bei vCenter Server an.
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. Wenn Sie vom System aufgefordert werden, geben Sie die Anmeldedaten Ihres vCenter Server ein.
5. Klicken Sie unter **STS-Signaturzertifikat** auf **Aktionen > Importieren und ersetzen**.
6. Wählen Sie die PEM-Datei aus.

   Die PEM-Datei enthält die Signaturzertifikatskette und den privaten Schlüssel.
7. Klicken Sie auf **Ersetzen**.

   Das STS-Signaturzertifikat wird auf diesem vCenter Server-System und auf allen verknüpften vCenter Server-Systemen ersetzt.
8. Starten Sie das vCenter Server-System und alle anderen vCenter Server-Systeme neu, die Teil einer Konfiguration mit dem erweiterten verknüpften Modus sind.

   Weitere Informationen zum Neustart des vCenter Server finden Sie in der Dokumentation *vCenter Server-Konfiguration*.

Ersetzen eines vCenter Server-STS-Zertifikats über die Befehlszeile

Sie können das vCenter Server-STS-Zertifikat über die CLI durch ein benutzerdefiniertes generiertes Zertifikat oder ein Drittanbieterzertifikat ersetzen.

Um ein im Unternehmen erforderliches Zertifikat zu verwenden oder ein Zertifikat zu aktualisieren, das fast abgelaufen ist, können Sie das vorhandene STS-Signaturzertifikat ersetzen. Um das standardmäßige STS-Signaturzertifikat zu ersetzen, müssen Sie zuerst ein neues Zertifikat generieren.

Das STS-Zertifikat ist kein externes Zertifikat. Ersetzen Sie dieses Zertifikat nur dann, wenn die Sicherheitsrichtlinien Ihres Unternehmens dies erfordern.

Vorsicht Sie müssen die hier beschriebenen Verfahren verwenden. Ersetzen Sie das Zertifikat nicht direkt im Dateisystem.

Voraussetzungen

Aktivieren Sie die SSH-Anmeldung bei vCenter Server. Weitere Informationen hierzu finden Sie unter Verwalten von vCenter Server über die vCenter Server-Shell.

Verfahren

1. Melden Sie sich bei der vCenter Server-Shell als Root-Benutzer an.
2. Erstellen Sie ein Zertifikat.
   a. 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/newsts
```

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

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

c Öffnen Sie die Kopie der Datei `certool.cfg` mit einem Befehlszeileneditor wie Vim und bearbeiten Sie sie so, dass die IP-Adresse und der Hostname des lokalen vCenter Server 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
```

d Generieren Sie den Schlüssel.

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

e 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
```

f Erstellen Sie eine PEM-Datei mit der Zertifikatskette und dem privaten Schlüssel.

```
cat newsts.cer /var/lib/vmware/vmca/root.cer sts.key > newsts.pem
```

3 Aktualisieren Sie das STS-Signaturzertifikat, z. B.:

```
/opt/vmware/bin/sso-config.sh -set_signing_cert -t vsphere.local /root/newsts/newsts.pem
```

4 Starten Sie das vCenter Server-System und alle anderen vCenter Server-Systeme neu, die Teil einer Konfiguration mit dem erweiterten verknüpften Modus sind. Weitere Informationen zum Neustart des vCenter Server finden Sie in der Dokumentation *vCenter Server-Konfiguration*.

Damit die Authentifizierung ordnungsgemäß funktioniert, müssen Sie den vCenter Server neu starten. Sowohl der STS-Dienst als auch der vSphere Client werden neu gestartet.

Anzeigen der aktiven vCenter Server-STS-Signaturzertifikatskette

Sie können den vSphere Client verwenden, um die aktive vCenter Server-STS-Signaturzertifikatskette anzuzeigen.

Sie können die folgenden Informationen zum aktiven STS-Zertifikat anzeigen.

- „Gültig bis“-Datum
- Ein grünes Häkchen für ein gültiges Zertifikat und eine Warnung mit einem orangefarbenen Häkchen für ein abgelaufenes Zertifikat
- Ein Link **Details anzeige**, um die aktive Zertifikatskette anzuzeigen

Verfahren

1. Melden Sie sich mit vSphere Client bei vCenter Server an.
2. Geben Sie den Benutzernamen und das Kennwort für einen Benutzer ein, der mindestens über Leseberechtigungen verfügt.
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. Wenn Sie vom System aufgefordert werden, geben Sie die Anmeldedaten Ihres vCenter Server ein.
5. Um Details für das aktive STS-Zertifikat anzuzeigen, klicken Sie auf **Details anzeigen**.

Ermitteln des Ablaufdatums eines LDAPS-SSL-Zertifikats

Wenn Sie Active Directory über LDAPS verwenden, können Sie ein SSL-Zertifikat für den LDAP-Datenverkehr hochladen. SSL-Zertifikate werden nach einer vordefinierten Laufzeit ungültig. Sie können das Ablaufdatum des Zertifikats anzeigen, um das Zertifikat vor seinem Ablauf zu ersetzen oder zu erneuern.

vCenter Server warnt Sie, wenn ein aktives LDAP-SSL-Zertifikat demnächst abläuft.

Sie sehen Daten zum Zertifikatsablauf nur, wenn Sie Active Directory über LDAP oder eine OpenLDAP-Identitätsquelle verwenden und eine `ldaps://`-URL für den Server angeben.

Voraussetzungen

Aktivieren Sie die SSH-Anmeldung bei vCenter Server. Weitere Informationen hierzu finden Sie unter Verwalten von vCenter Server über die vCenter Server-Shell.

Verfahren

1. Melden Sie sich beim vCenter Server als Root-Benutzer an.
2. Führen Sie den folgenden Befehl aus.

   ```
   /opt/vmware/bin/sso-config.sh -get_identity_sources
   ```

   Ignorieren Sie die SLF4J-Nachrichten.
3. Zum Festlegen des Ablaufdatums zeigen Sie die Details des SSL-Zertifikats an und überprüfen Sie das Feld `NotAfter`.

Verwalten der vCenter Single Sign On-Richtlinien

vCenter Single Sign On-Richtlinien erzwingen die Sicherheitsregeln für lokale Konten und Token im Allgemeinen. 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).

Standardmäßig laufen vCenter Single Sign On-Kennwörter für integrierte Benutzerkonten 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 .

Hinweis Das Administratorkonto (administrator@vsphere.local) wird nicht gesperrt und sein Kennwort läuft nicht ab. Eine gute Sicherheitspraxis besteht darin, Anmeldungen über dieses Konto zu überwachen und das Kennwort regelmäßig zu wechseln.

Verfahren

1 Melden Sie sich mit vSphere Client bei vCenter Server an.

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 **Lokale Konten**.

5 Klicken Sie auf **Bearbeiten** für die Zeile **Kennwortrichtlinie**.

6 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.

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

7 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 vSphere Client bei vCenter Server an.

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 **Lokale Konten**.
5 Klicken Sie auf **Bearbeiten** für die Zeile **Sperrrichtlinie**.

   Möglicherweise müssen Sie nach unten scrollen, um die Zeile **Sperrrichtlinie** zu sehen.
6 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.

7 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 vSphere Client bei vCenter Server an.
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 **Lokale Konten**.
5 Klicken Sie auf **Bearbeiten** für die Zeile **Tokenvertrauenswürdigkeit**.

   Möglicherweise müssen Sie nach unten scrollen, um die Zeile **Token-Vertrauenswürdigkeit** zu sehen.

6 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. Dieser Wert gibt die Lebensdauer eines Tokens des Typs 'holder-of-key' an, bevor das Token als ungültig markiert wird.

7 Klicken Sie auf **Speichern**.

Bearbeiten der Benachrichtigungsfrist zum Kennwortablauf für Active Directory-Benutzer (Integrierte Windows-Authentifizierung)

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. vSphere Client steuert die Benachrichtigungsfrist zum Kennwortablauf. Sie können die standardmäßige Benachrichtigungsfrist zum Kennwortablauf so ändern, dass sie die Sicherheitsstandards in Ihrem Unternehmen erfüllt.

Voraussetzungen

- Aktivieren Sie die SSH-Anmeldung bei vCenter Server. Weitere Informationen hierzu finden Sie unter Verwalten von vCenter Server über die vCenter Server-Shell.

Verfahren

1. Melden Sie sich bei der vCenter Server-Shell als Benutzer mit Administratorrechten an.

   Der Standardbenutzer mit der Superadministratorrolle ist „root“.

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

   ```
   cd /etc/vmware/vsphere-ui
   ```

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 vSphere Client neu.

   ```
   service-control --stop vsphere-ui
   service-control --start vsphere-ui
   ```

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.

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 vSphere Client bei vCenter Server an.

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 **Hinzufügen**.

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

   Für den Benutzernamen sind maximal 300 Zeichen zulässig.

   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 vSphere Client bei vCenter Server an.
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 vSphere Client bei vCenter Server an.
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 > Lokale Konten > Kennwortrichtlinie**.

Siehe auch Bearbeiten der vCenter Single Sign On-Kennwortrichtlinie.

Verfahren

1 Melden Sie sich mit vSphere Client bei vCenter Server an.

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 vSphere Client bei vCenter Server an.
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.

   Für den Gruppennamen sind maximal 300 Zeichen zulässig. Sie können den Gruppennamen nicht ändern, nachdem Sie die Gruppe angelegt haben.
6. Wählen Sie im Dropdown-Menü **Mitglieder hinzufügen** die Identitätsquelle aus, die das Mitglied enthält, das der Gruppe hinzugefügt werden soll.

   Wenn Sie einen externen Identitätsanbieter, wie z. B. AD FS, konfiguriert haben, kann die Domäne dieses Identitätsanbieters im Dropdown-Menü **Mitglieder hinzufügen** ausgewählt werden.
7. Geben Sie einen Suchbegriff ein.
8. Wählen Sie das Mitglied aus.

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

Nächste Schritte

Weitere Informationen hierzu finden Sie unter Hinzufügen von Mitgliedern zu einer vCenter Single Sign On-Gruppe.

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 vSphere Client bei vCenter Server an.
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. Wählen Sie im Dropdown-Menü **Mitglieder hinzufügen** die Identitätsquelle aus, die das Mitglied enthält, das der Gruppe hinzugefügt werden soll.

   Wenn Sie einen externen Identitätsanbieter, wie z. B. AD FS, konfiguriert haben, kann die Domäne dieses Identitätsanbieters im Dropdown-Menü **Mitglieder hinzufügen** ausgewählt werden.
6. Geben Sie einen Suchbegriff ein.
7. Wählen Sie das Mitglied aus.

   Sie können mehrere Mitglieder hinzufügen.
8. Klicken Sie auf **Speichern**.

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 vSphere Client bei vCenter Server an.

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.

Ändern des vCenter Single Sign On-Kennworts

Benutzer in der lokalen Domäne (standardmäßig „vsphere.local“) können ihre vCenter Single Sign On-Kennwörter über vSphere Client 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 Kennwörter 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 vSphere Client bei vCenter Server an.

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 **Bearbeiten** auswählen.

4 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 **Speichern**.

Grundlegendes zu anderen Authentifizierungsoptionen

Ab vSphere 7.0 ist der externe Identitätsanbieterverbund die bevorzugte Authentifizierungsmethode für vCenter Server. Sie können sich noch über Windows-Sitzungsauthentifizierung (SSPI) 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.

Externer Identitätsanbieterverbund

Mit dem externen Identitätsanbieterverbund können Sie die Authentifizierungsmechanismen verwenden, die vom externen Identitätsanbieter unterstützt werden, einschließlich der Multifaktor-Authentifizierung.

Smartcard-Authentifizierung

Mit der Smartcard-Authentifizierung erhalten nur die Benutzer Zugriff, die ein physisches Kartenlesegerät an den Computer 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 vCenter Server 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.

Hinweis Ab vSphere 7.0 Update 2 können Sie FIPS auf dem vCenter Server aktivieren. Informationen finden Sie in der Dokumentation *vSphere-Sicherheit*. RSA SecureID- und CAC-Authentifizierung werden nicht unterstützt, wenn FIPS aktiviert ist. Verwenden Sie den externen Identitätsanbieterverbund für die MFA-Authentifizierung. Weitere Informationen hierzu finden Sie unter Konfigurieren des vCenter Server-Identitätsanbieterverbunds.

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

1. Wenn ein Benutzer die Smartcard in das Smartcard-Lesegerät einschiebt, liest der Browser die Zertifikate auf der Karte.

2 Der Browser 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 ist. Wenn die Überprüfung des Widerrufs eingeschaltet ist, überprüft vCenter Single Sign On auch, ob das Zertifikat widerrufen wurde.

4 Wenn das Zertifikat vCenter Single Sign On bekannt ist und es sich nicht um ein widerrufenes Zertifikat handelt, wird der Benutzer authentifiziert und kann 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 Kennwortauthentifizierung und aktivieren Sie die Smartcard-Authentifizierung. Danach lässt der vSphere Client nur noch die Anmeldung mit der Smartcard zu. Nur Benutzer mit Root- oder Administratorrechten auf der Maschine können die Benutzernamen- und Kennwort-Authentifizierung erneut aktivieren, indem sie sich direkt beim vCenter Server anmelden.

Konfigurieren und Verwenden der Smartcard-Authentifizierung

Sie können Ihre Umgebung so einstellen, dass die Smartcard-Authentifizierung erforderlich ist, wenn ein Benutzer aus vSphere Client eine Verbindung zu vCenter Server herstellt.

Zum Konfigurieren von Smartcard-Authentifizierung müssen Sie zuerst den Reverse-Proxy einrichten. Danach wird Smartcard-Authentifizierung aktiviert und konfiguriert. Sie verwenden das Dienstprogramm `sso-config` zum Verwalten von Smartcard-Authentifizierung.

Konfigurieren des Reverse-Proxys zum Anfordern von Clientzertifikaten

Bevor Sie die Smartcard-Authentifizierung aktivieren, müssen Sie den Reverse-Proxy auf dem vCenter Server-System konfigurieren.

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

Voraussetzungen

Kopieren Sie die Zertifikate der Zertifizierungsstelle auf das vCenter Server-System.

Hinweis vCenter Server 7.0 unterstützt das HTTP/2-Protokoll. Alle modernen Browser und Anwendungen, einschließlich vSphere Client, stellen Verbindungen zu vCenter Server über HTTP/2 her. Für die Smartcard-Authentifizierung muss allerdings das HTTP/1.1-Protokoll verwendet werden. Durch das Aktivieren der Smartcard-Authentifizierung wird ALPN (Application-Layer Protocol Negotiation, https://tools.ietf.org/html/rfc7301) für HTTP/2 deaktiviert. Dadurch wird faktisch verhindert, dass der Browser HTTP/2 verwendet. Anwendungen, die nur HTTP/2 verwenden, ohne sich auf ALPN zu stützen, funktionieren weiterhin.

Verfahren

1 Melden Sie sich bei der vCenter Server-Shell als Root-Benutzer an.

2 Erstellen Sie einen vertrauenswürdigen Client-Zertifizierungsstellenspeicher.

Dieser Speicher enthält die Zertifikate der vertrauenswürdigen ausstellenden Zertifizierungsstelle für das Clientzertifikat. 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 vCenter Server 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
```

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

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.

```
/usr/lib/vmware-vmon/vmon-cli --restart 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 folgendem Verzeichnis:

```
/opt/vmware/bin/sso-config.sh
```

Die Konfiguration von unterstützten Authentifizierungstypen und Widerrufseinstellungen wird in VMware Directory Service gespeichert und über alle vCenter Server-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 vCenter Server-Befehlszeile aktivieren. Mit dem folgenden Befehl wird die Authentifizierung über den Benutzernamen und das Kennwort aktiviert.

```
sso-config.sh -set_authn_policy -pwdAuthn true -t tenant_name
```

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 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.
- 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.
- Vergewissern Sie sich, dass der Reverse-Proxy eingerichtet ist, 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.

   a Melden Sie sich bei der Appliance-Konsole entweder direkt oder mithilfe von SSH an.

   b Aktivieren Sie die Appliance-Shell wie folgt:

```
shell
chsh -s "/bin/bash" root
```

   c Kopieren Sie die Zertifikate mithilfe von WinSCP oder einem ähnlichen Dienstprogramm in das Verzeichnis `/usr/lib/vmware-sso/vmware-sts/conf` auf dem vCenter Server.

   d Sie können die Shell optional folgendermaßen deaktivieren.

```
chsh -s "/bin/appliancesh" root
```

2 Führen Sie zum Aktivieren der Smartcard-Authentifizierung den folgenden Befehl aus.

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

   Beispiel:

```
sso-config.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.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 Positivliste mit Zertifikatsrichtlinien den folgenden Befehl aus:

```
sso-config.sh -set_authn_policy -certPolicies policies
```

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

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

   In der Positivliste sind Objekt-IDs von Richtlinien angegeben, die in der Zertifikatsrichtlinienerweiterung des Zertifikats zulässig 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.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.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.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.sh -t tenantName -get_alt_ocsp]
```

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

```
sso-config.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.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 vCenter Server-Befehlszeile aktivieren. Mit dem folgenden Befehl wird die Authentifizierung über den Benutzernamen und das Kennwort aktiviert.

```
sso-config.sh -set_authn_policy -pwdAuthn true -t tenant_name
```

Voraussetzungen

- 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.
- 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.
- Vergewissern Sie sich, dass der Reverse-Proxy eingerichtet ist, 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.

   a Melden Sie sich bei der vCenter Server-Konsole entweder direkt oder mithilfe von SSH an.

   b Aktivieren Sie die Shell wie folgt:

   ```
   shell
   chsh -s "/bin/bash" root
   csh -s "bin/appliance/sh" root
   ```

   c Kopieren Sie die Zertifikate mithilfe von WinSCP oder einem ähnlichen Dienstprogramm in das Verzeichnis `/usr/lib/vmware-sso/vmware-sts/conf` auf dem vCenter Server.

   d Optional können Sie die Appliance-Shell wie folgt deaktivieren:

   ```
   chsh -s "/bin/appliancesh" root
   ```

2 Melden Sie sich mit vSphere Client bei vCenter Server an.

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 auf der Registerkarte **Identitätsanbieter** auf **Smartcard-Authentifizierung** und Sie dann 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 vCenter Server-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 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 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 vCenter Server-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.

Verfahren

1. Melden Sie sich mit vSphere Client bei vCenter Server an.
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 der Registerkarte **Identitätsanbieter** 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

- 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 vCenter Server-Hostnamen auflösen kann und dass das vCenter Server-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. Zum Auffinden der Datei `sdconf.rec` dekomprimieren Sie die Ergebnisdatei `AM_Config.zip`.
- Kopieren Sie die Datei `sdconf.rec` in den vCenter Server-Knoten.

Verfahren

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

```
/opt/vmware/bin
```

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

```
sso-config.sh -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 -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 -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 -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 Anmeldemeldung auf der vSphere Client-Anmeldeseite

Sie können eine Meldung erstellen, die auf der Anmeldeseite des vSphere Client angezeigt wird.

Sie können eine Nachricht, einen Haftungsausschluss oder Nutzungsbedingungen festlegen. Darüber hinaus können Sie die Nachricht so konfigurieren, dass eine Bestätigung vor der Anmeldung erforderlich ist.

Verwalten der Anmeldemeldung auf der vSphere Client-Anmeldeseite

Sie können eine Anmeldemeldung zur vSphere Client-Anmeldeseite hinzufügen. Sie können auch eine benutzerdefinierte Anmeldemeldung konfigurieren und ein Kontrollkästchen für die Zustimmung des Benutzers bereitstellen.

Verfahren

1 Melden Sie sich mit vSphere Client bei vCenter Server an.

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**.

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.

Fehlerbehebung bei der Authentifizierung

5

Die folgenden Themen bieten einen guten Einstieg in die Fehlerbehebung bei Authentifizierungsproblemen mit vCenter Server. 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 oder vSphere 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. 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. Vergewissern Sie sich, dass vCenter Single Sign On ausgeführt wird, indem Sie den Status des vmware-sso-Daemons von vCenter Single Sign On prüfen. 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. Suchen Sie in `VM_ssoreg.log` die Zeile, die die folgende Meldung enthält. `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. 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. 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 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).

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 eine Änderung der Standard-Identitätsquelle das Problem nicht behebt, führen Sie die folgenden zusätzlichen Schritte zur Fehlerbehebung durch.

1. Synchronisieren Sie die Uhren zwischen der vCenter Server 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 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 aus der Active Directory-Domäne und treten anschließend der Domäne wieder bei. Informationen finden Sie in der Dokumentation *vCenter Server-Konfiguration*.

4 Schließen Sie alle mit der vCenter Server 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-Anmeldeseite aus bei vCenter Server anmelden, zeigt eine Fehlermeldung an, dass das Benutzerkonto gesperrt ist.

Problem

Nach mehreren fehlgeschlagenen Versuchen können Sie sich mithilfe von vSphere Client nicht mehr beim vCenter Single Sign On 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 über den erweiterten verknüpften Modus verbundene vCenter Server-Instanzen vorhanden sind und eine der vCenter Server-Instanzen nicht mehr verfügbar ist, kann Ihre Umgebung weiterhin verwendet werden. Sobald der vCenter Server wieder verfügbar ist, werden Benutzerdaten und sonstige Informationen in der Regel innerhalb von 30 Sekunden mit Partnern repliziert, die über den erweiterten verknüpften Modus verbunden sind. Unter bestimmten Umständen kann die Replizierung jedoch viel Zeit in Anspruch nehmen.

Problem

In bestimmten Situationen wird die Replizierung für die VMware-Verzeichnisdienst-Instanzen nicht sofort angezeigt. Beispielsweise, wenn in Ihrer Umgebung mehrere vCenter Server-Instanzen an unterschiedlichen Orten vorhanden sind und Sie umfangreiche Änderungen vornehmen, während ein vCenter Server nicht verfügbar ist. Beispielsweise wird ein neuer Benutzer, der zu einer verfügbaren vCenter Server-Instanz hinzugefügt wurde, erst nach Abschluss der Replizierung in der anderen Instanz angezeigt. Abhängig von der Topologie des erweiterten verknüpften Modus kann die Replizierung viel Zeit in Anspruch nehmen.

Ursache

Im regulären Betrieb werden Änderungen an einer Instanz des VMware-Verzeichnisdiensts (vmdir) in einer vCenter Server-Instanz (Knoten) für den direkten Replizierungspartner innerhalb von etwa 30 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 vCenter Server-Support-Pakets

Sie können ein Support-Paket, das die Protokolldateien für die vCenter Server-Dienste enthält, über den vSphere Client oder mithilfe einer API exportieren. Nach dem Export können Sie die Protokolle lokal durchsuchen oder das Paket an den VMware-Support senden.

Weitere Informationen zur API finden Sie im *Programmierhandbuch zur vCenter Server-Verwaltung*.

Voraussetzungen

Stellen Sie sicher, dass die vCenter Server erfolgreich bereitgestellt wurde und ausgeführt wird.

Verfahren

1. Stellen Sie über einen Webbrowser eine Verbindung zur vCenter Server-Konfigurationsverwaltungsschnittstelle unter https://*vcenter_server_ip*:5480 her.
2. Melden Sie sich als Root-Benutzer für den vCenter Server 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.

Referenz zu Authentifizierungsdienstprotokollen

Die vCenter Server-Authentifizierungsdienste verwenden syslog zur Protokollierung. Sie können die Protokolldateien prüfen, um die Ursache von Fehlern zu ermitteln.

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. 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`.