vSphere-Sicherheit

Update 3
Geändert am 23. November 2022
VMware vSphere 7.0
VMware ESXi 7.0
vCenter Server 7.0

vmware®

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

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

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

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

Inhalt

Info zu vSphere Security

vSphere-Sicherheit bietet Informationen über das Sichern Ihrer vSphere®-Umgebung für VMware® vCenter® Server und VMware ESXi.

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.

Zum Schutz Ihrer vSphere-Umgebung werden in dieser Dokumentation verfügbare Sicherheitsfunktionen sowie die Maßnahmen, die Sie zum Schutz Ihrer Umgebung vor Angriffen ergreifen können, beschrieben.

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

Themen	Inhaltliche Schwerpunkte
Berechtigungen und Benutzerverwaltung	■ Berechtigungsmodell (Rollen, Gruppen, Objekte). ■ Erstellen von benutzerdefinierten Rollen. ■ Festlegen von Berechtigungen. ■ Verwalten globaler Berechtigungen.
Funktionen für die Sicherheit von Hosts	■ Sperrmodus und sonstige Sicherheitsprofilfunktionen. ■ Smartcard-Authentifizierung für Host. ■ vSphere Authentication Proxy. ■ UEFI Secure Boot ■ Trusted Platform Module (TPM) ■ VMware® vSphere Trust Authority™. ■ Sichere ESXi-Konfiguration und Konfigurationsversiegelung
Verschlüsselung virtueller Maschinen	■ VMware vSphere® Native Key Provider™. ■ Wie funktioniert VM-Verschlüsselung? ■ KMS-Einrichtung. ■ Verschlüsseln und Entschlüsseln von VMs. ■ Fehlerbehebung und Best Practices.
Sicherheit des Gastbetriebssystems	■ Virtuelles Trusted Platform Module (vTPM) ■ Virtualisierungsbasierte Sicherheit (VBS)
Verwalten der Konfiguration des TLS-Protokolls	Ändern der Konfiguration des TLS-Protokolls mithilfe eines Befehlszeilen-Dienstprogramms.

Tabelle 1-1. *vSphere-Sicherheit* – Schwerpunkte (Fortsetzung)

Themen	Inhaltliche Schwerpunkte
Best Practices und Hardening für die Sicherheit	Best Practices und Rat von VMware-Sicherheitsexperten. ■ Sicherheit von vCenter Server ■ Sicherheit von Hosts ■ Sicherheit virtueller Maschinen ■ Netzwerksicherheit
vSphere-Rechte	Vollständige Auflistung aller in dieser Version unterstützten vSphere-Rechte.

Verwandte Dokumentation

In einem Begleitdokument *vSphere-Authentifizierung* wird erläutert, wie Sie beispielsweise mithilfe von Authentifizierungsdiensten die Authentifizierung mit vCenter Single Sign-On sowie Zertifikate in Ihrer vSphere-Umgebung verwalten können.

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.

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*.

Zielgruppe

Die Informationen richten sich an erfahrene Systemadministratoren, die mit der VM-Technologie und den Vorgängen in Datencentern vertraut sind.

Zertifizierungen

VMware veröffentlicht eine öffentliche Liste der VMware-Produkte, die Common-Criteria-Zertifizierungen abgeschlossen haben. Weitere Informationen zur Zertifizierung einer bestimmten VMware-Produktversion finden Sie auf der Webseite „Common-Criteria-Bewertung und -Validierung“ unter https://www.vmware.com/security/certifications/common-criteria.html.

Aktualisierte Informationen

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

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

Revision	Beschreibung
23. NOV. 2022	■ Geringfügiges Update für vCenter Server-Systemrollen. ■ Schlüsselpersistenz – Übersicht und Aktivieren und Deaktivieren von Schlüsselpersistenz auf einem ESXi-Host wurden mit zusätzlichen Informationen zu vSphere Native Key Provider aktualisiert. ■ Geringfügiges Update für Sichern von VLANs.
13. OKT. 2022	■ Geringfügiges Update für Verwalten von ESXi-Überwachungsdatensätzen. ■ Ein Tippfehler in Aktualisieren eines vSphere Native Key Providers wurde behoben. ■ Geringfügige Updates für Virtualisierungsbasierte Sicherheit – Empfohlene Vorgehensweisen, Aktivieren der virtualisierungsbasierten Sicherheit auf einer virtuellen Maschine und Aktivieren der virtualisierungsbasierten Sicherheit auf einer vorhandenen virtuellen Maschine. ■ Verweise auf den Befehl `vifs` wurden entfernt. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/article/78473 .
22. August 2022	■ Geringfügiges Update für Verlängern oder Aktualisieren von ESXi-Zertifikaten. ■ Geringfügiges Update für Löschen eines vSphere Native Key Providers. ■ Das Beispiel in Erstellen des Schlüsselanbieters im Trust Authority-Cluster wurde korrigiert. ■ Deaktivieren des Hostverschlüsselungsmodus mithilfe der API wurde für die Verwendung des vCenter Server Managed Object Browsers (MOB) umgeschrieben. ■ Kleinere Aktualisierung für mehrere Themen zu Berechtigungen in VMware vSphere Lifecycle Manager.
28. JUL 2022	■ Geringfügiges Update für Voraussetzungen für ESXi-Zertifikatssignieranforderungen. ■ Geringfügiges Update für Virtual Trusted Platform Module – Übersicht. ■ Geringfügiges Update für MAC-Adressänderungen. ■ Mehrere Themen wurden aktualisiert, um darauf hinzuweisen, dass Sie Berechtigungen, die solche VMware vSphere Lifecycle Manager-APIs verwenden, die URLs akzeptieren, nur Administratoren oder vertrauenswürdigen Benutzern zuweisen sollten.
12. JUL 2022	■ Geringfügiges Update für Ändern der Einstellungen für die Benutzervalidierung. ■ Geringfügiges Update für Verlängern oder Aktualisieren von ESXi-Zertifikaten. ■ Geringfügiges Update für Aktivieren der Fault Tolerance-Vverschlüsselung. ■ Ein Problem beim Formatieren eines ESXCLI-Befehls in Aktivieren oder Deaktivieren der execInstalledOnly-Erzwingung für eine sichere ESXi-Konfiguration wurde behoben. ■ Geringfügiges Update für Deaktivieren nicht verwendeter Anzeigefunktionen. ■ Parameter, die jetzt auf TRUE festgelegt sind, wurden aus Deaktivieren nicht freigelegter Funktionen entfernt. ■ Die Schritte im Abschnitt Erstellen einer Speicherrichtlinie für die Verschlüsselung. wurden korrigiert.

Revision	Beschreibung
15. Juni 2022	■ Informationen zu vCenter Server und zur verschlüsselten Kommunikation mit Sichern von vCenter Server-Systemen und zugehörigen Diensten wurden hinzugefügt. ■ Informationen zum Zuweisen von Berechtigungen für vSphere Distributed Switches wurden zu Hierarchische Vererbung von Berechtigungen hinzugefügt. ■ Geringfügiges Update für UEFI Secure Boot für ESXi-Hosts. ■ Informationen zur verschlüsselten Kommunikation wurden zu Virtuelle Maschine – Empfohlene Vorgehensweisen für die Verschlüsselung hinzugefügt. ■ Geringfügiges Update für vSphere Native Key Provider – Übersicht. ■ Informationen zu `HostCryptoState` wurden zu Deaktivieren des Hostverschlüsselungsmodus mithilfe der API hinzugefügt. ■ Die erforderliche Berechtigung **Kryptografievorgänge.Migrieren** wurde zu Erstellen einer virtuellen Maschine mit einem Virtual Trusted Platform Module und Aktivieren des virtuellen Trusted Platform Module für eine vorhandene virtuelle Maschine hinzugefügt. Mit dieser Berechtigung kann eine virtuelle Maschine eingeschaltet werden, wenn DRS sie auf einem anderen Host startet. ■ Geringfügiges Update für Herstellen einer Verbindung mit der VM-Konsole über eine Firewall. ■ Geringfügiges Update für Aktivieren oder Deaktivieren von TLS-Versionen auf ESXi-Hosts. ■ Informationen zur Einstellung von Berechtigungen wurden zu Rechte für Inhaltsbibliotheken hinzugefügt. ■ Ein Tippfehler in vSphere-Tag-Berechtigungen wurde behoben.
29. APR 2022	■ In Verwalten von ESXi-Überwachungsdatensätzen ersetzt das `viewAudit`-Programm ab vSphere 7.0 Update 3d das `auditLogReader`-Programm. ■ Geringfügige Updates für Aktivieren oder Deaktivieren der Secure Boot-Erzwingung für eine sichere ESXi-Konfiguration und Aktivieren oder Deaktivieren der execInstalledOnly-Erzwingung für eine sichere ESXi-Konfiguration. ■ Geringfügige Updates für Wie vSphere Virtual Machine Encryption Ihre Umgebung schützt. ■ Informationen zu vSphere Native Key Provider und die Schlüsselpersistenz wurden in Schlüsselpersistenz – Übersicht, Sichern eines vSphere Native Key Providers und Aktivieren und Deaktivieren von Schlüsselpersistenz auf einem ESXi-Host aktualisiert. ■ Geringfügiges Update für vSphere Native Key Provider – Übersicht. ■ Befehle in Aktualisieren eines vSphere Native Key Providers wurden korrigiert. ■ Geringfügiges Update für Verbinden von ESXi-Hosts über Firewalls. ■ Geringfügiges Update für Speicheransichtsberechtigungen.

Revision	Beschreibung
10. MAR 2022	■ Geringfügiges Update für Host-Upgrades und Zertifikate. ■ Falsche Befehle in Schritt 4 in Verwenden benutzerdefinierter Zertifikate mit Auto Deploy wurden korrigiert. ■ Die Voraussetzungen in Hinzufügen von AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) zu einer virtuellen Maschine mit dem vSphere Client, Hinzufügen von AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) zu einer virtuellen Maschine, Aktivieren von AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) auf einer vorhandenen virtuellen Maschine mit dem vSphere Client und Aktivieren von AMD-SEV-ES (Secure Encrypted Virtualization-Encrypted State) auf einer vorhandenen virtuellen Maschine wurden aktualisiert. ■ Geringfügiges Update für Interoperabilität bei der Verschlüsselung von virtuellen Maschinen. ■ vSphere Native Key Provider – Übersicht wurde aktualisiert, um darauf hinzuweisen, dass der vSphere Native Key Provider kein TPM 2.0 erfordert. ■ In Konfigurieren des vertrauenswürdigen Schlüsselanbieters für vertrauenswürdige Hosts mithilfe des vSphere Client und Konfigurieren des vertrauenswürdigen Schlüsselanbieters für vertrauenswürdige Hosts mithilfe der Befehlszeile wurde verdeutlicht, dass es beim Hinzufügen eines vSphere Trust Authority-Schlüsselanbieters einige Zeit dauert, bis der Schlüsselanbieter zur Verwendung verfügbar ist. ■ Erforderliche Rechte wurden zu Erstellen einer virtuellen Maschine mit einem Virtual Trusted Platform Module, Aktivieren des virtuellen Trusted Platform Module für eine vorhandene virtuelle Maschine und Entfernen eines virtuellen Trusted Platform Module von einer virtuellen Maschine hinzugefügt.
19. Jan. 2022	■ Geringfügiges Update für Grundlegende Informationen zur Autorisierung in vSphere. ■ Geringfügiges Update für Wiederherstellen des ESXi-Zertifikats und der Schlüsseldateien. ■ Für einen eigenständigen ESXi-Host wurde in Aktivieren oder Deaktivieren von TLS-Versionen auf ESXi-Hosts klargestellt, dass Sie den Befehl `reconfigureEsx ESXiHost` über ein vCenter Server-System ausführen müssen. ■ Überlegungen bei der Verwendung von FIPS wurde mit Informationen zur dateibasierten Sicherung und Wiederherstellung von vCenter Server aktualisiert.
21. Dez. 2021	■ Ein Tippfehler in Hochladen eines SSH-Schlüssels mithilfe eines vifs-Befehls wurde behoben. ■ Geringfügiges Update für Übersicht über TPM-Versiegelungsrichtlinien. ■ Geringfügiges Update für Aktivieren oder Deaktivieren der Secure Boot-Erzwingung für eine sichere ESXi-Konfiguration. ■ Geringfügiges Update für Beheben von Problemen im Zusammenhang mit dem Verschlüsselungsmodus des ESXi-Hosts. ■ Geringfügiges Update für Verschlüsseltes vSphere vMotion.
07. Dez. 2021	■ Geringfügiges Update für Vergleich von vSphere-Schlüsselanbietern. ■ Das neue Thema Importieren eines vSphere Native Key Providers in eine Konfiguration mit erweitertem verknüpftem Modus wurde hinzugefügt. ■ Geringfügiges Update für vSphere Trust Authority – Best Practices, Einschränkungen und Interoperabilität. ■ Das neue Thema Erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine mithilfe des vSphere Client wurde hinzugefügt. ■ Rechte für Inhaltsbibliotheken wurde mit neuen Berechtigungen aktualisiert. ■ vSphere mit Tanzu-Berechtigungen wurde mit neuen Berechtigungen aktualisiert.

Revision	Beschreibung
03. Nov. 2021	■ Geringfügiges Update für Schützen der virtuellen Netzwerkebene. ■ Geringfügiges Update für Aktivieren oder Deaktivieren der execInstalledOnly-Erzwingung für eine sichere ESXi-Konfiguration. ■ Anzeigen von Informationen zum Ablauf von Zertifikaten für mehrere ESXi-Hosts, Angeben vTPM-fähiger virtueller Maschinen, Anzeigen von Zertifikaten des Virtual Trusted Platform Module-Geräts und Identifizieren von VBS-fähigen virtuellen Maschinen wurden aktualisiert, um eine geringfügige Änderung der Benutzeroberfläche mit dem Ein- und Ausblenden von Spalten wiederzugeben. ■ Verwalten von ESXi-Firewalleinstellungen und Hinzufügen von zulässigen IP-Adressen für einen ESXi-Host wurden aktualisiert, um geringfügige Änderungen an der Benutzeroberfläche wiederzugeben. ■ Es wurden verschlüsselungsrelevante Informationen zu Interoperabilität bei der Verschlüsselung von virtuellen Maschinen hinzugefügt. ■ MAC-Adressänderungen und Gefälschte Übertragungen wurden aktualisiert, um die Änderung der Standardeinstellung für beide Optionen von „Akzeptieren“ in „Ablehnen“ wiederzugeben. ■ Es wurde eine Berechtigung in Rechte für das Bereitstellen virtueller Maschinen korrigiert. ■ Geringfügiges Update für Single Sign-On-Audit-Ereignisse.
05. OKT. 2021	Erstversion.

Sicherheit in der vSphere-Umgebung

1

Die Komponenten einer vSphere-Umgebung sind ab Werk durch mehrere Merkmale wie Authentifizierung, Autorisierung, Firewalls auf jedem ESXi-Host usw. gesichert. Dieses Standardsetup können Sie auf vielerlei Art und Weise abändern, etwa durch die Festlegung von Berechtigungen für vCenter-Objekte, durch Öffnen von Firewall-Ports oder durch die Änderung der Standardzertifikate. Sie können Sicherheitsmaßnahmen für verschiedene Objekte in der vCenter-Objekthierarchie ergreifen, wie beispielsweise für vCenter Server-Systeme, ESXi-Hosts, virtuelle Maschinen sowie Netzwerk- und Speicherobjekte.

Eine Übersicht über die verschiedenen Bereiche von vSphere, die Ihre Aufmerksamkeit erfordern, hilft beim Planen der Sicherheitsstrategie. Darüber hinaus finden Sie auf der VMware-Website zusätzliche Ressourcen zur vSphere-Sicherheit.

Dieses Kapitel enthält die folgenden Themen:

Absichern des ESXi-Hypervisors

Der ESXi-Hypervisor ist standardmäßig gesichert. Sie können ESXi-Hosts mithilfe des Sperrmodus und anderer integrierter Funktionen noch besser schützen. Aus Konsistenzgründen können Sie einen Referenzhost einrichten und alle Hosts mit dem Hostprofil des Referenzhosts synchronisieren. Darüber hinaus können Sie Ihre Umgebung mit der Verwaltung durch Skripts schützen. Hiermit wird sichergestellt, dass Änderungen auf alle Hosts angewendet werden.

Sie können mithilfe der folgenden Aktionen den Schutz von ESXi-Hosts, die von vCenter Server verwaltet werden, noch verbessern. Im Whitepaper *Security of the VMware vSphere Hypervisor* finden Sie weitere Informationen.

Beschränken des ESXi-Zugriffs

Standardmäßig werden die ESXi Shell und die SSH-Dienste nicht ausgeführt, und nur der Root-Benutzer kann sich bei der Benutzerschnittstelle der direkten Konsole (DCUI) anmelden. Wenn Sie ESXi oder SSH-Zugriff ermöglichen möchten, können Sie Zeitüberschreitungen zum Beschränken des Risikos von nicht autorisiertem Zugriff festlegen.

Benutzer, die auf den ESXi-Host zugreifen können, müssen Berechtigungen zum Verwalten des Hosts haben. Sie legen Berechtigungen für das Hostobjekt über das vCenter Server-System fest, das den Host verwaltet.

Verwenden von benannten Benutzern und der geringsten Berechtigung

Standardmäßig kann der Root-Benutzer viele Aufgaben ausführen. Lassen Sie nicht zu, dass sich Administratoren beim ESXi-Host unter Verwendung des Root-Benutzerkontos anmelden. Erstellen Sie stattdessen benannte Administratorbenutzer von vCenter Server und weisen Sie diesen Benutzern die Administratorrolle zu. Sie können diesen Benutzern auch eine benutzerdefinierte Rolle zuweisen. Weitere Informationen hierzu finden Sie unter Erstellen einer benutzerdefinierten vCenter Server-Rolle.

Wenn Sie Benutzer direkt auf dem Host verwalten, sind die Rollenverwaltungsoptionen beschränkt. Informationen finden Sie in der Dokumentation *Verwaltung eines einzelnen Hosts von vSphere – VMware Host Client*.

Minimieren der Anzahl offener ESXi-Firewallports

Standardmäßig werden Firewallports auf Ihrem ESXi-Host erst geöffnet, wenn Sie einen entsprechenden Dienst starten. Sie können den vSphere Client oder ESXCLI- oder PowerCLI-Befehle zum Prüfen und Verwalten des Firewall-Portstatus verwenden.

Weitere Informationen hierzu finden Sie unter ESXi-Firewall-Konfiguration.

Automatisieren der ESXi-Hostverwaltung

Weil es oft wichtig ist, dass verschiedene Hosts im selben Datencenter synchronisiert sind, sollten Sie Skriptinstallation oder vSphere Auto Deploy zum Bereitstellen von Hosts verwenden. Sie können die Hosts mit Skripts verwalten. Hostprofile sind eine Alternative zur Verwaltung durch Skripts. Sie richten einen Referenzhost ein, exportieren das Hostprofil und wenden das Hostprofil auf alle Hosts an. Sie können das Hostprofil direkt oder als Teil der Bereitstellung mit Auto Deploy anwenden.

Unter Verwenden von Skripts zum Verwalten von Hostkonfigurationseinstellungen und in der Dokumentation *Installation und Einrichtung von vCenter Server* finden Sie Informationen zu vSphere Auto Deploy.

Verwenden des Sperrmodus

Im Sperrmodus kann auf ESXi-Hosts standardmäßig nur über vCenter Server zugegriffen werden. Sie können den strengen Sperrmodus oder den normalen Sperrmodus auswählen. Sie können Ausnahmebenutzer definieren, um direkten Zugriff auf Dienstkonten wie beispielsweise Backup-Agenten zu ermöglichen.

Weitere Informationen hierzu finden Sie unter Sperrmodus.

Prüfen der VIB-Paketintegrität

Jedes VIB-Paket ist mit einer Akzeptanzebene verknüpft. Sie können einem ESXi-Host nur dann ein VIB hinzufügen, wenn die VIB-Akzeptanzebene mindestens so gut wie die Akzeptanzebene des Hosts ist. Sie können einem Host nur dann ein VIB mit der Akzeptanzebene „CommunitySupported“ oder „PartnerSupported“ hinzufügen, wenn Sie die Akzeptanzebene des Hosts explizit ändern.

Weitere Informationen hierzu finden Sie unter Verwalten der Akzeptanzebenen von Hosts und VIBs.

Verwalten von ESXi-Zertifikaten

Die VMware Certificate Authority (VMCA) stellt für jeden ESXi-Host ein signiertes Zertifikat bereit, dessen Rootzertifizierungsstelle standardmäßig die VMCA ist. Wenn es von der bei Ihnen geltenden Unternehmensrichtlinie verlangt wird, können Sie die vorhandenen Zertifikate durch Zertifikate ersetzen, die von einer Zertifizierungsstelle eines Drittanbieters oder eines Unternehmens signiert wurden.

Weitere Informationen hierzu finden Sie unter Zertifikatsverwaltung für ESXi-Hosts.

Smartcard-Authentifizierung in Betracht ziehen

ESXi unterstützt die Verwendung der Smartcard-Authentifizierung anstelle der Authentifizierung mit Benutzername und Kennwort. Um die Sicherheit weiter zu steigern, können Sie die Smartcard-Authentifizierung konfigurieren. Die Zwei-Faktor-Authentifizierung wird auch von vCenter Server unterstützt. Sie können die Authentifizierung über Benutzernamen- und Kennwort gleichzeitig mit der Smartcard-Authentifizierung konfigurieren.

Weitere Informationen hierzu finden Sie unter Konfigurieren der Smartcard-Authentifizierung für ESXi.

Sperren des ESXi-Kontos in Betracht ziehen

Das Sperren von Konten für den Zugriff über SSH und das vSphere Web Services SDK wird unterstützt. Standardmäßig wird das Konto nach maximal 10 fehlgeschlagenen Anmeldeversuchen gesperrt. Das Konto wird standardmäßig nach zwei Minuten entsperrt.

Hinweis Die DCUI und die ESXi Shell unterstützen die Kontosperrung nicht.

Weitere Informationen hierzu finden Sie unter Kennwörter und Kontosperrung für ESXi.

Die Sicherheitsüberlegungen für eigenständige Hosts sind ähnlich, obwohl die Verwaltungsaufgaben sich möglicherweise unterscheiden. Informationen finden Sie in der Dokumentation *Verwaltung eines einzelnen Hosts von vSphere – VMware Host Client*.

Sichern von vCenter Server-Systemen und zugehörigen Diensten

Ihr vCenter Server-System und die zugehörigen Dienste sind durch Authentifizierung über vCenter Single Sign On und Autorisierung über das vCenter Server-Berechtigungsmodell geschützt. Sie können das Standardverhalten ändern und Maßnahmen ergreifen, um den Zugriff auf Ihre Umgebung zu beschränken.

Denken Sie beim Schutz Ihrer vSphere-Umgebung daran, dass alle mit den vCenter Server-Instanzen verbundenen Dienste geschützt werden müssen. In einigen Umgebungen können Sie mehrere vCenter Server-Instanzen schützen.

vCenter und verschlüsselte Kommunikation

Standardmäßig ist die gesamte Datenkommunikation zwischen vCenter Server und anderen vSphere-Komponenten verschlüsselt. Der Konfiguration Ihrer Umgebung entsprechend kann ein Teil des Datenverkehrs unverschlüsselt sein. Sie können z. B. unverschlüsseltes SMTP für E-Mail-Warnungen und unverschlüsseltes SNMP für die Überwachung konfigurieren. DNS-Datenverkehr ist ebenfalls unverschlüsselt. vCenter Server überwacht Port 80 (TCP) und Port 443 (TCP). Port 443 (TCP) ist der branchenübliche Port für HTTPS (sicheres HTTP) und über eine TLS 1.2-Verschlüsselung geschützt. Port 80 (TCP) ist der branchenübliche HTTP-Port und verwendet keine Verschlüsselung. Port 80 dient dazu, Anforderungen von Port 80 an Port 443 umzuleiten, wo sie sicher sind.

Absichern aller vCenter-Hostmaschinen

Der erste Schritt zum Schutz Ihrer vCenter-Umgebung besteht im Absichern jeder einzelnen Maschine, auf der vCenter Server oder ein zugehöriger Dienst ausgeführt wird. Dies gilt gleichermaßen für physische Rechner wie für virtuelle Maschinen. Installieren Sie immer die aktuellsten Sicherheitspatches für Ihr Betriebssystem und halten Sie sich an die branchenüblichen empfohlenen Vorgehensweisen zum Schutz der Hostmaschine.

Grundlegende Informationen zum vCenter-Zertifikatmodell

Standardmäßig stattet die VMware Certificate Authority (VMCA) alle ESXi-Hosts und alle Maschinen in der Umgebung und alle Lösungsbenutzer mit einem von VMCA signierten Zertifikat aus. Wenn die Unternehmensrichtlinie dies verlangt, können Sie das Standardverhalten ändern. Weitere Informationen finden Sie in der Dokumentation *vSphere-Authentifizierung*.

Um zusätzlichen Schutz zu gewährleisten, entfernen Sie abgelaufene oder widerrufene Zertifikate und fehlgeschlagene Installationen.

Konfigurieren von vCenter Single Sign On

vCenter Server und die zugehörigen Dienste sind durch vCenter Single Sign On und dessen Authentifizierungsframework geschützt. Bei der erstmaligen Installation der Software geben Sie ein Kennwort für den Administrator der vCenter Single Sign-On-Domäne an (standardmäßig administrator@vsphere.local). Nur diese Domäne ist anfangs

als Identitätsquelle verfügbar. Sie können einen externen Identitätsanbieter wie Microsoft Active Directory Federation Services (AD FS) für die Verbundauthentifizierung hinzufügen. Sie können weitere Identitätsquellen (entweder Active Directory oder LDAP) hinzufügen und eine Standardidentitätsquelle bestimmen. Benutzer, die sich bei diesen Identitätsquellen authentifizieren können, können auch Objekte anzeigen und Aufgaben ausführen, sofern sie die entsprechende Berechtigung besitzen. Weitere Informationen finden Sie in der Dokumentation *vSphere-Authentifizierung*.

Zuweisen von Rollen zu benannten Benutzern oder Gruppen

Zur besseren Protokollierung sollten Sie jede Berechtigung, die Sie für ein Objekt erteilen, mit einem benannten Benutzer oder einer benannten Gruppe sowie einer vordefinierten oder einer benutzerdefinierten Rolle verbinden. Das Berechtigungsmodell in vSphere ist mit seinen unterschiedlichen Möglichkeiten der Benutzer- oder Gruppenautorisierung äußerst flexibel. Weitere Informationen hierzu finden Sie unter Grundlegende Informationen zur Autorisierung in vSphere und Erforderliche Berechtigungen für allgemeine Aufgaben.

Beschränken Sie die Administratorrechte und die Verwendung der Administratorrolle. Wenn möglich, verzichten Sie auf den Einsatz des anonymen Administratorbenutzers.

PTP oder NTP einrichten

Richten Sie PTP oder NTP für jeden Knoten in Ihrer Umgebung ein. Die Zertifikatinfrastruktur erfordert einen genauen Zeitstempel und funktioniert nicht ordnungsgemäß, wenn die Knoten nicht synchronisiert sind.

Weitere Informationen hierzu finden Sie unter Synchronisieren der Systemuhren im vSphere-Netzwerk.

Sichern von virtuellen Maschinen

Zum Schutz Ihrer virtuellen Maschinen sorgen Sie dafür, dass alle Patches auf Ihren Gastbetriebssystemen installiert werden und Ihre Umgebung so geschützt wird, wie Sie auch einen physischen Computer schützen würden. Deaktivieren Sie eventuell alle ungenutzten Funktionen, minimieren Sie die Nutzung der Konsole für die virtuelle Maschine und halten Sie sich an alle anderen empfohlenen Vorgehensweisen.

Schutz des Gastbetriebssystems

Zum Schutz Ihres Gastbetriebssystems sollten stets die aktuellen Patches und, falls erforderlich, die nötigen Anti-Spyware- und Anti-Malware-Anwendungen installiert werden. Schlagen Sie in der Dokumentation zu Ihrem Gastbetriebssystem nach und konsultieren Sie bei Bedarf einschlägige Bücher oder Informationen im Internet für dieses Betriebssystem.

Deaktivieren ungenutzter Funktionen

Achten Sie darauf, ungenutzte Funktionen zu deaktivieren, um mögliche Angriffsstellen zu verringern. Viele Funktionen, die nicht häufig genutzt werden, sind bereits standardmäßig deaktiviert. Entfernen Sie nicht benötigte Hardware und deaktivieren Sie Funktionen wie

HGFS (Host-Guest Filesystem) oder Kopieren und Einfügen zwischen der virtuellen Maschine und einer Remote-Konsole.

Weitere Informationen hierzu finden Sie unter Deaktivieren unnötiger Funktionen innerhalb von virtuellen Maschinen.

Verwenden von Vorlagen und Verwaltung durch Skripts

Mit Vorlagen für virtuelle Maschinen können Sie das Betriebssystem so einrichten, dass es Ihren Anforderungen entspricht, und weitere virtuelle Maschinen mit denselben Einstellungen erstellen.

Wenn Sie nach der Erstbereitstellung die Einstellungen der virtuellen Maschine ändern möchten, ist dies mithilfe von Skripts wie PowerCLI möglich. In dieser Dokumentation wird erläutert, wie Sie mithilfe der grafischen Benutzeroberfläche Aufgaben ausführen. Verwenden Sie eventuell Skripts anstelle der grafischen Benutzeroberfläche, um für die Konsistenz Ihrer Umgebung zu sorgen. In großen Umgebungen können Sie virtuelle Maschine in Ordner gruppieren, um das Scripting zu erleichtern.

Weitere Informationen zu Vorlagen finden Sie unter Verwendung von Vorlagen zum Bereitstellen von virtuellen Maschinen und in der *vSphere-Administratorhandbuch für virtuelle Maschinen*-Dokumentation. Weitere Informationen zu PowerCLI finden Sie in der Dokumentation zu VMware PowerCLI.

Beschränken der Verwendung der VM-Konsole auf ein Minimum

Die VM-Konsole bietet für eine virtuelle Maschine dieselbe Funktionalität wie ein Monitor auf einem physischen Server. Benutzer mit Zugriff auf die Konsole der virtuellen Maschine haben Zugriff auf die Energieverwaltung der virtuellen Maschine und auf Konnektivitätssteuerelemente von Wechselmedien. Demzufolge kann die Konsole einer virtuellen Maschine einen böswilligen Angriff auf eine virtuelle Maschine ermöglichen.

Verwenden Sie UEFI Secure Boot

Sie können Ihre virtuelle Maschine für die Verwendung von UEFI Secure Boot konfigurieren. Wenn das Betriebssystem UEFI Secure Boot unterstützt, können Sie zur Erhöhung der Sicherheit diese Option für Ihre virtuellen Maschinen auswählen. Weitere Informationen hierzu finden Sie unter Aktivieren oder Deaktivieren von UEFI Secure Boot für eine virtuelle Maschine.

Überlegungen zu Carbon Black Cloud Workload

Sie können Carbon Black Cloud Workload installieren und verwenden, um Risiken zu identifizieren, Angriffe zu verhindern und ungewöhnliche Aktivitäten zu erkennen. Mit der in der Carbon Black Cloud-Plattform integrierten AppDefense-Funktionalität ist Carbon Black Cloud Workload das Nachfolgeprodukt für AppDefense.

Schützen der virtuellen Netzwerkebene

Zur virtuellen Netzwerkebene gehören virtuelle Netzwerkadapter, virtuelle Switches, verteilte virtuelle Switches, Ports und Portgruppen. ESXi verwendet die virtuelle Netzwerkebene zur Kommunikation zwischen den virtuellen Maschinen und ihren Benutzern. Außerdem verwendet ESXi die virtuelle Netzwerkebene zur Kommunikation mit iSCSI-SANs, NAS-Speichern usw.

vSphere umfasst das gesamte Funktionsangebot, das für eine sichere Netzwerkinfrastruktur erforderlich ist. Dabei kann jedes einzelne Element der Infrastruktur eigens geschützt werden, z. B. virtuelle Switches, verteilte virtuelle Switches und virtuelle Netzwerkadapter. Beachten Sie auch folgende Richtlinien, über die Sie ausführlicher unter Kapitel 13 Sichern der vSphere-Netzwerke nachlesen können.

Isolieren des Netzwerkdatenverkehrs

Die Isolierung des Netzwerkverkehrs ist entscheidend für eine sichere ESXi-Umgebung. Verschiedene Netzwerke erfordern verschiedenen Zugriff und verschiedene Isolierungsebenen. Ein Managementnetzwerk isoliert Datenverkehr des Clients, der Befehlszeilenschnittstelle oder der API sowie Datenverkehr von Drittsoftware von normalem Datenverkehr. Stellen Sie sicher, dass nur System-, Netzwerk- und Sicherheitsadministratoren Zugriff auf das Verwaltungsnetzwerk haben.

Weitere Informationen hierzu finden Sie unter ESXi-Netzwerksicherheitsempfehlungen.

Schützen virtueller Netzwerkelemente durch Firewalls

Sie können Firewall-Ports öffnen und schließen und alle Elemente im virtuellen Netzwerk eigens schützen. Für ESXi-Hosts verknüpfen Firewallregeln Dienste mit den entsprechenden Firewalls und können die Firewall in Abhängigkeit vom Dienststatus öffnen oder schließen.

Sie können auch Ports explizit für vCenter Server-Instanzen öffnen.

Eine Liste aller unterstützten Ports und Protokolle in VMware, einschließlich vSphere und vSAN, finden Sie im Tool VMware Ports and Protocols™ unter https://ports.vmware.com/. Sie können Ports nach VMware-Produkt durchsuchen, eine benutzerdefinierte Portliste erstellen und Portlisten drucken oder speichern.

Netzwerksicherheitsrichtlinien

Netzwerksicherheitsrichtlinien schützen den Datenverkehr vor Imitation von MAC-Adressen und unerwünschten Portscans. Die Sicherheitsrichtlinie eines Standard-Switches oder eines Distributed Switch ist auf Schicht 2 (Sicherungsschicht) des Netzwerkprotokoll-Stacks implementiert. Die drei Elemente der Sicherheitsrichtlinie sind der Promiscuous-Modus, Änderungen der MAC-Adresse und gefälschte Übertragungen.

Anweisungen hierzu finden Sie in der Dokumentation zu *vSphere-Netzwerk*.

Sichern des VM-Netzwerks

Die Methoden, die Sie zur Sicherung des VM-Netzwerks verwenden, hängen von mehreren Faktoren ab, darunter folgende:

- Das installierte Gastbetriebssystem
- Ob die VMs in einer vertrauenswürdigen Umgebung betrieben werden.

Virtuelle Switches und verteilte virtuelle Switches bieten einen hohen Grad an Sicherheit, wenn sie in Verbindung mit anderen üblichen Sicherheitsmaßnahmen verwendet werden, z. B. Firewalls.

Weitere Informationen hierzu finden Sie unter Kapitel 13 Sichern der vSphere-Netzwerke.

Schützen Ihrer Umgebung durch VLANs

ESXi unterstützt IEEE 802.1q VLANs. Mit VLANs können Sie ein physisches Netzwerk in Segmente aufteilen. Sie können VLANs verwenden, um den Schutz des VM-Netzwerks bzw. der Speicherkonfiguration weiter zu erhöhen. Bei Verwendung von VLANs können zwei VMs in demselben physischen Netzwerk nur dann Pakete untereinander übertragen, wenn sie sich in demselben VLAN befinden.

Weitere Informationen hierzu finden Sie unter Absichern virtueller Maschinen durch VLANs.

Schützen der Verbindungen zum virtualisierten Speicher

Virtuelle Maschinen speichern Betriebssystemdateien, Anwendungsdateien und andere Daten auf einer virtuellen Festplatte. Für die virtuelle Maschine ist die virtuelle Festplatte ein SCSI-Laufwerk mit einem verbundenen SCSI-Controller. Eine virtuelle Maschine ist von anderen Speicherelementen isoliert und hat keinen Zugriff auf die Daten der LUN, auf der die virtuelle Festplatte angesiedelt ist.

Das Virtual Machine File System (VMFS) ist ein verteiltes Dateisystem und ein Verwaltungswerkzeug für Volumes, das die virtuellen Volumes für den ESXi-Host erkennbar macht. Die Sicherheit der Verbindung zum Speicher liegt in Ihrer Verantwortung. Bei Verwendung von iSCSI-Speichern können Sie beispielsweise Ihre Umgebung zum Einsatz von CHAP konfigurieren. Wenn die Unternehmensrichtlinie dies verlangt, können Sie beiderseitiges CHAP einrichten. Verwenden Sie den vSphere Client oder CLIs, um CHAP einzurichten.

Weitere Informationen hierzu finden Sie unter Speichersicherheit, empfohlene Vorgehensweisen.

Verwendung von IPSec

ESXi unterstützt IPSec über IPv6. IPSec über IPv4 ist nicht möglich.

Weitere Informationen hierzu finden Sie unter Internet Protocol Security (IPsec).

Kennwörter in Ihrer vSphere-Umgebung

Kennwortbeschränkungen, der Ablauf von Kennwörtern und das Sperren von Konten in Ihrer vSphere-Umgebung sind abhängig vom System, das der Benutzer verwendet, vom Benutzer und von den festgelegten Richtlinien.

ESXi-Kennwörter

ESXi-Kennworteinschränkungen werden durch bestimmte Anforderungen bestimmt. Weitere Informationen hierzu finden Sie unter Kennwörter und Kontosperrung für ESXi.

Kennwörter für vCenter Server und andere vCenter-Dienste

vCenter Single Sign On verwaltet die Authentifizierung für alle Benutzer, die sich bei vCenter Server und anderen vCenter-Diensten anmelden. Die Kennwortbeschränkungen, der Kennwortablauf und das Sperren von Konten sind abhängig von der Domäne und der Identität des Benutzers.

vCenter Single Sign On-Administrator

Das Kennwort für den Benutzer „administrator@vsphere.local“ bzw. für den Benutzer „administrator@*meineDomäne*“, wenn Sie bei der Installation eine andere Domäne ausgewählt haben, läuft nicht ab und unterliegt nicht der Sperrrichtlinie. Ansonsten muss das Kennwort die in der vCenter Single Sign On-Kennwortrichtlinie festgelegten Beschränkungen einhalten. Weitere Informationen dazu finden Sie unter *vSphere-Authentifizierung*.

Sollten Sie das Kennwort für diesen Benutzer vergessen, suchen Sie im VMware-Knowledgebase-System nach Informationen zum Zurücksetzen des Kennworts. Zum Zurücksetzen sind zusätzliche Rechte erforderlich, wie beispielsweise Root-Zugriff auf das vCenter Server-System.

Andere Benutzer der vCenter Single Sign-On-Domäne

Kennwörter für andere vsphere.local-Benutzer bzw. für Benutzer der von Ihnen bei der Installation angegebenen Domäne müssen die von der vCenter Single Sign On-Kennwortrichtlinie und -Sperrrichtlinie festgelegten Beschränkungen einhalten. Weitere Informationen dazu finden Sie unter *vSphere-Authentifizierung*. Diese Kennwörter laufen standardmäßig nach 90 Tagen ab. Administratoren können jedoch den Kennwortablauf im Rahmen der Kennwortrichtlinie ändern.

Wenn Sie Ihr Kennwort für vsphere.local vergessen, kann ein Administratorbenutzer das Kennwort mit dem Befehl `dir-cli` zurücksetzen.

Andere Benutzer

Die Kennwortbeschränkungen, der Kennwortablauf und die Kontosperrungen für alle anderen Benutzer werden durch die Domäne (Identitätsquelle) bestimmt, bei der sich der Benutzer authentifizieren kann.

vCenter Single Sign On unterstützt eine standardmäßige Identitätsquelle. Benutzer können sich bei der entsprechenden Domäne beim vSphere Client mit Ihren Benutzernamen anmelden. Wenn sich Benutzer bei einer Nicht-Standarddomäne anmelden möchten, können sie den Domänennamen angeben, also *Benutzer@Domäne* oder *Domäne\Benutzer*. Die Parameter für das Domänenkennwort gelten für jede Domäne.

Kennwörter für DCUI-Benutzer der vCenter Server

Die vCenter Server Appliance ist eine vorkonfigurierte virtuelle Maschine, die für die Ausführung von vCenter Server und zugehörigen Diensten optimiert ist.

Bei der Bereitstellung der vCenter Server geben Sie die folgenden Kennwörter an.

- Kennwort für den Root-Benutzer.
- Kennwort für den Administrator der vCenter Single Sign On-Domäne, standardmäßig administrator@vsphere.local.

Über die vCenter Server-Verwaltungsschnittstelle können Sie das Kennwort des Root-Benutzers ändern und weitere Verwaltungsaufgaben für lokale Benutzer der vCenter Server ausführen. Siehe *vCenter Server-Konfiguration*.

Best Practices und Ressourcen für die Sicherheit

Wenn Sie sich an die Best Practices halten, können ESXi und vCenter Server so sicher wie eine Umgebung ohne Virtualisierung oder sogar noch sicherer sein.

Dieses Handbuch enthält empfohlene Vorgehensweisen für die verschiedenen Komponenten Ihrer vSphere-Infrastruktur.

Tabelle 1-1. Empfohlene Vorgehensweisen für die Sicherheit

vSphere-Komponente	Ressource
ESXi-Host	Kapitel 3 Sichern der ESXi-Hosts
vCenter Server-System	Empfohlene Vorgehensweisen für die vCenter Server-Sicherheit
Virtuelle Maschine	Virtuelle Maschine – Empfohlene Vorgehensweisen für die Sicherheit
vSphere-Netzwerk	vSphere Networking, empfohlene Vorgehensweisen für die Sicherheit

Dieses Handbuch ist eine von mehreren Ressourcen, die Sie für eine sichere Umgebung verwenden müssen.

Sicherheitsressourcen von VMware, einschließlich Sicherheitswarnungen und Downloads, sind im Internet verfügbar.

Tabelle 1-2. Sicherheitsressourcen von VMware im Internet

Thema	Ressource
Informationen zu ESXi- und vCenter Server-Sicherheit und -Vorgängen, einschließlich sichere Konfiguration und Hypervisorsicherheit.	https://core.vmware.com/security
Sicherheitsrichtlinien von VMware, aktuelle Sicherheitswarnungen, Sicherheitsdownloads und themenspezifische Abhandlungen zu Sicherheitslücken.	http://www.vmware.com/go/security
Richtlinie zur Sicherheitsantwort	http://www.vmware.com/support/policies/security_response.html VMware hat es sich zur Aufgabe gemacht, Sie bei der Absicherung Ihrer virtuellen Umgebung zu unterstützen. Sicherheitslücken werden so schnell wie möglich beseitigt. Die VMware-Richtlinie zur Sicherheitsantwort dokumentiert unseren Einsatz für die Behebung möglicher Schwachstellen in unseren Produkten.
Richtlinie zur Unterstützung von Drittanbieter-Software	http://www.vmware.com/support/policies/ VMware unterstützt viele Speichersysteme und Software-Agenten wie Sicherungs-Agenten, Systemverwaltungs-Agenten usw. Ein Verzeichnis der Agenten, Werkzeuge und anderer Software, die ESXi unterstützen, finden Sie, indem Sie unter http://www.vmware.com/vmtn/resources/ nach ESXi-Kompatibilitätshandbüchern suchen. Die Branche bietet mehr Produkte und Konfigurationen an, als VMware testen kann. Wenn VMware ein Produkt oder eine Konfiguration nicht in einem Kompatibilitätshandbuch nennt, versucht der technische Support, Ihnen bei Problemen zu helfen, kann jedoch nicht garantieren, dass das Produkt oder die Konfiguration verwendet werden kann. Testen Sie die Sicherheitsrisiken für nicht unterstützte Produkte oder Konfigurationen immer sorgfältig.
Übereinstimmungs- und Sicherheitsstandards sowie Partnerlösungen und vertiefende Informationen zu Virtualisierung und Übereinstimmung	https://core.vmware.com/compliance
Informationen zu Sicherheitszertifizierungen und -validierungen wie beispielsweise CCEVS und FIPS für verschiedene Versionen von vSphere-Komponenten.	https://www.vmware.com/support/support-resources/certifications.html
Handbücher für die Sicherheitskonfiguration (früher bekannt als „Handbücher für Hardening“) für verschiedene Versionen von vSphere und anderen VMware-Produkten.	https://core.vmware.com/security
Security of the VMware vSphere Hypervisor (Whitepaper)	http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf

vSphere-Berechtigungen und Benutzerverwaltungsaufgaben

2

Authentifizierung und Autorisierung steuern den Zugriff. vCenter Single Sign On unterstützt die Authentifizierung, d. h., es wird bestimmt, ob sich ein Benutzer überhaupt bei vSphere-Komponenten anmelden kann. Zum Anzeigen oder Bearbeiten von vSphere-Objekten muss jeder Benutzer auch autorisiert werden.

vSphere unterstützt verschiedene Autorisierungsmechanismen, die im Abschnitt Grundlegende Informationen zur Autorisierung in vSphere behandelt werden. Dieser Abschnitt befasst sich mit der Funktionsweise des vCenter Server-Berechtigungsmodells und der Durchführung von Benutzermanagementaufgaben.

vCenter Server ermöglicht die detaillierte Kontrolle der Autorisierung mit Berechtigungen und Rollen. Wenn Sie einem Objekt in der vCenter Server-Objekthierarchie eine Berechtigung zuweisen, geben Sie an, welcher Benutzer oder welche Gruppe über welche Rechte für dieses Objekt verfügt. Zum Angeben der Rechte verwenden Sie Rollen. Rollen bestehen aus einer Gruppe von Rechten.

Anfangs ist nur der Administrator der vCenter Single Sign-On-Domäne berechtigt, sich beim vCenter Server-System anzumelden. Die Standarddomäne ist „vsphere.local“ und der Standardadministrator administrator@vsphere.local. Sie können die Standarddomäne während der Installation von vSphere ändern.

Der Administratorbenutzer kann wie folgt fortfahren:

1. Hinzufügen einer Identitätsquelle, in der Benutzer und Gruppen für vCenter Single Sign On definiert sind. Informationen finden Sie in der Dokumentation *vSphere-Authentifizierung*.
2. Erteilen von Rechten für einen Benutzer oder eine Gruppe durch die Auswahl z. B. einer virtuellen Maschine oder eines vCenter Server-Systems und Zuweisen einer Rolle für dieses Objekt für die Benutzer bzw. Gruppe.

 (Zuweisen von Rollen und Berechtigungen mithilfe von vSphere Client)

Dieses Kapitel enthält die folgenden Themen:

- Grundlegende Informationen zur Autorisierung in vSphere
- Verwalten von Berechtigungen für vCenter-Komponenten
- Globale Berechtigungen

- Verwenden von Rollen zum Zuweisen von Rechten
- Best Practices für Rollen und Berechtigungen
- Erforderliche Berechtigungen für allgemeine Aufgaben

Grundlegende Informationen zur Autorisierung in vSphere

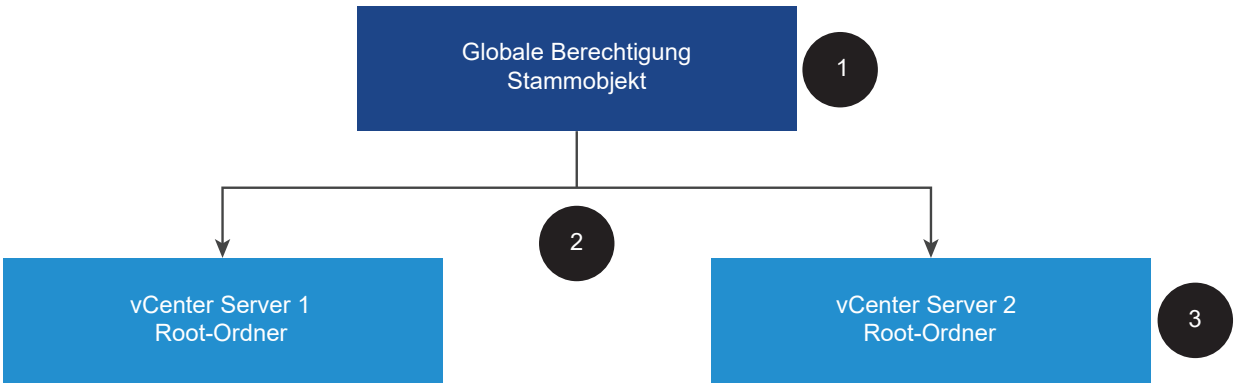
vSphere unterstützt mehrere Modelle, um zu ermitteln, ob ein Benutzer eine Aufgabe ausführen darf. Die Gruppenmitgliedschaft in einer vCenter Single Sign-On-Gruppe entscheidet, was Sie tun dürfen. Ihre Rolle für ein Objekt oder Ihre globale Berechtigung legt fest, ob Sie andere Aufgaben durchführen dürfen.

Autorisierungsübersicht

vSphere ermöglicht es Benutzern mit entsprechenden Rechten, anderen Benutzern Berechtigungen zum Durchführen von Aufgaben zu geben. Sie können globale oder lokale vCenter Server-Berechtigungen verwenden, um andere Benutzer für einzelne vCenter Server-Instanzen zu autorisieren.

Die folgende Abbildung veranschaulicht die Funktionsweise globaler und lokaler Berechtigungen.

Abbildung 2-1. Globale und lokale Berechtigungen



In dieser Abbildung:

1 Sie weisen eine globale Berechtigung auf der Root-Objektebene zu, wenn „An untergeordnete Objekte weitergeben“ ausgewählt ist.

2 vCenter Server gibt die Berechtigungen an die Objekthierarchien vCenter Server 1 und vCenter Server 2 in der Umgebung weiter.

3 Eine lokale Berechtigung für den Root-Ordner in vCenter Server 2 überschreibt die globale Berechtigung.

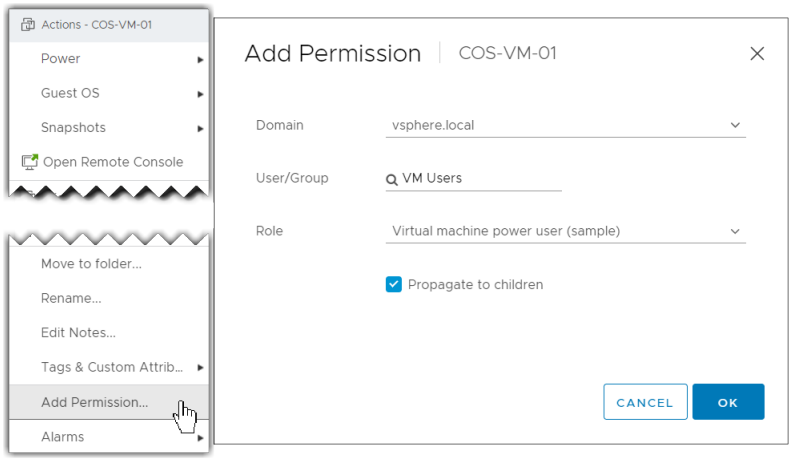
vCenter Server-Berechtigungen

Das Berechtigungsmodell für vCenter Server-Systeme basiert auf der Zuweisung von Berechtigungen zu Objekten in der Objekthierarchie. Benutzer erhalten Berechtigungen auf folgende Art und Weise.

- Von einer bestimmten Berechtigung für den Benutzer oder von den Gruppen, in denen der Benutzer Mitglied ist
- Von einer Berechtigung für das Objekt oder über die Vererbung von Berechtigungen von einem übergeordneten Objekt

Jede Berechtigung erteilt einem Benutzer oder einer Gruppe eine Reihe von Berechtigungen (d. h. eine Rolle) für das ausgewählte Objekt. Sie können den vSphere Client zum Hinzufügen von Berechtigungen verwenden. Sie können z. B. mit der rechten Maustaste auf eine virtuelle Maschine klicken, **Berechtigung hinzufügen** auswählen und das Dialogfeld beenden, um einer Gruppe von Benutzern eine Rolle zuzuweisen. Diese Rolle weist diesen Benutzern die entsprechenden Privilegien auf dieser virtuellen Maschine zu.

Abbildung 2-2. Hinzufügen von Berechtigungen zu einer virtuellen Maschine mithilfe von vSphere Client



Globale Berechtigungen

Mithilfe von globalen Berechtigungen werden einem Benutzer oder einer Gruppe Rechte zum Anzeigen oder Verwalten aller Objekte in allen Bestandslistenhierarchien der Lösungen Ihrer Bereitstellung erteilt. Das heißt, globale Berechtigungen werden auf ein globales Stammobjekt angewendet, das sich über Lösungsbestandshierarchien erstreckt. (Lösungen umfassen vCenter Server, vRealize Orchestrator usw.) Globale Berechtigungen gelten auch für globale Objekte wie Tags und Inhaltsbibliotheken. Betrachten Sie beispielsweise eine Bereitstellung, die aus zwei Lösungen besteht: vCenter Server und vRealize Orchestrator. Sie können anhand globaler Berechtigungen einer Gruppe von Benutzern, die über Leseberechtigungen für alle Objekte in den Objekthierarchien von vCenter Server und vRealize Orchestrator verfügen, eine Rolle zuweisen.

Globale Berechtigungen werden über die vCenter Single Sign-On-Domäne hinweg repliziert (standardmäßig „vsphere.local“). Sie dienen jedoch nicht zur Autorisierung von Diensten, die in den vCenter Single Sign-On-Domänengruppen verwaltet werden. Weitere Informationen hierzu finden Sie unter Globale Berechtigungen.

Gruppenmitgliedschaft in vCenter Single Sign-On-Gruppen

Mitglieder einer vCenter Single Sign-On-Domänengruppe können bestimmte Aufgaben ausführen. Wenn Sie beispielsweise Mitglied der Gruppe „LicenseService.Administrators“ sind, dürfen Sie Lizenzen verwalten. Informationen finden Sie in der Dokumentation *vSphere-Authentifizierung*.

Berechtigungen für lokale ESXi-Hosts

Wenn Sie einen eigenständigen ESXi-Host verwalten, der nicht von einem vCenter Server-System verwaltet wird, können Sie Benutzern eine der vordefinierten Rollen zuweisen. Informationen finden Sie in der Dokumentation *Verwaltung eines einzelnen Hosts von vSphere – VMware Host Client*.

Für verwaltete Hosts weisen Sie Rollen dem ESXi-Hostobjekt in der vCenter Server-Bestandsliste zu.

Einblick in das objektbezogene Berechtigungsmodell

Für einen Benutzer oder eine Gruppe autorisieren Sie die Ausführung von Aufgaben für vCenter Server-Objekte, indem Sie Berechtigungen für das Objekt verwenden. Wenn ein Benutzer versucht, einen Vorgang auszuführen, wird aus programmgesteuerter Sicht eine API-Methode ausgeführt. vCenter Server prüft die Berechtigungen für diese Methode, um zu ermitteln, ob der Benutzer für die Durchführung des Vorgangs autorisiert ist. Wenn beispielsweise ein Benutzer versucht, einen Host hinzuzufügen, wird die `AddStandaloneHost_Task`-Methode aufgerufen. Für diese Methode muss die Rolle für den Benutzer über die Berechtigung **Host. Bestandsliste.Eigenständigen Host hinzufügen** verfügen. Wenn bei der Prüfung dieses Recht nicht gefunden wird, wird dem Benutzer die Berechtigung zum Hinzufügen des Hosts verweigert.

Die folgenden Konzepte sind wichtig.

Berechtigungen

Jedem Objekt in der vCenter Server-Objekthierarchie sind Berechtigungen zugeordnet. Jede Berechtigung gibt für eine Gruppe oder einen Benutzer an, über welche Rechte diese Gruppe bzw. dieser Benutzer für das Objekt verfügt. Berechtigungen können an untergeordnete Objekte weitergegeben werden.

Benutzer und Gruppen

Auf vCenter Server-Systemen können Sie Rechte nur authentifizierten Benutzern oder Gruppen von authentifizierten Benutzern zuweisen. Die Benutzer werden über vCenter Single Sign On authentifiziert. Benutzer und Gruppen müssen in der Identitätsquelle definiert werden, die vCenter Single Sign On für die Authentifizierung verwendet. Definieren Sie Benutzer und Gruppen mithilfe der Tools in Ihrer Identitätsquelle, wie z. B. Active Directory.

Berechtigungen

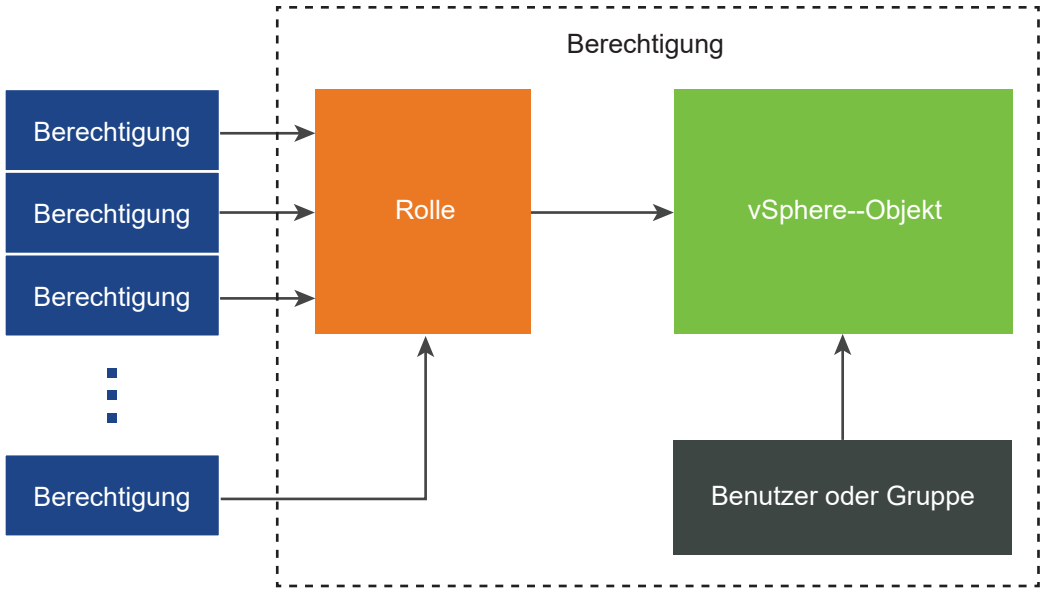
Rechte sind detaillierte Zugriffssteuerungsoptionen. Sie können diese Rechte nach Rollen gruppieren, die dann Benutzern oder Gruppen zugeordnet werden können.

Rollen

Rollen sind Gruppen von Rechten. Rollen ermöglichen die Zuweisung von Berechtigungen zu einem Objekt basierend auf typischen Aufgaben, die Benutzer ausführen. Systemrollen, wie z. B. Administrator, sind in vCenter Server vordefiniert und können nicht geändert werden. vCenter Server stellt auch bestimmte Standard-Beispielrollen bereit, wie z. B. Ressourcenpool-Administrator, die geändert werden können. Sie können benutzerdefinierte Rollen entweder von Grund auf neu oder aber durch Klonen und Ändern von Beispielrollen erstellen. Siehe Erstellen einer benutzerdefinierten vCenter Server-Rolle.

Die folgende Abbildung veranschaulicht, wie eine Berechtigung aus Rechten und Rollen erstellt und einem Benutzer oder einer Gruppe für ein vSphere-Objekt zugewiesen wird.

Abbildung 2-3. vSphere-Berechtigungen



Führen Sie die folgenden Schritte aus, um einem Objekt Berechtigungen zuzuweisen:

1. Wählen Sie das Objekt aus, auf das Sie die Berechtigung in der vCenter Server-Objekthierarchie anwenden möchten.
2. Wählen Sie die Gruppe oder den Benutzer aus, für die bzw. den Sie Rechte für das Objekt erteilen möchten.
3. Wählen Sie einzelne Rechte oder eine Rolle aus, bei der es sich um einen Satz von Rechten handelt, die die Gruppe bzw. der Benutzer für dieses Objekt haben sollte.

Standardmäßig ist „An untergeordnete Objekte weitergeben“ nicht ausgewählt. Sie müssen das Kontrollkästchen für die Gruppe oder den Benutzer aktivieren, damit die ausgewählte Rolle für das ausgewählte Objekt und dessen untergeordnete Objekte ausgewählt wird.

vCenter Server bietet Beispielrollen aus einer Kombination von häufig verwendeten Berechtigungssätzen. Sie können benutzerdefinierte Rollen auch erstellen, indem Sie einen Satz von Rollen kombinieren.

Oft müssen Berechtigungen sowohl für ein Quell- als auch für ein Zielobjekt definiert werden. Wenn Sie beispielsweise eine virtuelle Maschine verschieben, benötigen Sie Rechte für diese virtuelle Maschine, aber auch Rechte für das Zieldatencenter.

Siehe folgende Informationen.

Um mehr zu erfahren über…	Siehe…
Erstellen von benutzerdefinierten Rollen.	Erstellen einer benutzerdefinierten vCenter Server-Rolle
Alle Berechtigungen und die Objekte, auf die Sie die Berechtigungen anwenden können	Kapitel 16 Definierte Rechte
Gruppen von Berechtigungen, die für verschiedene Objekte und verschiedene Aufgaben erforderlich sind.	Erforderliche Berechtigungen für allgemeine Aufgaben

Das Berechtigungsmodell für eigenständige ESXi-Hosts ist einfacher. Weitere Informationen hierzu finden Sie unter Zuweisen von Rechten für ESXi-Hosts.

vCenter Server-Benutzervalidierung

vCenter Server-Systeme, die einen Verzeichnisdienst verwenden, validieren Benutzer und Gruppen regelmäßig anhand der Verzeichnisdomäne des Benutzers. Die Validierung wird in regelmäßigen Zeitabständen durchgeführt, die in den vCenter Server-Einstellungen angegeben sind. Beispiel: Dem Benutzer Schmidt wurde eine Rolle für mehrere Objekte zugewiesen. Der Domänenadministrator ändert den Namen in Schmidt2. Der Host folgert, dass Schmidt nicht mehr vorhanden ist, und entfernt während der nächsten Validierung die Berechtigungen von Benutzer Schmidt aus den vSphere-Objekten.

Wenn der Benutzer „Schmidt“ aus der Domäne entfernt wird, werden ebenfalls alle Berechtigungen für diesen Benutzer bei der nächsten Validierung entfernt. Wenn vor der nächsten Validierung ein neuer Benutzer namens „Schmidt“ zur Domäne hinzugefügt wird, ersetzt der neue Benutzer den alten Benutzer bei den Berechtigungen für ein Objekt.

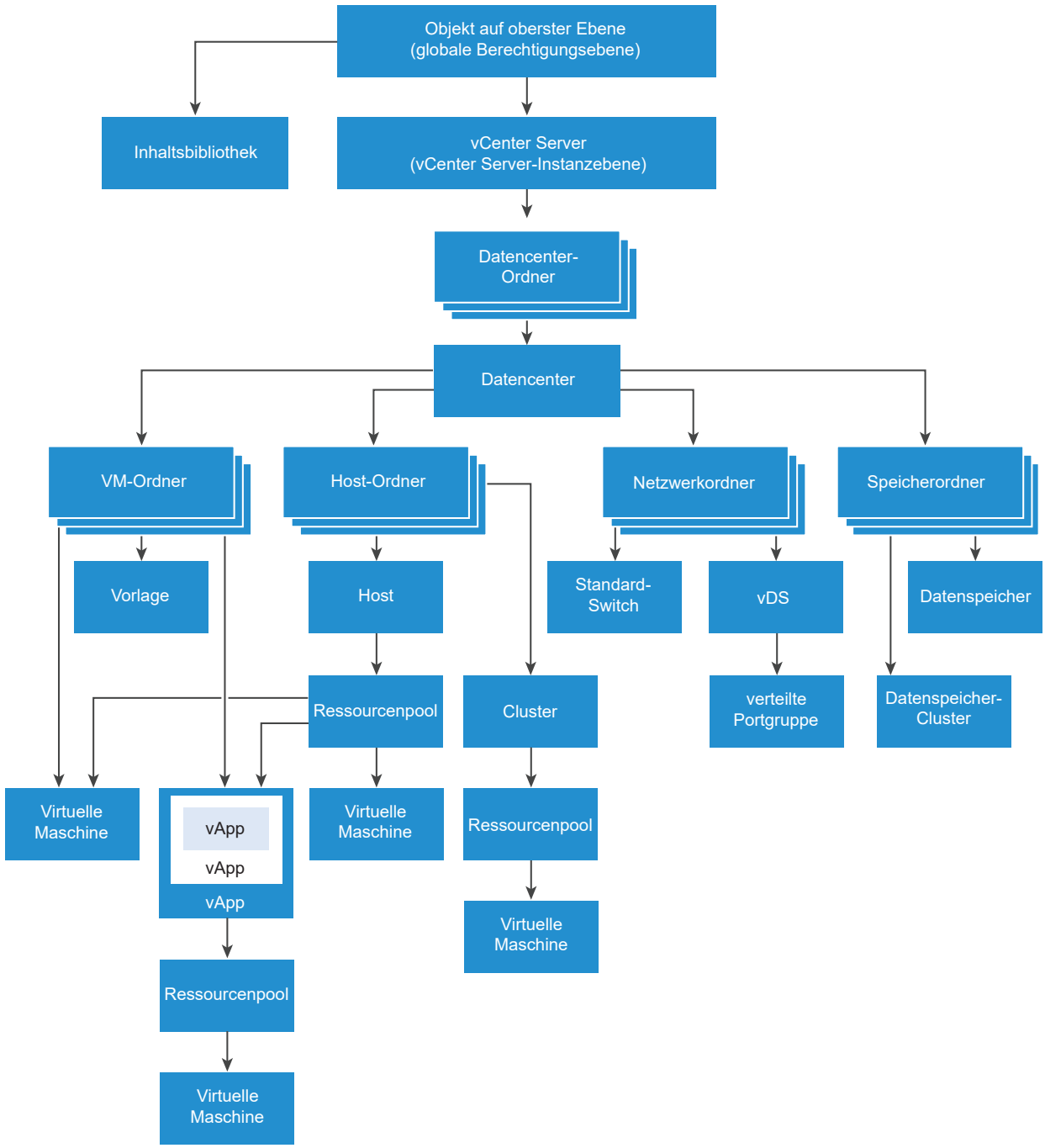
Hierarchische Vererbung von Berechtigungen

Wenn Sie einem Objekt eine Berechtigung zuweisen, können Sie auswählen, ob die Berechtigung über die Objekthierarchie nach unten weitergegeben wird. Sie legen die Weitergabe für jede Berechtigung fest. Die Weitergabe ist nicht universell einsetzbar. Für ein untergeordnetes Objekt definierte Berechtigungen setzen immer die von übergeordneten Objekten vererbten Berechtigungen außer Kraft.

In der folgenden Abbildung werden die Bestandslistenhierarchie und die Pfade dargestellt, über die Berechtigungen weitergegeben werden können.

Hinweis Globale Berechtigungen unterstützen das lösungsübergreifende Zuweisen von Berechtigungen von einem globalen Stammobjekt aus. Weitere Informationen hierzu finden Sie unter Globale Berechtigungen.

Abbildung 2-4. vSphere-Bestandslistenhierarchie



Über diese Abbildung:

- Sie können keine direkten Berechtigungen für die VM, den Host, das Netzwerk und die Speicherordner festlegen. Das heißt, diese Ordner fungieren als Container und sind daher für Benutzer nicht sichtbar.
- Sie können keine Berechtigungen für Standard-Switches festlegen.

Hinweis Um Berechtigungen auf einem vSphere Distributed Switch (VDS) festlegen und an untergeordnete Elemente weitergeben zu können, muss sich das Switchobjekt in einem Netzwerkordner befinden, der im Datencenter erstellt wurde.

Die meisten Bestandslistenobjekte übernehmen Berechtigungen von einem einzelnen übergeordneten Objekt in der Hierarchie. Beispielweise übernimmt ein Datenspeicher Berechtigungen entweder vom übergeordneten Datencenter-Ordner oder vom übergeordneten Datencenter. Virtuelle Maschinen übernehmen Berechtigungen sowohl von dem übergeordneten Ordner der virtuellen Maschine als auch vom übergeordneten Host, Cluster oder Ressourcenpool.

Legen Sie beispielsweise zum Festlegen von Berechtigungen für einen Distributed Switch und seine zugewiesenen verteilten Portgruppen Berechtigungen auf einem übergeordneten Objekt fest, z. B. auf einem Ordner oder Datencenter. Sie müssen auch die Option zum Weitergeben dieser Berechtigungen an untergeordnete Objekte wählen.

Berechtigungen nehmen in der Hierarchie verschiedene Formen an:

Verwaltete Instanzen

Verwaltete Elemente beziehen sich auf die folgenden vSphere-Objekte. Verwaltete Elemente bieten bestimmte Vorgänge, die je nach Entitätstyp variieren. Berechtigte Benutzer können Berechtigungen auf verwalteten Elemente definieren. Weitere Informationen zu vSphere-Objekten, -Eigenschaften und -Methoden finden Sie in der vSphere API-Dokumentation.

- Cluster
- Datencenter
- Datenspeicher
- Datenspeicher-Cluster
- Ordner
- „Hosts“
- Netzwerke (außer vSphere Distributed Switches)
- Verteilte Portgruppen
- Ressourcenpools
- Vorlagen
- virtuelle Maschinen

- vSphere-vApps

Globale Instanzen

Sie können keine Berechtigungen für Instanzen ändern, die ihre Berechtigungen aus dem vCenter Server-Stammsystem ableiten.

- Benutzerdefinierte Felder
- Lizenzen
- Rollen
- Statistikintervalle
- Sitzungen

Einstellungen für Mehrfachberechtigungen

Objekte können über mehrere Berechtigungen verfügen, jedoch nur über eine Berechtigung für jeden Benutzer bzw. jede Gruppe. Eine Berechtigung könnte zum Beispiel festlegen, dass GroupAdmin über die Administratorrolle für ein Objekt verfügt. Eine andere Berechtigung könnte festlegen, dass der GroupVMAdmin über die VM-Administratorrolle für dasselbe Objekt verfügt. Die GroupVMAdmin-Gruppe kann jedoch über keine weitere Berechtigung für dieselbe GroupVMAdmin für dieses Objekt verfügen.

Ein untergeordnetes Objekt übernimmt die Berechtigungen seines übergeordneten Objekts, wenn die Eigenschaft „Weitergeben“ des übergeordneten Objekts auf „true“ festgelegt ist. Eine Berechtigung, die direkt für ein untergeordnetes Objekt festgelegt wird, setzt die Berechtigung im übergeordneten Objekt außer Kraft. Weitere Informationen hierzu finden Sie unter Beispiel 2: Untergeordnete Berechtigungen, die übergeordnete Berechtigungen außer Kraft setzen.

Wenn für dasselbe Objekt mehrere Gruppenrollen definiert sind und ein Benutzer mindestens zwei dieser Gruppen angehört, gibt es zwei mögliche Situationen:

- Direkt für das Objekt wurde keine Berechtigung für den Benutzer definiert. In diesem Fall erhält der Benutzer die Summe der Berechtigungen, die die Gruppen für das Objekt haben.
- Es wurde eine Berechtigung für den Benutzer für das Objekt festgelegt. In diesem Fall haben die Berechtigungen für den Benutzer Vorrang vor allen Gruppenberechtigungen.

Beispiel 1: Berechtigungsübernahme von mehreren Gruppen

Dieses Beispiel zeigt, wie ein Objekt mehrere Berechtigungen von Gruppen übernehmen kann, die auf einem übergeordneten Objekt Berechtigungen erhalten haben.

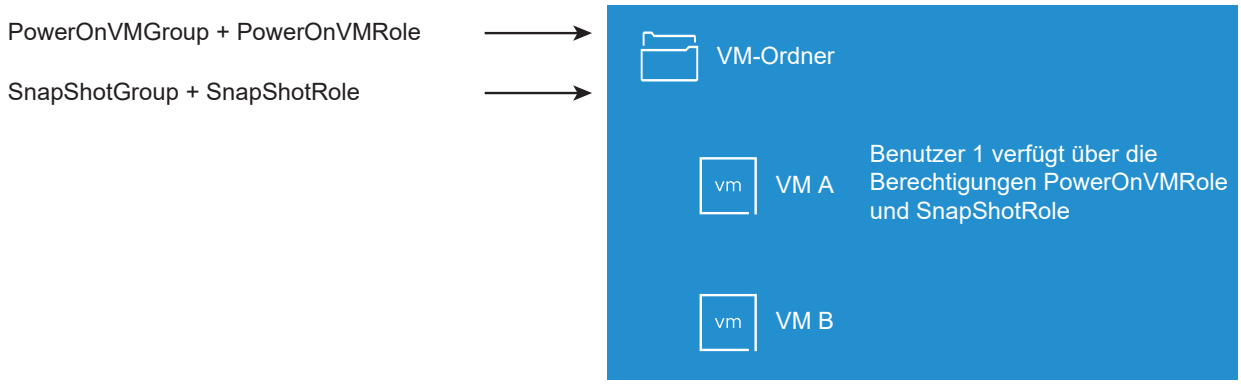
In diesem Beispiel werden zwei verschiedenen Gruppen zwei Berechtigungen für das gleiche Objekt zugewiesen.

- PowerOnVMRole kann virtuelle Maschinen einschalten.
- SnapShotRole kann Snapshots von virtuellen Maschinen erstellen.

- PowerOnVMGroup wird PowerOnVMRole auf VM-Ordner zugeteilt, mit der Berechtigung „An untergeordnete Objekte weitergeben“.
- SnapShotGroup wird SnapShotRole auf VM-Ordner zugeteilt, mit der Berechtigung „An untergeordnete Objekte weitergeben“.
- Benutzer 1 werden keine speziellen Rechte zugewiesen.

Benutzer 1, der sowohl zur PowerOnVMGroup als auch zur SnapShotGroup gehört, meldet sich an. Benutzer 1 kann sowohl VM A als auch VM B einschalten und von beiden Snapshots erstellen.

Abbildung 2-5. Beispiel 1: Berechtigungsübernahme von mehreren Gruppen



Beispiel 2: Untergeordnete Berechtigungen, die übergeordnete Berechtigungen außer Kraft setzen

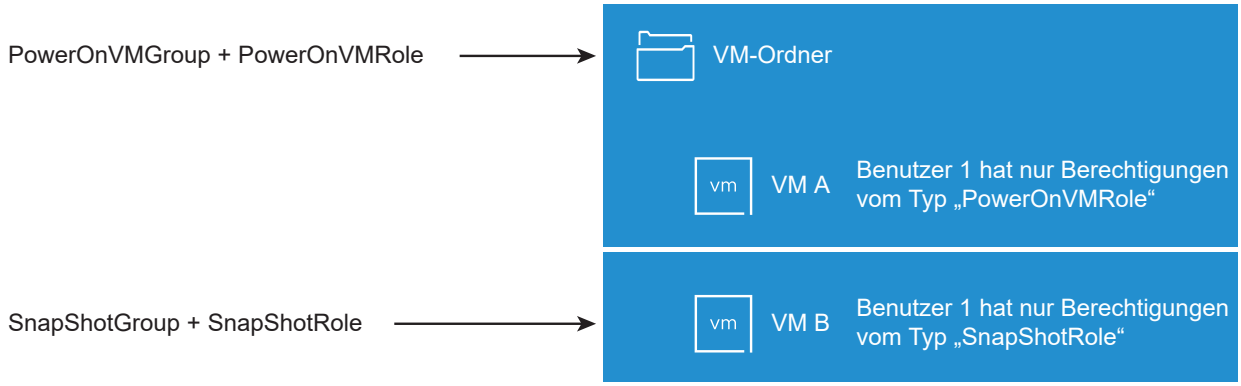
Dieses Beispiel zeigt, wie Berechtigungen, die einem untergeordneten Objekt zugewiesen wurden, die Berechtigungen, die einem übergeordneten Objekt zugewiesen wurden, außer Kraft setzen. Sie können dieses Verhalten dazu verwenden, um den Benutzerzugriff auf bestimmte Bereiche der Bestandsliste einzuschränken.

In diesem Beispiel werden Berechtigungen für zwei verschiedene Objekte und für zwei verschiedene Gruppen definiert.

- PowerOnVMRole kann virtuelle Maschinen einschalten.
- SnapShotRole kann Snapshots von virtuellen Maschinen erstellen.
- PowerOnVMGroup wird PowerOnVMRole auf VM-Ordner zugeteilt, mit der Berechtigung „An untergeordnete Objekte weitergeben“.
- SnapShotGroup wird SnapShotRole auf VM B zugeteilt.

Benutzer 1, der sowohl zur PowerOnVMGroup als auch zur SnapShotGroup gehört, meldet sich an. Weil SnapShotRole auf einer niedrigeren Hierarchieebene zugewiesen wird wie PowerOnVMRole, setzt sie PowerOnVMRole auf VM B außer Kraft. Benutzer 1 kann zwar VM A einschalten, aber keinen Snapshot erstellen. Benutzer 1 kann zwar Snapshots von VM B erstellen, aber sie nicht einschalten.

Abbildung 2-6. Beispiel 2: Untergeordnete Berechtigungen, die übergeordnete Berechtigungen außer Kraft setzen



Beispiel 3: Benutzerrolle, die Gruppenrolle außer Kraft setzt

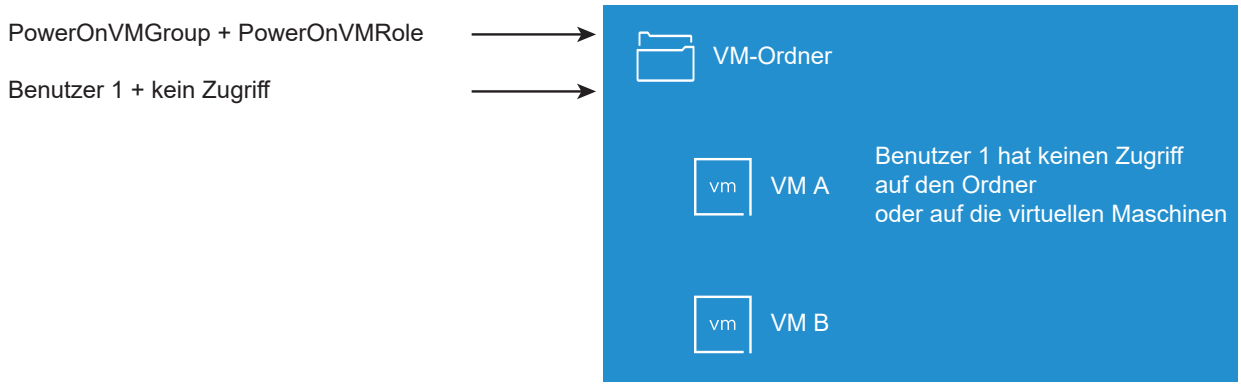
Dieses Beispiel zeigt, wie die einem individuellen Benutzer direkt zugewiesene Rolle die Rechte einer Rolle überschreibt, die einer Gruppe zugeordnet ist.

In diesem Beispiel werden Berechtigungen für dasselbe Objekt definiert. Eine Berechtigung ordnet einer Gruppe eine Rolle zu, die andere Berechtigung ordnet einem individuellen Benutzer eine Rolle zu. Der Benutzer ist ein Mitglied der Gruppe.

- PowerOnVMRole kann virtuelle Maschinen einschalten.
- PowerOnVMGroup wird PowerOnVMRole auf VM-Ordner zugeteilt.
- Benutzer 1 erhält die NoAccess-Rolle auf VM-Ordner.

Benutzer 1, der zur PowerOnVMGroup gehört, meldet sich an. Die dem Benutzer 1 zugeteilte NoAccess-Rolle für den VM-Ordner überschreibt die der Gruppe zugewiesene Rolle. Benutzer 1 hat keinen Zugriff auf den VM-Ordner oder die VMs A und B. Die VMs A und B sind in der Hierarchie für Benutzer 1 nicht sichtbar.

Abbildung 2-7. Beispiel 3: Benutzerberechtigungen, die Gruppenberechtigungen außer Kraft setzen



Verwalten von Berechtigungen für vCenter-Komponenten

Eine Berechtigung wird für ein Objekt in der vCenter-Objekthierarchie festgelegt. Jede Berechtigung ordnet das Objekt einer Gruppe bzw. einem Benutzer sowie den Zugriffsrollen der Gruppe bzw. des Benutzers zu. Beispielsweise können Sie ein VM-Objekt auswählen, eine Berechtigung zum Erteilen der Rolle „Nur Lesen“ (ReadOnly) für Gruppe 1 und eine zweite Berechtigung zum Erstellen der Administratorrolle für Benutzer 2 hinzufügen.

Indem Sie einer Gruppe von Benutzern verschiedene Rollen für verschiedene Objekte zuweisen, können Sie steuern, welche Aufgaben Benutzer in Ihrer vSphere-Umgebung ausführen können. Wenn Sie beispielsweise einer Gruppe das Konfigurieren von Arbeitsspeicher für den Host erlauben möchten, wählen Sie den entsprechenden Host aus und fügen eine Berechtigung hinzu, mit der der Gruppe eine Rolle erteilt wird, die das Recht **Host.Konfiguration.Arbeitsspeicherkonfiguration** enthält.

Konzeptuelle Informationen zu Berechtigungen finden Sie in der Diskussion unter Einblick in das objektbezogene Berechtigungsmodell.

Sie können Objekten auf verschiedenen Hierarchieebenen Berechtigungen zuweisen. Beispielsweise können Sie einem Hostobjekt oder einem Ordnerobjekt, das alle Hostobjekte beinhaltet, Berechtigungen zuweisen. Siehe Hierarchische Vererbung von Berechtigungen. Darüber hinaus können Sie einem globalen Stammobjekt Weitergabeberechtigungen zuweisen, um die Berechtigungen auf alle Objekte in allen Lösungen anzuwenden. Weitere Informationen hierzu finden Sie unter Globale Berechtigungen.

Hinzufügen einer Berechtigung zu einem Bestandslistenobjekt

Nachdem Sie Benutzer und Gruppen erstellen und Rollen festlegen, müssen Sie die Benutzer und Gruppen und ihre Rollen den relevanten Bestandslistenobjekten zuordnen. Sie können dieselben Berechtigungen gleichzeitig mehreren Objekten zuweisen, indem Sie die Objekte in einen Ordner verschieben und die Berechtigungen für den Ordner festlegen.

Wenn Sie Berechtigungen zuweisen, müssen die Benutzer- und Gruppennamen denjenigen in Active Directory genau entsprechen, einschließlich der Groß- und Kleinschreibung. Wenn nach einem Upgrade von einer früheren Version von vSphere Probleme mit Gruppen auftreten, überprüfen Sie, ob Inkonsistenzen bei der Groß-/Kleinschreibung vorliegen.

Voraussetzungen

Für das Objekt, dessen Berechtigungen Sie ändern möchten, benötigen Sie eine Rolle, die das Recht **Berechtigungen.Berechtigung ändern** beinhaltet.

Verfahren

1. Navigieren Sie im Objektnavigator des vSphere Client zu dem Objekt, für das Sie Berechtigungen zuweisen möchten.
2. Klicken Sie auf die Registerkarte **Berechtigungen**.
3. Klicken Sie auf **Hinzufügen**.

4 (Optional) Wenn Sie einen externen Identitätsanbieter für die Verbundauthentifizierung konfiguriert haben, kann die Domäne dieses Identitätsanbieters im Dropdown-Menü **Domäne** ausgewählt werden.

5 Wählen Sie den Benutzer oder die Gruppe aus, für den bzw. die die Rechte mithilfe der ausgewählten Rolle definiert werden.

   a Wählen Sie im Dropdown-Menü **Domäne** die Domäne für den Benutzer oder die Gruppe aus.

   b Geben Sie einen Namen im Feld „Suchen“ ein.

   Das System sucht nach Benutzer- und Gruppennamen.

   c Wählen Sie den Benutzer oder die Gruppe aus.

6 Wählen Sie eine Rolle aus dem Dropdown-Menü **Rolle** aus.

7 (Optional) Zur Weitergabe der Berechtigungen aktivieren Sie das Kontrollkästchen **An untergeordnete Objekte weitergeben**.

   Die Rolle wird auf das ausgewählte Objekt angewendet und an die untergeordneten Objekte weitergegeben.

8 Klicken Sie auf **OK**.

Ändern oder Entfernen von Berechtigungen

Wenn eine Kombination aus Rolle und Benutzer oder Gruppe für ein Bestandslistenobjekt festgelegt wurde, können Sie Änderungen an der Rolle für den Benutzer oder die Gruppe vornehmen oder die Einstellung des Kontrollkästchens **An untergeordnete Objekte weitergeben** ändern. Sie können auch die Berechtigungseinstellung entfernen.

Verfahren

1 Navigieren Sie zum Objekt im Objektnavigator des vSphere Client.

2 Klicken Sie auf die Registerkarte **Berechtigungen**.

3 Klicken Sie auf eine Zeile, um eine Berechtigung auszuwählen.

Aufgabe	Schritte
Ändern von Berechtigungen	a Klicken Sie auf das Symbol **Rolle ändern**. b Wählen Sie im Dropdown-Menü **Rolle** eine Rolle für den Benutzer oder die Gruppe aus. c Aktivieren Sie das Kontrollkästchen **An untergeordnete Objekte weitergeben**, um die Vererbung von Berechtigungen zu ändern. d Klicken Sie auf **OK**.
Entfernen von Berechtigungen	Klicken Sie auf das Symbol **Berechtigung entfernen**.

Ändern der Einstellungen für die Benutzervalidierung

vCenter Server validiert die Benutzer- und Gruppenlisten regelmäßig anhand der Benutzer und Gruppen im Benutzerverzeichnis. Er entfernt anschließend Benutzer oder Gruppen, die nicht mehr in der Domäne vorhanden sind. Sie können das Validieren deaktivieren oder das Intervall zwischen Validierungen ändern. Wenn Sie über Domänen mit Tausenden von Benutzern oder Gruppen verfügen oder wenn Suchvorgänge viel Zeit in Anspruch nehmen, sollten Sie eventuell die Sucheinstellungen anpassen.

Für vCenter Server-Versionen vor vCenter Server 5.0 gelten diese Einstellungen für eine Active Directory-Instanz, die vCenter Server zugeordnet ist. Für vCenter Server 5.0 und höher gelten diese Einstellungen für vCenter Single Sign On-Identitätsquellen.

Hinweis Die beschriebene Vorgehensweise bezieht sich nur auf vCenter Server-Benutzerlisten. ESXi-Benutzerlisten können nicht auf diese Weise durchsucht werden.

Verfahren

1 Navigieren Sie im Objektnavigator des vSphere Client zum vCenter Server-System.

2 Wählen Sie **Konfigurieren** und klicken Sie auf **Einstellungen > Allgemein**.

3 Klicken Sie auf **Bearbeiten** und wählen Sie **Benutzerverzeichnis** aus.

4 Ändern Sie die Werte nach Bedarf und klicken Sie auf **Speichern**.

Option	Beschreibung
Benutzerverzeichnis - Zeitüberschreitung	Zeitüberschreitungsintervall in Sekunden für das Herstellen einer Verbindung mit dem Active Directory-Server. Dieser Wert gibt an, wie lange die Suche für die ausgewählte Domäne in vCenter Server höchstens dauern darf. Das Suchen in großen Domänen kann sehr lange dauern.
Abfragegrenze	Aktivieren Sie die Option, um die maximale Anzahl von Benutzern und Gruppen festzulegen, die vCenter Server anzeigt.
Größe der Abfragegrenze	Maximale Anzahl der Benutzer und Gruppen der ausgewählten Domäne, die von vCenter Server im Dialogfeld **Benutzer oder Gruppen auswählen** angezeigt werden. Bei Eingabe des Werts 0 (Null) werden alle Benutzer und Gruppen angezeigt.

Globale Berechtigungen

Globale Berechtigungen werden auf ein globales Stammobjekt angewendet, das für mehrere Lösungen verwendet wird. In einem lokalen SDDC können sich globale Berechtigungen sowohl auf vCenter Server als auch auf vRealize Orchestrator erstrecken. Für jedes vSphere SDDC gelten jedoch globale Berechtigungen für globale Objekte wie Tags und Inhaltsbibliotheken.

Sie können Benutzern oder Gruppen globale Berechtigungen zuweisen und für jeden Benutzer oder jede Gruppe die Rolle festlegen. Die Rolle bestimmt die Rechte, über die der Benutzer oder die Gruppe für alle Objekte in der Hierarchie verfügt. Sie können eine vordefinierte Rolle zuweisen oder benutzerdefinierte Rollen erstellen. Weitere Informationen hierzu finden Sie unter Verwenden von Rollen zum Zuweisen von Rechten.

Sie sollten unbedingt zwischen vCenter Server-Berechtigungen und globalen Berechtigungen unterscheiden.

vCenter Server-Berechtigungen

In der Regel wenden Sie eine Berechtigung auf ein vCenter Server-Bestandslistenobjekt an, wie beispielsweise eine virtuelle Maschine. Dabei geben Sie an, dass ein Benutzer oder eine Gruppe über eine Rolle (eine Reihe von Berechtigungen) für das Objekt verfügt.

Globale Berechtigungen

Mithilfe von globalen Berechtigungen werden einem Benutzer oder einer Gruppe Rechte zum Anzeigen oder Verwalten aller Objekte in allen Bestandslistenhierarchien Ihrer Bereitstellung erteilt. Globale Berechtigungen gelten auch für globale Objekte wie Tags und Inhaltsbibliotheken. Weitere Informationen hierzu finden Sie unter Berechtigungen für Tag-Objekte.

Wenn Sie eine globale Berechtigung zuweisen und „Weitergeben“ nicht auswählen, haben die Benutzer oder Gruppen, denen diese Berechtigung zugeordnet ist, keinen Zugriff auf die Objekte in der Hierarchie. Sie haben nur Zugriff auf bestimmte globale Funktionen wie etwa das Erstellen von Rollen.

Wichtig Globale Berechtigungen sollten Sie mit Vorsicht verwenden. Vergewissern Sie sich, ob wirklich allen Objekten in allen Bestandslistenhierarchien Berechtigungen zugewiesen werden sollen.

Hinzufügen einer globalen Berechtigung

Mithilfe von globalen Berechtigungen können Sie einem Benutzer oder einer Gruppe Rechte für alle Objekte in allen Bestandslistenhierarchien Ihrer Bereitstellung erteilen.

Wichtig Globale Berechtigungen sollten Sie mit Vorsicht verwenden. Vergewissern Sie sich, ob wirklich allen Objekten in allen Bestandslistenhierarchien Berechtigungen zugewiesen werden sollen.

Voraussetzungen

Um diese Aufgabe auszuführen, benötigen Sie das Recht **Berechtigungen.Berechtigung ändern** für das Stammobjekt aller Bestandslistenhierarchien.

Verfahren

1 Melden Sie sich beim vCenter Server mit dem vSphere Client an.

2 Wählen Sie **Verwaltung** aus und klicken Sie im Zugriffssteuerungsbereich auf **Globale Berechtigungen**.

3 Wählen Sie die Domäne im Dropdown-Menü **Berechtigungsanbieter** aus.

4 (Optional) Wenn Sie einen externen Identitätsanbieter für die Verbundauthentifizierung konfiguriert haben, kann die Domäne dieses Identitätsanbieters im Dropdown-Menü **Domäne** ausgewählt werden.

5 Klicken Sie auf **Hinzufügen**.

6 Wählen Sie den Benutzer oder die Gruppe aus, für den bzw. die die Rechte mithilfe der ausgewählten Rolle definiert werden.

   a Wählen Sie im Dropdown-Menü **Domäne** die Domäne für den Benutzer oder die Gruppe aus.

   b Geben Sie einen Namen im Feld „Suchen“ ein.

      Das System sucht nach Benutzer- und Gruppennamen.

   c Wählen Sie den Benutzer oder die Gruppe aus.

7 Wählen Sie eine Rolle aus dem Dropdown-Menü **Rolle** aus.

8 Geben Sie an, ob die Berechtigungen weitergegeben werden sollen, indem Sie das Kontrollkästchen **An untergeordnete Objekte weitergeben** aktivieren.

   Wenn Sie eine globale Berechtigung zuweisen und **An untergeordnete Objekte weitergeben** nicht aktivieren, haben die Benutzer oder Gruppen, denen diese Berechtigung zugeordnet ist, keinen Zugriff auf die Objekte in der Hierarchie. Sie haben nur Zugriff auf bestimmte globale Funktionen wie etwa das Erstellen von Rollen.

9 Klicken Sie auf **OK**.

Berechtigungen für Tag-Objekte

In der Objekthierarchie von vCenter Server sind Tag-Objekte keine untergeordneten Objekte von vCenter Server, sondern werden auf der obersten Ebene von vCenter Server erstellt. In Umgebungen mit mehreren vCenter Server-Instanzen werden Tag-Objekte von vCenter Server-Instanzen gemeinsam genutzt. Die Berechtigungen für Tag-Objekte unterscheiden sich von Berechtigungen für andere Objekte in der Objekthierarchie von vCenter Server.

Nur globale Berechtigungen oder dem Tag-Objekt zugewiesene Berechtigungen werden angewendet

Wenn Sie einem Benutzer Berechtigungen für ein vCenter Server-Bestandslistenobjekt wie beispielsweise eine virtuelle Maschine erteilen, kann der Benutzer die mit der Berechtigung verbundenen Aufgaben durchführen. Der Benutzer kann jedoch keine Tag-Vorgänge für das Objekt durchführen.

Wenn Sie beispielsweise das Recht **vSphere-Tag zuweisen** der Benutzerin Dana auf dem Host TPA gewähren, hat diese Berechtigung keine Auswirkungen darauf, ob Dana Tags auf dem Host TPA zuweisen kann. Dana benötigt das Recht **vSphere-Tag zuweisen** auf der obersten Ebene, d. h. eine globale Berechtigung, oder sie benötigt das Recht für das Tag-Objekt.

Tabelle 2-1. Festlegung der durch Benutzer ausführbaren Aktionen mittels globaler Berechtigungen und Berechtigungen für Tag-Objekte

Globale Berechtigung	Berechtigung auf Tag-Ebene	vCenter Server-Berechtigung auf Objektebene	Effektive Berechtigung
Es sind keine Tag-Berechtigungen zugewiesen.	Dana verfügt über das Recht **vSphere-Tag zuweisen oder Zuweisung aufheben** für das Tag.	Dana verfügt über das Recht **vSphere-Tag löschen** für ESXi-Host-TPA.	Dana verfügt über das Recht **vSphere-Tag zuweisen oder Zuweisung aufheben** für das Tag.
Dana verfügt über das Recht **vSphere-Tag zuweisen oder Zuweisung aufheben**.	Für das Tag sind keine Rechte zugewiesen.	Dana verfügt über das Recht **vSphere-Tag löschen** für ESXi-Host-TPA.	Dana verfügt über das globale Recht **vSphere-Tag zuweisen oder Zuweisung aufheben**. Dies beinhaltet Rechte auf der Tag-Ebene.
Es sind keine Tag-Berechtigungen zugewiesen.	Für das Tag sind keine Rechte zugewiesen.	Dana verfügt über das Recht **vSphere-Tag zuweisen oder Zuweisung aufheben** für ESXi-Host-TPA.	Dana verfügt über keine Tag-Berechtigungen für Objekte, einschließlich Host-TPA.

Globale Berechtigungen ergänzen Berechtigungen für Tag-Objekte

Globale Berechtigungen, also für das Objekt der obersten Ebene zugewiesene Berechtigungen, ergänzen die Berechtigungen für Tag-Objekte, wenn die Berechtigungen für die Tag-Objekte restriktiver sind. Die vCenter Server-Berechtigungen haben keine Auswirkungen auf die Tag-Objekte.

Angenommen, Sie weisen das Recht **vSphere-Tag löschen** dem Benutzer Robin auf der obersten Ebene zu, d. h. mithilfe von globalen Berechtigungen. Für das Tag „Production“ weisen Sie dem Benutzer Robin nicht das Recht **vSphere-Tag löschen** zu. In diesem Fall verfügt Robin für das Tag „Production“ über dieses Recht, da Robin über die globale Berechtigung verfügt, die von der obersten Ebene aus weitergegeben wird. Berechtigungen können Sie nur beschränken, indem Sie die globale Berechtigung ändern.

Tabelle 2-2. Globale Berechtigungen ergänzen Berechtigungen auf Tag-Ebene

Globale Berechtigung	Berechtigung auf Tag-Ebene	Effektive Berechtigung
Robin verfügt über das Recht **vSphere-Tag löschen**.	Robin verfügt nicht über das Recht **vSphere-Tag löschen** für das Tag.	Robin verfügt über das Recht **vSphere-Tag löschen**.
Es sind keine Tag-Berechtigungen zugewiesen.	Robin ist das Recht **vSphere-Tag löschen** nicht für das Tag zugewiesen.	Robin verfügt nicht über das Recht **vSphere-Tag löschen**.

Berechtigungen auf Tag-Ebene können globale Berechtigungen erweitern

Mithilfe von Berechtigungen auf Tag-Ebene können Sie globale Berechtigungen erweitern. Dies bedeutet, dass Benutzer sowohl über eine globale Berechtigung als auch über eine Berechtigung auf Tag-Ebene für ein Tag verfügen können.

Hinweis Dieses Verhalten unterscheidet sich von der Art und Weise, wie vCenter Server-Berechtigungen übernommen werden. Für ein untergeordnetes Objekt definierte Berechtigungen in vCenter Server setzen immer die von übergeordneten Objekten vererbten Berechtigungen außer Kraft.

Tabelle 2-3. Globale Berechtigungen erweitern Berechtigungen auf Tag-Ebene

Globale Berechtigung	Berechtigung auf Tag-Ebene	Effektive Berechtigung
Lee verfügt über das Recht **vSphere-Tag zuweisen oder Zuweisung aufheben**.	Lee verfügt über das Recht **vSphere-Tag löschen**.	Lee verfügt über die Rechte **vSphere-Tag zuweisen** und **vSphere-Tag löschen** für das Tag.
Es sind keine Tag-Berechtigungen zugewiesen.	Lee ist das Recht **vSphere-Tag löschen** für das Tag zugewiesen.	Lee verfügt über das Recht **vSphere-Tag löschen** für das Tag.

Verwenden von Rollen zum Zuweisen von Rechten

Bei einer Rolle handelt es sich um einen vordefinierten Satz an Rechten. Berechtigungen definieren Leseeigenschaften und Rechte zum Ausführen von Aktionen. Die Rolle des VM-Administrators ermöglicht beispielsweise einem Benutzer, die Attribute einer virtuellen Maschine zu lesen und zu ändern.

Beim Zuweisen von Berechtigungen weisen Sie einen Benutzer oder einer Gruppe einer Rolle zu und verknüpfen diese Zuweisung mit einem Bestandslistenobjekt. Ein Benutzer oder eine Gruppe kann verschiedene Rollen für verschiedene Objekte in der Bestandsliste aufweisen.

Nehmen Sie z. B. an, dass zwei Ressourcenpools in Ihrer Bestandsliste vorhanden sind: Pool A und Pool B. Sie können der Gruppe „Vertrieb“ die VM-Benutzerrolle auf Pool A und die Nur-Lese-Rolle auf Pool B zuweisen. Mit diesen Zuweisungen können die Benutzer der Gruppe „Vertrieb“ die virtuellen Maschinen in Pool A einschalten, aber die virtuellen Maschinen in Pool B nur anzeigen.

vCenter Server bietet standardmäßig System- und Beispielrollen.

Systemrollen

Systemrollen sind dauerhaft. Sie können die Berechtigungen, die diesen Rollen zugewiesen sind, nicht bearbeiten.

Beispielrollen

VMware bietet Beispielrollen für einige gängige Aufgabenkombinationen. Diese Rollen können Sie klonen, abändern oder entfernen.

Hinweis Um die vordefinierten Einstellungen einer Rolle nicht zu verlieren, sollten Sie die Rolle zunächst klonen und die gewünschten Änderungen dann am Klon vornehmen. Das Beispiel kann nicht auf die Standardeinstellungen zurückgesetzt werden.

Ein Benutzer kann eine Aufgabe nur dann planen, wenn er zum Zeitpunkt der Aufgabenerstellung eine Rolle mit der Berechtigung zum Ausführen dieser Aufgabe besitzt.

Hinweis Änderungen an Berechtigungen und Rollen werden sofort wirksam, auch wenn die betroffenen Benutzer gerade angemeldet sind. Eine Ausnahme bilden Änderungen an Suchberechtigungen, denn diese Änderungen werden erst wirksam, wenn der Benutzer sich abgemeldet und wieder angemeldet hat.

Benutzerdefinierte Rollen in vCenter Server und ESXi

Sie können benutzerdefinierte Rollen für vCenter Server und alle von ihm verwalteten Objekte oder für einzelne Hosts erstellen.

Benutzerdefinierte Rolle in vCenter Server (empfohlen)

Benutzerdefinierte Rollen können Sie mit den Rollenbearbeitungsdienstprogrammen im vSphere Client erstellen und an Ihre Anforderungen anpassen.

Benutzerdefinierte Rollen in ESXi

Sie können mithilfe einer Befehlszeilenschnittstelle oder des VMware Host Client Rollen für einzelne Hosts erstellen. Informationen finden Sie in der Dokumentation *Verwaltung eines einzelnen Hosts von vSphere – VMware Host Client*. Auf benutzerdefinierte Hostrollen ist in vCenter Server kein Zugriff möglich.

Wenn Sie ESXi-Hosts über vCenter Server verwalten, unterhalten Sie keine benutzerdefinierten Rollen sowohl auf dem Host als auch auf dem vCenter Server. Definieren Sie Rollen auf der vCenter Server-Ebene.

Bei der Verwaltung von Hosts mit vCenter Server werden die zugehörigen Berechtigungen mit vCenter Server erstellt und in vCenter Server gespeichert. Bei Direktverbindungen mit dem Host sind nur jene Rollen verfügbar, die direkt auf dem Host erstellt wurden.

Hinweis Wenn Sie eine benutzerdefinierte Rolle hinzufügen, ohne ihr Berechtigungen zuzuweisen, wird sie als schreibgeschützte Rolle mit drei systemdefinierten Berechtigungen erstellt: **System. Anonym**, **System.Anzeigen** und **System.Lesen**. Diese Berechtigungen sind im vSphere Client nicht sichtbar, werden jedoch zum Lesen bestimmter Eigenschaften einiger verwalteter Objekte verwendet. Alle vordefinierten Rollen in vCenter Server enthalten diese drei systemdefinierten Berechtigungen. Weitere Informationen finden Sie in der Dokumentation *vSphere Web Services-API*.

Erstellen einer benutzerdefinierten vCenter Server-Rolle

Sie können benutzerdefinierte vCenter Server-Rollen erstellen, um den Zugriff entsprechend den Anforderungen Ihrer Umgebung zu steuern. Sie können eine Rolle erstellen oder eine vorhandene Rolle klonen.

Sie können eine Rolle in einem vCenter Server-System erstellen oder bearbeiten, das Teil derselben vCenter Single Sign-On-Domäne wie andere vCenter Server-Systeme ist. Der VMware Directory Service (vmdir) propagiert die von Ihnen vorgenommenen Rollenänderungen an alle anderen vCenter Server-Systeme in der Gruppe. Zuweisungen von Rollen zu bestimmten Benutzern und Objekten werden innerhalb von vCenter Server-Systemen jedoch nicht weitergegeben.

Voraussetzungen

Stellen Sie sicher, dass Sie mit Administratorrechten angemeldet sind.

Verfahren

1 Melden Sie sich beim vCenter Server mit dem vSphere Client an.

2 Wählen Sie **Verwaltung** aus und klicken Sie auf **Rollen** im Bereich **Zugriffssteuerung**.

3 Erstellen Sie die Rolle:

Option	Beschreibung
So erstellen Sie eine Rolle:	Klicken Sie auf **Neu**.
Erstellen der Rolle durch Klonen	Wählen Sie eine Rolle aus und klicken Sie auf **Klonen**.

Weitere Informationen hierzu finden Sie unter vCenter Server-Systemrollen.

4 Geben Sie einen Namen für die neue Rolle ein.

5 Aktivieren und deaktivieren Sie Rechte für die Rolle.

Führen Sie einen Bildlauf durch die Berechtigungskategorien durch und wählen Sie alle Rechte oder eine Teilmenge der Rechte für diese Kategorie aus. Sie können alle, ausgewählte oder nicht ausgewählte Kategorien anzeigen. Sie können auch alle, ausgewählte oder nicht ausgewählte Berechtigungen anzeigen.

Weitere Informationen hierzu finden Sie unter Kapitel 16 Definierte Rechte.

Hinweis Wenn Sie eine geklonte Rolle erstellen, können Rechte nicht geändert werden. Zum Ändern von Berechtigungen wählen Sie die geklonte Rolle aus und klicken auf **Bearbeiten**.

6 Klicken Sie auf **Hinzufügen**.

Nächste Schritte

Sie können nun Berechtigungen erstellen, indem Sie ein Objekt auswählen und für dieses Objekt die Rolle einem Benutzer oder einer Gruppe zuweisen.

vCenter Server-Systemrollen

Bei einer Rolle handelt es sich um einen vordefinierten Satz an Rechten. Wenn Sie einem Objekt Berechtigungen hinzufügen, koppeln Sie einen Benutzer oder eine Gruppe mit einer Rolle. vCenter Server enthält einige Standardsystemrollen, die Sie nicht ändern können.

vCenter Server enthält mehrere Standardrollen. Es ist nicht möglich, die Rechte für die Standardrollen zu ändern. Die Standardrollen sind hierarchisch angeordnet. Jede Rolle übernimmt die Rechte der vorherigen Rolle. So übernimmt beispielsweise die Rolle „Administrator“ die Rechte der Rolle „Nur lesen“.

Um die mit einer Standardrolle verknüpften Rechte anzuzeigen, navigieren Sie zu der Rolle im vSphere Client (**Menü > Verwaltung > Rollen**) und klicken Sie auf die Registerkarte **Rechte** .

Informationen zum Anzeigen aller vSphere-Berechtigungen und -Beschreibungen finden Sie unter Kapitel 16 Definierte Rechte.

Die Hierarchie der vCenter Server-Rollen enthält auch mehrere Beispielrollen. Sie können eine Beispielrolle klonen, um eine ähnliche Rolle zu erstellen.

Wenn Sie eine Rolle erstellen, übernimmt diese keine Rechte von Systemrollen.

Administratorrolle

Benutzer mit der Administratorrolle für ein Objekt können sämtliche Vorgänge auf ein Objekt anwenden und diese anzeigen. Zu dieser Rolle gehören alle Rechte der „Nur Lesen“-Rolle. Wenn Sie über die Administratorrolle für ein Objekt verfügen, können Sie einzelnen Benutzern und Gruppen Rechte zuweisen.

Wenn Sie die Rolle des Administrators in vCenter Server innehaben, können Sie Benutzern und Gruppen in der standardmäßigen vCenter Single Sign On-Identitätsquelle Rechte zuweisen. Weitere Informationen finden Sie in der Dokumentation *vSphere-Authentifizierung* für unterstützte Identitätsdienste.

Nach der Installation verfügt der Benutzer „administrator@vsphere.local“ standardmäßig über die Administratorrolle in vCenter Single Sign On und vCenter Server. Dieser Benutzer kann dann anderen Benutzern die Administratorrolle in vCenter Server zuordnen.

Rolle „Nur Lesen“

Benutzer mit der Rolle „Nur Lesen“ für ein Objekt können den Status des Objekts und Details zum Objekt anzeigen. Beispielsweise können Benutzer mit dieser Rolle VM-, Host- und Ressourcenpoolattribute anzeigen, aber die Remote-Konsole für einen Host können sie nicht anzeigen. Alle Vorgänge über die Menüs und Symbolleisten sind nicht zugelassen.

Rolle „Kein Zugriff“

Benutzer mit der Rolle „Kein Zugriff“ für ein bestimmtes Objekt können das Objekt weder anzeigen noch ändern. Neuen Benutzern und Gruppen wird diese Rolle standardmäßig zugewiesen. Sie können die Rolle objektabhängig ändern.

Dem Administrator der vCenter Single Sign-On-Domäne (standardmäßig administrator@vsphere.local), dem Root-Benutzer und vpxuser wird standardmäßig die Administratorrolle zugewiesen. Anderen Benutzern wird standardmäßig die Rolle „Kein Zugriff“ zugewiesen.

Es wird empfohlen, einen Benutzer auf der Root-Ebene zu erstellen und diesem Benutzer die Administratorrolle zuzuweisen. Nach der Erstellung eines benannten Benutzers mit Administratorrechten können Sie den Root-Benutzer aus allen Berechtigungen entfernen oder dessen Rolle in „Kein Zugriff“ ändern.

Best Practices für Rollen und Berechtigungen

Folgen Sie den Best Practices für Rollen und Berechtigungen, um die Sicherheit und Verwaltbarkeit Ihrer vCenter Server-Umgebung zu maximieren.

Folgen Sie diesen Best Practices beim Konfigurieren von Rollen und Berechtigungen in Ihrer vCenter Server-Umgebung:

- Sofern möglich, weisen Sie eine Rolle nicht einzelnen Benutzern sondern einer Gruppe zu.
- Erteilen Sie Berechtigungen nur für die entsprechenden erforderlichen Objekte und weisen Sie Rechte nur den entsprechenden erforderlichen Benutzern oder Gruppen zu. Vergeben Sie möglichst wenige Berechtigungen, um das Verstehen und Verwalten Ihrer Berechtigungsstruktur zu erleichtern.
- Wenn Sie einer Gruppe eine restriktive Rolle zuweisen, überprüfen Sie, dass die Gruppe weder den Administrator noch Benutzer mit Administratorrechten enthält. Anderenfalls schränken Sie möglicherweise die Rechte eines Administrators in den Teilen der Bestandslistenhierarchie ungewollt ein, für die Sie der Gruppe die restriktive Rolle zugewiesen haben.
- Verwenden Sie Ordner, um Objekte zu gruppieren. Um beispielsweise einer Hostgruppe die Änderungsberechtigung und einer anderen Hostgruppe die Anzeigeberechtigung zuzuweisen, platzieren Sie die jeweiligen Hostgruppen in einem Ordner.
- Gehen Sie vorsichtig vor, wenn Sie den vCenter Server-Stammobjekten eine Berechtigung hinzufügen. Benutzer mit Rechten auf der Root-Ebene haben Zugriff auf globale Daten auf vCenter Server, wie z. B. Rollen, benutzerdefinierte Attribute und vCenter Server-Einstellungen.
- Ziehen Sie die Aktivierung der Weitergabe in Betracht, wenn Sie einem Objekt Berechtigungen zuweisen. Durch die Weitergabe wird sichergestellt, dass neue Objekte in der Objekthierarchie Berechtigungen erben. Sie können z. B. eine Berechtigung zu einem Ordner der virtuellen Maschine zuweisen und die Weitergabe aktivieren, um sicherzustellen, dass die Berechtigung für alle VMs im Ordner gilt.
- Verwenden Sie die Rolle „Kein Zugriff“, um bestimmte Bereiche der Hierarchie zu maskieren. Die Rolle „Kein Zugriff“ beschränkt den Zugriff auf die Benutzer oder Gruppen mit dieser Rolle.

- Änderungen an Lizenzen werden an alle verknüpften vCenter Server-Systeme in derselben vCenter Single Sign On-Domäne weitergegeben.
- Die Lizenzweitergabe erfolgt selbst dann, wenn der Benutzer nicht über Rechte auf allen vCenter Server-Systemen verfügt.

Erforderliche Berechtigungen für allgemeine Aufgaben

Viele Aufgaben erfordern Berechtigungen für mehrere Objekte in der Bestandsliste. Wenn der Benutzer, der die Aufgabe auszuführen versucht, nur über Berechtigungen für ein Objekt verfügt, kann die Aufgabe nicht erfolgreich abgeschlossen werden.

In der folgenden Tabelle werden allgemeine Aufgaben aufgelistet, die mehr als eine Berechtigung erfordern. Sie können Berechtigungen zu Bestandslistenobjekten hinzufügen, indem Sie einen Benutzer mit einer der vordefinierten Rollen oder mit mehreren Berechtigungen koppeln. Wenn Sie davon ausgehen, dass Sie einen Berechtigungssatz mehrmals zuweisen werden, erstellen Sie benutzerdefinierte Rollen.

In der *vSphere Web Services-API-Referenz* finden Sie Informationen dazu, wie Vorgänge in der vSphere Client-Benutzeroberfläche API-Aufrufen zuordnen und welche Berechtigungen zum Ausführen von Vorgängen erforderlich sind. Beispielsweise gibt die API-Dokumentation für die `AddHost_Task(addHost)`-Methode an, dass die Berechtigung **Host.Bestandsliste.AddHostToCluster** erforderlich ist, um einen Host zu einem Cluster hinzuzufügen.

Falls die Aufgabe, die Sie durchführen möchten, nicht in der Tabelle vorhanden ist, erläutern die folgenden Regeln, wo Sie Berechtigungen zuweisen müssen, um bestimmte Vorgänge zuzulassen:

- Alle Vorgänge, die Speicherplatz belegen, erfordern die Berechtigung **Datenspeicher.Speicher zuteilen** auf dem Zieldatenspeicher sowie die Berechtigung zum Ausführen des Vorgangs selbst. Sie müssen über diese Berechtigungen verfügen, wenn Sie beispielsweise eine virtuelle Festplatte oder einen Snapshot erstellen.
- Das Verschieben eines Objekts in der Bestandslistenhierarchie erfordert entsprechende Berechtigungen auf dem Objekt selbst, dem übergeordneten Quellobjekt (z. B. einem Ordner oder Cluster) und dem übergeordneten Zielobjekt.
- Jeder Host und Cluster hat seinen eigenen impliziten Ressourcenpool, der alle Ressourcen des Hosts oder Clusters enthält. Das direkte Bereitstellen einer virtuellen Maschine auf einem Host oder Cluster erfordert das Recht **Ressource.Virtuelle Maschine zu Ressourcenpool zuweisen**.

Tabelle 2-4. Erforderliche Berechtigungen für allgemeine Aufgaben

Aufgabe	Erforderliche Berechtigungen	Gültige Rolle
Erstellen einer virtuellen Maschine	Im Zielordner oder Datencenter: ■ **Virtuelle Maschine.Bestandsliste.Neu erstellen** ■ **Virtuelle Maschine.Konfiguration.Neue Festplatte hinzufügen** (wenn eine neue virtuelle Festplatte erstellt wird) ■ **Virtuelle Maschine.Konfiguration.Vorhandene Festplatte hinzufügen** (wenn eine vorhandene virtuelle Festplatte verwendet wird) ■ **Virtuelle Maschine.Konfiguration.Rohgerät konfigurieren** (wenn eine RDM oder ein SCSI-Passthrough-Gerät verwendet wird)	Administrator
	Auf dem Zielhost, -cluster oder -ressourcenpool: **Ressource.Virtuelle Maschine zu Ressourcenpool zuweisen**	Ressourcenpool-Administrator oder Administrator
	Auf dem Zieldatenspeicher oder im Ordner, der den Datenspeicher enthält: **Datenspeicher.Speicher zuteilen**	Datenspeicherkonsument oder Administrator
	Im Netzwerk, dem die virtuelle Maschine zugewiesen wird: **Netzwerk.Netzwerk zuweisen**	Netzwerkkonsument oder Administrator
Einschalten einer virtuellen Maschine	Im Datencenter, in dem die virtuelle Maschine bereitgestellt wird: **Virtuelle Maschine.Interaktion.Einschalten**	Hauptbenutzer virtueller Maschinen oder Administrator
	Auf der virtuellen Maschine oder einem Ordner mit virtuellen Maschinen: **Virtuelle Maschine.Interaktion.Einschalten**	
Virtuelle Maschine aus einer Vorlage bereitstellen	Im Zielordner oder Datencenter: ■ **Virtuelle Maschine.Bestandsliste.Aus vorhandener erstellen** ■ **Virtuelle Maschine.Konfiguration.Neue Festplatte hinzufügen**	Administrator
	In einer Vorlage oder einem Vorlagenordner: **Virtuelle Maschine.Bereitstellung.Vorlage bereitstellen**	Administrator
	Auf dem Zielhost, -cluster oder -ressourcenpool: ■ **Ressource.Virtuelle Maschine zu Ressourcenpool zuweisen** ■ **vApp.Importieren**	Administrator
	Auf dem Zieldatenspeicher oder -datenspeicherordner: **Datenspeicher.Speicher zuteilen**	Datenspeicherkonsument oder Administrator
	Im Netzwerk, dem die virtuelle Maschine zugewiesen wird: **Netzwerk.Netzwerk zuweisen**	Netzwerkkonsument oder Administrator
Erstellen eines Snapshots der virtuellen Maschine	Auf der virtuellen Maschine oder einem Ordner mit virtuellen Maschinen: **Virtuelle Maschine.Snapshot-Verwaltung.Snapshot erstellen**	Hauptbenutzer virtueller Maschinen oder Administrator

Tabelle 2-4. Erforderliche Berechtigungen für allgemeine Aufgaben (Fortsetzung)

Aufgabe	Erforderliche Berechtigungen	Gültige Rolle
Verschieben einer virtuellen Maschine in einen Ressourcenpool	Auf der virtuellen Maschine oder einem Ordner mit virtuellen Maschinen: ■ **Ressource.Virtuelle Maschine zu Ressourcenpool zuweisen** ■ **Virtuelle Maschine.Bestandsliste.Verschieben**	Administrator
	Auf dem Zielressourcenpool: **Ressource.Virtuelle Maschine zu Ressourcenpool zuweisen**	Administrator
Installieren eines Gastbetriebssystems auf einer virtuellen Maschine	Auf der virtuellen Maschine oder einem Ordner mit virtuellen Maschinen: ■ **Virtuelle Maschine.Interaktion.Frage beantworten** ■ **Virtuelle Maschine.Interaktion.Konsoleninteraktion** ■ **Virtuelle Maschine.Interaktion.Geräteverbindung** ■ **Virtuelle Maschine.Interaktion.Ausschalten** ■ **Virtuelle Maschine.Interaktion.Einschalten** ■ **Virtuelle Maschine.Interaktion.Zurücksetzen** ■ **Virtuelle Maschine.Interaktion.CD-Medien konfigurieren** (wenn von einer CD installiert wird) ■ **Virtuelle Maschine.Interaktion.Diskettenmedien konfigurieren** (wenn von einer Diskette installiert wird) ■ **Virtuelle Maschine.Interaktion.VMware Tools installieren**	Hauptbenutzer virtueller Maschinen oder Administrator
	Auf einem Datenspeicher, der das Installationsmedium mit dem ISO-Image enthält: **Datenspeicher.Datenspeicher durchsuchen** (wenn von einem ISO-Image auf einem Datenspeicher installiert wird) Auf dem Datenspeicher, auf den Sie das ISO-Image des Installationsmediums hochladen: ■ **Datenspeicher.Datenspeicher durchsuchen** ■ **Datenspeicher.Dateivorgänge auf niedriger Ebene**	Hauptbenutzer virtueller Maschinen oder Administrator
Migrieren einer virtuellen Maschine mit vMotion	Auf der virtuellen Maschine oder einem Ordner mit virtuellen Maschinen: ■ **Ressourcen.Eingeschaltete virtuelle Maschine migrieren** ■ **Ressource.Virtuelle Maschine zu Ressourcenpool zuweisen** (wenn das Ziel ein anderer Ressourcenpool als die Quelle ist)	Ressourcenpool-Administrator oder Administrator
	Auf dem Zielhost, -cluster oder -ressourcenpool (wenn anders als die Quelle): **Ressource.Virtuelle Maschine zu Ressourcenpool zuweisen**	Ressourcenpool-Administrator oder Administrator
Cold-Migration (Verlagern) einer virtuellen Maschine	Auf der virtuellen Maschine oder einem Ordner mit virtuellen Maschinen: ■ **Ressourcen.Ausgeschaltete virtuelle Maschine migrieren** ■ **Ressource.Virtuelle Maschine zu Ressourcenpool zuweisen** (wenn das Ziel ein anderer Ressourcenpool als die Quelle ist)	Ressourcenpool-Administrator oder Administrator

Tabelle 2-4. Erforderliche Berechtigungen für allgemeine Aufgaben (Fortsetzung)

Aufgabe	Erforderliche Berechtigungen	Gültige Rolle
	Auf dem Zielhost, -cluster oder -ressourcenpool (wenn anders als die Quelle): **Ressource.Virtuelle Maschine zu Ressourcenpool zuweisen**	Ressourcenpool-Administrator oder Administrator
	Auf dem Zieldatenspeicher (wenn anders als die Quelle): **Datenspeicher.Speicher zuteilen**	Datenspeicherkonsument oder Administrator
Migrieren einer virtuellen Maschine mit Storage vMotion	Auf der virtuellen Maschine oder einem Ordner mit virtuellen Maschinen: **Ressourcen.Eingeschaltete virtuelle Maschine migrieren**	Ressourcenpool-Administrator oder Administrator
	Auf dem Zieldatenspeicher: **Datenspeicher.Speicher zuteilen**	Datenspeicherkonsument oder Administrator
Einen Host in einen Cluster verschieben	Auf dem Host: **Host.Bestandsliste.Host zu Cluster hinzufügen**	Administrator
	Auf dem Zielcluster: ■ **Host.Bestandsliste.Host zu Cluster hinzufügen** ■ **Host.Bestandsliste.Cluster ändern**	Administrator
Hinzufügen eines einzelnen Hosts zu einem Datencenter mithilfe des vSphere Client oder Hinzufügen eines einzelnen Hosts zu einem Cluster mithilfe der PowerCLI oder API (Nutzung der addHost-API)	Auf dem Host: **Host.Bestandsliste.Host zu Cluster hinzufügen**	Administrator
	Auf dem Cluster: ■ **Host.Bestandsliste.Cluster ändern** ■ **Host.Bestandsliste.Host zu Cluster hinzufügen**	Administrator
	Im Datencenter: **Host.Bestandsliste.Eigenständigen Host hinzufügen**	Administrator
Hinzufügen mehrerer Hosts zu einem Cluster	Auf dem Cluster: ■ **Host.Bestandsliste.Cluster ändern** ■ **Host.Bestandsliste.Host zu Cluster hinzufügen**	Administrator
	Im übergeordneten Datencenter des Clusters (mit Weitergabe): ■ **Host.Bestandsliste.Eigenständigen Host hinzufügen** ■ **Host.Bestandsliste.Host verschieben** ■ **Host.Bestandsliste.Cluster ändern** ■ **Host.Konfiguration.Wartung**	Administrator
Verschlüsseln einer virtuellen Maschine	Eine Verschlüsselung ist nur in Umgebungen mit vCenter Server möglich. Zusätzlich muss für die meisten Verschlüsselungsaufgaben bei dem ESXi-Host der Verschlüsselungsmodus aktiviert sein. Der Benutzer, der diese Aufgaben durchführt, muss über die entsprechenden Berechtigungen verfügen. Eine Gruppe von Berechtigungen für **Kryptografievorgänge** ermöglicht eine detaillierte Steuerung. Weitere Informationen hierzu finden Sie unter Voraussetzungen und erforderliche Berechtigungen für die Verschlüsselung.	Administrator

Sichern der ESXi-Hosts

3

Die ESXi-Hypervisorarchitektur verfügt über viele integrierte Sicherheitsfunktionen wie CPU-Isolierung, Arbeitsspeicherisolierung und Geräteisolierung. Sie können weitere Funktionen wie Sperrmodus, Zertifikatsersetzung und Chipkarten-Authentifizierung zum Erhöhen der Sicherheit konfigurieren.

Ein ESXi-Host wird außerdem durch eine Firewall geschützt. Sie können Ports für eingehenden und ausgehenden Datenverkehr nach Bedarf öffnen, sollten aber den Zugriff auf Dienste und Ports einschränken. Das Verwenden des ESXi-Sperrmodus und das Einschränken des Zugriffs auf ESXi Shell kann außerdem zu einer sichereren Umgebung beitragen. ESXi-Hosts nehmen an der Zertifikatinfrastruktur teil. Für Hosts werden Zertifikate bereitgestellt, die standardmäßig durch die VMware Certificate Authority (VMCA) signiert werden.

Im VMware-Whitepaper *Security of the VMware vSphere Hypervisor* finden Sie weitere Informationen zur ESXi-Sicherheit.

Hinweis ESXi baut nicht auf dem Linux-Kernel oder einer verbraucherorientierten Linux-Distribution auf. Es verwendet seinen eigenen VMware-spezifischen und proprietären Kernel und eigene Software-Tools, die als eigenständige Einheit bereitgestellt werden und keine Anwendungen und Komponenten aus Linux-Distributionen enthalten.

Dieses Kapitel enthält die folgenden Themen:

- ESXi-Protokolldateien
- Verwalten von ESXi-Überwachungsdatensätzen
- Sichern der ESXi-Konfiguration

Allgemeine ESXi-Sicherheitsempfehlungen

Um einen ESXi-Host gegen unbefugten Zugriff und Missbrauch abzusichern, werden von VMware Beschränkungen für mehrere Parameter, Einstellungen und Aktivitäten auferlegt. Sie können die Beschränkungen lockern, um sie an Ihre Konfigurationsanforderungen anzupassen. Stellen Sie in diesem Fall sicher, dass Sie in einer vertrauenswürdigen Umgebung arbeiten und weitere Sicherheitsmaßnahmen ergreifen.

Integrierte Sicherheitsfunktionen

Die Risiken für die Hosts werden wie folgt verringert:

- ESXi Shell- und SSH-Schnittstellen sind standardmäßig deaktiviert. Aktivieren Sie diese Schnittstellen erst, wenn Fehlerbehebungs- oder Supportaktivitäten durchgeführt werden müssen. Verwenden Sie für die täglichen Aktivitäten den vSphere Client, wobei die Aktivität der rollenbasierten Zugriffssteuerung und modernen Zugriffssteuerungsmethoden unterliegt.
- Nur eine begrenzte Anzahl von Firewallports ist standardmäßig geöffnet. Sie können explizit weitere Firewallports öffnen, die mit speziellen Diensten verknüpft sind.
- ESXi führt nur Dienste aus, die zum Verwalten seiner Funktionen wesentlich sind. Die Distribution beschränkt sich auf die Funktionen, die zum Betrieb von ESXi erforderlich sind.
- Standardmäßig sind alle Ports, die nicht für den Verwaltungszugriff auf den Host notwendig sind, geschlossen. Öffnen Sie Ports, falls Sie zusätzliche Dienste benötigen.
- Standardmäßig sind schwache Schlüssel deaktiviert und die Kommunikation der Clients wird durch SSL gesichert. Die genauen Algorithmen, die zum Sichern des Kanals verwendet werden, hängen vom SSL-Handshake ab. In ESXi erstellte Standardzertifikate verwenden PKCS#1 SHA-256 mit RSA-Verschlüsselung als Signaturalgorithmus.
- Ein interner Webdienst wird von ESXi zur Unterstützung des Zugriffs durch Webclients verwendet. Der Dienst wurde geändert, um nur Funktionen auszuführen, die ein Webclient für die Verwaltung und Überwachung benötigt. Daher ist ESXi nicht von den Webdienst-Sicherheitslücken betroffen, die für Tomcat in weiter gefassten Anwendungsbereichen gemeldet wurden.
- VMware überwacht alle Sicherheitswarnungen, die die Sicherheit von ESXi beeinträchtigen können, und gibt ggf. einen Sicherheits-Patch aus. Sie können die Mailingliste „VMware Security Advisories and Security Alerts“ abonnieren, um Sicherheitswarnungen zu erhalten. Weitere Informationen finden Sie auf der Webseite unter http://lists.vmware.com/mailman/listinfo/security-announce.
- Unsichere Dienste, wie z. B. FTP und Telnet sind nicht installiert, und die Ports für diese Dienste sind standardmäßig geschlossen.

- Verwenden Sie UEFI Secure Boot, damit Hosts keine Treiber und Anwendungen laden können, die nicht kryptografisch signiert sind. Die Aktivierung von Secure Boot erfolgt im System-BIOS. Auf dem ESXi-Host sind keine zusätzlichen Konfigurationsänderungen erforderlich, z. B. für Festplattenpartitionen. Weitere Informationen hierzu finden Sie unter UEFI Secure Boot für ESXi-Hosts.
- Wenn Ihr ESXi-Host über einen TPM 2.0-Chip verfügt, aktivieren und konfigurieren Sie diesen im System-BIOS. In Zusammenarbeit mit Secure Boot bietet TPM 2.0 verbesserte Sicherheit und vertrauenswürdige Zuverlässigkeit, die in der Hardware verankert ist. Weitere Informationen hierzu finden Sie unter Sichern von ESXi-Hosts mit Trusted Platform Module.

Weitere Sicherheitsmaßnahmen

Berücksichtigen Sie bei der Bewertung der Hostsicherheit und -verwaltung die folgenden Empfehlungen.

Beschränkung des Zugriffs

Wenn Sie den Zugriff auf die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI), die ESXi Shell oder auf SSH ermöglichen, müssen Sie strenge Zugriffssicherheitsrichtlinien durchsetzen.

Die ESXi Shell hat privilegierten Zugriff auf bestimmte Teile des Hosts. Gewähren Sie nur vertrauenswürdigen Benutzern Anmeldezugriff auf die ESXi Shell.

Greifen Sie nicht direkt auf verwaltete Hosts zu

Verwenden Sie den vSphere Client, um ESXi-Hosts zu verwalten, die von einem vCenter Server verwaltet werden. Greifen Sie mit dem VMware Host Client nicht direkt auf verwaltete Hosts zu und ändern Sie keine verwalteten Hosts über DCUI.

Wenn Sie Hosts mit einer Schnittstelle oder API zur Skripterstellung verwalten, dürfen Sie nicht den Host direkt als Ziel verwenden. Verwenden Sie stattdessen als Ziel das vCenter Server-System, das den Host verwaltet, und geben Sie den Hostnamen an.

Verwenden Sie DCUI nur für die Fehlerbehebung

Greifen Sie als Root-Benutzer nur zur Fehlerbehebung von der DCUI oder der ESXi Shell auf den Host zu. Um Ihre ESXi-Hosts zu verwalten, verwenden Sie einen der GUI-Clients oder eine der VMware-CLIs oder -APIs. Weitere Informationen finden Sie in *ESXCLI – Konzepte und Beispiele* unter https://code.vmware.com/. Wenn Sie die ESXi Shell oder SSH verwenden, sollten Sie die zugriffsberechtigten Konten beschränken und Zeitüberschreitungswerte festlegen.

Verwenden Sie nur VMware-Quellen für das Upgrade von ESXi-Komponenten.

Der Host führt mehrere Drittanbieterpakete aus, um Verwaltungsschnittstellen oder von Ihnen durchzuführende Aufgaben zu unterstützen. VMware unterstützt nur Upgrades auf Pakete, die aus einer VMware-Quelle stammen. Wenn Sie einen Download oder Patch aus einer anderen Quelle verwenden, können die Sicherheit und die Funktionen der Verwaltungsschnittstelle

gefährdet werden. Überprüfen Sie die Internetseiten von Drittanbietern und die VMware-Wissensdatenbank auf Sicherheitswarnungen.

Hinweis Befolgen Sie die VMware-Sicherheitswarnungen unter http://www.vmware.com/security/.

Erweiterte Systemeinstellungen

Erweiterte Systemeinstellungen steuern Aspekte des ESXi-Verhaltens, wie z. B. Protokollierung, Systemressourcen und Sicherheit.

Die folgende Tabelle enthält einige wichtige erweiterte ESXi-Systemeinstellungen für die Sicherheit. Informationen zum Anzeigen aller erweiterten Systemeinstellungen finden Sie entweder im vSphere Client (**Host > Konfigurieren > System > Erweiterte Systemeinstellungen)** oder in der API für eine bestimmte Version.

Tabelle 3-1. Teilliste der erweiterten Systemeinstellungen für die Sicherheit

Erweiterte Systemeinstellung	Beschreibung	Standardwert
Annotations.WelcomeMessage	Zeigt vor der Anmeldung eine Begrüßungsnachricht im Host Client oder in der DCUI auf dem Standardbildschirm an. In der DCUI ersetzt die Begrüßungsnachricht Text, wie z. B. die IP-Adresse des Hosts.	(Leer)
Config.Etc.issue	Zeigt während einer SSH-Anmeldesitzung ein Banner an. Verwenden Sie einen abschließenden Zeilenumbruch, um optimale Ergebnisse zu erzielen.	(Leer)
Config.Etc.motd	Zeigt die Meldung des Tages bei der SSH-Anmeldung an.	(Leer)
Config.HostAgent.vmacore.soap.sessionTimeout	Legt die Leerlaufzeit in Minuten fest, bevor das System eine VIM-API automatisch abmeldet. Mit dem Wert 0 (Null) wird die Leerlaufzeit deaktiviert. Diese Einstellung gilt nur für neue Sitzungen.	30 (Minuten)
Mem.MemEagerZero	Aktiviert das unwiderrufliche Löschen (Page Zeroing) der Benutzer-World- und Gastarbeitsspeicherseiten in den VMkernel-Betriebssystemen (einschließlich des VMM-Prozesses) nach dem Beenden einer virtuellen Maschine. Der Standardwert (0) verwendet Lazy Zeroing. Der Wert 1 verwendet Eager Zeroing.	0 (deaktiviert)

Tabelle 3-1. Teilliste der erweiterten Systemeinstellungen für die Sicherheit (Fortsetzung)

Erweiterte Systemeinstellung	Beschreibung	Standardwert
Security.AccountLockFailures	Legt die maximale Anzahl fehlgeschlagener Anmeldeversuche fest, bevor das Konto eines Benutzers vom System gesperrt wird. Beispiel: Zum Sperren des Kontos beim fünften Anmeldefehler legen Sie diesen Wert auf 4 fest. Mit dem Wert 0 (Null) wird die Kontosperrung deaktiviert. Aus Implementierungsgründen werden einige Anmeldemechanismen falsch gewertet: ■ VIM-Anmeldungen (einschließlich des VMware Host Client) und ESXCLI geben die genaue Anzahl fehlgeschlagener Anmeldungen an. ■ SSH-Verbindungen werden bei der Anzeige einer Kennwortaufforderung als Anmeldeversuch gezählt. Diese Anzahl wird nach erfolgreicher Anmeldung verringert. Dies ist normales Verhalten bei der Challenge-Response-Kommunikation. ■ Bei CGI-Anmeldungen werden Anmeldefehler doppelt gezählt. **Vorsicht** Aufgrund dieses Problems kann ein Benutzer bei Verwendung der CGI-Schnittstelle schneller gesperrt werden als die Anzahl fehlgeschlagener Anmeldungen steigt.	5
Security.AccountUnlockTime	Legt die Anzahl der Sekunden fest, die ein Benutzer gesperrt wird. Bei jedem Anmeldeversuch innerhalb der angegebenen Sperrenzeitüberschreitung wird diese neu gestartet.	900 (15 Minuten)
Security.PasswordHistory	Gibt die Anzahl der für jeden Benutzer zu speichernden Kennwörter an. Diese Einstellung verhindert doppelte oder ähnliche Kennwörter.	0
Security.PasswordMaxDays	Legt die maximale Anzahl an Tagen zwischen Kennwortänderungen fest.	99999

Tabelle 3-1. Teilliste der erweiterten Systemeinstellungen für die Sicherheit (Fortsetzung)

Erweiterte Systemeinstellung	Beschreibung	Standardwert

Security.PasswordQualityControl	Ändert die erforderliche Länge und die erforderliche Zeichenklasse oder erlaubt Kennwortsätze in der `Pam_passwdqc`-Konfiguration. Sie können Sonderzeichen in Kennwörtern verwenden. Kennwortlängen von mindestens 15 Zeichen sind möglich. Die Standardeinstellung erfordert drei Zeichenklassen und eine Mindestlänge von sieben Zeichen.
	Bei der Implementierung des DoD-Anhangs können Sie die Option `similar=deny` mit einer Kennwortmindestlänge kombinieren und die Anforderung durchsetzen, dass Kennwörter ausreichend unterschiedlich sind. Die Einstellung für den Kennwortverlauf wird nur für Kennwörter erzwungen, die über die VIM-API `LocalAccountManager.changePassword` geändert wurden. Zum Ändern des Kennworts muss der Benutzer über Administratorberechtigungen verfügen. Die Einstellung „PasswordQualityControl“ mit der Einstellung „PasswordMaxDays“ erfüllt die Anforderungen des DoD-Anhangs:
	`min=disabled,disabled,disabled,disabled,15`
	`similar=deny`
		retry=3 min=disabled,disabled,disabled,7,7

UserVars.DcuiTimeOut	Legt die Leerlaufzeit in Sekunden fest, bevor das System die DCUI automatisch abmeldet. Mit dem Wert 0 (Null) wird die Zeitüberschreitung deaktiviert.	600 (10 Minuten)
UserVars.ESXiShellInteractiveTimeOut	Legt die Leerlaufzeit in Sekunden fest, bevor das System eine interaktive Shell automatisch abmeldet. Diese Einstellung wird nur für neue Sitzungen wirksam. Mit dem Wert 0 (Null) wird die Leerlaufzeit deaktiviert. Gilt sowohl für die DCUI als auch für die SSH-Shell.	0

Tabelle 3-1. Teilliste der erweiterten Systemeinstellungen für die Sicherheit (Fortsetzung)

Erweiterte Systemeinstellung	Beschreibung	Standardwert
UserVars.ESXiShellTimeOut	Legt die Zeit in Sekunden fest, die eine Anmelde-Shell auf die Anmeldung wartet. Mit dem Wert 0 (Null) wird die Zeitüberschreitung deaktiviert. Gilt sowohl für die DCUI als auch für die SSH-Shell.	0
UserVars.HostClientSessionTimeout	Legt die Leerlaufzeit in Sekunden fest, bevor das System den Host Client automatisch abmeldet. Mit dem Wert 0 (Null) wird die Leerlaufzeit deaktiviert.	900 (15 Minuten)
UserVars.HostClientWelcomeMessage	Zeigt bei der Anmeldung eine Begrüßungsnachricht im Host Client an. Die Nachricht wird nach der Anmeldung als „Hinweis“ angezeigt.	(Leer)

Konfigurieren von ESXi-Hosts mit Hostprofilen

Mit Hostprofilen können Sie Standardkonfigurationen für Ihre ESXi-Hosts einrichten und die Einhaltung dieser Konfigurationseinstellungen automatisch sicherstellen. Mit Hostprofilen können Sie viele Aspekte der Hostkonfiguration, einschließlich Arbeitsspeicher, Permanentspeicher, Netzwerk usw., steuern.

Sie können Hostprofile für einen Referenzhost über den vSphere Client konfigurieren und das Hostprofil auf alle Hosts anwenden, die dieselben Merkmale wie der Referenzhost haben. Sie können außerdem Hostprofile zum Überwachen von Hosts in Bezug auf Änderungen der Hostkonfiguration verwenden. Weitere Informationen finden Sie in der Dokumentation *vSphere-Hostprofile*.

Sie können das Hostprofil einem Cluster zuordnen, um es auf alle Hosts im Cluster anzuwenden.

Verfahren

1. Richten Sie den Referenzhost gemäß der Spezifikation ein und erstellen Sie ein Hostprofil.
2. Weisen Sie das Profil einem Host oder Cluster zu.
3. Übernehmen Sie das Hostprofil des Referenzhosts für andere Hosts oder Cluster.

Verwenden von Skripts zum Verwalten von Hostkonfigurationseinstellungen

In Umgebungen mit zahlreichen Hosts lassen sich Hosts mit Skripts schneller und fehlerfreier verwalten als über den vSphere Client.

vSphere umfasst mehrere Skriptsprachen für die Hostverwaltung. In der *ESXCLI-Dokumentation* und der *vSphere API/SDK-Dokumentation* finden Sie Referenzinformationen und Programmiertipps. VMware-Communitys können weitere Tipps für die Verwaltung mit Skripts geben. In der vSphere-Administratordokumentation wird hauptsächlich die Verwendung des vSphere Client für die Verwaltung beschrieben.

VMware PowerCLI

VMware PowerCLI ist eine Windows PowerShell-Schnittstelle zur vSphere API. VMware PowerCLI enthält PowerShell-Cmdlets für die Verwaltung von vSphere-Komponenten.

VMware PowerCLI enthält Hunderte von Cmdlets, eine Reihe von Beispielskripts und eine Funktionsbibliothek für die Verwaltung und Automatisierung. Weitere Informationen hierzu finden Sie unter https://developer.vmware.com/powercli.

ESXCLI

ESXCLI enthält eine Reihe von Befehlen für die Verwaltung von ESXi-Hosts und virtuellen Maschinen. Weitere Informationen hierzu finden Sie in der *ESXCLI-Dokumentation*.

Sie können auch eine der Skriptschnittstellen zum vSphere Automation SDK, wie beispielsweise vSphere Automation SDK for Python, verwenden.

Verfahren

1. Erstellen Sie eine benutzerdefinierte Rolle mit eingeschränkten Berechtigungen.

   Sie können z. B. eine Rolle erstellen, die eine Reihe von Berechtigungen für die Hostverwaltung, aber keine Berechtigungen für die Verwaltung von virtuellen Maschinen, Speicher oder Netzwerken besitzt. Wenn das Skript, das Sie verwenden möchten, nur Informationen extrahiert, können Sie eine Rolle mit Lesezugriff für den Host erstellen.

2. Erstellen Sie über den vSphere Client ein Dienstkonto und weisen Sie ihm die benutzerdefinierte Rolle zu.

   Sie können mehrere benutzerdefinierte Rollen mit unterschiedlichen Zugriffsebenen erstellen, wenn der Zugriff auf bestimmte Hosts stark eingeschränkt werden soll.

3 Schreiben Sie Skripts zum Prüfen oder Ändern von Parametern und führen Sie sie aus.

Sie können z. B. die interaktive Shell-Zeitüberschreitung eines Hosts wie folgt prüfen oder festlegen:

Sprache	Befehle

ESXCLI	`esxcli <conn_options> system settings advanced get / UserVars/ESXiShellTimeOut`
	
	`esxcli --formatter=csv --format-param=fields="Path,Int Value" system settings advanced list | grep /UserVars/ ESXiShellTimeOut`

PowerCLI	`#List UserVars.ESXiShellInteractiveTimeOut for each host Get-VMHost | Select Name, @{N="UserVars.ESXiShellInteractiveTimeOut";E={$_ | Get-AdvancedSetting -Name UserVars.ESXiShellInteractiveTimeOut | Select -ExpandProperty Value}}`
	
	`# Set UserVars.ESXiShellTimeOut to 900 on all hosts Get-VMHost | Foreach { Get-AdvancedSetting -Entity $_ -Name UserVars.ESXiShellInteractiveTimeOut | Set-AdvancedSetting -Value 900 }`

4 Erstellen Sie in großen Umgebungen Rollen mit unterschiedlichen Zugriffsrechten und gruppieren Sie Hosts gemäßen den Aufgaben, die Sie ausführen möchten, in Ordnern. Anschließend können Sie Skripts für unterschiedliche Ordner mithilfe verschiedener Dienstkonten ausführen.

5 Stellen Sie sicher, dass die Änderungen nach der Ausführung des Befehls vorgenommen wurden.

Kennwörter und Kontosperrung für ESXi

Für ESXi-Hosts müssen Sie ein Kennwort mit vordefinierten Anforderungen verwenden. Mithilfe der erweiterten Option `Security.PasswordQualityControl` können Sie die erforderliche Länge und die erforderliche Zeichenklasse ändern sowie Kennwortsätze erlauben. Sie können auch die Anzahl der Kennwörter festlegen, die für jeden Benutzer gespeichert werden soll. Verwenden Sie dazu die erweiterte Option `Security.PasswordHistory`.

Hinweis Die Standardanforderungen für ESXi-Kennwörter können versionsabhängig variieren. Mit der erweiterten Option `Security.PasswordQualityControl` können Sie die standardmäßigen Kennwortbeschränkungen prüfen und ändern.

ESXi-Kennwörter

ESXi erzwingt Kennwortanforderungen für den Zugriff über die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI), die ESXi Shell, SSH oder den VMware Host Client.

- Beim Erstellen eines Kennworts müssen darin standardmäßig Zeichen aus drei der vier folgenden Zeichenklassen enthalten sein: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen (z. B. Unter- oder Schrägstriche).
- Standardmäßig besteht ein Kennwort aus mindestens 7 und weniger als 40 Zeichen.
- Kennwörter dürfen kein Wort aus einem Wörterbuch und keinen Teil eines Worts aus einem Wörterbuch enthalten.

Hinweis Wenn ein Kennwort mit einem Großbuchstaben beginnt, wird dieser bei der Berechnung der verwendeten Zeichenklassen nicht berücksichtigt. Endet ein Kennwort mit einer Ziffer, wird diese bei der Berechnung der verwendeten Zeichenklassen ebenfalls nicht berücksichtigt. Ein Wort aus einem Wörterbuch, das in einem Kennwort verwendet wird, verringert die Sicherheit des Kennworts.

Beispiele für ESXi-Kennwörter

Die folgenden Beispielkennwörter veranschaulichen potenzielle Kennwörter, wenn die Option wie folgt festgelegt ist.

```
retry=3 min=disabled,disabled,disabled,7,7
```

Mit dieser Einstellung wird ein Benutzer bis zu drei Mal (retry=3) zur Eingabe eines neuen Kennworts aufgefordert, wenn ein Kennwort nicht ausreichend stark ist oder das Kennwort zweimal nicht korrekt eingegeben wurde. Kennwörter mit einer oder zwei Zeichenklassen und Kennwortsätzen sind nicht zulässig, da die ersten drei Elemente deaktiviert sind. Kennwörter mit drei oder vier Zeichenklassen erfordern sieben Zeichen. Weitere Informationen zu weiteren Optionen, wie z. B. `max`, `passphrase` und so weiter, finden Sie auf der `pam_passwdqc`-Manpage.

Mit diesen Einstellungen sind die folgenden Kennwörter zulässig.

- xQaTEhb!: Enthält acht Zeichen aus drei Zeichenklassen.
- xQaT3#A: Enthält sieben Zeichen aus vier Zeichenklassen.

Die folgenden Beispielkennwörter entsprechen nicht den Anforderungen.

- Xqat3hi: Beginnt mit einem Großbuchstaben, sodass nur zwei anstelle von drei Zeichenklassen berücksichtigt werden. Mindestens drei Zeichenklassen müssen vorhanden sein.
- xQaTEh2: Endet mit einer Ziffer, sodass nur zwei anstelle von drei Zeichenklassen berücksichtigt werden. Mindestens drei Zeichenklassen müssen vorhanden sein.

ESXi-Kennwortsatz

Anstelle eines Kennworts können Sie auch einen Kennwortsatz verwenden. Kennwortsätze sind jedoch standardmäßig deaktiviert. Die Standardeinstellung oder sonstige Einstellungen können Sie mithilfe der erweiterten Option `Security.PasswordQualityControl` über den vSphere Client ändern.

Beispielsweise können Sie diese Option wie folgt ändern.

```
retry=3 min=disabled,disabled,16,7,7
```

In diesem Beispiel sind Passphrasen mit mindestens 16 Zeichen und mindestens drei Wörtern zulässig.

Änderungen an der Datei `/etc/pam.d/passwd` werden für Legacy-Hosts weiterhin unterstützt, in zukünftigen Versionen ist dies jedoch nicht mehr der Fall. Verwenden Sie stattdessen die erweiterte Option `Security.PasswordQualityControl`.

Ändern der standardmäßigen Kennwortbeschränkungen

Die standardmäßige Beschränkung für Kennwörter oder Kennwortsätze können Sie mithilfe der erweiterten Option `Security.PasswordQualityControl` für Ihren ESXi-Host ändern. In der Dokumentation *vCenter Server und Hostverwaltung* finden Sie weitere Informationen zum Festlegen der erweiterten ESXi-Optionen.

Sie können den Standardwert wie folgt ändern, damit beispielsweise mindestens 15 Zeichen und mindestens vier Wörter (`passphrase=4`) erforderlich sind:

```
retry=3 min=disabled,disabled,15,7,7 passphrase=4
```

Ausführliche Informationen finden Sie auf der Manpage zu `pam_passwdqc`.

Hinweis Nicht alle möglichen Kombinationen von Kennwortoptionen wurden getestet. Führen Sie Tests durch, nachdem Sie Änderungen an den Einstellungen für das Standardkennwort vorgenommen haben.

In diesem Beispiel wird die Kennwortkomplexität auf acht Zeichen aus vier Zeichenklassen festgelegt, wobei ein erheblicher Unterschied zwischen den Kennwörtern, eine gespeicherter Verlauf von fünf Kennwörtern und eine 90-tägige Rotationsrichtlinie erzwungen wird:

```
min=disabled,disabled,disabled,disabled,8 similar=deny
```

Legen Sie die Option `Security.PasswordHistory` auf 5 und die Option `Security.PasswordMaxDays` auf 90 fest.

ESXi-Kontosperrverhalten

Das Sperren von Konten für den Zugriff über SSH und das vSphere Web Services SDK wird unterstützt. Die DCUI und die ESXi Shell unterstützen die Kontosperrung nicht. Standardmäßig wird das Konto nach maximal fünf fehlgeschlagenen Anmeldeversuchen gesperrt. Das Konto wird standardmäßig nach 15 Minuten entsperrt.

Konfigurieren des Anmeldeverhaltens

Das Anmeldeverhalten für Ihren ESXi-Host können Sie mit den folgenden erweiterten Optionen konfigurieren:

- `Security.AccountLockFailures`. Maximal zulässige Anzahl fehlgeschlagener Anmeldeversuche, bevor das Konto eines Benutzers gesperrt wird. Mit dem Wert „0“ wird das Sperren von Konten deaktiviert.
- `Security.AccountUnlockTime`. Die Anzahl der Sekunden, die ein Benutzer gesperrt wird.
- `Security.PasswordHistory`. Anzahl der für jeden Benutzer zu speichernden Kennwörter. Mit dem Wert „0“ wird der Kennwortverlauf deaktiviert.

Weitere Informationen zum Festlegen der erweiterten ESXi-Optionen finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.

Erzeugung des kryptografischen Schlüssels

ESXi erzeugt mehrere asymmetrische Schlüssel für den normalen Betrieb. Der TLS-Schlüssel (Transport Layer Security) sichert die Kommunikation mit dem ESXi-Host mithilfe des TLS-Protokolls. Der SSH-Schlüssel sichert die Kommunikation mit dem ESXi-Host unter Verwendung des SSH-Protokolls.

TLS-Schlüssel (Transport Layer Security)

Der TLS-Schlüssel (Transport Layer Security) sichert die Kommunikation mit dem Host mithilfe des TLS-Protokolls. Beim ersten Start erzeugt der ESXi-Host den TLS-Schlüssel als 2048-Bit-RSA-Schlüssel. Aktuell wird die automatische Erzeugung von ECDSA-Schlüsseln für TLS von ESXi nicht implementiert. Der private TLS-Schlüssel ist nicht für die Verwendung durch den Administrator vorgesehen.

Der TLS-Schlüssel befindet sich in folgendem nicht dauerhaften Speicherort:

```
/etc/vmware/ssl/rui.key
```

Der öffentliche TLS-Schlüssel (einschließlich Zwischenzertifizierungsstellen) befindet sich als X.509 v3-Zertifikat in folgendem nicht dauerhaften Speicherort:

```
/etc/vmware/ssl/rui.crt
```

Wenn Sie vCenter Server mit Ihren ESXi-Hosts verwenden, erzeugt vCenter Server automatisch eine CSR, signiert sie mithilfe der VMware Certificate Authority (VMCA) und erstellt das Zertifikat. Wenn Sie einen ESXi-Host zu vCenter Server hinzufügen, installiert vCenter Server das resultierende Zertifikat auf dem ESXi-Host.

Das TLS-Standardzertifikat ist selbstsigniert, wobei ein subjectAltName-Feld mit dem Hostnamen bei der Installation übereinstimmt. Sie können ein anderes Zertifikat installieren, um beispielsweise einen anderen subjectAltName zu verwenden oder um eine bestimmte Zertifizierungsstelle (CA) in die Verifizierungskette aufzunehmen. Weitere Informationen finden Sie unter Ersetzen von ESXi SSL-Zertifikaten und -Schlüsseln.

Sie können auch den VMware Host Client verwenden, um das Zertifikat zu ersetzen. Weitere Informationen finden Sie unter *Verwaltung eines einzelnen Hosts von vSphere – VMware Host Client*.

SSH-Schlüssel

Der SSH-Schlüssel sichert die Kommunikation mit dem ESXi-Host unter Verwendung des SSH-Protokolls. Beim ersten Start erzeugt das System einen nistp256-ECDSA-Schlüssel und die SSH-Schlüssel als 2048-Bit-RSA-Schlüssel. Der SSH-Server ist standardmäßig deaktiviert. Der SSH-Zugriff ist in erster Linie zur Fehlerbehebung gedacht. Die SSH-Schlüssel sind nicht für die Verwendung durch den Administrator vorgesehen. Für die Anmeldung über SSH sind Administratorrechte erforderlich, die gleichbedeutend mit allen Hostberechtigungen sind. Informationen zum Aktivieren von SSH-Zugriff finden Sie unter Aktivieren des Zugriffs auf die ESXi Shell.

Die öffentlichen SSH-Schlüssel befinden sich in folgendem Speicherort:

```
/etc/ssh/ssh_host_rsa_key.pub
```

```
/etc/ssh/ssh_host_ecdsa_key.pub
```

Die privaten SSH-Schlüssel befinden sich in folgendem Speicherort:

```
/etc/ssh/ssh_host_rsa_key
```

```
/etc/ssh/ssh_host_ecdsa_key
```

Erstellung des kryptografischen TLS-Schlüssels

Die Erstellungskonfiguration des kryptografischen TLS-Schlüssels wird durch Auswahl von TLS-Verschlüsselungs-Suites bestimmt, die einen der RSA-basierten Schlüsseltransporte (wie in NIST Special Publication 800-56B angegeben) oder ECC-basierte Schlüsselvereinbarungen mit Ecliptic Curve Diffie-Hellman (ECDH) auswählen (wie in NIST Special Publication 800-56A angegeben).

Erstellung des kryptografischen SSH-Schlüssels

Die Erstellungskonfiguration des kryptografischen SSH-Schlüssels wird über die SSHD-Konfiguration gesteuert. ESXi stellt eine Standardkonfiguration bereit, die RSA-basierten Schlüsseltransport (wie in NIST Special Publication 800-56B angegeben), eine Schlüsselvereinbarung mit Ephemeral Diffie-Hellman (DH) (wie in NIST Special Publication 800-56A angegeben) und Ecliptic Curve Diffie-Hellman (ECHD) (wie in NIST Special Publication 800-56A angegeben) zulässt. Die SSHD-Konfiguration ist nicht für die Verwendung durch den Administrator vorgesehen.

SSH-Sicherheit

ESXi Shell- und SSH-Schnittstellen sind standardmäßig deaktiviert. Aktivieren Sie diese Schnittstellen erst, wenn Fehlerbehebungs- oder Supportaktivitäten durchgeführt werden müssen. Verwenden Sie für die täglichen Aktivitäten den vSphere Client, wobei die Aktivität der rollenbasierten Zugriffssteuerung und modernen Zugriffssteuerungsmethoden unterliegt.

Die SSH-Konfiguration in ESXi verwendet die folgenden Einstellungen:

Version 1 SSH-Protokoll deaktiviert

VMware bietet keine Unterstützung für das SSH-Protokoll Version 1, sondern verwendet ausschließlich das Protokoll der Version 2. In Version 2 wurden einige in Version 1 enthaltenen Sicherheitsprobleme behoben, wodurch Sie die Möglichkeit haben, sicher mit der Verwaltungsschnittstelle zu kommunizieren.

Verbesserte Schlüsselqualität

SSH unterstützt lediglich 256-Bit- und 128-Bit-AES-Verschlüsselungen für Ihre Verbindungen.

Diese Einstellungen wurden so entworfen, dass die Daten, die Sie über SSH an die Verwaltungsschnittstelle übertragen, gut geschützt werden. Sie können diese Einstellungen nicht ändern.

ESXi-SSH-Schlüssel

SSH-Schlüssel können den Zugang zu einem ESXi-Host beschränken, steuern und sichern. Mithilfe eines SSH-Schlüssels kann sich ein vertrauenswürdiger Benutzer oder ein Skript bei einem Host anmelden, ohne ein Kennwort einzugeben.

Sie können den SSH-Schlüssel mithilfe des Befehls `vifs` auf den Host kopieren. Sie können auch HTTPS PUT verwenden, um den SSH-Schlüssel auf den Host zu kopieren.

Anstatt die Schlüssel extern zu generieren und hochzuladen, können Sie diese auf dem ESXi-Host erstellen und herunterladen. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/1002866.

Das Aktivieren von SSH und das Hinzufügen von SSH-Schlüsseln zum Host birgt gewisse Risiken. Wägen Sie das potenzielle Risiko, einen Benutzernamen und ein Kennwort verfügbar zu machen, gegen das Risiko eines Eindringlings mit einem vertrauenswürdigen Schlüssel ab.

Hochladen eines SSH-Schlüssels mithilfe eines vifs-Befehls

Wenn Sie autorisierte Schlüssel zum Anmelden bei einem Host mit SSH verwenden möchten, können Sie mithilfe des `vifs`-Befehls autorisierte Schlüssel hochladen.

Hinweis Da autorisierte Schlüssel den SSH-Zugriff ohne Benutzerauthentifizierung ermöglichen, muss sorgfältig geprüft werden, ob Sie SSH-Schlüssel in Ihrer Umgebung verwenden möchten.

Autorisierte Schlüssel ermöglichen Ihnen die Authentifizierung des Remotezugriffs auf einen Host. Wenn Benutzer oder Skripts versuchen, mit SSH auf einen Host zuzugreifen, bietet der Schlüssel eine Authentifizierung ohne Kennwort. Mit autorisierten Schlüsseln können Sie die Authentifizierung automatisieren, was nützlich ist, wenn Sie Skripte zum Ausführen von Routinetätigkeiten schreiben.

Sie können die folgenden Typen von SSH-Schlüsseln auf einen Host hochladen.

- Autorisierte Schlüsseldatei für den Root-Benutzer
- RSA-Schlüssel
- Öffentlicher RSA-Schlüssel

Ab vSphere 6.0 Update 2 werden DSS-/DSA-Schlüssel nicht mehr unterstützt.

Wichtig Ändern Sie die Datei `/etc/ssh/sshd_config` nicht. Falls Sie dies doch tun, nehmen Sie eine Änderung vor, von der der Host-Daemon (`hostd`) nichts weiß.

Verfahren

- Verwenden Sie in der Befehlszeile oder auf einem Verwaltungsserver den `vifs`-Befehl, um den SSH-Schlüssel auf einen entsprechenden Speicherort auf dem ESXi-Host hochzuladen.

```
vifs --server hostname --username username --put filename /host/ssh_host_dsa_key_pub
```

Schlüsseltyp	Speicherort
Autorisierte Schlüsseldateien für den Root-Benutzer	`/host/ssh_root_authorized_keys` Sie benötigen zum Hochladen dieser Datei vollständige Administratorrechte.
RSA-Schlüssel	`/host/ssh_host_rsa_key`
Öffentliche RSA-Schlüssel	`/host/ssh_host_rsa_key`

Hochladen eines SSH-Schlüssels anhand von HTTPS PUT

Sie können autorisierte Schlüssel zum Anmelden bei einem Host mit SSH verwenden. Sie können autorisierte Schlüssel mit HTTPS PUT hochladen.

Autorisierte Schlüssel ermöglichen Ihnen die Authentifizierung des Remotezugriffs auf einen Host. Wenn Benutzer oder Skripts versuchen, mit SSH auf einen Host zuzugreifen, bietet der Schlüssel eine Authentifizierung ohne Kennwort. Mit autorisierten Schlüsseln können Sie die Authentifizierung automatisieren, was nützlich ist, wenn Sie Skripts zum Ausführen von Routinetätigkeiten schreiben.

Sie können unter Verwendung von HTTPS PUT die folgenden Typen von SSH-Schlüsseln auf einen Host hochladen:

- Autorisierte Schlüsseldatei für Root-Benutzer
- DSA-Schlüssel
- Öffentlicher DSA-Schlüssel

- RSA-Schlüssel
- Öffentlicher RSA-Schlüssel

Wichtig Ändern Sie die Datei `/etc/ssh/sshd_config` nicht.

Verfahren

1 Öffnen Sie die Schlüsseldatei in der Anwendung, die Sie für das Hochladen verwenden.

2 Veröffentlichen Sie die Datei an den folgenden Speicherorten.

Schlüsseltyp	Speicherort
Autorisierte Schlüsseldateien für den Root-Benutzer	`https://`*`Hostname_oder_IP-Adresse`*`/host/ssh_root_authorized_keys` Sie benötigen zum Hochladen dieser Datei vollständige Administratorrechte auf dem Host.
DSA-Schlüssel	`https://`*`Hostname_oder_IP-Adresse`*`/host/ssh_host_dsa_key`
Öffentliche DSA-Schlüssel	`https://`*`Hostname_oder_IP-Adresse`*`/host/ssh_host_dsa_key_pub`
RSA-Schlüssel	`https://`*`Hostname_oder_IP-Adresse`*`/host/ssh_host_rsa_key`
Öffentliche RSA-Schlüssel	`https://`*`Hostname_oder_IP-Adresse`*`/host/ssh_host_rsa_key_pub`

PCI- und PCIe-Geräte sowie ESXi

Die Verwendung der Funktion VMware DirectPath I/O zum Passieren eines PCI- oder PCIe-Geräts zu einer virtuellen Maschine führt zu einer möglichen Sicherheitslücke. Die Schwachstelle kann ausgelöst werden, wenn fehlerhafter oder bösartiger Code, wie z. B. ein Gerätetreiber, im Gastbetriebssystem im privilegierten Modus ausgeführt wird. Branchenübliche Hardware und Firmware verfügen derzeit nicht über ausreichend Unterstützung zur Fehlereingrenzung, damit ESXi-Hosts Angriffe auf die Schwachstelle abwehren können.

Verwenden Sie PCI- oder PCIe-Passthrough zu einer virtuellen Maschine nur dann, wenn sich die virtuelle Maschine im Besitz einer vertrauenswürdigen Entität befindet und von dieser verwaltet wird. Sie müssen sicherstellen, dass diese Entität nicht den Versuch unternimmt, den Host von der virtuellen Maschine aus zum Absturz zu bringen oder auszunutzen.

Ihr Host ist möglicherweise auf eine der folgenden Weisen gefährdet.

- Das Gastbetriebssystem generiert möglicherweise einen nicht behebbaren PCI- oder PCIe-Fehler. Ein solcher Fehler beschädigt keine Daten, kann aber zum Absturz des ESXi-Hosts führen. Solche Fehler können aufgrund von Fehlern bzw. Inkompatibilitäten in den Hardwaregeräten auftreten, für die das Passthrough durchgeführt wird. Zu den weiteren Fehlergründen gehören Probleme mit Treibern im Gastbetriebssystem.
- Das Gastbetriebssystem startet möglicherweise einen DMA-Vorgang, der einen IOMMU-Seitenfehler auf dem ESXi-Host verursacht. Dieser Vorgang ist möglicherweise das Ergebnis eines DMA-Vorgangs, der eine Adresse außerhalb des virtuellen Maschinenspeichers

anvisiert. Auf einigen Maschinen konfiguriert Host-Firmware IOMMU-Fehler, um durch ein nicht maskierbares Interrupt (NMI) einen schweren Fehler zu melden. Dieser schwerwiegende Fehler verursacht einen Absturz des ESXi-Hosts. Dieses Problem kann aufgrund von Problemen mit den Treibern im Gastbetriebssystem auftreten.

- Wenn das Betriebssystem auf dem ESXi-Host nicht das Neuzuordnen von Interrupts verwendet, injiziert das Gastbetriebssystem möglicherweise einen störenden Interrupt in den ESXi-Host auf einem beliebigen Vektor. ESXi verwendet derzeit das Neuzuordnen von Interrupts auf den Intel-Plattformen, wo diese Funktion verfügbar ist. Das Neuzuordnen von Interrupts stellt einen Teil des Intel VT-d-Funktionssatzes dar. ESXi verwendet das Neuzuordnen von Interrupts nicht auf AMD-Plattformen. Falsche Interrupts können zum Absturz des ESXi-Hosts führen. Theoretisch kann es weitere Möglichkeiten geben, diese fehlerhaften Interrupts auszunutzen.

Deaktivieren des Browsers für verwaltete Objekte

Mit dem Browser für verwaltete Objekte (Managed Object Browser, MOB) kann das VMkernel-Objektmodell durchsucht werden. Allerdings können Angreifer diese Schnittstelle in böswilliger Absicht verwenden, um Konfigurationsänderungen oder andere Aktionen durchzuführen, denn mit dem MOB kann die Hostkonfiguration geändert werden. Verwenden Sie den MOB nur für das Debugging und achten Sie darauf, dass er in Produktionssystemen deaktiviert ist.

Der MOB ist standardmäßig deaktiviert. Für bestimmte Aufgaben, wie z. B. das Extrahieren des alten Zertifikats aus einem System, müssen Sie den MOB jedoch verwenden. Den MOB können Sie wie folgt aktivieren und deaktivieren.

Verfahren

1. Navigieren Sie zum Host im Navigator von vSphere Client.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter „System“ auf **Erweiterte Systemeinstellungen**.
4. Überprüfen Sie den Wert von **Config.HostAgent.plugins.solo.enableMob** und klicken Sie auf **Bearbeiten**, um ihn entsprechend zu ändern.

   Verwenden Sie `vim-cmd` nicht über die ESXi Shell.

ESXi-Netzwerksicherheitsempfehlungen

Die Isolierung des Netzwerkverkehrs ist entscheidend für eine sichere ESXi-Umgebung. Verschiedene Netzwerke benötigen verschiedene Zugriffsmöglichkeiten und Isolierungsebenen.

Ihr ESXi-Host verwendet mehrere Netzwerke. Verwenden Sie angemessene Sicherheitsmaßnahmen für jedes Netzwerk und isolieren Sie Datenverkehr für bestimmte Anwendungen und Funktionen. Stellen Sie beispielsweise sicher, dass VMware vSphere® vMotion®-Datenverkehr nicht über Netzwerke gesendet wird, in denen sich virtuelle Maschinen befinden. Durch Isolierung wird Snooping verhindert. Getrennte Netzwerke werden auch aus Leistungsgründen empfohlen.

- Netzwerke der vSphere-Infrastruktur werden für Funktionen wie vSphere vMotion, VMware vSphere Fault Tolerance, VMware vSAN und Speicher verwendet. Isolieren Sie diese Netzwerke nach ihren spezifischen Funktionen. Es ist meistens nicht nötig, diese Netzwerke außerhalb eines einzelnen physischen Server-Racks zu routen.
- Ein Verwaltungsnetzwerk isoliert Datenverkehr des Clients, der Befehlszeilenschnittstelle (CLI) oder der API sowie Datenverkehr von Drittsoftware von anderem Datenverkehr. Im Allgemeinen haben nur System-, Netzwerk- und Sicherheitsadministratoren Zugriff auf das Verwaltungsnetzwerk. Um den Zugriff auf das Verwaltungsnetzwerk zu sichern, verwenden Sie einen Bastionhost oder ein virtuelles privates Netzwerk (VPN). Führen Sie eine strenge Kontrolle für den Zugriff innerhalb dieses Netzwerks durch.
- Der Datenverkehr von virtuellen Maschinen kann über ein oder zahlreiche Netzwerke fließen. Sie können die Isolierung von virtuellen Maschinen verbessern, indem Sie virtuelle Firewalllösungen einsetzen, in denen Firewallregeln beim virtuellen Netzwerkcontroller festgelegt werden. Diese Einstellungen werden zusammen mit der virtuellen Maschine migriert, wenn diese von einem Host zu einem anderen in der vSphere-Umgebung migriert wird.

Ändern von ESXi-Web-Proxy-Einstellungen

Beim Ändern von Web-Proxy-Einstellungen müssen mehrere Richtlinien für Verschlüsselung und Benutzersicherheit berücksichtigt werden.

Hinweis Starten Sie den Hostprozess neu, nachdem Sie Änderungen an den Hostverzeichnissen oder den Authentifizierungsmechanismen vorgenommen haben.

- Richten Sie keine Zertifikate ein, in denen Kennwörter oder Kennwortsätze verwendet werden. ESXi unterstützt keine Web-Proxys mit Kennwörtern oder Kennwortsätzen (verschlüsselte Schlüssel). Wenn Sie einen Web-Proxy einrichten, der ein Kennwort oder einen Kennwortsatz benötigt, können die ESXi-Prozesse nicht korrekt gestartet werden.
- Zur Unterstützung von Verschlüsselung für Benutzernamen, Kennwörter und Pakete wird SSL standardmäßig für vSphere Web Services SDK-Verbindungen aktiviert. Wenn Sie diese Verbindungen so konfigurieren möchten, dass Übertragungen nicht verschlüsselt werden, deaktivieren Sie SSL für Ihre vSphere Web Services SDK-Verbindung, indem Sie die Verbindung von HTTPS auf HTTP umstellen.

Deaktivieren Sie SSL nur dann, wenn Sie eine vollständig vertrauenswürdige Umgebung für die Clients geschaffen haben, d. h. Firewalls wurden installiert und die Übertragungen zum und vom Host sind vollständig isoliert. Die Deaktivierung von SSL kann die Leistung verbessern, da der für die Verschlüsselung notwendige Verarbeitungsaufwand nicht anfällt.

- Um den Missbrauch von ESXi-Diensten zu verhindern, kann auf die meisten internen ESXi-Dienste nur über Port 443, den für HTTPS-Übertragungen verwendeten Port, zugegriffen werden. Port 443 dient als Reverse-Proxy für ESXi. Sie können eine Liste der Dienste auf dem ESXi-Host auf einer HTTP-Begrüßungsseite sehen. Sie können direkt aber nur auf die Speicheradapterdienste zugreifen, wenn Sie über die entsprechenden Berechtigungen verfügen.

  Sie können diese Einstellung ändern, sodass auf bestimmte Dienste direkt über HTTP-Verbindungen zugegriffen werden kann. Nehmen diese Änderung nur vor, wenn Sie ESXi in einer vertrauenswürdigen Umgebung verwenden.

- Wenn Sie Ihre Umgebung aktualisieren, wird das Zertifikat beibehalten.

vSphere Auto Deploy-Sicherheitsüberlegungen

Wenn Sie vSphere Auto Deploy verwenden, achten Sie besonders auf die Netzwerksicherheit, die Sicherheit des Start-Images und eine mögliche Kennwortoffenlegung durch Hostprofile, um Ihre Umgebung zu schützen.

Netzwerksicherheit

Sichern Sie Ihr Netzwerk genau wie das Netzwerk für andere PXE-basierte Bereitstellungsmethoden. vSphere Auto Deploy überträgt Daten über SSL, um gelegentliche Störungen und Webspionage zu verhindern. Allerdings wird die Authentizität des Clients oder des Auto Deploy-Servers während des Startens per PXE-Startvorgang nicht überprüft.

Sie können das Sicherheitsrisiko von Auto Deploy erheblich reduzieren, indem Sie das Netzwerk, in dem Auto Deploy eingesetzt wird, vollständig isolieren.

Start-Image- und Hostprofilsicherheit

Das Start-Image, das der vSphere Auto Deploy-Server auf eine Maschine herunterlädt, kann über die folgenden Komponenten verfügen.

- Das Start-Image enthält immer die VIB-Pakete, aus denen das Image-Profil besteht.
- Das Hostprofil und die Hostanpassung sind im Start-Image enthalten, wenn Auto Deploy-Regeln so eingerichtet sind, dass der Host mit einem Hostprofil- oder einer Hostanpassung bereitgestellt wird.
  - Das Administratorkennwort (root) und die Benutzerkennwörter, die im Hostprofil und in der Hostanpassung enthalten sind, sind mit SHA-512 gehasht.
  - Alle anderen Kennwörter in Verbindung mit Profilen sind unverschlüsselt. Wenn Sie Active Directory mithilfe von Hostprofilen einrichten, werden die Kennwörter nicht geschützt.

Verwenden Sie den vSphere Authentication Proxy, um zu verhindern, dass die Active Directory-Kennwörter offengelegt werden. Wenn Sie Active Directory mithilfe von Hostprofilen einrichten, werden die Kennwörter nicht geschützt.

- Die öffentlichen und privaten SSL-Schlüssel und das Zertifikat des Hosts sind im Start-Image enthalten.

Steuern des Zugriffs für CIM-basierte Hardwareüberwachungstools

Das CIM-System (Common Information Model) bietet eine Schnittstelle, mit der es möglich ist, Hardware von Remoteanwendungen aus mit einem Standard-API-Satz zu verwalten. Um die Sicherheit der CIM-Schnittstelle sicherzustellen, sollten Sie diesen Remoteanwendungen nur den nötigen Mindestzugriff einräumen. Wenn Sie eine Remoteanwendung mit einem Root- oder Administratorkonto bereitstellen und die Anwendung manipuliert wird, besteht für die virtuelle Umgebung ein Sicherheitsrisiko.

CIM ist ein offener Standard, der ein Framework für die agentenlose und standardbasierte Überwachung von Hardwareressourcen für ESXi-Hosts definiert. Dieses Framework besteht aus einem CIM Object Manager, häufig auch CIM-Broker genannt, und einem Satz von CIM-Anbietern.

CIM-Anbieter unterstützen den Verwaltungszugriff auf Gerätetreiber und zugrunde liegende Hardware. Hardwareanbieter, einschließlich Serverhersteller und Hardwaregeräteanbieter, können Anbieter erstellen, die ihre Geräte überwachen und verwalten. VMware schreibt Anbieter, mit denen die Serverhardware, ESXi-Speicherinfrastruktur und virtualisierungsspezifische Ressourcen überwacht werden. Diese Lightweight-Anbieter werden innerhalb des ESXi-Hosts ausgeführt und sind auf spezielle Verwaltungsaufgaben fokussiert. Der CIM-Broker ruft Informationen von allen CIM-Anbietern ab und zeigt sie extern mithilfe von Standard-APIs an, wobei WS-MAN die geläufigste ist.

Stellen Sie Remoteanwendungen, die auf die CIM-Schnittstelle zugreifen, keine Root-Anmeldedaten bereit. Stattdessen erstellen Sie ein vSphere-Benutzerkonto mit weniger Berechtigungen für diese Anwendungen und verwenden zur Authentifizierung beim CIM die VIM-API-Ticketfunktion zur Ausgabe einer Sitzungs-ID (als „Ticket“ bezeichnet) für dieses Benutzerkonto. Wenn dem Konto die Berechtigung zum Abrufen von CIM-Tickets erteilt wurde, kann die VIM-API das Ticket im CIM bereitstellen. Diese Tickets werden dann als Benutzer-ID und Kennwort für alle CIM-XML-API-Aufrufe angegeben. Weitere Informationen finden Sie in der `AcquireCimServicesTicket()`-Methode.

Der CIM-Dienst startet, wenn Sie das CIM-VIB eines Drittanbieters installieren, beispielsweise beim Ausführen des Befehls `esxcli software vib install -n VIBname`.

Wenn Sie den CIM-Dienst manuell aktivieren müssen, führen Sie folgenden Befehl aus:

```
esxcli system wbem set -e true
```

Sie können wsman (WSManagement Service) gegebenenfalls deaktivieren, damit nur der CIM-Dienst ausgeführt wird:

```
esxcli system wbem set -W false
```

Führen Sie folgenden Befehl aus, um zu bestätigen, dass wsman deaktiviert ist:

```
esxcli system wbem get
…
WSManagement PID: 0
WSManagement Service: false
```

Weitere Informationen zu ESXCLI-Befehlen finden Sie unter *ESXCLI-Dokumentation*. Weitere Informationen zum Aktivieren des CIM-Diensts finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/kb/1025757.

Verfahren

1 Erstellen Sie in vSphere ein Nicht-Root-Benutzerkonto für CIM-Anwendungen.

   Weitere Informationen finden Sie im Thema zum Hinzufügen von vCenter Single Sign-On-Benutzern unter *vSphere-Authentifizierung*. Die erforderliche vSphere-Berechtigung für das Benutzerkonto lautet **Host.CIM.Interaktion**.

2 Verwenden Sie das vSphere API-SDK Ihrer Wahl, um das Benutzerkonto bei vCenter Server zu authentifizieren. Rufen Sie anschließend `AcquireCimServicesTicket()` auf, um ein Ticket zur Authentifizierung mit ESXi als Administratorebenenkonto unter Verwendung der API „CIM-XML port 5989“ oder der API „WS-Man port 433“ zurückzugeben.

   Weitere Informationen finden Sie in der *vSphere Web Services-API-Referenz*.

3 Verlängern Sie das Ticket gegebenenfalls alle zwei Minuten.

Zertifikatsverwaltung für ESXi-Hosts

Die VMware Certificate Authority (VMCA) stellt für jeden neuen ESXi-Host ein signiertes Zertifikat bereit, dessen Rootzertifizierungsstelle standardmäßig die VMCA ist. Diese Bereitstellung findet statt, wenn der Host explizit oder im Zuge der Installation von ESXi 6.0 oder höher bzw. eines Upgrades auf diese Versionen zu vCenter Server hinzugefügt wird.

Sie können ESXi-Zertifikate in vSphere Client und über die `vim.CertificateManager`-API im vSphere Web Services SDK anzeigen und verwalten. Es ist nicht möglich, ESXi-Zertifikate mithilfe von Management-CLIs für vCenter Server-Zertifikate anzuzeigen oder zu verwalten.

Zertifikate in vSphere 6.0 und höher

Bei der Kommunikation zwischen ESXi und vCenter Server kommt TLS für beinahe den gesamten Verwaltungsdatenverkehr zum Einsatz.

Ab vSphere 6.0 unterstützt vCenter Server für ESXi-Hosts die folgenden Zertifikatmodi.

Tabelle 3-2. Zertifikatmodi für ESXi-Hosts

Zertifikatmodus	Beschreibung
VMware Certificate Authority (Standard)	Verwenden Sie diesen Modus, wenn VMCA die Zertifikate für alle ESXi-Hosts bereitstellt, entweder als Zertifizierungsstelle der obersten Ebene oder als Zwischenzertifizierungsstelle. Standardmäßig liefert VMCA alle Zertifikate für ESXi-Hosts. In diesem Modus können Sie Zertifikate in vSphere Client aktualisieren und verlängern.
Benutzerdefinierte Zertifizierungsstelle	Verwenden Sie diesen Modus, wenn Sie ausschließlich benutzerdefinierte, von einer Drittanbieter- oder Unternehmens-Zertifizierungsstelle signierte Zertifikate verwenden möchten. In diesem Modus sind Sie für die Verwaltung der Zertifikate verantwortlich. Hier können Sie die Zertifikate nicht in vSphere Client aktualisieren und verlängern. **Hinweis** Wenn Sie den Zertifikatmodus nicht in „Benutzerdefinierte Zertifizierungsstelle“ ändern, kann VMCA benutzerdefinierte Zertifikate ersetzen, beispielsweise wenn Sie die Option **Verlängern** in vSphere Client wählen.
Fingerabdruckmodus	vSphere 5.5 verwendete den Fingerabdruckmodus, und dieser Modus ist in vSphere 6.x nach wie vor als Notfallmodus verfügbar. In diesem Modus prüft vCenter Server, ob das Zertifikat korrekt formatiert ist, jedoch nicht die Gültigkeit des Zertifikats. Selbst abgelaufene Zertifikate werden akzeptiert. Verwenden Sie diesen Modus nur, wenn Sie auf Probleme stoßen, die in den anderen beiden Modi nicht zu beheben sind. Einige Dienste aus vCenter 6.x und höher funktionieren möglicherweise im Fingerabdruckmodus nicht korrekt.

Zertifikatsablauf

Sie können im vSphere Client Informationen über den Ablauf von Zertifikaten anzeigen, die von VMCA oder Drittanbieter-Zertifizierungsstellen signiert wurden. Sie können Informationen zu allen Hosts, die von einem vCenter Server-System verwaltet werden, oder zu einzelnen Hosts abrufen. Ein gelber Alarm wird ausgelöst, wenn sich das Zertifikat im Status **Läuft in Kürze ab** (weniger als acht Monate) befindet. Ein roter Alarm wird ausgelöst, wenn sich das Zertifikat im Status **Ablauf steht bevor** (weniger als zwei Monate) befindet.

ESXi-Bereitstellung und VMCA

Beim Start eines ESXi-Hosts von einem Installationsmedium besitzt der Host zunächst ein automatisch generiertes Zertifikat. Sobald er dem vCenter Server-System hinzugefügt wird, erhält er ein von VMCA als Stammzertifizierungsstelle signiertes Zertifikat.

Der Vorgang ist ähnlich für Hosts, die mit Auto Deploy bereitgestellt werden. Da diese Hosts jedoch keine Statusdaten speichern, wird das signierte Zertifikat vom Auto Deploy-Server in seinem lokalen Zertifikatspeicher gespeichert. Das Zertifikat wird bei nachfolgenden Starts der ESXi-Hosts wiederverwendet. Ein Auto Deploy-Server ist Teil einer eingebetteten Bereitstellung oder eines vCenter Server-Systems.

Wenn VMCA nicht verfügbar ist, wenn ein Auto Deploy-Host zum ersten Mal startet, versucht der Host zunächst, eine Verbindung herzustellen. Wenn der Host keine Verbindung herstellen kann, durchläuft er den Herunterfahren- und Neustartzyklus so lange, bis VMCA verfügbar wird und dem Host ein signiertes Zertifikat bereitgestellt werden kann.

Erforderliche Berechtigungen für die ESXi-Zertifikatsverwaltung

Die Zertifikatsverwaltung für ESXi-Hosts erfordert das Recht **Zertifikate.Zertifikate verwalten**. Dieses Recht können Sie über den vSphere Client festlegen.

Hostname und IP-Adresse

Eine Änderung des Hostnamens oder der IP-Adresse kann sich darauf auswirken, ob vCenter Server das Zertifikat eines Hosts als gültig erachtet oder nicht. Wie Sie den Host zu vCenter Server hinzugefügt haben bestimmt, ob ein manueller Eingriff notwendig wird. Manueller Eingriff bedeutet, dass Sie den Host neu verbinden bzw. ihn von vCenter Server abtrennen und wieder hinzufügen.

Tabelle 3-3. Notwendigkeit eines manuellen Eingriffs bei Hostnamen- oder IP-Adressänderung

Host zu vCenter Server hinzugefügt mithilfe ...	Änderungen des Hostnamens	Änderungen der IP-Adresse
Hostname	Problem bei vCenter Server-Verbindung Manueller Eingriff erforderlich	Kein Eingriff erforderlich
IP-Adresse	Kein Eingriff erforderlich	Problem bei vCenter Server-Verbindung Manueller Eingriff erforderlich

Host-Upgrades und Zertifikate

Wenn Sie ein Upgrade eines ESXi-Hosts auf ESXi 6.5 oder höher durchführen, werden beim Upgrade-Prozess die selbstsignierten (Fingerabdruck) Zertifikate durch VMCA-signierte Zertifikate ersetzt. Wenn der ESXi-Host benutzerdefinierte Zertifikate verwendet, werden diese Zertifikate beim Upgrade-Prozess beibehalten, selbst wenn diese Zertifikate abgelaufen oder ungültig sind.

Der empfohlene Upgrade-Workflow hängt von den aktuellen Zertifikaten ab.

Host mit bereitgestellten Fingerabdruckzertifikaten

Wenn der Host derzeit Fingerabdruckzertifikate verwendet, werden ihm im Rahmen des Upgrade-Prozesses automatisch VMCA-Zertifikate zugewiesen.

Hinweis Sie können keine VMCA-Zertifikate auf Legacy-Hosts bereitstellen. Sie müssen für diese Hosts ein Upgrade auf ESXi 6.5 oder höher durchführen.

Host mit bereitgestellten benutzerdefinierten Zertifikaten

Wenn Ihr Host mit benutzerdefinierten Zertifikaten bereitgestellt wird, in der Regel von einer Zertifizierungsstelle signierte Zertifikate eines Drittanbieters, dann werden diese Zertifikate während des Upgrades beibehalten. Ändern Sie den Zertifikatmodus in **Benutzerdefiniert**, um sicherzustellen, dass die Zertifikate später während einer Zertifikataktualisierung nicht versehentlich ersetzt werden.

Hinweis Wenn sich Ihre Umgebung im VMCA-Modus befindet und Sie die Zertifikate über den vSphere Client aktualisieren, werden alle vorhandenen Zertifikate durch von VMCA signierte Zertifikate ersetzt.

Von diesem Zeitpunkt an überwacht vCenter Server die Zertifikate und zeigt Informationen, z. B. über ablaufende Zertifikate, im vSphere Client an.

Hosts, die mit Auto Deploy bereitgestellt werden

Hosts, die mit Auto Deploy bereitgestellt werden, werden immer neue Zertifikate zugewiesen, wenn sie zum ersten Mal mit ESXi 6.5 oder höher gestartet werden. Wenn Sie ein Upgrade für einen Host mit Bereitstellung durch Auto Deploy durchführen, generiert der Auto Deploy-Server eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) für den Host und sendet diese an VMCA. VMCA speichert das signierte Zertifikat für den Host. Wenn der Auto Deploy-Server Bereitstellungen für den Host durchführt, ruft er das Zertifikat von VMCA ab und schließt es als Bestandteil des Bereitstellungsprozesses ein.

Sie können Auto Deploy mit benutzerdefinierten Zertifikaten verwenden.

Weitere Informationen hierzu finden Sie unter Verwenden benutzerdefinierter Zertifikate mit Auto Deploy.

Moduswechsel-Workflows für Zertifikate

Ab vSphere 6.0 sind ESXi-Hosts standardmäßig mit Zertifikaten der VMCA ausgestattet. Sie können stattdessen den benutzerdefinierten Zertifikatmodus oder zur Fehlerbehebung den alten Fingerabdruckmodus verwenden. In den meisten Fällen unterbrechen Moduswechsel den Betrieb und sind nicht erforderlich. Wenn Sie einen Moduswechsel benötigen, sollten Sie die möglichen Auswirkungen vor Beginn prüfen.

Ab vSphere 6.0 unterstützt vCenter Server für ESXi-Hosts die folgenden Zertifikatmodi.

Zertifikatmodus	Beschreibung
VMware Certificate Authority (Standard)	Standardmäßig wird die VMware Certificate Authority als Zertifizierungsstelle für ESXi-Hostzertifikate verwendet. VMCA ist standardmäßig die Root-Zertifizierungsstelle, kann aber als Zwischenzertifizierungsstelle für eine andere Zertifizierungsstelle eingerichtet werden. In diesem Modus können die Benutzer Zertifikate über den vSphere Client verwalten. Er wird auch verwendet, wenn VMCA ein untergeordnetes Zertifikat ist.
Benutzerdefinierte Zertifizierungsstelle	Manche Kunden möchten eine eigene externe Zertifizierungsstelle verwalten. In diesem Modus sind die Kunden für die Verwaltung der Zertifikate verantwortlich und können diese nicht über den vSphere Client verwalten.
Fingerabdruckmodus	In vSphere 5.5 gab es den Fingerabdruckmodus, der in vSphere 6.0 nach wie vor als Notfallmodus verfügbar ist. Verwenden Sie diesen Modus nur, wenn mit einem der anderen beiden Modi Probleme aufgetreten sind, die Sie nicht beheben können. Einige Dienste aus vCenter 6.0 und höher funktionieren möglicherweise nicht korrekt im Fingerabdruckmodus.

Verwenden von benutzerdefinierten ESXi-Zertifikaten

Wenn Ihre Unternehmensrichtlinie die Verwendung einer anderen Root-Zertifizierungsstelle als VMCA erfordert, können Sie den Zertifikatmodus in Ihrer Umgebung nach sorgfältiger Planung wechseln. Der Workflow lautet wie folgt:

1 Wählen Sie die Zertifikate aus, die Sie verwenden möchten.

2 Versetzen Sie den Host bzw. die Hosts in den Wartungsmodus und trennen Sie ihn bzw. sie vom vCenter Server.

3 Fügen Sie das benutzerdefinierte Root-Zertifikat der Zertifizierungsstelle zu VECS hinzu.

4 Stellen Sie die Zertifikate der benutzerdefinierten Zertifizierungsstelle an die einzelnen Hosts bereit, und starten Sie die Dienste auf den betreffenden Hosts neu.

5 Wechseln Sie in den benutzerdefinierten Zertifizierungsstellen-Modus. Weitere Informationen hierzu finden Sie unter Ändern des Zertifikatmodus.

6 Verbinden Sie den Host bzw. die Hosts mit dem vCenter Server-System.

Wechseln vom benutzerdefinierten Zertifizierungsstellen-Modus zum VMCA-Modus

Wenn Sie den benutzerdefinierten Zertifizierungsstellen-Modus verwenden und zu dem Schluss kommen, dass VMCA sich für Ihre Umgebung besser eignet, können Sie nach sorgfältiger Planung den Modus wechseln. Der Workflow lautet wie folgt:

1 Entfernen Sie alle Hosts aus dem vCenter Server-System.

2 Entfernen Sie auf dem vCenter Server-System das Root-Zertifikat der Drittanbieterzertifizierungsstelle aus VECS.

3 Wechseln Sie in den VMCA-Modus. Weitere Informationen hierzu finden Sie unter Ändern des Zertifikatmodus.

4 Fügen Sie die Hosts zum vCenter Server-System hinzu.

Hinweis Jeder andere Workflow für diesen Moduswechsel kann zu unvorhergesehenem Verhalten führen.

Beibehalten von Zertifikaten des Fingerabdruckmodus während des Upgrade

Der Wechsel vom VMCA-Modus zum Fingerabdruckmodus kann erforderlich sein, wenn Sie Probleme mit den VMCA-Zertifikaten haben. Im Fingerabdruckmodus prüft das vCenter Server-System nur, ob ein Zertifikat vorhanden und richtig formatiert ist, aber nicht, ob das Zertifikat gültig ist. Weitere Anweisungen finden Sie im Abschnitt Ändern des Zertifikatmodus.

Wechseln vom Fingerabdruckmodus in den VMCA-Modus

Wenn Sie den Fingerabdruckmodus verwenden und VMCA-signierte Zertifikate verwenden möchten, ist für den Wechsel einige Planung erforderlich. Der Workflow lautet wie folgt:

1 Entfernen Sie alle Hosts aus dem vCenter Server-System.

2 Wechseln Sie in den VMCA-Zertifikatmodus. Weitere Informationen hierzu finden Sie unter Ändern des Zertifikatmodus.

3 Fügen Sie die Hosts zum vCenter Server-System hinzu.

Hinweis Jeder andere Workflow für diesen Moduswechsel kann zu unvorhergesehenem Verhalten führen.

Wechseln vom benutzerdefinierten Zertifizierungsstellen-Modus in den Fingerabdruckmodus

Wenn Sie Probleme mit der benutzerdefinierten Zertifizierungsstelle haben, können Sie vorübergehend in den Fingerabdruckmodus wechseln. Der Wechsel funktioniert nahtlos, wenn Sie den Anweisungen unter Ändern des Zertifikatmodus folgen. Nach dem Moduswechsel prüft das vCenter Server-System nur das Format des Zertifikats, aber nicht mehr die Gültigkeit des Zertifikats selbst.

Wechseln vom Fingerabdruckmodus in den benutzerdefinierten Zertifizierungsstellen-Modus

Wenn Sie zur Fehlerbehebung in Ihrer Umgebung in den Fingerabdruckmodus gewechselt sind und wieder den benutzerdefinierten Zertifizierungsstellen-Modus verwenden möchten, müssen Sie zunächst die erforderlichen Zertifikate generieren. Der Workflow lautet wie folgt:

1 Entfernen Sie alle Hosts aus dem vCenter Server-System.

2 Fügen Sie das Root-Zertifikat der benutzerdefinierten Zertifizierungsstelle dem TRUSTED_ROOTSF-Speicher auf VECS im vCenter Server-System hinzu. Weitere Informationen hierzu finden Sie unter Aktualisieren des vCenter Server-Speichers TRUSTED_ROOTS (Benutzerdefinierte Zertifikate).

3 Gehen Sie für jeden ESXi-Host wie folgt vor:

   a Stellen Sie das Zertifikat und den Schlüssel der benutzerdefinierten Zertifizierungsstelle bereit.

   b Starten Sie die Dienste auf dem Host neu.

4 Wechseln Sie in den benutzerdefinierten Modus. Weitere Informationen hierzu finden Sie unter Ändern des Zertifikatmodus.

5 Fügen Sie die Hosts zum vCenter Server-System hinzu.

Standardeinstellungen für ESXi-Zertifikate

Wenn ein Host zu einem vCenter Server-System hinzugefügt wird, sendet vCenter Server eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) für den Host an VMCA. Die meisten Standardwerte sind für viele Situationen gut geeignet, aber unternehmensspezifische Daten können geändert werden.

Sie können viele Standardeinstellungen über den vSphere Client ändern. Ändern Sie eventuell das Unternehmen und Ortsangaben. Weitere Informationen hierzu finden Sie unter Ändern der Standardeinstellungen für Zertifikate.

Tabelle 3-4. CSR-Einstellungen für ESXi

Parameter	Standardwert	Erweiterte Option
Schlüssellänge	2048	Nicht zutreffend
Schlüsselalgorithmus	RSA	Nicht zutreffend
Zertifikat-Signaturalgorithmus	sha256WithRSAEncryption	Nicht zutreffend
Allgemeiner Name	Der Name des Hosts, wenn dieser dem vCenter Server nach dem Hostnamen hinzugefügt wurde. Die IP-Adresse des Hosts, wenn dieser dem vCenter Server nach der IP-Adresse hinzugefügt wurde.	Nicht zutreffend
Land	USA	vpxd.certmgmt.certs.cn.country
E-Mail-Adresse	vmca@vmware.com	vpxd.certmgmt.certs.cn.email
Ort	Palo Alto	vpxd.certmgmt.certs.cn.localityName
Name der Organisationseinheit	VMware Engineering	vpxd.certmgmt.certs.cn.organizationalUnitName
Organisationsname	VMware	vpxd.certmgmt.certs.cn.organizationName
Bundesland/Kanton	Kalifornien	vpxd.certmgmt.certs.cn.state
Anzahl der Tage, die das Zertifikat gültig ist.	1825	vpxd.certmgmt.certs.daysValid

Tabelle 3-4. CSR-Einstellungen für ESXi (Fortsetzung)

Parameter	Standardwert	Erweiterte Option
Fester Schwellenwert für den Ablauf des Zertifikats. vCenter Server löst einen roten Alarm aus, wenn dieser Schwellenwert erreicht wird.	30 Tage	vpxd.certmgmt.certs.cn.hardThreshold
Abfrageintervall für Überprüfungen der Gültigkeit des vCenter Server-Zertifikats.	5 Tage	vpxd.certmgmt.certs.cn.pollIntervalDays
Soft-Schwellenwert für den Ablauf des Zertifikats. vCenter Server löst ein Ereignis aus, wenn dieser Schwellenwert erreicht wird.	240 Tage	vpxd.certmgmt.certs.cn.softThreshold
Modus, den vCenter Server verwendet, um zu ermitteln, ob vorhandene Zertifikate ersetzt werden. Ändern Sie diesen Modus, um benutzerdefinierte Zertifikate beim Upgrade beizubehalten. Weitere Informationen hierzu finden Sie unter Host-Upgrades und Zertifikate.	vmca Sie können auch „Fingerabdruck“ oder „benutzerdefiniert“ festlegen. Weitere Informationen hierzu finden Sie unter Ändern des Zertifikatmodus.	vpxd.certmgmt.mode

Ändern der Standardeinstellungen für Zertifikate

Wenn ein Host zu einem vCenter Server-System hinzugefügt wird, sendet vCenter Server eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) für den Host an VMCA. Sie können einige der Standardeinstellungen in der CSR ändern, indem Sie die erweiterten Einstellungen von vCenter Server im vSphere Client verwenden.

Eine Liste der Standardeinstellungen finden Sie unter Standardeinstellungen für ESXi-Zertifikate. Einige der Standardwerte können nicht geändert werden.

Verfahren

1. Wählen Sie im vSphere Client das vCenter Server-System aus, das die Hosts verwaltet.
2. Klicken Sie auf **Konfigurieren** und anschließend auf **Erweiterte Einstellungen**.
3. Klicken Sie auf **Einstellungen bearbeiten**.
4. Klicken Sie auf das Symbol **Filter** in der Spalte „Name“ und geben Sie im Feld „Filter“ den Wert **`vpxd.certmgmt`** ein, um ausschließlich Parameter der Zertifikatsverwaltung anzuzeigen.

5 Ändern Sie den Wert der vorhandenen Parameter entsprechend der Unternehmensrichtlinie und klicken Sie auf **Speichern**.

   Wenn Sie das nächste Mal einen Host zu vCenter Server hinzufügen, werden die neuen Einstellungen in der CSR, die vCenter Server an VMCA sendet, sowie im Zertifikat verwendet, das dem Host zugewiesen ist.

Nächste Schritte

Änderungen an den Zertifikatmetadaten betreffen nur neue Zertifikate. Wenn Sie die Zertifikate von Hosts ändern möchten, die bereits vom vCenter Server-System verwaltet werden, können Sie die Hosts trennen und erneut verbinden oder die Zertifikate verlängern.

Anzeigen von Informationen zum Ablauf von Zertifikaten für mehrere ESXi-Hosts

Wenn Sie ESXi 6.0 oder höher verwenden, können Sie den Zertifikatsstatus aller Hosts anzeigen, die von Ihrem vCenter Server-System verwaltet werden. Damit können Sie feststellen, ob irgendwelche Zertifikate bald ablaufen.

Sie können Zertifikatsstatusinformationen für Hosts, die den VMCA-Modus verwenden, und für Hosts, die den benutzerdefinierten Modus verwenden, im vSphere Client anzeigen. Sie können keine Zertifikatsstatusinformationen für Hosts im Fingerabdruckmodus anzeigen.

Verfahren

1 Melden Sie sich beim vCenter Server mit dem vSphere Client an.

2 Durchsuchen Sie die Bestandsliste und wählen Sie die vCenter Server-Instanz aus.

3 Wählen Sie **Hosts und Cluster > Hosts** aus.

   Standardmäßig wird der Zertifikatsstatus in der Anzeige der Hosts nicht eingeblendet.

4 Um Spalten ein- oder auszublenden, klicken Sie in der unteren linken Ecke auf das **Spaltenauswahl**-Symbol mit den drei Balken.

5 Aktivieren Sie das Kontrollkästchen **Zertifikat gültig bis** und führen Sie gegebenenfalls einen Bildlauf nach rechts durch, um die hinzugefügte Spalte anzuzeigen.

   Bei den Zertifikatsinformationen wird das Ablaufdatum des Zertifikats angezeigt.

   Wenn vCenter Server ein Host hinzugefügt wird oder die Verbindung mit einem Host nach einer Unterbrechung wieder hergestellt wird, erneuert vCenter Server das Zertifikat, wenn der Status „Abgelaufen“, „Läuft ab“, „Läuft in Kürze ab“ oder „Ablauf steht bevor“ lautet. Der Status lautet „Läuft ab“, wenn das Zertifikat für weniger als acht Monate gültig ist, er lautet „Läuft in Kürze ab“, wenn das Zertifikat für weniger als zwei Monate gültig ist, und er lautet „Ablauf steht bevor“, wenn das Zertifikat für weniger als einen Monat gültig ist.

6 (Optional) Heben Sie die Auswahl von anderen Spalten auf, damit die relevanten Informationen leichter zu sehen sind.

Nächste Schritte

Verlängern Sie die Zertifikate, die demnächst ablaufen. Weitere Informationen hierzu finden Sie unter Verlängern oder Aktualisieren von ESXi-Zertifikaten.

Anzeigen der Zertifikatsdetails für einen einzelnen ESXi-Host

Für Hosts der Versionen ESXi 6.0 oder höher im VMCA-Modus oder im benutzerdefinierten Modus können Sie Zertifikatsdetails über den vSphere Client anzeigen. Die Informationen über das Zertifikat können bei der Fehlerbehebung nützlich sein.

Verfahren

1. Navigieren Sie zum Host im Navigator von vSphere Client.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter **System** auf **Zertifikat**.

   Sie können die folgenden Informationen prüfen. Diese Informationen sind nur in der Einzelhostansicht verfügbar.

Feld	Beschreibung
Betreff	Der während der Zertifikatgenerierung verwendete Betreff.
Aussteller	Der Aussteller des Zertifikats.
Gültig von	Das Datum, an dem das Zertifikat generiert wurde.
Gültig bis	Das Datum, an dem das Zertifikat abläuft.
Status	Status des Zertifikats. Folgende Status sind möglich: **Gut** Normaler Betrieb. **Läuft ab** Zertifikat läuft bald ab. **Läuft in Kürze ab** Es fehlen nur noch acht Monate oder weniger bis zum Ablauf des Zertifikats (Standard). **Ablauf steht bevor** Es fehlen nur noch zwei Monate oder weniger bis zum Ablauf des Zertifikats (Standard). **Abgelaufen** Das Zertifikat ist nicht gültig, weil es abgelaufen ist.

Verlängern oder Aktualisieren von ESXi-Zertifikaten

Wenn VMCA Ihren ESXi-Hosts (6.0 oder höher) Zertifikate zuweist, können Sie diese Zertifikate über den vSphere Client erneuern. Sie können außerdem alle Zertifikate aus dem mit vCenter Server verknüpften Speicher TRUSTED_ROOTS aktualisieren.

Sie können Zertifikate erneuern, bevor sie ablaufen oder wenn Sie für den Host aus anderen Gründen ein neues Zertifikat bereitstellen möchten. Wenn Sie das Zertifikat nicht vor Ablauf erneuern, wird das Zertifikat von vCenter Server erneuert, wenn die Verbindung zum Host getrennt und wiederhergestellt wird. Durch das erneute Hinzufügen des Hosts zu vCenter Server wird die Vertrauensstellung wiederhergestellt und es vCenter Server ermöglicht, das erneuerte Zertifikat uneingeschränkt auszustellen.

Standardmäßig erneuert vCenter Server die Zertifikate eines Hosts mit dem Status „Abgelaufen“, „Ablauf steht bevor“ oder „Läuft in Kürze ab“ immer, wenn der Host der Bestandsliste hinzugefügt wird oder wenn seine Verbindung wiederhergestellt wird.

Voraussetzungen

Überprüfen Sie Folgendes:

- Die ESXi-Hosts sind mit dem vCenter Server-System verbunden.
- Zwischen dem vCenter Server-System und den ESXi-Hosts findet eine ordnungsgemäße Uhrzeitsynchronisierung statt.
- DNS-Auflösung funktioniert zwischen dem vCenter Server-System und den ESXi-Hosts.
- Die Zertifikate MACHINE_SSL_CERT und Trusted_Root des vCenter Server-Systems sind gültig und nicht abgelaufen. Informationen finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/2111411.
- Die ESXi-Hosts befinden sich nicht im Wartungsmodus.

Verfahren

1. Navigieren Sie zum Host im Navigator von vSphere Client.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter **System** auf **Zertifikat**.

   Sie können detaillierte Informationen zum Zertifikat des ausgewählten Hosts anzeigen.
4. Klicken Sie auf **Verlängern** oder **CA-Zertifikate aktualisieren**.

Option	Beschreibung
Verlängern	Lädt ein frisch signiertes Zertifikat für den Host von der VMCA.
CA-Zertifikate aktualisieren	Überträgt alle Zertifikate im TRUSTED_ROOTS-Speicher im VECS-Speicher von vCenter Server an den Host.

5. Klicken Sie auf **Ja**, um den Vorgang zu bestätigen.

Ändern des Zertifikatmodus

Verwenden Sie VMCA für die Bereitstellung der ESXi-Hosts in Ihrer Umgebung, es sei denn, Ihre Unternehmensrichtlinie verlangt, dass Sie benutzerdefinierte Zertifikate verwenden. Um benutzerdefinierte Zertifikate mit einer anderen Stammzertifizierungsstelle zu verwenden, können Sie die erweiterte Option vCenter Server `vpxd.certmgmt.mode` bearbeiten. Nach der Änderung werden die Hosts nicht mehr automatisch durch VMCA-Zertifikate bereitgestellt, wenn Sie die Zertifikate aktualisieren. Sie sind verantwortlich für die Zertifikatsverwaltung in Ihrer Umgebung.

In den erweiterten Einstellungen von vCenter Server können Sie in den Fingerabdruckmodus oder den benutzerdefinierten Zertifizierungsstellenmodus wechseln. Der Fingerabdruckmodus sollte lediglich im Notfall eingesetzt werden.

Verfahren

1. Wählen Sie im vSphere Client das vCenter Server-System aus, das die Hosts verwaltet.
2. Klicken Sie auf **Konfigurieren** und unter „Einstellungen“ auf **Erweiterte Einstellungen**.
3. Klicken Sie auf **Einstellungen bearbeiten**.
4. Klicken Sie auf das Symbol **Filter** in der Spalte „Name“ und geben Sie im Feld „Filter“ den Wert **`vpxd.certmgmt`** ein, um ausschließlich Parameter der Zertifikatsverwaltung anzuzeigen.
5. Ändern Sie den Wert von `vpxd.certmgmt.mode` in **custom**, wenn Sie eigene Zertifikate verwalten möchten, oder in **thumbprint**, wenn Sie vorübergehend in den Fingerabdruckmodus wechseln möchten. Klicken Sie anschließend auf **Speichern**.
6. Starten Sie den vCenter Server-Dienst neu.

   Informationen zum Neustarten von Diensten finden Sie in der Dokumentation *vCenter Server-Konfiguration*.

Ersetzen von ESXi SSL-Zertifikaten und -Schlüsseln

Die Sicherheitsrichtlinien Ihres Unternehmens erfordern möglicherweise, dass Sie das ESXi-Standard-SSL-Zertifikat durch ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat eines Drittanbieters auf jedem Host ersetzen.

Die vSphere-Komponenten verwenden standardmäßig das VMCA-signierte Zertifikat und den Schüssel, das/der während der Installation erstellt wird. Wenn Sie versehentlich das VMCA-signierte Zertifikat löschen, entfernen Sie den Host vom vCenter Server-System und fügen Sie ihn dann wieder hinzu. Wenn Sie den Host hinzufügen, fordert der vCenter Server ein neues Zertifikat von der VMCA an und stellt es für den Host bereit.

Ersetzen Sie VMCA-signierte Zertifikate durch Zertifikate einer vertrauenswürdigen Zertifizierungsstelle, d. h. entweder einer kommerziellen Zertifizierungsstelle oder einer unternehmenseigenen Zertifizierungsstelle, wenn Ihre Unternehmensrichtlinie dies vorsieht.

Die Standardzertifikate befinden sich am selben Speicherort wie die vSphere 5.5-Zertifikate. Es gibt verschiedene Möglichkeiten, Standardzertifikate durch vertrauenswürdige Zertifikate zu ersetzen.

Hinweis Sie können außerdem die durch `vim.CertificateManager` und `vim.host.CertificateManager` verwalteten Objekte im vSphere Web Services SDK verwenden. Siehe die Dokumentation zu vSphere Web Services SDK.

Nach dem Ersetzen des Zertifikats müssen Sie den Speicher TRUSTED_ROOTS in VECS auf dem vCenter Server-System, das den Host verwaltet, aktualisieren, um sicherzustellen, dass der vCenter Server und der ESXi-Host ein Vertrauensverhältnis haben.

Detaillierte Anweisungen zum Verwenden von CA-signierten Zertifikaten für ESXi-Hosts finden Sie unter Moduswechsel-Workflows für Zertifikate.

Hinweis Wenn Sie SSL-Zertifikate auf einem ESXi-Host entfernen, der zu einem vSAN-Cluster gehört, führen Sie die im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/56441 angegebenen Schritte durch.

- Voraussetzungen für ESXi-Zertifikatssignieranforderungen

  Wenn Sie ein Unternehmenszertifikat oder ein von einer Zertifizierungsstelle eines Drittanbieters bzw. einer untergeordneten Zertifizierungsstelle signiertes Zertifikat verwenden möchten, müssen Sie eine Zertifikatssignieranforderung (Certificate Signing Request, CSR) an die Zertifizierungsstelle senden.
- Ersetzen des Standardzertifikats und -schlüssels über die ESXi Shell

  Sie können die standardmäßigen VMCA-signierten ESXi-Zertifikate über die ESXi Shell ersetzen.
- Ersetzen eines Standardzertifikats und -schlüssels mit dem vifs-Befehl

  Sie können die standardmäßigen VMCA-signierten ESXi-Zertifikate mithilfe des `vifs`-Befehls ersetzen.
- Ersetzen eines Standardzertifikats mit HTTPS PUT

  Mit Drittanbieteranwendungen können Sie Zertifikate und Schlüssel hochladen. Anwendungen mit Unterstützung für HTTPS PUT-Operationen können mit der HTTPS-Schnittstelle verwendet werden, die im Lieferumfang von ESXi enthalten ist.
- Aktualisieren des vCenter Server-Speichers TRUSTED_ROOTS (Benutzerdefinierte Zertifikate)

  Wenn Sie Ihre ESXi-Hosts so einrichten, dass benutzerdefinierte Zertifikate verwendet werden, müssen Sie den Speicher `TRUSTED_ROOTS` auf dem vCenter Server-System, das die Hosts verwaltet, aktualisieren.

Voraussetzungen für ESXi-Zertifikatssignieranforderungen

Wenn Sie ein Unternehmenszertifikat oder ein von einer Zertifizierungsstelle eines Drittanbieters bzw. einer untergeordneten Zertifizierungsstelle signiertes Zertifikat verwenden möchten,

müssen Sie eine Zertifikatssignieranforderung (Certificate Signing Request, CSR) an die Zertifizierungsstelle senden.

Verwenden Sie eine Zertifikatssignieranforderung mit den folgenden Eigenschaften:

- 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, Unleugbarkeit, 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.

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.

Informationen darüber, wie Sie die CSR generieren, finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/2113926.

Ersetzen des Standardzertifikats und -schlüssels über die ESXi Shell

Sie können die standardmäßigen VMCA-signierten ESXi-Zertifikate über die ESXi Shell ersetzen.

Voraussetzungen

- Wenn Sie CA-signierte Zertifikate von Drittanbietern verwenden, generieren Sie die Zertifikatsanforderung, senden Sie sie an die Zertifizierungsstelle und speichern Sie die Zertifikate auf jedem ESXi-Host.
- Aktivieren Sie ggf. ESXi Shell oder SSH-Datenverkehr vom vSphere Client.
- Alle Dateiübertragungen und andere Kommunikationsvorgänge erfolgen über eine sichere HTTPS-Sitzung. Der zum Authentifizieren der Sitzung verwendete Benutzer muss über das Recht **Host.Config.AdvancedConfig** auf dem Host verfügen.

Verfahren

1. Melden Sie sich bei der ESXi Shell entweder direkt von der DCUI oder von einem SSH-Client als Benutzer mit Administratorrechten an.
2. Benennen Sie im Verzeichnis `/etc/vmware/ssl` die vorhandenen Zertifikate mit folgenden Befehlen um.

   ```
   mv rui.crt orig.rui.crt
   mv rui.key orig.rui.key
   ```

3. Kopieren Sie die Zertifikate, die Sie verwenden möchten, in `/etc/vmware/ssl`.
4. Benennen Sie das neue Zertifikat und den Schlüssel um in `rui.crt` und `rui.key`.
5. Starten Sie den Host nach der Installation des neuen Zertifikats neu.

   Alternativ können Sie den Host in den Wartungsmodus versetzen, das neue Zertifikat installieren, die Verwaltungs-Agenten über die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) neu starten und den Host festlegen, um den Wartungsmodus zu beenden.

Nächste Schritte

Aktualisieren Sie den Speicher vCenter Server TRUSTED_ROOTS. Weitere Informationen hierzu finden Sie unter Aktualisieren des vCenter Server-Speichers TRUSTED_ROOTS (Benutzerdefinierte Zertifikate).

Ersetzen eines Standardzertifikats und -schlüssels mit dem vifs-Befehl

Sie können die standardmäßigen VMCA-signierten ESXi-Zertifikate mithilfe des `vifs`-Befehls ersetzen.

Voraussetzungen

- Wenn Sie CA-signierte Zertifikate von Drittanbietern verwenden, generieren Sie die Zertifikatsanforderung, senden Sie sie an die Zertifizierungsstelle und speichern Sie die Zertifikate auf jedem ESXi-Host.
- Aktivieren Sie ggf. ESXi Shell oder SSH-Datenverkehr vom vSphere Client.
- Alle Dateiübertragungen und andere Kommunikationsvorgänge erfolgen über eine sichere HTTPS-Sitzung. Der zum Authentifizieren der Sitzung verwendete Benutzer muss über das Recht **Host.Config.AdvancedConfig** auf dem Host verfügen.

Verfahren

1. Sichern Sie die vorhandenen Zertifikate.
2. Generieren Sie eine Zertifikatsanforderung gemäß den Anweisungen der Zertifizierungsstelle.

   Weitere Informationen hierzu finden Sie unter Voraussetzungen für ESXi-Zertifikatssignieranforderungen.

3 Wenn Sie das Zertifikat haben, verwenden Sie den `vifs`-Befehl, um das Zertifikat über eine SSH-Verbindung mit dem Host an die entsprechende Position auf dem Host hochzuladen.

```
vifs --server Hostname --username Benutzername --put rui.crt /host/ssl_cert
vifs --server Hostname --username Benutzername --put rui.key /host/ssl_key
```

4 Starten Sie den Host neu.

Alternativ können Sie den Host in den Wartungsmodus versetzen, das neue Zertifikat installieren, die Verwaltungs-Agenten über die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) neu starten und den Host festlegen, um den Wartungsmodus zu beenden.

Nächste Schritte

Aktualisieren Sie den Speicher vCenter Server TRUSTED_ROOTS. Weitere Informationen hierzu finden Sie unter Aktualisieren des vCenter Server-Speichers TRUSTED_ROOTS (Benutzerdefinierte Zertifikate).

Ersetzen eines Standardzertifikats mit HTTPS PUT

Mit Drittanbieteranwendungen können Sie Zertifikate und Schlüssel hochladen. Anwendungen mit Unterstützung für HTTPS PUT-Operationen können mit der HTTPS-Schnittstelle verwendet werden, die im Lieferumfang von ESXi enthalten ist.

Voraussetzungen

- Wenn Sie CA-signierte Zertifikate von Drittanbietern verwenden, generieren Sie die Zertifikatsanforderung, senden Sie sie an die Zertifizierungsstelle und speichern Sie die Zertifikate auf jedem ESXi-Host.
- Aktivieren Sie ggf. ESXi Shell oder SSH-Datenverkehr vom vSphere Client.
- Alle Dateiübertragungen und andere Kommunikationsvorgänge erfolgen über eine sichere HTTPS-Sitzung. Der zum Authentifizieren der Sitzung verwendete Benutzer muss über das Recht **Host.Config.AdvancedConfig** auf dem Host verfügen.

Verfahren

1 Sichern Sie die vorhandenen Zertifikate.

2 Gehen Sie in Ihrer Upload-Anwendung mit jeder Datei wie folgt vor.

a Öffnen Sie die Datei.

b Veröffentlichen Sie die Datei an einem der folgenden Speicherorte.

Option	Beschreibung
Zertifikate	`https://hostname/host/ssl_cert`
Schlüssel	`https://hostname/host/ssl_key`

Die Speicherorte `/host/ssl_cert` und `host/ssl_key` sind mit den Zertifikatsdateien unter `/etc/vmware/ssl` verknüpft.

3 Starten Sie den Host neu.

Alternativ können Sie den Host in den Wartungsmodus versetzen, das neue Zertifikat installieren, die Verwaltungs-Agenten über die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) neu starten und den Host festlegen, um den Wartungsmodus zu beenden.

Nächste Schritte

Aktualisieren Sie den Speicher vCenter Server TRUSTED_ROOTS. Weitere Informationen hierzu finden Sie unter Aktualisieren des vCenter Server-Speichers TRUSTED_ROOTS (Benutzerdefinierte Zertifikate).

Aktualisieren des vCenter Server-Speichers TRUSTED_ROOTS (Benutzerdefinierte Zertifikate)

Wenn Sie Ihre ESXi-Hosts so einrichten, dass benutzerdefinierte Zertifikate verwendet werden, müssen Sie den Speicher `TRUSTED_ROOTS` auf dem vCenter Server-System, das die Hosts verwaltet, aktualisieren.

Voraussetzungen

Ersetzen Sie die Zertifikate auf jedem Host durch benutzerdefinierte Zertifikate.

Hinweis Dieser Schritt ist nicht erforderlich, wenn das vCenter Server-System ebenfalls mit benutzerdefinierten Zertifikaten ausgeführt wird, die von der gleichen Zertifizierungsstelle wie die auf den ESXi-Hosts installierten ausgestellt wurden.

Verfahren

1 Melden Sie sich bei der vCenter Server-Shell des vCenter Server-Systems an, das die ESXi-Hosts verwaltet.

2 Um die neuen Zertifikate zum Speicher `TRUSTED_ROOTS` hinzuzufügen, führen Sie `dir-cli` aus. Beispiel:

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert path_to_RootCA
```

3 Geben Sie bei Aufforderung die Single Sign-On-Administrator-Anmeldedaten ein.

4 Wenn Ihre benutzerdefinierten Zertifikate von einer Zwischenzertifizierungsstelle ausgestellt werden, müssen Sie auch die Zwischenzertifizierungsstelle zum Speicher `TRUSTED_ROOTS` auf dem vCenter Server hinzufügen. z. B.:

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert path_to_intermediateCA
```

Nächste Schritte

Setzen Sie den Zertifikatsmodus auf „Benutzerdefiniert“. Wenn VMCA, der Standardwert, der Zertifikatsmodus ist und Sie ein Zertifikat aktualisieren, werden Ihre benutzerdefinierten Zertifikate durch VMCA-signierte Zertifikate ersetzt. Weitere Informationen hierzu finden Sie unter Ändern des Zertifikatmodus.

Verwenden benutzerdefinierter Zertifikate mit Auto Deploy

Standardmäßig stattet der Auto Deploy-Server jeden Host mit Zertifikaten aus, die von VMCA signiert wurden. Sie können den Auto Deploy-Server jedoch auch so konfigurieren, dass er alle Hosts mit nicht von VMCA signierten Zertifikaten ausstattet. Dabei wird der Auto Deploy-Server zu einer Zwischenzertifizierungsstelle für Ihre Drittanbieter-Zertifizierungsstelle.

Voraussetzungen

- Fordern Sie ein Zertifikat von Ihrer Zertifizierungsstelle an. Die Zertifikatsdatei 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, Unleugbarkeit, 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.
- Benennen Sie die Zertifikatdatei als `rbd-ca.crt` und die Schlüsseldatei als `rbd-ca.key`.

Verfahren

1. Sichern Sie die standardmäßigen ESXi-Zertifikate.

   Die Zertifikate befinden sich im Verzeichnis `/etc/vmware-rbd/ssl/`.

2 Halten Sie den vSphere Authentication Proxy-Dienst an.

Tool	Schritte
vCenter Server-Verwaltungsschnittstelle	a Navigieren Sie in einem Webbrowser zur vCenter Server-Verwaltungsschnittstelle (https://*vcenter-IP-adresse-oder-FQDN*:5480). b Melden Sie sich als „root“ an. Das standardmäßige Root-Kennwort ist das Kennwort, das Sie während der Bereitstellung der vCenter Server festlegen. c Klicken Sie auf **Dienste** und anschließend auf den **VMware vSphere Authentication Proxy-Dienst**. d Klicken Sie auf **Beenden**.
Befehlszeilenschnittstelle	`service-control --stop vmcam`

3 Ersetzen Sie auf dem System, auf dem der Auto Deploy-Dienst ausgeführt wird, die Dateien `rbd-ca.crt` und `rbd-ca.key` in `/etc/vmware-rbd/ssl/` durch Ihr benutzerdefiniertes Zertifikat bzw. die Schlüsseldateien.

4 Führen Sie auf dem System, auf dem der Dienst „Automatischer Einsatz“ ausgeführt wird, den folgenden Befehl aus, um den TRUSTED_ROOTS-Speicher in VECS zu aktualisieren und Ihre neuen Zertifikate nutzen zu können.

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert /etc/vmware-rbd/ssl/rbd-ca.crt
/usr/lib/vmware-vmafd/bin/vecs-cli force-refresh
```

5 Erstellen Sie die Datei `castore.pem`, die den Inhalt des TRUSTED_ROOTS-Speichers enthält, und fügen Sie sie in das Verzeichnis `/etc/vmware-rbd/ssl/` ein.

Im benutzerdefinierten Modus sind Sie für die Wartung dieser Datei verantwortlich.

6 Ändern Sie den ESXi-Zertifikatmodus für das vCenter Server-System in **`benutzerdefiniert`**.

Weitere Informationen hierzu finden Sie unter Ändern des Zertifikatmodus.

7 Starten Sie den vCenter Server-Dienst neu und starten Sie den Auto Deploy-Dienst.

Ergebnisse

Das nächste Mal, wenn Sie einen für die Verwendung von Auto Deploy eingerichteten Host bereitstellen, generiert der Auto Deploy-Server ein Zertifikat. Der Server zur automatischen Bereitstellung verwendet das Root-Zertifikat, das Sie zum TRUSTED_ROOTS-Speicher hinzugefügt haben.

Hinweis Wenn Sie Probleme mit dem automatischen Einsatz nach der Zertifikatsersetzung haben, lesen Sie sich den VMware-Knowledgebase-Artikel unter http://kb.vmware.com/kb/2000988 durch.

Wiederherstellen des ESXi-Zertifikats und der Schlüsseldateien

Wenn Sie ein Zertifikat auf einem ESXi-Host mithilfe der vSphere Web Services SDK ersetzen, werden das vorherige Zertifikat und der Schlüssel einer `BAK`-Datei hinzugefügt. Sie können vorherige Zertifikate durch Verschieben der Daten in der `BAK`-Datei in das aktuelle Zertifikat und die Schlüsseldateien wiederherstellen.

Das Hostzertifikat und der Schlüssel befinden sich am Speicherort `/etc/vmware/ssl/rui.crt` bzw. `/etc/vmware/ssl/rui.key`. Wenn Sie ein Hostzertifikat und einen Schlüssel mithilfe des verwalteten Objekts `vim.CertificateManager` von vSphere Web Services SDK ersetzen, werden der vorherige Schlüssel und das Zertifikat der Datei `/etc/vmware/ssl/rui.bak` hinzugefügt.

Hinweis Wenn Sie das Zertifikat mithilfe von HTTP PUT, `vifs` oder über die ESXi Shell ersetzen, werden die vorhandenen Zertifikate nicht der `BAK`-Datei hinzugefügt.

Verfahren

1 Suchen Sie auf dem ESXi-Host die Datei `/etc/vmware/ssl/rui.bak`.

Die Datei weist das folgende Format auf.

```
#
# Host private key and certificate backup from 2014-06-20 08:02:49.961
#

-----BEGIN PRIVATE KEY-----
previous key
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
previous cert
-----END CERTIFICATE-----
```

2 Kopieren Sie den Text von `-----BEGIN PRIVATE KEY-----` bis `-----END PRIVATE KEY-----` in die Datei `/etc/vmware/ssl/rui.key`.

`-----BEGIN PRIVATE KEY-----` und `-----END PRIVATE KEY-----` müssen im Text enthalten sein.

3 Kopieren Sie den Text von `-----BEGIN CERTIFICATE-----` bis `-----END CERTIFICATE-----` in die Datei `/etc/vmware/ssl/rui.crt`.

`-----BEGIN CERTIFICATE-----` und `-----END CERTIFICATE-----` müssen im Text enthalten sein.

4 Starten Sie das ESXi-System neu.

Alternativ können Sie den Host in den Wartungsmodus versetzen, die Verwaltungs-Agenten über die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) neu starten, und den Host festlegen, um den Wartungsmodus zu beenden.

Anpassen von Hosts mit dem Sicherheitsprofil

Viele wichtige Sicherheitseinstellungen für Ihren Host können Sie über die Bereiche „Sicherheitsprofil“, „Dienste“ und „Firewall“ im vSphere Client anpassen. Das Sicherheitsprofil ist insbesondere für die Verwaltung eines einzelnen Hosts hilfreich. Falls Sie mehrere Hosts verwalten, sollten Sie eine CLI oder ein SDK verwenden und die Anpassung automatisieren.

ESXi-Firewall-Konfiguration

ESXi enthält eine Firewall, die standardmäßig aktiviert ist.

Während der Installation wird die ESXi-Firewall so konfiguriert, dass mit Ausnahme des Datenverkehrs für Dienste, die im Sicherheitsprofil des Hosts aktiviert sind, der ein- und ausgehende Datenverkehr blockiert wird.

Beim Öffnen der Ports in der Firewall müssen Sie sich bewusst sein, dass der uneingeschränkte Zugriff auf die Dienste eines ESXi-Hosts den Host für Angriffe von außen und nicht autorisierten Zugriff verwundbar machen. Verringern Sie dieses Risiko, indem Sie die ESXi-Firewall so konfigurieren, dass sie nur den Zugriff über autorisierte Netzwerke zulässt.

Hinweis Die Firewall lässt auch Internet Control Message Protocol (ICMP)-Pings und Kommunikation mit DHCP- und DNS- Clients (nur UDP) zu.

Sie können ESXi-Firewallports wie folgt verwalten:

- Verwenden Sie **Konfigurieren > Firewall** für jeden Host im vSphere Client. Weitere Informationen hierzu finden Sie unter Verwalten von ESXi-Firewalleinstellungen.
- Verwenden Sie ESXCLI-Befehle über die Befehlszeile oder in Skripts. Weitere Informationen hierzu finden Sie unter ESXi ESXCLI-Firewall-Befehle.
- Verwenden Sie ein benutzerdefiniertes VIB, wenn der Port, der geöffnet werden soll, nicht im Sicherheitsprofil enthalten ist.

  Um das benutzerdefinierte VIB zu installieren, müssen Sie die Akzeptanzebene des ESXi-Hosts in „CommunitySupported“ ändern.

  Hinweis Wenn Sie den technischen Support von VMware um Hilfe bei einem Problem auf einem ESXi-Host mit einem installierten CommunitySupported VIB bitten, können Sie vom VMware Support zur Deinstallation dieses VIB aufgefordert werden. Hierbei handelt es sich um einen der Schritte zur Fehlerbehebung, mit dem festgestellt werden soll, ob das VIB mit dem geprüften Problem in Zusammenhang steht.

Das Verhalten des NFS-Client-Regelsatzes (`nfsClient`) unterscheidet sich von dem Verhalten anderer Regelsätze. Wenn der NFS-Client-Regelsatz aktiviert ist, sind alle ausgehenden TCP-Ports für die Zielhosts in der Liste der zulässigen IP-Adressen offen. Weitere Informationen hierzu finden Sie unter NFS-Client-Firewallverhalten.

Verwalten von ESXi-Firewalleinstellungen

Sie können eingehende und ausgehende Firewallverbindungen für einen Dienst oder Management-Agent über den vSphere Client oder an der Befehlszeile konfigurieren.

In dieser Aufgabe wird die Verwendung des vSphere Client zum Konfigurieren von ESXi-Firewalleinstellungen beschrieben. Sie können die ESXi Shell oder ESXCLI-Befehle verwenden, um ESXi an der Befehlszeile zu konfigurieren und die Firewallkonfiguration zu automatisieren. Unter *Erste Schritte mit ESXCLI* erhalten Sie eine Einleitung und unter *ESXCLI – Konzepte und Beispiele* Beispiele zur Verwendung der ESXCLI zum Ändern von Firewalls und Firewallregeln.

Hinweis Wenn sich die Portregeln verschiedener Dienste überschneiden, kann das Aktivieren eines Diensts möglicherweise dazu führen, dass implizit weitere Dienste aktiviert werden. Sie können angeben, welche IP-Adressen auf jeden Dienst auf dem Host zugreifen können, um dieses Problem zu vermeiden.

Verfahren

1. Melden Sie sich beim vCenter Server mit dem vSphere Client an.
2. Navigieren Sie zum Host in der Bestandsliste.
3. Klicken Sie auf **Konfigurieren** und dann unter **System** auf **Firewall**.

   Sie können zwischen eingehenden und ausgehenden Verbindungen wechseln, indem Sie auf **Eingehend** und **Ausgehend** klicken.
4. Klicken Sie im Abschnitt „Firewall“ auf **Bearbeiten**.
5. Wählen Sie aus einer der drei Dienstgruppen **Nicht gruppiert**, **Secure Shell** und **Simple Network Management Protocol** aus.
6. Wählen Sie die zu aktivierenden Regelsätze oder heben Sie die Auswahl der zu deaktivierenden Regelsätze auf.
7. Für bestimmte Dienste können Sie auch Dienstdetails verwalten, indem Sie unter „System“ zu **Konfigurieren > Dienste** navigieren.

   Weitere Informationen zum Starten, Stoppen und Neustarten von Diensten finden Sie unter Aktivieren oder Deaktivieren eines Dienstes.
8. Bei einigen Diensten können Sie ausdrücklich IP-Adressen angeben, von denen aus Verbindungen zulässig sind.

   Weitere Informationen hierzu finden Sie unter Hinzufügen von zulässigen IP-Adressen für einen ESXi-Host.
9. Klicken Sie auf **OK**.

Hinzufügen von zulässigen IP-Adressen für einen ESXi-Host

Standardmäßig lässt die Firewall für jeden Dienst den Zugriff auf alle IP-Adressen zu. Um den Datenverkehr einzuschränken, ändern Sie jeden Dienst so, dass nur Datenverkehr aus Ihrem

Verwaltungssubnetz zugelassen wird. Sie können auch einige Dienste deaktivieren, wenn diese in Ihrer Umgebung nicht verwendet werden.

Um die Liste zulässiger IP-Adressen für einen Dienst zu aktualisieren, können Sie den vSphere Client, ESXCLI oder PowerCLI verwenden. Standardmäßig sind für einen Dienst alle IP-Adressen zugelassen. Diese Aufgabe beschreibt, wie Sie vSphere Client verwenden. Anweisungen zur Verwendung der ESXCLI finden Sie im Thema zur Verwaltung der Firewall in *ESXCLI Concepts and Examples* unter https://code.vmware.com/.

Verfahren

1. Melden Sie sich beim vCenter Server mit dem vSphere Client an.
2. Navigieren Sie zum ESXi-Host.
3. Klicken Sie auf **Konfigurieren** und dann unter **System** auf **Firewall**.

   Sie können zwischen eingehenden und ausgehenden Verbindungen wechseln, indem Sie auf **Eingehend** und **Ausgehend** klicken.
4. Klicken Sie im Abschnitt „Firewall“ auf **Bearbeiten**.
5. Wählen Sie aus einer der drei Dienstgruppen **Nicht gruppiert**, **Secure Shell** und **Simple Network Management Protocol** aus.
6. Um den Abschnitt „Zulässige IP-Adressen“ anzuzeigen, erweitern Sie einen Dienst.
7. Deaktivieren Sie im Abschnitt „Zulässige IP-Adressen“ die Option **Verbindungen von jeder beliebigen IP-Adresse zulassen** und geben Sie die IP-Adressen der Netzwerke ein, die eine Verbindung zum Host herstellen dürfen.

   Trennen Sie mehrere IP-Adressen durch Kommas. Sie können die folgenden Adressformate verwenden:

   - 192.168.0.0/24
   - 192.168.1.2, 2001::1/64
   - fd3e:29a6:0a81:e478::/64
8. Stellen Sie sicher, dass der Dienst selbst ausgewählt ist.
9. Klicken Sie auf **OK**.
10. Überprüfen Sie Ihre Änderung in der Spalte **Zulässige IP-Adressen** für den Dienst.

Ein- und ausgehende Firewall-Ports für ESXi-Hosts

Im vSphere Client und im VMware Host Client können Sie für jeden Dienst die Firewall öffnen oder schließen oder den Datenverkehr aus bestimmten IP-Adressen durchlassen.

ESXi enthält eine Firewall, die standardmäßig aktiviert ist. Während der Installation wird die ESXi-Firewall so konfiguriert, dass mit Ausnahme des Datenverkehrs für Dienste, die im Sicherheitsprofil des Hosts aktiviert sind, der ein- und ausgehende Datenverkehr blockiert wird. Eine Liste der unterstützten Ports und Protokolle in der ESXi-Firewall finden Sie im Tool VMware Ports and Protocols™ unter https://ports.vmware.com/.

Im Tool VMware Ports and Protocols werden Portinformationen für Dienste aufgelistet, die standardmäßig installiert sind. Wenn Sie andere VIBs auf Ihrem Host installieren, stehen Ihnen möglicherweise weitere Dienste und Firewall-Ports zur Verfügung. Die Informationen gelten in erster Linie für Dienste, die im vSphere Client angezeigt werden. Das Tool VMware Ports and Protocols enthält jedoch auch einige andere Ports.

NFS-Client-Firewallverhalten

Der NFS-Client-Firewallregelsatz weist ein anderes Verhalten als andere ESXi-Firewallregelsätze auf. ESXi konfiguriert NFS-Client-Einstellungen, wenn Sie einen NFS-Datenspeicher mounten oder unmounten. Das Verhalten unterscheidet sich je nach NFS-Version.

Beim Hinzufügen, Mounten und Unmounten eines NFS-Datenspeichers hängt das Verhalten von der NFS-Version ab.

Firewallverhalten in NFS v3

Wenn Sie einen NFS-v3-Datenspeicher hinzufügen oder mounten, überprüft ESXi den Status des NFS-Client-Firewallregelsatzes (`nfsClient`).

- Wenn der Regelsatz `nfsClient` deaktiviert ist, aktiviert ihn ESXi und deaktiviert die Richtlinie „Alle IP-Adressen zulassen“, indem das Flag `allowedAll` auf `FALSE` gesetzt wird. Die IP-Adresse des NFS-Servers wird der zugelassenen Liste für ausgehende IP-Adressen hinzugefügt.
- Wenn `nfsClient` aktiviert ist, bleiben der Status des Regelsatzes und die Richtlinien der zugelassenen IP-Adressen unverändert. Die IP-Adresse des NFS-Servers wird der zugelassenen Liste für ausgehende IP-Adressen hinzugefügt.

Hinweis Wenn Sie vor oder nach dem Hinzufügen eines NFS-v3-Datenspeichers zum System den Regelsatz `nfsClient` manuell aktivieren oder die Richtlinie „Alle IP-Adressen zulassen“ manuell festlegen, werden Ihre Einstellungen nach dem Unmounten des letzten NFS-v3-Datenspeichers überschrieben. Der Regelsatz `nfsClient` wird nach dem Unmounten aller NFS-v3-Datenspeicher deaktiviert.

Beim Entfernen oder Unmounten eines NFS-v3-Datenspeichers führt ESXi eine der folgenden Aktionen aus.

- Wenn keiner der verbleibenden NFS-v3-Datenspeicher von dem Server gemountet werden, auf dem der ungemountete Datenspeicher angesiedelt ist, entfernt ESXi die IP-Adresse des Servers aus der Liste der ausgehenden IP-Adressen.
- Wenn nach dem Unmounten keine gemounteten NFS-v3-Datenspeicher mehr übrig bleiben, deaktiviert ESXi den Firewallregelsatz `nfsClient`.

Firewallverhalten in NFS v4.1

Beim Mounten des ersten NFS-v4.1-Datenspeichers aktiviert ESXi den Regelsatz `nfs41client` und setzt das Flag `allowedAll` auf TRUE. Dabei wird Port 2049 für alle IP-Adressen geöffnet. Das Unmounten eines NFS-v4.1-Datenspeichers hat keine Auswirkungen auf den Status der Firewall. Das heißt, dass durch den ersten gemounteten NFS-v4.1-Datenspeicher Port 2049 geöffnet wird und dieser so lange geöffnet bleibt, bis Sie ihn explizit schließen.

ESXi ESXCLI-Firewall-Befehle

Wenn Ihre Umgebung mehrere ESXi-Hosts umfasst, automatisieren Sie die Firewallkonfiguration anhand von ESXCLI-Befehlen oder mit dem vSphere Web Services SDK.

Firewall-Befehlsreferenz

Sie können die ESXi Shell- oder ESXCLI-Befehle verwenden, um ESXi an der Befehlszeile zu konfigurieren und die Firewallkonfiguration zu automatisieren. Unter *Erste Schritte mit ESXCLI* finden Sie eine Einführung zum Umgang mit Firewalls und Firewallregeln. *ESXCLI – Konzepte und Beispiele* enthält Beispiele für die Verwendung von ESXCLI.

In ESXi 7.0 und höher ist der Zugriff auf die Datei `service.xml`, die zum Erstellen benutzerdefinierter Firewallregeln verwendet wird, eingeschränkt. Im VMware-Knowledgebase-Artikel 2008226 finden Sie Informationen zum Erstellen benutzerdefinierter Firewallregeln mithilfe der Datei `/etc/rc.local.d/local.sh`.

Tabelle 3-5. Firewall-Befehle

Befehl	Beschreibung
`esxcli network firewall get`	Gibt den aktivierten oder deaktivierten Status der Firewall zurück und listet die Standardaktionen auf.
`esxcli network firewall set --default-action`	Legen Sie „true“ fest, um die Standardaktion auszuführen. Legen Sie „false“ fest, um die Standardaktion nicht auszuführen.
`esxcli network firewall set --enabled`	Aktiviert bzw. deaktiviert die ESXi-Firewall.
`esxcli network firewall load`	Lädt das Firewallmodul und die Konfigurationsdateien des Regelsatzes.
`esxcli network firewall refresh`	Aktualisiert die Firewall-Konfiguration durch das Einlesen der Regelsatzdateien, wenn das Firewallmodul geladen ist.
`esxcli network firewall unload`	Löscht Filter und entlädt das Firewallmodul.
`esxcli network firewall ruleset list`	Listet Informationen zu Regelsätzen auf.
`esxcli network firewall ruleset set --allowed-all`	Legen Sie „true“ fest, um den Zugriff auf alle IP-Adressen zu erlauben. Legen Sie „false“ fest, um eine Liste mit zulässigen IP-Adressen zu verwenden.
`esxcli network firewall ruleset set --enabled --ruleset-id=<string>`	Setzen Sie „Aktiviert“ auf „true“, um den angegebenen Regelsatz zu aktivieren. Setzen Sie „Aktiviert“ auf „false“, um den angegebenen Regelsatz zu deaktivieren.

Tabelle 3-5. Firewall-Befehle (Fortsetzung)

Befehl	Beschreibung
`esxcli network firewall ruleset allowedip list`	Listet die zulässigen IP-Adressen des angegebenen Regelsatzes auf.
`esxcli network firewall ruleset allowedip add`	Ermöglicht den Zugriff auf den Regelsatz von der angegebenen IP-Adresse oder einem Bereich von IP-Adressen aus.
`esxcli network firewall ruleset allowedip remove`	Deaktiviert den Zugriff auf den Regelsatz von der angegebenen IP-Adresse oder einem Bereich von IP-Adressen aus.
`esxcli network firewall ruleset rule list`	Listet die Regeln jedes Regelsatzes in der Firewall auf.

Anpassen von ESXi-Diensten über das Sicherheitsprofil

Ein ESXi-Host umfasst mehrere Dienste, die standardmäßig ausgeführt werden. Wenn Ihre Unternehmensrichtlinie dies zulässt, können Sie Dienste aus dem Sicherheitsprofil deaktivieren oder Dienste aktivieren.

Aktivieren oder Deaktivieren eines Dienstes ist ein Beispiel dafür, wie ein Dienst aktiviert wird.

Hinweis Durch die Aktivierung von Diensten kann die Sicherheit des Hosts beeinträchtigt werden. Aktivieren Sie einen Dienst also nur, wenn es absolut notwendig ist.

Welche Dienste verfügbar sind, hängt von den VIBs ab, die im ESXi-Host installiert sind. Ohne Installation eines VIB können Sie keine Dienste hinzufügen. Einige VMware-Produkte wie vSphere HA installieren VIBs auf Hosts und stellen Dienste und die entsprechenden Firewall-Ports zur Verfügung.

In einer Standardinstallation können Sie den Status der folgenden Dienste über vSphere Client ändern.

Tabelle 3-6. ESXi-Dienste im Sicherheitsprofil

Dienst	Standard	Beschreibung
Benutzerschnittstelle der direkten Konsole	Wird ausgeführt	Die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) ermöglicht die Interaktion zwischen einem ESXi-Host und dem lokalen Konsolenhost unter Verwendung textbasierter Menüs.
ESXi Shell	Gestoppt	ESXi Shell steht in der Benutzerschnittstelle der direkten Konsole zur Verfügung und umfasst einen Satz vollständig unterstützter Befehle sowie einen Satz von Befehlen zur Fehlerbehebung und Standardisierung. Der Zugriff auf ESXi Shell muss über die direkte Konsole jedes Systems aktiviert werden. Sie können den Zugriff auf die lokale ESXi Shell oder den Zugriff auf die ESXi Shell mit SSH aktivieren.

Tabelle 3-6. ESXi-Dienste im Sicherheitsprofil (Fortsetzung)

Dienst	Standard	Beschreibung
SSH	Gestoppt	Der SSH-Clientdienst, der Remoteverbindungen über Secure Shell ermöglicht
Auslastungsbasierter Gruppierungs-Daemon	Wird ausgeführt	Auslastungsbasierte Gruppierung
bestätigt	Gestoppt	vSphere Trust Authority-Bestätigungsdienst.
kmxd	Gestoppt	vSphere Trust Authority-Schlüsselanbieterdienst.
Active Directory-Dienst	Gestoppt	Wenn Sie ESXi für Active Directory konfigurieren, wird dieser Dienst gestartet.
NTP-Daemon	Gestoppt	Network Time Protocol-Daemon
PC/SC Smartcard-Daemon	Gestoppt	Wenn Sie den Host für Smartcard-Authentifizierung aktivieren, wird dieser Dienst ausgeführt. Weitere Informationen hierzu finden Sie unter Konfigurieren der Smartcard-Authentifizierung für ESXi.
CIM-Server	Wird ausgeführt	Ein Dienst, der von CIM-Anwendungen (Common Information Model) genutzt werden kann
SNMP-Server	Gestoppt	SNMP-Daemon. Informationen zur Konfiguration von SNMP v1, v2 und v3 erhalten Sie unter *vSphere-Überwachung und -Leistung*.
Syslog-Server	Gestoppt	Syslog-Daemon. Syslog kann in den erweiterten Systemeinstellungen in vSphere Client aktiviert werden. Siehe *Installation und Einrichtung von vCenter Server*.
VMware vCenter Agent	Wird ausgeführt	vCenter Server-Agent. Ermöglicht die Verbindung zwischen vCenter Server und ESXi-Host. vpxa ist der Kommunikationskanal zum Hostdaemon, der wiederum mit dem ESXi-Kernel kommuniziert.
X.Org-Server	Gestoppt	X.Org-Server. Dieses optionale Feature wird intern für 3D-Grafiken in virtuellen Maschinen genutzt.

Aktivieren oder Deaktivieren eines Dienstes

Sie können die Dienste über den vSphere Client aktivieren oder deaktivieren.

Nach der Installation werden bestimmte Dienste standardmäßig ausgeführt, andere sind angehalten. In bestimmten Fällen sind zusätzliche Einrichtungsschritte erforderlich, damit ein Dienst auf der Benutzeroberfläche verfügbar wird. Beispielsweise kann der NTP-Dienst präzise Uhrzeitinformationen bereitstellen, doch dieser Dienst funktioniert nur, wenn die benötigten Ports in der Firewall geöffnet sind.

Voraussetzungen

Stellen Sie eine Verbindung mit vCenter Server mit dem vSphere Client her.

Verfahren

1 Navigieren Sie zu einem Host in der Bestandsliste.

2 Klicken Sie auf **Konfigurieren** und dann unter „System“ auf **Dienste**.

3 Wählen Sie den Dienst, den Sie ändern möchten.

   a Wählen Sie für eine einmalige Änderung des Hoststatus **Neustart**, **Starten** oder **Beenden**.

   b Um den Status des Hosts für mehrere Neustarts zu ändern, klicken Sie auf **Startrichtlinie bearbeiten** und wählen Sie eine Richtlinie aus.

   - **Mit dem Host starten und beenden**: Der Dienst wird unmittelbar nach dem Host gestartet und unmittelbar vor dem Herunterfahren des Hosts beendet. Ähnlich wie bei der Option **Mit Port-Verwendung starten und beenden** besagt diese Option, dass der Dienst regelmäßig versucht, seine Aufgaben abzuschließen, wie z. B. das Herstellen einer Verbindung zum angegebenen NTP-Server. Wenn der Port geschlossen war, später jedoch geöffnet wird, beginnt der Client unmittelbar mit der Erledigung seiner Aufgaben.
   - **Manuell starten und beenden**: Der Host übernimmt unabhängig davon, welche Ports offen oder geschlossen sind, die vom Benutzer festgelegten Diensteinstellungen. Wenn ein Benutzer den NTP-Dienst startet, wird dieser Dienst so lange ausgeführt, bis der Host ausgeschaltet wird. Wenn der Dienst gestartet und der Host ausgeschaltet wird, wird der Dienst beim Herunterfahren angehalten. Wenn der Host eingeschaltet ist, wird der Dienst erneut gestartet, wobei der vom Benutzer festgelegte Status beibehalten wird.
   - **Mit Port-Verwendung starten und beenden**: Die Standardeinstellung für diese Dienste. Falls ein beliebiger Port geöffnet ist, versucht der Client, die Netzwerkressourcen für den Dienst zu kontaktieren. Wenn einige Ports geöffnet sind, der Port für einen bestimmten Dienst aber geschlossen ist, schlägt der Versuch fehl. Wird der zugehörige ausgehende Port geöffnet, beginnt der Dienst mit dem Abschluss des Startvorgangs.

   Hinweis Diese Einstellungen gelten nur für Diensteinstellungen, die über die Benutzeroberfläche konfiguriert wurden, oder für Anwendungen, die mit dem vSphere Web Services SDK erstellt wurden. Konfigurationen, die mit anderen Mitteln, wie z. B. ESXi Shell oder Konfigurationsdateien erstellt werden, sind von diesen Einstellungen nicht betroffen.

4 Klicken Sie auf **OK**.

Sperrmodus

Um die Sicherheit von ESXi-Hosts zu verbessern, können Sie diese in den Sperrmodus versetzen. Im Sperrmodus müssen alle Hostvorgänge standardmäßig über vCenter Server durchgeführt werden.

Sie können zwischen dem normalen und dem strengen Sperrmodus mit jeweils unterschiedlicher Sperrstärke wählen. Sie können auch die Liste der ausgenommenen Benutzer verwenden. Ausgenommene Benutzer verlieren ihre Rechte nicht, wenn der Host in den Sperrmodus wechselt. In die Liste der ausgenommenen Benutzer können Sie Konten von Drittanbieterlösungen und externe Anwendungen aufnehmen, die auch im Sperrmodus direkten Zugang zum Host benötigen. Weitere Informationen hierzu finden Sie unter Angeben der Benutzerausnahmen für den Sperrmodus.

Verhalten im Sperrmodus

Im Sperrmodus sind einige Dienste deaktiviert und auf einige Dienste haben nur bestimmte Benutzer Zugriff.

Sperrmodus-Dienste für unterschiedliche Benutzer

Wenn der Host ausgeführt wird, sind die verfügbaren Dienste davon abhängig, ob der Sperrmodus aktiviert ist, und welcher Sperrmodustyp verwendet wird.

- Im strengen und normalen Sperrmodus haben berechtigte Benutzer über vCenter Server Zugriff auf den Host, und zwar über den vSphere Client oder mit dem vSphere Web Services SDK.
- Das Verhalten der Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) ist für den strengen Sperrmodus und den normalen Sperrmodus unterschiedlich.
  - Im strengen Sperrmodus ist der DCUI-Dienst deaktiviert.
  - Im normalen Sperrmodus können Konten in der Liste der ausgenommenen Benutzer auf die DCUI zugreifen, wenn sie über Administratorrechte verfügen. Darüber hinaus können alle Benutzer, die in der erweiterten Systemeinstellung `DCUI.Access` angegeben sind, auf die DCUI zugreifen.
- Falls die ESXi Shell oder SSH aktiviert ist und der Host in den normalen Sperrmodus wechselt, können diese Dienste von Konten in der Liste der ausgenommenen Benutzer mit Administratorrechten verwendet werden. Für alle anderen Benutzer ist ESXi Shell oder SSH deaktiviert. ESXi- oder SSH-Sitzungen werden für Benutzer ohne Administratorrechte geschlossen.

Alle Zugriffe werden für den strengen und den normalen Sperrmodus protokolliert.

Tabelle 3-7. Verhalten im Sperrmodus

Dienst	Normaler Modus	Normaler Sperrmodus	Strenger Sperrmodus
vSphere Web Services-API	Alle Benutzer, basierend auf Berechtigungen	vCenter (vpxuser) Ausgenommene Benutzer, basierend auf Berechtigungen vCloud Director (vslauser, soweit verfügbar)	vCenter (vpxuser) Ausgenommene Benutzer, basierend auf Berechtigungen vCloud Director (vslauser, soweit verfügbar)
CIM-Anbieter	Benutzer mit Administratorrechten auf dem Host	vCenter (vpxuser) Ausgenommene Benutzer, basierend auf Berechtigungen vCloud Director (vslauser, soweit verfügbar)	vCenter (vpxuser) Ausgenommene Benutzer, basierend auf Berechtigungen vCloud Director (vslauser, soweit verfügbar)
Die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI)	Benutzer mit Administratorrechten auf dem Host und Benutzer in der erweiterten Option `DCUI.Access`	In der erweiterten Option `DCUI.Access` definierte Benutzer Ausgenommene Benutzer mit Administratorrechten auf dem Host	DCUI-Dienst wird angehalten.
ESXi Shell (falls aktiviert) und SSH (falls aktiviert)	Benutzer mit Administratorrechten auf dem Host	In der erweiterten Option `DCUI.Access` definierte Benutzer Ausgenommene Benutzer mit Administratorrechten auf dem Host	In der erweiterten Option `DCUI.Access` definierte Benutzer Ausgenommene Benutzer mit Administratorrechten auf dem Host

Bei aktiviertem Sperrmodus bei der ESXi Shell angemeldete Benutzer

Benutzer melden sich unter Umständen an der ESXi Shell an oder greifen über SSH auf den Host zu, bevor der Sperrmodus aktiviert wird. In diesem Fall bleiben Benutzer, die sich in der Liste der ausgenommenen Benutzer befinden und über Administratorrechte auf dem Host verfügen, angemeldet. Die Sitzung ist für alle anderen Benutzer geschlossen. Dies betrifft sowohl den normalen als auch den strengen Sperrmodus.

Aktivieren des Sperrmodus

Aktivieren Sie den Sperrmodus, damit alle Konfigurationsänderungen vCenter Server durchlaufen müssen. vSphere 6.0 und höher unterstützt den normalen Sperrmodus und den strengen Sperrmodus.

Wenn Sie den direkten Zugriff auf einen Host vollständig unterbinden möchten, können Sie den strengen Sperrmodus auswählen. Im strengen Sperrmodus ist der Zugriff auf einen Host nicht möglich, falls vCenter Server nicht verfügbar ist und SSH und die ESXi Shell deaktiviert sind. Weitere Informationen hierzu finden Sie unter Verhalten im Sperrmodus.

Verfahren

1 Navigieren Sie zum Host im Navigator des vSphere Client.

2 Klicken Sie auf **Konfigurieren**.

3 Klicken Sie unter „System“ auf **Sicherheitsprofil**.

4 Klicken Sie im Bereich „Sperrmodus“ auf **Bearbeiten**.

5 Klicken Sie auf **Sperrmodus** und wählen Sie eine der Optionen für den Sperrmodus aus.

Option	Beschreibung
Normal	Der Zugriff auf den Host ist über vCenter Server möglich. Nur Benutzer in der Liste „Ausnahme für Benutzer“ und mit Administratorrechten können sich bei der Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) anmelden. Falls SSH oder die ESXi Shell aktiviert ist, könnte der Zugriff möglich sein.
Streng	Der Zugriff auf den Host ist nur über vCenter Server möglich. Falls SSH oder die ESXi Shell aktiviert ist, ist die Ausführung von Sitzungen für Konten über die erweiterte Option `DCUI.Access` und für Benutzerausnahmekonten mit Administratorrechten weiterhin möglich. Alle anderen Sitzungen werden geschlossen.

6 Klicken Sie auf **OK**.

Deaktivieren des Sperrmodus

Deaktivieren Sie den Sperrmodus, um Konfigurationsänderungen über Direktverbindungen mit dem ESXi-Host zuzulassen. Wenn Sie den Sperrmodus aktiviert lassen, bedeutet dies eine sicherere Umgebung.

Sie können den Sperrmodus folgendermaßen deaktivieren:

Über die grafische Benutzeroberfläche

Benutzer können sowohl den normalen Sperrmodus als auch den strengen Sperrmodus über den vSphere Client deaktivieren.

Über die DCUI

Benutzer, die auf dem ESXi-Host Zugriff auf die DCUI haben, können den normalen Sperrmodus deaktivieren. Im strengen Sperrmodus wird der DCUI-Dienst beendet.

Verfahren

1 Navigieren Sie zu einem Host in der Bestandsliste des vSphere Client.

2 Klicken Sie auf **Konfigurieren**.

3 Klicken Sie unter „System“ auf **Sicherheitsprofil**.

4 Klicken Sie im Bereich „Sperrmodus“ auf **Bearbeiten**.

5 Klicken Sie auf **Sperrmodus** und wählen Sie **Deaktiviert** aus, um den Sperrmodus zu deaktivieren.

6 Klicken Sie auf **OK**.

Ergebnisse

Der Sperrmodus wird beendet, vCenter Server zeigt einen Alarm an und dem Überwachungsprotokoll wird ein Eintrag hinzugefügt.

Aktivieren oder Deaktivieren des normalen Sperrmodus über die Benutzerschnittstelle der direkten Konsole

Sie können den normalen Sperrmodus über die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) aktivieren und deaktivieren. Den strengen Sperrmodus können Sie nur über den vSphere Client aktivieren und deaktivieren.

Wenn sich der Host im normalen Sperrmodus befindet, können die folgenden Konten auf die DCUI zugreifen:

- Konten in der Liste „Ausnahme für Benutzer“ mit Administratorrechten für den Host. Die Liste „Ausnahme für Benutzer“ ist für Dienstkonten wie z. B. einen Backup-Agenten gedacht.
- In der erweiterten Option `DCUI.Access` für den Host definierte Benutzer. Mithilfe dieser Option kann der Zugriff bei einem schwerwiegenden Fehler aktiviert werden.

Benutzerberechtigungen werden beibehalten, wenn Sie den Sperrmodus aktivieren. Die Benutzerberechtigen werden wiederhergestellt, wenn Sie den Sperrmodus über die DCUI deaktivieren.

Hinweis Wenn Sie ein Upgrade für einen im Sperrmodus befindlichen Host auf ESXi 6.0 durchführen, ohne den Sperrmodus zu beenden, und wenn Sie den Sperrmodus nach dem Upgrade beenden, gehen alle vor dem Wechsel des Hosts in den Sperrmodus definierten Berechtigungen verloren. Die Administratorrolle wird allen Benutzern zugewiesen, die in der erweiterten Option `DCUI.Access` gefunden werden, um sicherzustellen, dass der Zugriff auf den Host weiterhin möglich ist.

Um die Berechtigungen beizubehalten, deaktivieren Sie vor dem Upgrade den Sperrmodus für den Host über den vSphere Client.

Verfahren

1 Drücken Sie F2 an der Benutzerschnittstelle der direkten Konsole des Hosts und melden Sie sich an.

2 Führen Sie einen Bildlauf nach unten zur Einstellung **Sperrmodus konfigurieren** aus und drücken Sie die Eingabetaste, um die aktuelle Einstellung umzuschalten.

3 Drücken Sie die Esc-Taste wiederholt, bis Sie zurück zum Hauptmenü der Benutzerschnittstelle der direkten Konsole gelangt sind.

Angeben von Konten mit Zugriffsrechten im Sperrmodus

Sie können Dienstkonten angeben, die direkten Zugriff auf den ESXi-Host haben, indem Sie sie zur Liste „Ausnahme für Benutzer“ hinzufügen. Sie können einen einzelnen Benutzer angeben, der auf den ESXi-Host zugreifen kann, wenn es auf dem vCenter Server zu einem schwerwiegenden Fehler kommt.

Die Version von vSphere bestimmt, was die verschiedenen Konten standardmäßig bei aktiviertem Sperrmodus tun können und wie Sie das Standardverhalten ändern können.

- In vSphere 5.0 und früheren Versionen kann sich nur der Root-Benutzer bei der Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) auf einem ESXi-Host anmelden, der sich im Sperrmodus befindet.
- In vSphere 5.1 und höher können Sie der erweiterten Systemeinstellung `DCUI.Access` für jeden Host einen Benutzer hinzufügen. Die Option ist für schwerwiegende Fehler auf dem vCenter Server vorgesehen. Unternehmen sperren in der Regel das Kennwort des Benutzers mit diesem Zugriff. Ein Benutzer in der `DCUI.Access`-Liste benötigt keine vollständigen Administratorrechte auf dem Host.
- In vSphere 6.0 und höher wird die erweiterte Systemeinstellung `DCUI.Access` weiterhin unterstützt. Darüber hinaus unterstützt vSphere 6.0 und höher eine Liste „Ausnahme für Benutzer“ für Dienstkonten, die sich direkt am Host anmelden müssen. Konten mit Administratorrechten, die sich in der Liste „Ausnahme für Benutzer“ befinden, können sich bei der ESXi Shell anmelden. Darüber hinaus können sich diese Benutzer bei der DCUI eines Hosts im normalen Sperrmodus anmelden und können den Sperrmodus beenden.

  Ausgenommene Benutzer geben Sie über den vSphere Client an.

  Hinweis Ausgenommene Benutzer sind lokale Hostbenutzer oder Active Directory-Benutzer mit lokal für den ESXi-Host definierten Rechten. Benutzer, die zu einer Active Directory-Gruppe gehören, verlieren ihre Berechtigungen, wenn sich der Host im Sperrmodus befindet.

Hinzufügen von Benutzern zur erweiterten Option DCUI.Access

Bei einem schwerwiegenden Fehler können Sie den Sperrmodus über die erweiterte Option `DCUI.Access` beenden, wenn Sie nicht über vCenter Server auf den Host zugreifen können. Sie fügen Benutzer zur Liste hinzu, indem Sie die erweiterten Einstellungen für den Host über den vSphere Client bearbeiten.

Hinweis Benutzer in der DCUI.Access-Liste können die Einstellungen des Sperrmodus unabhängig von ihren Rechten ändern. Die Möglichkeit, Sperrmodi zu ändern, kann sich auf die Sicherheit Ihres Hosts auswirken. Für Dienstkonten, die direkten Zugriff auf den Host benötigen, sollten Sie eventuell stattdessen Benutzer zur Liste „Ausnahme für Benutzer“ hinzufügen. Die Benutzer in dieser Liste können nur Aufgaben ausführen, für die sie über die erforderlichen Rechte verfügen. Weitere Informationen hierzu finden Sie unter Angeben der Benutzerausnahmen für den Sperrmodus.

Verfahren

1 Navigieren Sie zum Host im Navigator von vSphere Client.

2 Klicken Sie auf **Konfigurieren**.

3 Klicken Sie unter „System“ auf **Erweiterte Systemeinstellungen** und dann auf **Bearbeiten**.

4 Filtern Sie nach „DCUI“.

5 Geben Sie im Textfeld **DCUI.Access** die lokalen ESXi-Benutzernamen durch Komma getrennt ein.

   Der Root-Benutzer ist standardmäßig einbezogen. Zur besseren Überprüfung sollten Sie eventuell den Root-Benutzer aus der DCUI.Access-Liste entfernen und ein benanntes Konto angeben.

6 Klicken Sie auf **OK**.

Angeben der Benutzerausnahmen für den Sperrmodus

Sie können Benutzer über den vSphere Client zur Liste „Ausgenommene Benutzer“ hinzufügen. Diese Benutzer verlieren ihre Berechtigungen nicht, wenn der Host in den Sperrmodus wechselt. Es ist sinnvoll, Dienstkonten wie beispielsweise einen Backup-Agenten zur Liste „Ausnahme für Benutzer“ hinzuzufügen.

Ausgenommene Benutzer verlieren ihre Rechte nicht, wenn der Host in den Sperrmodus wechselt. Bei diesen Konten handelt es sich in der Regel um Drittanbieterlösungen und externe Anwendungen, die auch im Sperrmodus weiterhin funktionieren müssen.

Hinweis Die Liste „Ausnahme für Benutzer“ ist nicht für Administratoren, sondern für Dienstkonten gedacht, mit denen sehr spezielle Aufgaben ausgeführt werden. Wenn Sie der Liste „Ausnahme für Benutzer“ Administratoren hinzufügen, widerspricht dies dem Zweck des Sperrmodus.

Ausgenommene Benutzer sind lokale Hostbenutzer oder Active Directory-Benutzer mit lokal für den ESXi-Host definierten Rechten. Sie sind keine Mitglieder einer Active Directory-Gruppe und keine vCenter Server-Benutzer. Diese Benutzer dürfen Vorgänge auf dem Host in Abhängigkeit von ihren Rechten durchführen. Dies bedeutet, dass beispielsweise ein Benutzer mit der Berechtigung „Nur Lesen“ den Sperrmodus auf einem Host nicht deaktivieren kann.

Verfahren

1 Navigieren Sie zum Host im Navigator des vSphere Client.

2 Klicken Sie auf **Konfigurieren**.

3 Klicken Sie unter „System“ auf **Sicherheitsprofil**.

4 Klicken Sie im Bereich „Sperrmodus“ auf **Bearbeiten**.

5 Klicken Sie auf **Ausnahme für Benutzer** und klicken Sie dann auf das Symbol **Benutzer hinzufügen**, um ausgenommene Benutzer hinzuzufügen.

Verwenden von VIBs zum Durchführen sicherer Updates

Für ein ESXi-Upgrade mit ESXCLI müssen Sie VIBs, Image-Profile und Software-Depots verstehen.

ESXi besteht aus einem Image-Profil, das einen Satz von vSphere-Installationspaketen (vSphere Installation Bundles, VIBs) beschreibt, die die eigentliche Software enthalten. Ein VIB ist eine signierte Ramdisk, die eine Komponente des Systems darstellt – ungefähr analog zu einem RPM oder DEB auf einem Linux-System. Ein Image-Profil ist eine Sammlung von VIBs. Ein Software-Depot ist eine Sammlung von VIBs und Image-Profilen. ESXi-Patches und -Depots enthalten aktualisierte Image-Profile, die aus einem gemeinsamen Satz von VIBs bestehen.

Sie können ESXi-Updates mithilfe der `esxcli software`-Befehle auf einem eigenständigen Host installieren. Weitere Informationen finden Sie in der Dokumentation *VMware ESXi-Upgrade*.

Hinweis In einer Umgebung mit vSphere 7.0 und höher verwenden Sie für die Lebenszyklusverwaltung von ESXi-Hosts in der Regel VMware vSphere® Lifecycle Manager.

Um alle installierten VIBs und deren aktuelle Version oder das aktuelle Image-Profil aufzulisten, können Sie die folgenden ESXCLI-Befehle verwenden.

- `esxcli software vib list`
- `esxcli software profile get`

Für ein sicheres Upgrade von ESXi führen Sie generell diese allgemeinen Schritte aus:

- Versetzen Sie den ESXi-Host in den Wartungsmodus.
- Führen Sie einen `esxcli software profile update`-Befehl aus, der auf eine URL oder eine ZIP-Datei verweist, die über SSH an den Host übertragen wurde.
- Starten Sie den ESXi-Host neu.

Da VIBs von VMware kryptografisch signiert werden, ist keine sichere Übertragung von VIBs oder des gesamten Depots erforderlich. Die betreffenden Signaturen werden während des Aktualisierungsvorgangs überprüft.

Verwalten der Akzeptanzebenen von Hosts und VIBs

Die Akzeptanzebene eines VIB hängt von der Zertifizierungsmenge dieses VIB ab. Die Akzeptanzebene des Hosts hängt von der Ebene des niedrigsten VIB ab. Wenn Sie VIBs auf unterer Ebene zulassen möchten, können Sie die Akzeptanzebene des Hosts ändern. Sie können CommunitySupported-VIBs entfernen, um die Host-Akzeptanzebene ändern zu können.

VIBs sind Softwarepakete, die eine Signatur von VMware oder eines VMware-Partners enthalten. Um die Integrität des ESXi-Hosts zu schützen, lassen Sie es nicht zu, dass VIBs ohne Signatur (von der Community unterstützt) installiert werden. Ein VIB ohne Signatur enthält Programmcode, der von VMware oder seinen Partnern nicht zertifiziert ist, akzeptiert oder unterstützt wird. Von der Community unterstützte VIBs haben keine digitale Signatur.

Die Akzeptanzebene des Hosts darf nicht restriktiver als die Akzeptanzebene des VIBs sein, das Sie zu diesem Host hinzufügen möchten. Wenn beispielsweise die Host-Akzeptanzebene „VMwareAccepted“ ist, können Sie keine VIBs auf der Ebene „PartnerSupported“ installieren. Sie können ESXCLI-Befehle verwenden, um eine Akzeptanzebene für einen Host festzulegen. Um die Sicherheit und Integrität Ihrer ESXi-Hosts zu schützen, lassen Sie es nicht zu, dass VIBs ohne Signatur („CommunitySupported“, von der Community unterstützt) auf Hosts in Produktionssystemen installiert werden.

Die Akzeptanzebene für einen ESXi-Host wird unter **Sicherheitsprofil** im vSphere Client angezeigt.

Folgende Akzeptanzebenen werden unterstützt:

VMwareCertified

Die Akzeptanzebene „VMwareCertified“ hat die strengsten Anforderungen. VIBs dieser Ebene unterliegen einer gründlichen Prüfung entsprechend den internen VMware-Qualitätssicherungstests für die gleiche Technologie. Zurzeit werden nur Programmtreiber im Rahmen des IOVP (I/O Vendor Program) auf dieser Ebene veröffentlicht. VMware übernimmt Support-Anrufe für VIBs dieser Akzeptanzebene.

VMwareAccepted

VIBs dieser Akzeptanzebene unterliegen einer Verifizierungsprüfung; es wird jedoch nicht jede Funktion der Software in vollem Umfang getestet. Der Partner führt die Tests durch und VMware verifiziert das Ergebnis. Heute gehören CIM-Anbieter und PSA-Plug-Ins zu den VIBs, die auf dieser Ebene veröffentlicht werden. Kunden mit Support-Anrufen für VIBs dieser Akzeptanzebene werden von VMware gebeten, sich an die Support-Organisation des Partners zu wenden.

PartnerSupported

VIBs mit der Akzeptanzebene „PartnerSupported“ werden von einem Partner veröffentlicht, dem VMware vertraut. Der Partner führt alle Tests durch. VMware überprüft die Ergebnisse nicht. Diese Ebene wird für eine neue oder nicht etablierte Technologie verwendet, die Partner für VMware-Systeme aktivieren möchten. Auf dieser Ebene sind heute Treiber-VIB-Technologien mit nicht standardisierten Hardwaretreibern, wie z. B. Infiniband, ATAoE und SSD. Kunden mit Support-Anrufen für VIBs dieser Akzeptanzebene werden von VMware gebeten, sich an die Support-Organisation des Partners zu wenden.

CommunitySupported

Die Akzeptanzebene „CommunitySupported“ ist für VIBs gedacht, die von Einzelpersonen oder Unternehmen außerhalb der VMware Partner-Programme erstellt wurden. VIBs auf dieser Ebene wurden nicht im Rahmen eines von VMware zugelassenen Testprogramms getestet und werden weder von VMware Technical Support noch von einem VMware-Partner unterstützt.

Verfahren

1 Stellen Sie eine Verbindung zu jedem ESXi-Host her und stellen Sie sicher, dass die Akzeptanzebene auf „VMwareCertified“, „VMwareAccepted“ oder „PartnerSupported“ gesetzt ist, indem Sie den folgenden Befehl ausführen.

```
esxcli software acceptance get
```

2 Wenn es sich bei der Akzeptanzebene des Hosts um „CommunitySupported“ handelt, stellen Sie fest, ob sich VIBs auf der Ebene „CommunitySupported“ befinden, indem Sie folgende Befehle ausführen:

```
esxcli software vib list
esxcli software vib get -n vibname
```

3 Entfernen Sie alle „CommunitySupported“-VIBs, indem Sie folgenden Befehl ausführen:

```
esxcli software vib remove --vibname vib
```

4 Ändern Sie die Akzeptanzebene des Hosts unter Verwendung einer der folgenden Methoden.

Option	Beschreibung
CLI-Befehl	`esxcli software acceptance set --level level` Der Parameter `level` ist erforderlich und gibt die festzulegende Akzeptanzebene an. Hierbei sollte es sich um **`VMwareCertified`**, **`VMwareAccepted`**, **`PartnerSupported`**, oder **`CommunitySupported`** handeln. Weitere Informationen hierzu finden Sie unter *ESXCLI – Referenz*.
vSphere Client	a Wählen Sie einen Host in der Bestandsliste aus. b Klicken Sie auf **Konfigurieren**. c Klicken Sie unter „System“ auf **Sicherheitsprofil**. d Klicken Sie auf **Bearbeiten** für die Akzeptanzebene des Host-Image-Profils und wählen Sie die Akzeptanzebene aus.

Ergebnisse

Die neue Akzeptanzebene ist wirksam.

Hinweis ESXi führt Integritätsprüfungen von VIBs durch, die von der Akzeptanzebene gesteuert werden. Mithilfe der Einstellung `VMkernel.Boot.execInstalledOnly` können Sie ESXi anweisen, nur Binärdateien auszuführen, die aus einem gültigen auf dem Host installierten VIB stammen. Gemeinsam mit Secure Boot stellt diese Einstellung sicher, dass jeder einzelne jemals auf einem ESXi-Host ausgeführte Prozess signiert, zugelassen und erwartet wird. Standardmäßig ist die Einstellung `VMkernel.Boot.execInstalledOnly` für Partnerkompatibilität in vSphere 7 aktiviert. Durch Aktivierung dieser Einstellung (wenn möglich) wird die Sicherheit erhöht. Weitere Informationen zum Konfigurieren erweiterter Optionen für ESXi finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/kb/1038578.

Zuweisen von Rechten für ESXi-Hosts

In der Regel erteilen Sie Benutzern Berechtigungen, indem Sie Rechte für ESXi-Hostobjekte zuweisen, die von einem vCenter Server-System verwaltet werden. Wenn Sie mit einem eigenständigen ESXi-Host arbeiten, können Sie Berechtigungen direkt zuweisen.

Zuweisen von Berechtigungen für ESXi-Hosts, die von vCenter Server verwaltet werden

Wenn Ihr ESXi-Host von einem vCenter Server verwaltet wird, führen Sie die Verwaltungsaufgaben im vSphere Client aus.

Sie können das ESXi-Hostobjekt in der vCenter Server-Objekthierarchie auswählen und die einer begrenzten Anzahl von Benutzern die Administratorrolle zuweisen. Diese Benutzer können dann direkt Verwaltungsaufgaben auf dem ESXi-Host durchführen. Weitere Informationen hierzu finden Sie unter Verwenden von Rollen zum Zuweisen von Rechten.

Es wird empfohlen, mindestens ein benanntes Benutzerkonto zu erstellen, diesem Konto vollständige Administratorrechte auf dem Host zuzuweisen und es anstelle des Root-Kontos zu verwenden. Legen Sie ein hochkomplexes Kennwort für das Root-Konto fest und schränken Sie die Verwendung des Root-Kontos ein. Entfernen Sie das Root-Konto aber nicht.

Zuweisen von Berechtigungen für eigenständige ESXi-Hosts

Auf der Registerkarte „Management“ des VMware Host Client können Sie lokale Benutzer hinzufügen und benutzerdefinierte Rollen definieren. Informationen finden Sie in der Dokumentation *Verwaltung eines einzelnen Hosts von vSphere – VMware Host Client*.

Für alle Versionen von ESXi können Sie die Liste der vordefinierten Benutzer in der Datei `/etc/passwd` anzeigen.

Die folgenden Rollen sind vordefiniert.

Nur Lesen

Erlaubt Benutzern die Anzeige von Objekten des ESXi-Hosts, aber nicht deren Änderung.

Administrator

Administratorrolle.

Kein Zugriff

Kein Zugriff Dies ist die Standardrolle. Sie können die Standardrolle außer Kraft setzen.

Sie können lokale Benutzer und Gruppen verwalten und lokale benutzerdefinierte Rollen zu einem ESXi-Host hinzufügen, indem Sie einen VMware Host Clientverwenden, der direkt mit dem ESXi-Host verbunden ist. Informationen finden Sie in der Dokumentation *Verwaltung eines einzelnen Hosts von vSphere – VMware Host Client*.

Ab vSphere 6.0 können Sie mithilfe von ESXCLI-Kontoverwaltungsbefehlen lokale ESXi-Benutzerkonten verwalten. Mit ESXCLI-Kontoverwaltungsbefehlen können Sie Berechtigungen für Active Directory-Konten (Benutzer und Gruppen) und lokale ESXi-Konten (nur Benutzer) einrichten und entfernen.

Hinweis Wenn Sie über eine Host-Direktverbindung einen Benutzer für den ESXi-Host definieren und es in vCenter Server einen Benutzer mit demselben Namen gibt, gelten die beiden als zwei verschiedene Benutzer. Wenn Sie dem ESXi-Benutzer eine Rolle zuweisen, gilt die Rolle nicht für den vCenter Server-Benutzer.

Vordefinierte Berechtigungen

In Umgebungen ohne vCenter Server-System sind die folgenden Benutzer vordefiniert.

Root-Benutzer

Standardmäßig verfügt jeder ESXi-Host über ein (1) Root-Benutzerkonto mit der Rolle „Administrator“. Dieses kann für die lokale Verwaltung und die Verbindung zwischen Host und vCenter Server verwendet werden.

Die Zuweisung von Root-Benutzerberechtigungen kann das Eindringen in einen ESXi-Host erleichtern, da der Name bereits bekannt ist. Ein gemeinsames Root-Konto erschwert außerdem den Abgleich von Aktionen mit Benutzern.

Um die Überwachung zu verbessern, sollten Sie einzelne Konten mit Administratorberechtigungen erstellen. Legen Sie ein hochkomplexes Kennwort für das Root-Konto fest und schränken Sie die Verwendung dieses Kontos ein, z. B. nur zum Hinzufügen eines Hosts zu vCenter Server. Entfernen Sie das Root-Konto aber nicht. Weitere Informationen zum Zuweisen von Berechtigungen zu einem Benutzer für einen ESXi-Host finden Sie in der Dokumentation zu *Verwaltung eines einzelnen Hosts von vSphere – VMware Host Client*.

Empfohlen wird sicherzustellen, dass alle Konten mit Administratorrolle auf einem ESXi-Host einem bestimmten Benutzer mit einem benannten Konto zugewiesen sind. Verwenden Sie dazu die Active Directory-Funktionen von ESXi, mit denen Sie die Active Directory-Anmeldedaten verwalten können.

Wichtig Sie können die Zugriffsberechtigungen für den Root-Benutzer entfernen. Sie müssen jedoch auf der Root-Ebene zunächst eine andere Berechtigung erteilen, die ein anderer Benutzer mit der Rolle des Administrators erhält.

vpxuser-Benutzer

vCenter Server verwendet vpxuser-Rechte beim Verwalten von Aktivitäten für den Host.

Der Administrator von vCenter Server kann viele der Aufgaben des Root-Benutzers auf dem Host durchführen und Aufgaben planen, Vorlagen nutzen usw. Der vCenter Server-Administrator kann jedoch lokale Benutzer und Gruppen für Hosts nicht direkt erstellen, löschen oder bearbeiten. Diese Aufgaben können nur von einem Benutzer mit Administratorberechtigungen direkt auf einem Host durchgeführt werden.

Hinweis Sie können den Benutzers „vpxuser“.nicht mithilfe von Active Directory verwalten.

Vorsicht Verändern Sie keinerlei Einstellungen des Benutzers „vpxuser“. Ändern Sie nicht das Kennwort. Ändern Sie nicht die Berechtigungen. Falls Änderungen vorgenommen werden, können Probleme beim Arbeiten mit Hosts in vCenter Server auftreten.

dcui-Benutzer

Der Benutzer „dcui“ wird auf Hosts ausgeführt und agiert mit Administratorrechten. Der Hauptzweck dieses Benutzers ist die Konfiguration von Hosts für den Sperrmodus über den DCUI-Dienst (Direct Console User Interface, Benutzerschnittstelle der direkten Konsole).

Dieser Benutzer dient als Agent für die direkte Konsole und kann von interaktiven Benutzern nicht geändert bzw. verwendet werden.

Verwenden von Active Directory zum Verwalten von ESXi-Benutzern

Sie können ESXi so konfigurieren, dass es einen Verzeichnisdienst, wie z. B. Active Directory, zur Benutzerverwaltung verwendet.

Das Erstellen von lokalen Benutzerkonten auf jedem Host stellt Herausforderungen beim Synchronisieren von Kontonamen und Kennwörtern über mehrere Hosts hinweg dar. Weisen Sie ESXi-Hosts eine Active Directory-Domäne zu, damit Sie lokale Benutzerkonten weder erstellen noch pflegen müssen. Durch die Verwendung von Active Directory für die Authentifizierung von Benutzern wird die Konfiguration des ESXi-Hosts vereinfacht und das Risiko von Konfigurationsproblemen, die einen unbefugten Zugriff ermöglichen, reduziert.

Wenn Sie Active Directory verwenden, geben Benutzer beim Hinzufügen eines Hosts zu einer Domäne die Active Directory-Anmeldedaten und den Domänennamen des Active Directory-Servers an.

Konfigurieren eines Hosts für die Verwendung von Active Directory

Sie können einen Host so konfigurieren, dass er Benutzer und Gruppen mithilfe eines Verzeichnisdienstes, wie z. B. Active Directory, verwaltet.

Wenn Sie einen ESXi-Host zu Active Directory hinzufügen, wird der DOMAIN-Gruppe **ESX Admins** (falls vorhanden) vollständiger Administratorzugriff auf den Host gewährt. Wenn Sie Benutzern den vollständigen Administratorzugriff nicht gewähren möchten, finden Sie eine Ausweichlösung im VMware-Knowledgebaseartikel 1025569.

Wenn der Host mit Auto Deploy bereitgestellt wurde, können die Active Directory-Anmeldedaten nicht in den Hosts gespeichert werden. Sie können vSphere Authentication Proxy verwenden, um mit dem Host einer Active Directory-Domäne beizutreten. Da zwischen vSphere Authentication Proxy und dem Host eine Vertrauenskette besteht, ist Authentication Proxy berechtigt, den Host in die Active Directory-Domäne einzufügen. Weitere Informationen hierzu finden Sie unter Verwenden des vSphere Authentication Proxy.

Hinweis Beim Definieren von Benutzerkonteneinstellungen in Active Directory können Sie die Computer, die ein Benutzer zum Anmelden verwenden darf, nach Computername einschränken. Standardmäßig werden keine gleichwertigen Beschränkungen auf einem Benutzerkonto festgelegt. Wenn Sie diese Einschränkung festlegen, schlagen LDAP-Bindungsanforderungen für das Benutzerkonto auch dann mit der Meldung `LDAP binding not successful` fehl, wenn die Anforderung von einem der aufgeführten Computern stammt. Sie können dieses Problem vermeiden, indem Sie den NetBIOS-Namen für den Active Directory-Server zur Liste der Computer hinzufügen, bei denen sich das Benutzerkonto anmelden kann.

Voraussetzungen

- Stellen Sie sicher, dass Sie eine Active Directory-Domäne eingerichtet haben. Weitere Informationen finden Sie in der Dokumentation Ihres Verzeichnisservers.
- Stellen Sie sicher, dass der Name des ESXi-Hosts mit dem Domänennamen der Active Directory-Gesamtstruktur vollständig qualifiziert angegeben ist.

  Vollständig qualifizierter Domänenname = Hostname.Domänename

Verfahren

1. Synchronisieren Sie die Uhrzeit von ESXi mit der des Verzeichnisdienst-Systems.

   Unter Synchronisieren der ESXi-Systemuhren mit einem NTP-Server oder in der VMware-Knowledgebase finden Sie Informationen über das Synchronisieren der ESXi-Uhrzeit mit einem Microsoft-Domänencontroller.

2. Stellen Sie sicher, dass die DNS-Server, die Sie für den Host konfiguriert haben, die Hostnamen für die Active Directory-Controller auflösen können.
   a. Navigieren Sie zum Host im Navigator von vSphere Client.
   b. Klicken Sie auf **Konfigurieren**.
   c. Klicken Sie unter Netzwerk auf **TCP/IP-Konfiguration**.
   d. Klicken Sie unter TCP/IP Stack: Standard auf **DNS** und stellen Sie sicher, dass der Hostname und die DNS-Server-Informationen für den Host richtig sind.

Nächste Schritte

Fügen Sie den Host zu einer Verzeichnisdienstdomäne hinzu. Weitere Informationen hierzu finden Sie unter Hinzufügen eines Hosts zu einer Verzeichnisdienst-Domäne. Für Hosts, die mit Auto Deploy bereitgestellt wurden, müssen Sie vSphere Authentication Proxy einrichten. Weitere Informationen hierzu finden Sie unter Verwenden des vSphere Authentication Proxy.

Sie können Berechtigungen konfigurieren, damit Benutzer und Gruppen aus der hinzugefügten Active Directory-Domäne auf die vCenter Server-Komponenten zugreifen können. Informationen zum Verwalten von Berechtigungen finden Sie unter Hinzufügen einer Berechtigung zu einem Bestandslistenobjekt .

Hinzufügen eines Hosts zu einer Verzeichnisdienst-Domäne

Damit der Host einen Verzeichnisdienst verwenden kann, müssen Sie den Host mit der Verzeichnisdienst-Domäne verbinden.

Sie können den Domänennamen auf zwei Arten eingeben:

- **`name.tld`** (Beispiel: **`domain.com`**): Das Konto wird unter dem Standardcontainer erstellt.
- **`name.tld/container/path`** (Beispiel: **`domain.com/OU1/OU2`**): Das Konto wird unter der angegebenen Organisationseinheit (Organizational Unit, OU) erstellt.

Informationen zur Verwendung des vSphere Authentication Proxy-Diensts finden Sie unter Verwenden des vSphere Authentication Proxy.

Verfahren

1. Navigieren Sie zu einem Host in der Bestandsliste des vSphere Client.
2. Klicken Sie auf **Konfigurieren**.
3. Wählen Sie unter „System“ die Option **Authentifizierungsdienste**.
4. Klicken Sie auf **Domäne beitreten**.
5. Geben Sie eine Domäne ein.

   Verwenden Sie das Fomular **`name.tld`** oder **`name.tld/container/path`**.
6. Geben Sie den Benutzernamen und das Kennwort eines Verzeichnisdienstbenutzers ein, der über die Berechtigung verfügt, den Host mit der Domäne zu verbinden, und klicken Sie auf **OK**.
7. (Optional) Wenn Sie einen Authentifizierungs-Proxy verwenden möchten, geben Sie die IP-Adresse des Proxy-Servers ein.
8. Klicken Sie auf **OK** um das Dialogfeld für die Verzeichnisdienstkonfiguration zu schließen.

Nächste Schritte

Sie können Berechtigungen konfigurieren, damit Benutzer und Gruppen aus der hinzugefügten Active Directory-Domäne auf die vCenter Server-Komponenten zugreifen können. Informationen zum Verwalten von Berechtigungen finden Sie unter Hinzufügen einer Berechtigung zu einem Bestandslistenobjekt .

Anzeigen der Verzeichnisdiensteinstellungen

Sie können (soweit vorhanden) den Typ des Verzeichnisservers, den der Host zum Authentifizieren von Benutzern verwendet, sowie die Verzeichnisservereinstellungen anzeigen.

Verfahren

1. Navigieren Sie zum Host im Navigator des vSphere Client.
2. Klicken Sie auf **Konfigurieren**.
3. Wählen Sie unter „System“ die Option **Authentifizierungsdienste**.

   Auf der Seite „Authentifizierungsdienste“ werden der Verzeichnisdienst und die Domäneneinstellungen angezeigt.

Nächste Schritte

Sie können Berechtigungen konfigurieren, damit Benutzer und Gruppen aus der hinzugefügten Active Directory-Domäne auf die vCenter Server-Komponenten zugreifen können. Informationen zum Verwalten von Berechtigungen finden Sie unter Hinzufügen einer Berechtigung zu einem Bestandslistenobjekt .

Verwenden des vSphere Authentication Proxy

Statt Hosts explizit zur Active Directory-Domäne hinzuzufügen, können Sie mithilfe von vSphere Authentication Proxy ESXi-Hosts zu einer Active Directory-Domäne hinzufügen.

Sie müssen den Host nur so einrichten, dass er den Domänennamen des Active Directory-Servers und die IP-Adresse von vSphere Authentication Proxy kennt. Wenn vSphere Authentication Proxy aktiviert ist, werden Hosts, die mit Auto Deploy bereitgestellt werden, automatisch zur Active Directory-Domäne hinzugefügt. Sie können vSphere Authentication Proxy auch mit Hosts verwenden, die nicht mithilfe von Auto Deploy bereitgestellt werden.

Weitere Informationen zu den von vSphere Authentication Proxy verwendeten TCP-Ports finden Sie unter Erforderliche Ports für vCenter Server.

Auto Deploy

Wenn Sie Hosts mithilfe von Auto Deploy bereitstellen, können Sie einen Referenzhost einrichten, der auf Authentication Proxy verweist. Sie richten dann eine Regel ein, die das Profil des Referenzhosts auf jeden mithilfe von Auto Deploy bereitgestellten ESXi-Host anwendet. vSphere Authentication Proxy speichert in der Zugriffssteuerungsliste (Access Control List, ACL) die IP-Adressen aller Hosts, die Auto Deploy mithilfe von PXE bereitstellt. Wenn der Host gestartet wird, kontaktiert er vSphere Authentication Proxy, und vSphere Authentication Proxy sorgt dafür, dass diese Hosts, die bereits in der ACL aufgeführt werden, der Active Directory-Domäne beitreten.

Auch dann, wenn Sie vSphere Authentication Proxy in einer Umgebung verwenden, die von VMCA bereitgestellten Zertifikate oder Zertifikate von Drittanbietern verwendet, funktioniert der Prozess nahtlos, wenn Sie die Anweisungen für die Verwendung von benutzerdefinierten Zertifikaten mit Auto Deploy befolgen.

Weitere Informationen hierzu finden Sie unter Verwenden benutzerdefinierter Zertifikate mit Auto Deploy.

Andere ESXi-Hosts

Sie können andere Hosts für die Verwendung von vSphere Authentication Proxy einrichten, wenn Sie möchten, dass der Host der Domäne ohne Verwendung der Active Directory-Anmeldedaten beitreten kann. Dies bedeutet, dass Sie keine Active Directory-Anmeldeinformationen an den Host übertragen und sie nicht im Hostprofil speichern müssen.

In diesem Fall fügen Sie die IP-Adresse des Hosts zur ACL von vSphere Authentication Proxy hinzu und vSphere Authentication Proxy autorisiert den Host standardmäßig anhand dessen IP-Adresse. Sie können die Clientauthentifizierung so konfigurieren, dass vSphere Authentication Proxy das Zertifikat des Hosts überprüft.

Hinweis Sie können vSphere Authentication Proxy nicht in einer Umgebung verwenden, die nur IPv6 unterstützt.

Aktiveren von VMware vSphere Authentication Proxy

Der vSphere Authentication Proxy-Dienst steht auf jedem vCenter Server-System zur Verfügung. Standardmäßig wird der Dienst nicht ausgeführt. Wenn Sie vSphere Authentication Proxy in Ihrer Umgebung verwenden möchten, können Sie den Dienst über die vCenter Server-Verwaltungsschnittstelle oder die Befehlszeile starten.

Der vSphere Authentication Proxy-Dienst bindet an eine IPv4-Adresse für die Kommunikation mit vCenter Server und bietet keine Unterstützung für IPv6. Die vCenter Server-Instanz kann sich auf einer Hostmaschine in einer reinen IPv4-Netzwerkumgebung oder im gemischten IPv4/IPv6-Modus befinden. Wenn Sie jedoch die Adresse des vSphere Authentication Proxy angeben, müssen Sie eine IPv4-Adresse angeben.

Voraussetzungen

Stellen Sie sicher, dass Sie vCenter Server 6.5 oder höher einsetzen. In früheren Versionen von vSphere erfolgt die Installation von vSphere Authentication Proxy separat. Entsprechende Anweisungen dazu finden Sie in der Dokumentation zu der jeweiligen früheren Produktversion.

Verfahren

1 Starten Sie den VMware vSphere Authentication Proxy-Dienst.

Option	Beschreibung
vCenter Server-Verwaltungsschnittstelle	a Navigieren Sie in einem Webbrowser zur vCenter Server-Verwaltungsschnittstelle (https://*vcenter-IP-adresse-oder-FQDN*:5480). b Melden Sie sich als „root“ an. Das standardmäßige Root-Kennwort ist das Kennwort, das Sie während der Bereitstellung der vCenter Server festlegen. c Klicken Sie auf **Dienste** und anschließend auf den **VMware vSphere Authentication Proxy**-Dienst. d Klicken Sie auf **Start**. e (Optional) Klicken Sie nach dem Start des Diensts auf **Starttyp festlegen** und dann auf **Automatisch**, um automatische Starts zu ermöglichen.
Befehlszeilenschnittstelle	`service-control --start vmcam`

2 Bestätigen Sie, dass der Dienst erfolgreich gestartet wurde.

Ergebnisse

Jetzt können Sie die vSphere Authentication Proxy-Domäne festlegen. Danach verwaltet der vSphere Authentication Proxy alle mit Auto Deploy bereitgestellten Hosts, und Sie können Hosts explizit zu vSphere Authentication Proxy hinzufügen.

Hinzufügen einer Domäne zu vSphere Authentication Proxy mit dem vSphere Client

Sie können vSphere Authentication Proxy eine Domäne über den vSphere Client oder mithilfe des Befehls `camconfig` hinzufügen.

Sie können eine Domäne nur nach der Aktivierung des Proxys zu vSphere Authentication Proxy hinzufügen. Nachdem Sie die Domäne hinzugefügt haben, fügt vSphere Authentication Proxy alle von Ihnen bereitgestellten Hosts mit Auto Deploy zu dieser Domäne hinzu. Sie können für andere Hosts auch vSphere Authentication Proxy verwenden, wenn Sie diesen Hosts keine Domänenberechtigungen geben möchten.

Verfahren

1 Stellen Sie mit dem vSphere Client eine Verbindung zu einem vCenter Server-System her.

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

3 Klicken Sie auf **Authentication Proxy** und auf **Bearbeiten**.

4 Geben Sie den Namen der Domäne ein, der Hosts mithilfe von vSphere Authentication Proxy hinzugefügt werden, sowie den Namen und das Kennwort eines Benutzers mit Active Directory-Berechtigungen, um Hosts zur Domäne hinzuzufügen.

5 Klicken Sie auf **Speichern**.

Hinzufügen einer Domäne zu vSphere Authentication Proxy mit dem Befehl „camconfig“

Sie können mithilfe des Befehls `camconfig` eine Domäne zu vSphere Authentication Proxy hinzufügen.

Sie können eine Domäne nur nach der Aktivierung des Proxys zu vSphere Authentication Proxy hinzufügen. Nachdem Sie die Domäne hinzugefügt haben, fügt vSphere Authentication Proxy alle von Ihnen bereitgestellten Hosts mit Auto Deploy zu dieser Domäne hinzu. Sie können für andere Hosts auch vSphere Authentication Proxy verwenden, wenn Sie diesen Hosts keine Domänenberechtigungen geben möchten.

Verfahren

1. Melden Sie sich als Benutzer mit Administratorrechten beim vCenter Server-System an.
2. Führen Sie den Befehl aus, um den Zugriff auf die Bash-Shell zu aktivieren.

   ```
   shell
   ```

3. Wechseln Sie zum Verzeichnis `/usr/lib/vmware-vmcam/bin/`, in dem sich das Skript **camconfig** befindet.
4. Um die Active Directory-Anmeldedaten für Domäne und Benutzer der Authentication Proxy-Konfiguration hinzuzufügen, führen Sie den folgenden Befehl aus.

   ```
   camconfig add-domain -d domain -u user
   ```

   Sie werden zur Eingabe eines Kennworts aufgefordert.

   vSphere Authentication Proxy speichert diesen Benutzernamen und das Kennwort. Sie können den Benutzer nach Bedarf entfernen und neu erstellen. Die Domäne muss über DNS erreichbar sein. Es muss sich aber nicht um eine vCenter Single Sign-On-Identitätsquelle handeln.

   vSphere Authentication Proxy verwendet den vom *Benutzer* angegebenen Benutzernamen, um die Konten für ESXi-Hosts in Active Directory zu erstellen. Der Benutzer muss über Berechtigungen zum Erstellen von Konten in der Active Directory-Domäne verfügen, zu der Sie die Hosts hinzufügen. Zum Zeitpunkt der Zusammenstellung dieser Informationen enthielt der Microsoft Knowledge Base-Artikel 932455 Hintergrundinformationen zu den Kontoerstellungsberechtigungen.
5. Wenn Sie später die Domäne und die Benutzerinformationen aus vSphere Authentication Proxy entfernen möchten, führen Sie folgenden Befehl aus.

   ```
   camconfig remove-domain -d domain
   ```

Verwenden des vSphere Authentication Proxy zum Hinzufügen eines Hosts zu einer Domäne

Der Auto Deploy-Server fügt alle Hosts hinzu, die er für vSphere Authentication Proxy bereitstellt, und vSphere Authentication Proxy fügt diese Hosts zur Domäne hinzu. Wenn Sie mithilfe von vSphere Authentication Proxy weitere Hosts zu einer Domäne hinzufügen möchten, können Sie diese Hosts explizit zu vSphere Authentication Proxy hinzufügen. Danach fügt der vSphere Authentication Proxy-Server diese Hosts zur Domäne hinzu. Folglich müssen vom Benutzer angegebene Anmeldeinformationen nicht mehr an das vCenter Server-System übermittelt werden.

Sie können den Domänennamen auf zwei Arten eingeben:

- **`name.tld`** (Beispiel: **`domain.com`**): Das Konto wird unter dem Standardcontainer erstellt.
- **`name.tld/container/path`** (Beispiel: **`domain.com/OU1/OU2`**): Das Konto wird unter der angegebenen Organisationseinheit (Organizational Unit, OU) erstellt.

Voraussetzungen

- Wenn der ESXi-Host ein VMCA-signiertes Zertifikat verwendet, stellen Sie sicher, dass der Host zum vCenter Server hinzugefügt wurde. Anderenfalls kann der Authentication Proxy-Dienst dem ESXi-Host nicht vertrauen.
- Wenn der ESXi-Host ein von einer Stammzertifizierungsstelle signiertes Zertifikat verwendet, stellen Sie sicher, dass das entsprechende von einer Stammzertifizierungsstelle signierte Zertifikat zum vCenter Server-System hinzugefügt wurde. Weitere Informationen hierzu finden Sie unter Zertifikatsverwaltung für ESXi-Hosts.

Verfahren

1. Navigieren Sie zum Host im Navigator von vSphere Client.
2. Klicken Sie auf **Konfigurieren**.
3. Wählen Sie unter **System** die Option **Authentifizierungsdienste**.
4. Klicken Sie auf **Domäne beitreten**.
5. Geben Sie eine Domäne ein.

   Verwenden Sie das Format **`name.tld`** (Beispiel: **`meinedomaene.com`**) oder **`name.tld/container/pfad`** (Beispiel: **`meinedomaene.com/organisationseinheit1/organisationseinheit2`**).
6. Wählen Sie **Proxy-Server verwenden** aus.
7. Geben Sie die IP-Adresse des Authentication Proxy-Servers ein. Diese Adresse ist mit der IP-Adresse des vCenter Server-Systems identisch.
8. Klicken Sie auf **OK**.

Aktivieren der Client-Authentifizierung für vSphere Authentication Proxy

Standardmäßig fügt vSphere Authentication Proxy einen beliebigen Host hinzu, wenn die IP-Adresse dieses Hosts in seiner Zugriffssteuerungsliste vorhanden ist. Um die Sicherheit weiter zu steigern, können Sie Client-Authentifizierung aktivieren. Wenn Client-Authentifizierung aktiviert ist, prüft vSphere Authentication Proxy auch das Zertifikat des Hosts.

Voraussetzungen

- Stellen Sie sicher, dass das vCenter Server-System dem Host vertraut. Wenn Sie einen Host zu vCenter Server hinzufügen, wird dem Host standardmäßig ein Zertifikat zugewiesen, das von einer vCenter Server vertrauenswürdigen Stammzertifizierungsstelle signiert ist. vSphere Authentication Proxy vertraut vCenter Server vertrauenswürdiger Stammzertifizierungsstelle.
- Wenn Sie vorhaben, ESXi-Zertifikate in Ihrer Umgebung zu ersetzen, nehmen Sie die Ersetzung vor, bevor Sie den vSphere Authentication Proxy aktivieren. Die Zertifikate auf dem ESXi-Host müssen mit denen der Host-Registrierung übereinstimmen.

Verfahren

1. Melden Sie sich als Benutzer mit Administratorrechten beim vCenter Server-System an.
2. Führen Sie den Befehl aus, um den Zugriff auf die Bash-Shell zu aktivieren.

   ```
   shell
   ```

3. Wechseln Sie zum Verzeichnis `/usr/lib/vmware-vmcam/bin/`, in dem sich das Skript **camconfig** befindet.
4. Führen Sie den folgenden Befehl aus, um die Client-Authentifizierung zu aktivieren.

   ```
   camconfig ssl-cliAuth -e
   ```

   Ab diesem Zeitpunkt prüft vSphere Authentication Proxy das Zertifikat von jedem Host, der hinzugefügt wird.
5. Wenn Sie diese Client-Authentifizierung später wieder deaktivieren möchten, führen Sie den folgenden Befehl aus.

   ```
   camconfig ssl-cliAuth -n
   ```

Importieren des vSphere Authentication Proxy-Zertifikats in den ESXi-Host

Standardmäßig erfordern ESXi-Hosts eine explizite Verifizierung des vSphere Authentication Proxy-Zertifikats. Wenn Sie vSphere Auto Deploy verwenden, übernimmt der Auto Deploy-Dienst das Hinzufügen des Zertifikats zu den Hosts, die er bereitstellt. Bei anderen Hosts müssen Sie das Zertifikat explizit hinzufügen.

Voraussetzungen

- Laden Sie das vSphere Authentication Proxy-Zertifikat auf einen Datenspeicher, auf den der ESXi-Host zugreifen kann. Mit einer SFTP-Anwendung wie WinSCP können Sie das Zertifikat vom vCenter Server-Host am folgenden Speicherort herunterladen.

  `/var/lib/vmware/vmcam/ssl/rui.crt`

- Stellen Sie sicher, dass die fortgeschrittene Einstellung für `UserVars.ActiveDirectoryVerifyCAMCertificate` ESXi auf 1 festgelegt ist (Standardwert).

Verfahren

1. Wählen Sie den ESXi-Host aus und klicken Sie auf **Konfigurieren**.
2. Wählen Sie unter **System** die Option **Authentifizierungsdienste**.
3. Klicken Sie auf **Zertifikat importieren**.
4. Geben Sie den Pfad zur Zertifikatsdatei im Format `[`*`Datenspeicher`*`]/`*`Pfad/Zertifikatsname`*`.crt` ein und klicken Sie auf **OK**.

Erstellen eines neuen Zertifikats für vSphere Authentication Proxy

Sie können ein neues von VMCA bereitgestelltes Zertifikat oder ein neues Zertifikat erstellen, das VMCA als untergeordnetes Zertifikat enthält.

Wenn Sie ein benutzerdefiniertes Zertifikat verwenden möchten, das von der Zertifizierungsstelle eines Drittanbieters oder Unternehmens signiert wurde, finden Sie weitere Informationen unter Einrichten von vSphere Authentication Proxy für die Verwendung von benutzerdefinierten Zertifikaten.

Voraussetzungen

Sie müssen über Root- oder Administratorrechte auf dem System verfügen, auf dem der vSphere Authentication Proxy ausgeführt wird.

Verfahren

1. Erstellen Sie eine Kopie der Datei `certool.cfg`.

   ```
   cp /usr/lib/vmware-vmca/share/config/certool.cfg /var/lib/vmware/vmcam/ssl/vmcam.cfg
   ```

2. Fügen Sie in die Kopie Informationen über Ihre Organisation ein, wie im folgenden Beispiel beschrieben.

   ```
   Country = IE
   Name = vmcam
   Organization = VMware
   OrgUnit = vTSU
   State = Cork
   Locality = Cork
   Hostname = test-cam-1.test1.vmware.com
   ```

3 Erzeugen Sie den neuen privaten Schlüssel in `/var/lib/vmware/vmcam/ssl/`.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=/var/lib/vmware/vmcam/ssl/rui.key --
pubkey=/tmp/vmcam.pub --server=localhost
```

Geben Sie unter *localhost* den FQDN des vCenter Servers an.

4 Erzeugen Sie das neue Zertifikat in `/var/lib/vmware/vmcam/ssl/` unter Verwendung des Schlüssels und der Datei `vmcam.cfg`, die Sie in Schritt 1 und Schritt 2 erstellt haben.

```
/usr/lib/vmware-vmca/bin/certool --server=localhost --gencert --privkey=/var/lib/
vmware/vmcam/ssl/rui.key --cert=/var/lib/vmware/vmcam/ssl/rui.crt --config=/var/lib/vmware/
vmcam/ssl/vmcam.cfg
```

Geben Sie unter *localhost* den FQDN des vCenter Servers an.

Einrichten von vSphere Authentication Proxy für die Verwendung von benutzerdefinierten Zertifikaten

Für das Verwenden von benutzerdefinierten Zertifikaten mit vSphere Authentication Proxy sind mehrere Schritte erforderlich. Als Erstes generieren Sie einen CSR und leiten diesen zum Signieren an Ihre Zertifizierungsstelle weiter. Dann speichern Sie das signierte Zertifikat und die Schlüsseldatei an einem Speicherort, auf den vSphere Authentication Proxy zugreifen kann.

Standardmäßig generiert vSphere Authentication Proxy einen CSR während des anfänglichen Startvorgangs und fordert VMCA auf, diesen CSR zu signieren. vSphere Authentication Proxy verwendet dieses Zertifikat, um sich bei vCenter Server zu registrieren. Sie können benutzerdefinierte Zertifikate in Ihrer Umgebung verwenden, wenn Sie diese Zertifikate zu vCenter Server hinzufügen.

Verfahren

1 Generieren Sie einen CSR für vSphere Authentication Proxy.

   a Erstellen Sie die Konfigurationsdatei `/var/lib/vmware/vmcam/ssl/vmcam.cfg` nach dem nachfolgenden Beispiel.

```
[ req ]
distinguished_name = req_distinguished_name
encrypt_key = no
prompt = no
string_mask = nombstr
req_extensions = v3_req
[ v3_req ]
basicConstraints = CA:false
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = DNS:dns.static-1.csl.vmware.com
[ req_distinguished_name ]
countryName = IE
stateOrProvinceName = Cork
localityName = Cork
0.organizationName = VMware
organizationalUnitName = vTSU
commonName = test-cam-1.test1.vmware.com
```

   b Führen Sie unter Angabe der Konfigurationsdatei `openssl` aus, um eine CSR- und eine Schlüsseldatei zu generieren.

```
openssl req -new -nodes -out vmcam.csr -newkey rsa:2048 -keyout /var/lib/vmware/
vmcam/ssl/rui.key -config /var/lib/vmware/vmcam/ssl/vmcam.cfg
```

2 Sichern Sie die Zertifikatsdateien `rui.crt` und `rui.key`, welche sich im folgenden Speicherort befinden.

   `/var/lib/vmware/vmcam/ssl/rui.crt`

3 Heben Sie die Registrierung von vSphere Authentication Proxy auf.

   a Navigieren Sie zum Verzeichnis `/usr/lib/vmware-vmcam/bin`, in dem sich das Skript `camregister` befindet.

   b Führen Sie den folgenden Befehl aus.

```
camregister --unregister -a VC_address -u Benutzer
```

   Benutzer muss ein vCenter Single Sign-On-Benutzer mit Administratorberechtigungen für vCenter Server sein.

4 Halten Sie den vSphere Authentication Proxy-Dienst an.

Tool	Schritte
vCenter Server-Konfigurationsverwaltungsschnittstelle	a Navigieren Sie in einem Webbrowser zur vCenter Server-Konfigurationsverwaltungsschnittstelle (https://*vcenter-IP-address-or-FQDN*:5480). b Melden Sie sich als „root“ an. Das standardmäßige Root-Kennwort ist das Kennwort, das Sie während der Bereitstellung der vCenter Server festlegen. c Klicken Sie auf **Dienste** und anschließend auf den **VMware vSphere Authentication Proxy-Dienst**. d Klicken Sie auf **Beenden**.
Befehlszeilenschnittstelle	`service-control --stop vmcam`

5 Ersetzen Sie die bestehenden Zertifikatsdateien `rui.crt` und `rui.key` durch die Dateien, die Sie von Ihrer Zertifizierungsstelle erhalten haben.

6 Starten Sie den vSphere Authentication Proxy-Dienst neu.

7 Registrieren Sie vSphere Authentication Proxy mithilfe des neuen Zertifikats und des neuen Schlüssels explizit bei vCenter Server neu.

```
camregister --register -a VC_address -u user -c vollständiger_Pfad_von_rui.crt -k
vollständiger_Pfad_von_rui.key
```

Konfigurieren der Smartcard-Authentifizierung für ESXi

Sie können sich mit der Smartcard-Authentifizierung bei der ESXi-Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) anmelden, indem Sie eine persönliche Identitätsprüfung (Personal Identity Verification, PIV), eine allgemeine Zugriffskarte (Common Access Card, CAC) oder eine SC650-Smartcard anstelle der Eingabe eines Benutzernamens und eines Kennworts verwenden.

Eine Smartcard (Chipkarte) ist eine kleine Plastikkarte mit einem integrierten Schaltkreis (Chip). Viele staatliche Behörden und große Unternehmen verwenden eine auf Smartcards basierende Zwei-Faktor-Authentifizierung, um die Sicherheit ihrer Systeme zu erhöhen und bestehende Sicherheitsbestimmungen zu erfüllen.

Wenn die Smartcard-Authentifizierung auf einem ESXi-Host aktiviert ist, werden Sie von der DCUI zur Eingabe einer Smartcard und einer PIN-Kombination anstelle des standardmäßigen Benutzernamens und Kennworts aufgefordert.

1 Wenn Sie die Smartcard in den Kartenleser stecken, liest der ESXi-Host die darauf gespeicherten Anmeldedaten.

2 Die ESXi-DCUI zeigt Ihre Anmeldekennung an und fordert Sie zur Eingabe Ihrer PIN auf.

3 Nach der Eingabe Ihrer PIN vergleicht der ESXi-Host sie mit der auf der Smartcard gespeicherten PIN und überprüft das Zertifikat auf der Smartcard mit Active Directory.

4 Nach erfolgreicher Prüfung des Smartcard-Zertifikats schließt ESXi die Anmeldung bei der DCUI ab.

Sie können durch Drücken von F3 zur Benutzernamen- und Kennwort-Authentifizierung über die DCUI wechseln.

Nach einigen aufeinanderfolgenden falschen PIN-Eingaben (gewöhnlich drei) wird die Smartcard gesperrt. Eine gesperrte Smartcard kann nur von ausgewähltem Personal entsperrt werden.

Aktivieren von Smartcard-Authentifizierung

Aktivieren Sie die Smartcard-Authentifizierung, um eine Chipkarte und eine PIN-Kombination zum Anmelden bei der ESXi-DCUI zu verlangen.

Voraussetzungen

- Richten Sie die Infrastruktur zur Smartcard-Authentifizierung ein, wie beispielsweise Konten in der Active Directory-Domäne, Smartcard-Lesegeräte und Smartcards.
- Konfigurieren Sie ESXi für den Beitritt zu einer Active Directory-Domäne, die die Smartcard-Authentifizierung unterstützt. Weitere Informationen finden Sie unter Verwenden von Active Directory zum Verwalten von ESXi-Benutzern .
- Verwenden Sie den vSphere Client zum Hinzufügen von Stammzertifikaten. Weitere Informationen hierzu finden Sie unter Zertifikatsverwaltung für ESXi-Hosts.

Verfahren

1 Navigieren Sie zum Host im Navigator des vSphere Client.

2 Klicken Sie auf **Konfigurieren**.

3 Wählen Sie unter „System“ die Option **Authentifizierungsdienste**.

Der aktuelle Status der Smartcard-Authentifizierung und eine Liste mit importierten Zertifikaten werden angezeigt.

4 Klicken Sie im Fensterbereich „Smartcard-Authentifizierung“ auf **Bearbeiten**.

5 Wählen Sie im Dialogfeld zum Bearbeiten der Smartcard-Authentifizierung die Seite für Zertifikate aus.

6 Fügen Sie vertrauenswürdige CA-Zertifikate hinzu, zum Beispiel Zertifikate von Root- und zwischengeschalteten Zertifizierungsstellen (CA).

Zertifikate müssen im PEM-Format sein.

7 Öffnen Sie die Seite „Smartcard-Authentifizierung“, aktivieren Sie das Kontrollkästchen **Smartcard-Authentifizierung aktivieren** und klicken Sie auf **OK**.

Deaktivieren von Smartcard-Authentifizierung

Deaktivieren Sie die Smartcard-Authentifizierung, um zur standardmäßigen Authentifizierung mit Benutzernamen und Kennwort bei der ESXi-DCUI-Anmeldung zurückzukehren.

Verfahren

1. Navigieren Sie zum Host im Navigator des vSphere Client.
2. Klicken Sie auf **Konfigurieren**.
3. Wählen Sie unter „System“ die Option **Authentifizierungsdienste**.

   Der aktuelle Status der Smartcard-Authentifizierung und eine Liste mit importierten Zertifikaten werden angezeigt.
4. Klicken Sie im Fensterbereich „Smartcard-Authentifizierung“ auf **Bearbeiten**.
5. Deaktivieren Sie auf der Seite „Smartcard-Authentifizierung“ das Kontrollkästchen **Smartcard-Authentifizierung aktivieren** und klicken Sie auf **OK**.

Authentifizieren mit Benutzernamen und Kennwort bei Verbindungsproblemen

Sollte der Active Directory-(AD-)Domänenserver nicht erreichbar sein, können Sie sich bei der ESXi-DCUI mit Benutzername-und-Kennwort-Authentifizierung anmelden und Notfallmaßnahmen auf dem Host ergreifen.

In Ausnahmefällen kann es vorkommen, dass der AD-Domänenserver aufgrund von Verbindungsproblemen, Netzwerkausfällen oder Naturkatastrophen nicht erreichbar ist und die Benutzeranmeldedaten auf der Smartcard nicht authentifiziert werden können. In diesem Fall können Sie sich bei der ESXi-DCUI mit den Anmeldeinformationen eines lokalen ESXi-Administratorbenutzers anmelden. Nach der Anmeldung können Sie Diagnosen oder andere Notfallmaßnahmen durchführen. Der Fallback auf die Anmeldung mit Benutzernamen und Kennwort wird im Protokoll vermerkt. Sobald die Verbindung mit AD wieder hergestellt ist, ist auch die Smartcard-Authentifizierung wieder verfügbar.

Hinweis Der Verlust der Netzwerkverbindung zu vCenter Server hat keinen Einfluss auf die Smartcard-Authentifizierung, solange der Active Directory-Domänenserver verfügbar bleibt.

Verwenden der Smartcard-Authentifizierung im Sperrmodus

Wenn aktiviert, erhöht der Sperrmodus auf dem ESXi-Host die Sicherheit des Hosts und beschränkt den Zugriff auf die DCUI. Im Sperrmodus ist die Smartcard-Authentifizierung unter Umständen nicht verfügbar.

Im normalen Sperrmodus haben nur Benutzer, die Administratorrechte besitzen und in der Liste der ausgenommenen Benutzer geführt werden, Zugriff auf die DCUI. Ausgenommene Benutzer sind lokale Hostbenutzer oder Active Directory-Benutzer mit lokal für den ESXi-Host definierten Rechten. Wenn Sie die Smartcard-Authentifizierung auch im normalen Sperrmodus nutzen

möchten, müssen Sie Benutzer mithilfe des vSphere Client in die Liste der ausgenommenen Benutzer aufnehmen. Diese Benutzer behalten ihre Berechtigungen auch dann, wenn der Host in den normalen Sperrmodus versetzt wird, und können sich auch weiterhin bei der DCUI anmelden. Weitere Informationen finden Sie unter Angeben der Benutzerausnahmen für den Sperrmodus.

Im strengen Sperrmodus wird der DCUI-Dienst beendet. Daher ist auch kein Zugriff auf den Host über Smartcard-Authentifizierung möglich.

Verwenden der ESXi Shell

Die ESXi Shell ist auf ESXi-Hosts standardmäßig deaktiviert. Sie können bei Bedarf lokalen Zugriff und Remotezugriff auf die Shell aktivieren.

Um das Risiko eines nicht autorisierten Zugriffs zu reduzieren, aktivieren Sie die ESXi Shell nur zur Fehlerbehebung.

Die ESXi Shell ist unabhängig vom Sperrmodus. Selbst wenn der Host im Sperrmodus ausgeführt wird, können Sie sich weiterhin bei der ESXi Shell anmelden, soweit sie aktiviert ist.

ESXi Shell

Aktivieren Sie diesen Dienst, um lokal auf die ESXi Shell zuzugreifen.

SSH

Aktivieren Sie diesen Dienst, um die ESXi Shell remote über SSH aufzurufen.

Der Root-Benutzer und Benutzer mit der Rolle „Administrator“ können auf die ESXi Shell zugreifen. Benutzern, die zur Active Directory-Gruppe „ESX Admins“ gehören, wird automatisch die Rolle „Administrator“ zugewiesen. Standardmäßig kann nur der Root-Benutzer Systembefehle (z. B. `vmware -v`) über die ESXi Shell ausführen.

Hinweis Aktivieren Sie die ESXi Shell nur, wenn dies wirklich erforderlich ist.

- Aktivieren des Zugriffs auf die ESXi Shell

  ESXi Shell- und SSH-Schnittstellen sind standardmäßig deaktiviert. Aktivieren Sie diese Schnittstellen erst, wenn Fehlerbehebungs- oder Supportaktivitäten durchgeführt werden müssen. Verwenden Sie für die täglichen Aktivitäten den vSphere Client, wobei die Aktivität der rollenbasierten Zugriffssteuerung und modernen Zugriffssteuerungsmethoden unterliegt.
- Verwenden der Benutzerschnittstelle der direkten Konsole für den Zugriff auf die ESXi Shell

  Mithilfe der Benutzerschnittstelle der direkten Konsole (DCUI) können Sie lokal unter Verwendung textbasierter Menüs mit dem Hosts interagieren. Wägen Sie sorgfältig ab, ob die Sicherheitsanforderungen Ihrer Umgebung die Benutzerschnittstelle der direkten Konsole unterstützen.

- Anmelden bei der ESXi Shell zur Fehlerbehebung

  Führen Sie ESXi-Konfigurationsaufgaben mit vSphere Client, ESXCLI oder VMware PowerCLI aus. Melden Sie sich bei der ESXi Shell (vormals Support-Modus oder TSM) nur zwecks Fehlerbehebung an.

Aktivieren des Zugriffs auf die ESXi Shell

ESXi Shell- und SSH-Schnittstellen sind standardmäßig deaktiviert. Aktivieren Sie diese Schnittstellen erst, wenn Fehlerbehebungs- oder Supportaktivitäten durchgeführt werden müssen. Verwenden Sie für die täglichen Aktivitäten den vSphere Client, wobei die Aktivität der rollenbasierten Zugriffssteuerung und modernen Zugriffssteuerungsmethoden unterliegt.

Hinweis Greifen Sie auf den Host zu, indem Sie den vSphere Client, Remote-Befehlszeilentools (ESXCLI und PowerCLI) und veröffentlichte APIs verwenden. Aktivieren Sie den Remotezugriff auf den Host nicht mit SSH, es sei denn, bestimmte Umstände erfordern eine Aktivierung des SSH-Zugangs.

Voraussetzungen

Wenn Sie einen autorisierten SSH-Schlüssel verwenden möchten, können Sie ihn hochladen. Weitere Informationen hierzu finden Sie unter ESXi-SSH-Schlüssel.

Verfahren

1. Navigieren Sie zum Host in der Bestandsliste.
2. Klicken Sie auf **Konfigurieren** und dann unter „System“ auf **Dienste**.
3. Verwalten Sie ESXi-, SSH- oder Dienste der Benutzerschnittstelle der direkten Konsole.
   a. Wählen Sie im Fenster „Dienste“ den Dienst aus.
   b. Klicken Sie auf **Startrichtlinie bearbeiten** und wählen Sie die Startrichtlinie **Manuell starten und stoppen** aus.
   c. Klicken Sie zum Aktivieren des Diensts auf **Starten**.

   Wenn Sie **Manuell starten und beenden** wählen, wird der Dienst nicht gestartet, wenn Sie den Host neu starten. Wenn Sie den Dienst beim Neustart des Hosts starten möchten, wählen Sie **Mit dem Host starten und beenden**.

Nächste Schritte

Legen Sie die Zeitüberschreitungswerte für die Verfügbarkeits- und Leerlaufzeiten der ESXi Shell fest. Weitere Informationen hierzu finden Sie unter Erstellen einer Zeitüberschreitung für dieESXi Shell-Verfügbarkeit und Erstellen einer Zeitüberschreitung für ESXi Shell-Sitzungen im Leerlauf.

Erstellen einer Zeitüberschreitung für dieESXi Shell-Verfügbarkeit

Standardmäßig ist die ESXi Shell deaktiviert. Sie können einen Zeitüberschreitungswert für die Verfügbarkeit für die ESXi Shell festlegen, um die Sicherheit beim Aktivieren der Shell zu erhöhen.

Der Zeitüberschreitungswert für die Verfügbarkeit gibt die Zeitspanne an, während der Sie sich nach der Aktivierung der ESXi Shell anmelden müssen. Nach Ablauf dieser Zeitspanne wird der Dienst deaktiviert und die Benutzer können sich nicht mehr anmelden.

Verfahren

1. Navigieren Sie zum Host im Navigator des vSphere Client.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter „System“ auf **Erweiterte Systemeinstellungen**.
4. Klicken Sie auf **Bearbeiten** und wählen Sie `UserVars.ESXiShellTimeOut` aus.
5. Geben Sie den Zeitüberschreitungswert für den Leerlauf ein.

   Sie müssen den SSH-Dienst und den ESXi Shell-Dienst neu starten, damit die Einstellungen wirksam werden.
6. Klicken Sie auf **OK**.

Ergebnisse

Wenn Sie zu diesem Zeitpunkt angemeldet sind, bleibt Ihre Sitzung bestehen. Wenn Sie sich jedoch abmelden oder die Sitzung beendet wird, können Sie sich nicht mehr anmelden.

Erstellen einer Zeitüberschreitung für ESXi Shell-Sitzungen im Leerlauf

Wenn Sie die ESXi Shell auf einem Host aktivieren, sich aber nicht von der Sitzung abmelden, bleibt die Sitzung im Leerlauf für unbestimmte Zeit bestehen. Die offene Verbindung erhöht die Möglichkeit für einen privilegierten Zugriff auf den Host. Verhindern Sie dies, indem Sie eine Zeitüberschreitung für Sitzungen im Leerlauf festlegen.

Der Zeitüberschreitungswert für die Leerlaufzeit gibt die Zeitspanne an, die verstreichen darf, bis ein Benutzer bei interaktiven Sitzungen, die sich im Leerlauf befinden, abgemeldet wird. Sie können die Zeit sowohl für lokale als auch Remote-Sitzungen (SSH) vom Direct Console Interface (DCUI) oder vom vSphere Client aus steuern.

Verfahren

1. Navigieren Sie zum Host im Navigator des vSphere Client.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter „System“ auf **Erweiterte Systemeinstellungen**.
4. Klicken Sie auf **Bearbeiten**, wählen Sie `UserVars.ESXiShellInteractiveTimeOut` aus und geben Sie die Einstellung für die Zeitüberschreitung ein.

   Mit dem Wert NULL (0) wird die Leerlaufzeit deaktiviert.
5. Sie müssen den ESXi Shell-Dienst neu starten, damit die Einstellungen wirksam werden.

Ergebnisse

Wenn die Sitzung sich im Leerlauf befindet, werden die Benutzer nach Ablauf der Zeitüberschreitungszeitspanne abgemeldet.

Verwenden der Benutzerschnittstelle der direkten Konsole für den Zugriff auf die ESXi Shell

Mithilfe der Benutzerschnittstelle der direkten Konsole (DCUI) können Sie lokal unter Verwendung textbasierter Menüs mit dem Hosts interagieren. Wägen Sie sorgfältig ab, ob die Sicherheitsanforderungen Ihrer Umgebung die Benutzerschnittstelle der direkten Konsole unterstützen.

Sie können die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) verwenden, um lokalen und Remotezugriff auf die ESXi Shell zu ermöglichen. Sie greifen über die mit dem Host verbundene physische Konsole auf die Benutzerschnittstelle der direkten Konsole zu. Nachdem der Host neu gestartet und ESXi geladen wurde, drücken Sie F2 zum Anmelden bei der DCUI. Geben Sie die Anmeldedaten ein, die Sie bei der Installation von ESXi erstellt haben.

Hinweis Änderungen am Host, die mit der Benutzerschnittstelle der direkten Konsole, dem vSphere Client, ESXCLI oder anderen Verwaltungs-Tools vorgenommen wurden, werden stündlich oder beim ordnungsgemäßen Herunterfahren des Systems dauerhaft gespeichert. Wenn der Host ausfällt, bevor die Änderungen vorgenommen wurden, gehen sie möglicherweise verloren.

Verfahren

1. Drücken Sie in Direct Console User Interface die Taste F2, um das Menü für die Systemanpassung aufzurufen.
2. Wählen Sie **Fehlerbehebungsoptionen** und drücken Sie die Eingabetaste.
3. Wählen Sie im Menü „Optionen für den Fehlerbehebungsmodus“ einen Dienst aus, der aktiviert werden soll.
   - Aktivieren von ESXi Shell
   - Aktivieren von SSH
4. Drücken Sie die Eingabetaste, um den Dienst zu starten.
5. Drücken Sie die Esc-Taste wiederholt, bis Sie zurück zum Hauptmenü der Benutzerschnittstelle der direkten Konsole gelangt sind.

Nächste Schritte

Legen Sie die Zeitüberschreitungswerte für die Verfügbarkeits- und Leerlaufzeiten der ESXi Shell fest. Weitere Informationen hierzu finden Sie unter Festlegen von Zeitüberschreitungswerten für Verfügbarkeit oder Leerlauf für die ESXi Shell.

Festlegen von Zeitüberschreitungswerten für Verfügbarkeit oder Leerlauf für die ESXi Shell

Standardmäßig ist die ESXi Shell deaktiviert. Zur Erhöhung der Sicherheit beim Aktivieren der Shell können Sie einen Zeitüberschreitungswert für Verfügbarkeit und/oder Leerlauf festlegen.

Die beiden Zeitüberschreitungstypen treten in verschiedenen Situationen auf.

Leerlauf-Zeitüberschreitung

Wenn ein Benutzer die ESXi Shell auf einem Host aktiviert, aber vergisst, sich von der Sitzung abzumelden, bleibt die Sitzung im Leerlauf für unbestimmte Zeit bestehen. Die offene Verbindung kann die Möglichkeit für einen privilegierten Zugriff auf den Host erhöhen. Diese Situation können Sie verhindern, indem Sie eine Zeitüberschreitung für Sitzungen im Leerlauf festlegen.

Verfügbarkeits-Zeitüberschreitung

Der Zeitüberschreitungswert für Verfügbarkeit bestimmt, wie viel Zeit bis zur Anmeldung nach der anfänglichen Aktivierung der Shell vergehen kann. Wenn Sie länger warten, wird der Dienst deaktiviert und eine Anmeldung bei der ESXi Shell ist nicht möglich.

Voraussetzungen

Aktivieren Sie die ESXi Shell. Weitere Informationen hierzu finden Sie unter Verwenden der Benutzerschnittstelle der direkten Konsole für den Zugriff auf die ESXi Shell.

Verfahren

1. Melden Sie sich beim ESXi Shell an.
2. Wählen Sie im Menü „Optionen für den Fehlerbehebungsmodus“ die Option **ESXi Shell- und SSH-Zeitüberschreitungen ändern** aus und drücken Sie die Eingabetaste.
3. Geben Sie den Zeitüberschreitungswert für Leerlauf (in Sekunden) oder den Zeitüberschreitungswert für Verfügbarkeit ein.

   Sie müssen den SSH-Dienst und den ESXi Shell-Dienst neu starten, damit die Einstellungen wirksam werden.
4. Drücken Sie wiederholt die Eingabetaste und die Esc-Taste, bis Sie zurück zum Hauptmenü der Benutzerschnittstelle der direkten Konsole gelangt sind.
5. Klicken Sie auf **OK**.

Ergebnisse

- Bei festgelegtem Zeitüberschreitungswert für Leerlauf werden Benutzer abgemeldet, wenn sich die Sitzung während des angegebenen Zeitraums im Leerlauf befindet.
- Wenn Sie den Zeitüberschreitungswert für Verfügbarkeit festlegen und sich nicht vor Ablauf dieses Zeitüberschreitungswerts anmelden, werden die Anmeldungen erneut deaktiviert.

Anmelden bei der ESXi Shell zur Fehlerbehebung

Führen Sie ESXi-Konfigurationsaufgaben mit vSphere Client, ESXCLI oder VMware PowerCLI aus. Melden Sie sich bei der ESXi Shell (vormals Support-Modus oder TSM) nur zwecks Fehlerbehebung an.

Verfahren

1. Melden Sie sich an der ESXi Shell mit einer der folgenden Methoden an:
   - Wenn Sie direkten Zugriff auf den Host haben, drücken Sie Alt+F1, um den Anmeldebildschirm auf der physischen Konsole der Maschine aufzurufen.
   - Wenn Sie eine Verbindung mit dem Host remote herstellen, verwenden Sie SSH oder eine andere Remote-Konsolenverbindung, um eine Sitzung auf dem Host zu starten.
2. Geben Sie einen Benutzernamen und ein Kennwort ein, die vom Host erkannt werden.

UEFI Secure Boot für ESXi-Hosts

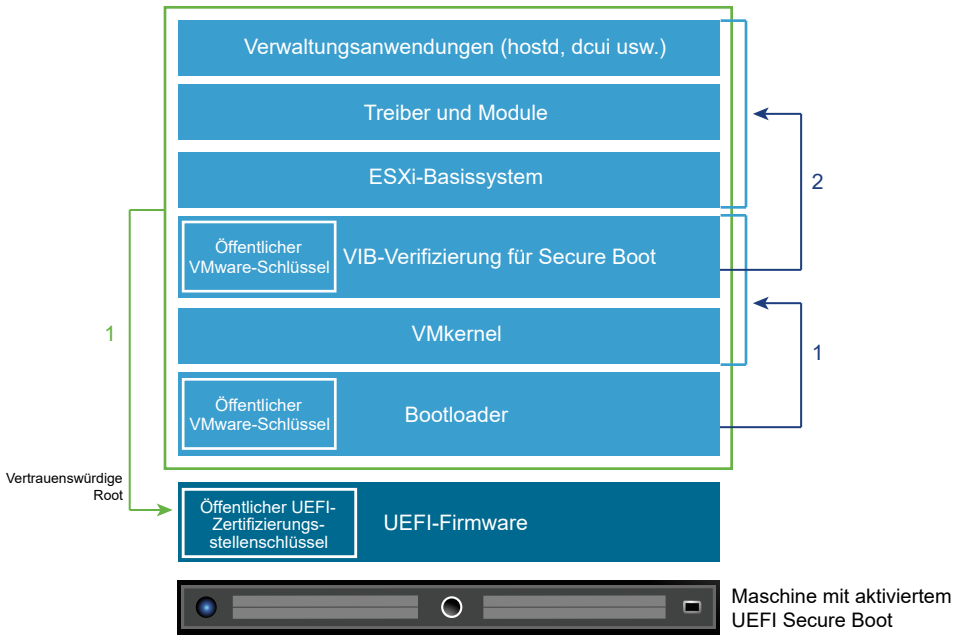
Secure Boot (sicherer Start) ist Bestandteil des UEFI-Firmwarestandards. Bei aktiviertem Secure Boot lädt eine Maschine UEFI-Treiber oder -Apps nur, wenn der Bootloader des Betriebssystems kryptografisch signiert ist. Ab vSphere 6.5 unterstützt ESXi den sicheren Start, falls die entsprechende Option in der Hardware aktiviert ist.

Verwendung von UEFI Secure Boot durch ESXi

ESXi Version 6.5 und höher unterstützt UEFI Secure Boot auf jeder Ebene des Boot-Stacks.

Hinweis Vor der Verwendung von UEFI Secure Boot auf einem aktualisierten Host überprüfen Sie die Kompatibilität anhand der Anweisungen unter Ausführen des Validierungsskripts für den sicheren Start auf einem aktualisierten ESXi-Host.

Abbildung 3-1. UEFI Secure Boot



Bei aktiviertem Secure Boot sieht die Startsequenz wie folgt aus.

1 Ab vSphere 6.5 enthält der ESXi-Bootloader einen öffentlichen VMware-Schlüssel. Der Bootloader überprüft mithilfe dieses Schlüssels die Signatur des Kernels und einen kleinen Teil des Systems, das eine VIB-Verifizierung für Secure Boot beinhaltet.

2 Die VIB-Verifizierung überprüft jedes im System installierte VIB-Paket.

Zu diesem Zeitpunkt wird das gesamte System gestartet, mit der vertrauenswürdigen Root in Zertifikaten, die Bestandteil der UEFI-Firmware sind.

Hinweis Wenn Sie vSphere 7.0 Update 2 oder höher installieren oder ein Upgrade auf diese Version durchführen und ein ESXi-Host über ein TPM verfügt, versiegelt das TPM die vertraulichen Informationen mithilfe einer TPM-Richtlinie. Diese basiert auf PCR-Werten für UEFI Secure Boot. Dieser Wert wird bei nachfolgenden Neustarts geladen, wenn die Richtlinie als wahr erfüllt ist. Informationen zum Deaktivieren oder Aktivieren von UEFI Secure Boot in vSphere 7.0 Update 2 oder höher finden Sie unter Aktivieren oder Deaktivieren der Secure Boot-Erzwingung für eine sichere ESXi-Konfiguration.

Fehlerbehebung bei UEFI Secure Boot

Wenn Secure Boot auf keiner Ebene der Startsequenz erfolgreich ist, wird ein Fehler gemeldet.

Die Fehlermeldung ist abhängig vom Hardwareanbieter und von der Ebene, auf der die Verifizierung fehlgeschlagen ist.

- Wenn Sie versuchen, mit einem nicht signierten oder manipulierten Bootloader zu starten, wird während der Startsequenz ein Fehler gemeldet. Die genaue Fehlermeldung ist abhängig vom Hardwareanbieter. Die Fehlermeldung kann so oder ähnlich wie die folgende Fehlermeldung lauten.

  ```
  UEFI0073: Unable to boot PXE Device...because of the Secure Boot policy
  ```

- Wenn der Kernel manipuliert wurde, wird eine Fehlermeldung ähnlich der folgenden angezeigt:

  ```
  Fatal error: 39 (Secure Boot Failed)
  ```

- Wenn ein Paket (VIB oder Treiber) manipuliert wurde, wird ein lilafarbener Bildschirm mit der folgenden Fehlermeldung angezeigt:

  ```
  UEFI Secure Boot failed:
  Failed to verify signatures of the following vibs (XX)
  ```

Führen Sie die folgenden Schritte aus, um Probleme mit Secure Boot zu beheben:

1 Führen Sie einen Neustart des Hosts mit deaktivierter Funktion für Secure Boot durch.

2 Führen Sie das Skript für die Prüfung des sicheren Starts aus (siehe Ausführen des Validierungsskripts für den sicheren Start auf einem aktualisierten ESXi-Host).

3 Analysieren Sie die Informationen in der Datei `/var/log/esxupdate.log`.

Ausführen des Validierungsskripts für den sicheren Start auf einem aktualisierten ESXi-Host

Nach dem Upgrade eines ESXi-Hosts von einer früheren ESXi-Version, die UEFI Secure Boot nicht unterstützte, können Sie möglicherweise den sicheren Start aktivieren. Ob Sie den sicheren Start aktivieren können, richtet sich danach, wie Sie das Upgrade durchgeführt haben und ob beim Upgrade alle vorhandenen VIBs ersetzt oder bestimmte VIBs unverändert belassen wurden. Sie können nach der Durchführung des Upgrades ein Validierungsskript ausführen, um festzustellen, ob der sichere Start von der aktualisierten Installation unterstützt wird.

Für eine erfolgreiche Durchführung des sicheren Starts müssen die Signaturen aller installierten VIBs auf dem System vorhanden sein. In älteren ESXi-Versionen werden die Signaturen beim Installieren von VIBs nicht gespeichert.

- Wenn Sie das Upgrade mithilfe von ESXCLI-Befehlen durchführen, führt die alte Version von ESXi die Installation der neuen VIBs durch, sodass ihre Signaturen nicht gespeichert werden und ein sicherer Start (Secure Boot) nicht möglich ist.
- Wenn Sie das Upgrade mithilfe des ISO-Images durchführen, werden die Signaturen der neuen VIBs gespeichert. Dies gilt auch für vSphere Lifecycle Manager-Upgrades, die das ISO-Image verwenden.

- Wenn alte VIBs auf dem System verbleiben, stehen die Signaturen dieser VIBs nicht zur Verfügung und ein sicherer Start ist nicht möglich.
  - Wenn das System einen Drittanbietertreiber verwendet und das VMware-Upgrade keine neue Version des Treiber-VIB enthält, verbleibt das alte VIB nach dem Upgrade auf dem System.
  - In seltenen Fällen stellt VMware die fortlaufende Entwicklung eines bestimmten VIB ein, ohne ein neues VIB bereitzustellen, das das alte ersetzt oder überflüssig macht. In diesem Fall verbleibt das alte VIB nach dem Upgrade auf dem System.

Hinweis Für den sicheren Start über UEFI ist außerdem ein aktueller Bootloader erforderlich. Mit diesem Skript wird nicht geprüft, ob ein aktueller Bootloader vorhanden ist.

Voraussetzungen

- Stellen Sie sicher, dass die Hardware den sicheren Start über UEFI unterstützt.
- Stellen Sie sicher, dass alle VIBs mindestens mit der Akzeptanzebene „PartnerSupported“ signiert sind. Wenn Sie VIBs auf der Ebene „CommunitySupported“ einbeziehen, können Sie den sicheren Start nicht verwenden.

Verfahren

1. Führen Sie ein Upgrade für ESXi durch und führen Sie den folgenden Befehl aus.

   ```
   /usr/lib/vmware/secureboot/bin/secureBoot.py -c
   ```

2. Prüfen Sie die Ausgabe.

   Die Ausgabe enthält entweder `Secure boot can be enabled` oder `Secure boot CANNOT be enabled`.

Sichern von ESXi-Hosts mit Trusted Platform Module

ESXi-Hosts können die Funktionalität von TPM-Chips (Trusted Platform Modules) nutzen. Hierbei handelt es sich um sichere Kryptoprozessoren, die die Hostsicherheit erhöhen, indem sie eine Zusicherung der Vertrauenswürdigkeit ermöglichen, die in Hardware und nicht in Software verankert ist.

TPM ist ein branchenweiter Standard für sichere Kryptoprozessoren. TPM-Chips sind in den meisten modernen Computern zu finden. Dies gilt gleichermaßen für Laptops, Desktop-Computer und sogar Server. vSphere 6.7 und höher unterstützt TPM Version 2.0.

Ein TPM 2.0-Chip bestätigt die Integrität der Identität eines ESXi-Hosts. Ein Host-Integritätsnachweis ist der Prozess der Authentifizierung und Bescheinigung des Zustands der Software eines Hosts zu einem bestimmten Zeitpunkt. Die Implementierung des UEFI Secure Boot-Mechanismus, der sicherstellt, dass beim Starten nur signierte Software geladen wird, ist eine Voraussetzung für einen erfolgreichen Integritätsnachweis. Der TPM 2.0-Chip zeichnet die Messungen der im System gestarteten Softwaremodule auf und speichert sie sicher ab, was extern von vCenter Server überprüft wird.

Der Fernbescheinigungsprozess umfasst die folgenden allgemeinen Schritte:

1 Stellen Sie die Vertrauenswürdigkeit des Remote-TPMs fest und erstellen Sie darauf basierend einen Integritätsnachweisschlüssel (Attestation Key, AK).

   Wenn ein ESXi-Host zu vCenter Server hinzugefügt, von dort aus neu gestartet oder erneut mit vCenter Server verbunden wird, fordert vCenter Server einen AK vom Host an. Ein Teil des AK-Erstellungsprozesses beinhaltet auch die Überprüfung der TPM-Hardware selbst, um sicherzustellen, dass sie von einem bekannten (und vertrauenswürdigen) Anbieter produziert wurde.

2 Rufen Sie den Integritätsnachweisbericht (Attestation Report) vom Host ab.

   vCenter Server verlangt, dass der Host einen Integritätsnachweisbericht sendet, der einen vom TPM signierten Auszug der Werte in den Platform Configuration Registers (PCRs) sowie andere signierte binäre Metadaten des Hosts enthält. Durch Überprüfung, ob die Informationen mit einer Konfiguration übereinstimmen, die er für vertrauenswürdig hält, identifiziert ein vCenter Server die Plattform auf einem zuvor nicht vertrauenswürdigen Host.

3 Überprüfen Sie die Authentizität des Hosts.

   vCenter Server prüft die Echtheit des signierten Datenauszugs, leitet die Softwareversionen ab und bestimmt deren Vertrauenswürdigkeit. Wenn vCenter Server feststellt, dass der signierte Auszug ungültig ist, schlägt die Fernbescheinigung fehl, und der Host gilt als nicht vertrauenswürdig.

Um einen TPM 2.0-Chip verwenden zu können, muss Ihre Umgebung vCenter Server die folgenden Anforderungen erfüllen:

- vCenter Server 6.7 oder höher
- ESXi 6.7-Host oder höher mit installiertem und in UEFI aktivierten TPM 2.0-Chip
- UEFI Secure Boot ist aktiviert

Stellen Sie sicher, dass das TPM im BIOS des ESXi-Hosts so konfiguriert ist, dass es den SHA-256-Hashing-Algorithmus und die TIS/FIFO-Schnittstelle (First-In, First-Out) verwendet und nicht CRB (Command Response Buffer). Informationen zum Einstellen dieser erforderlichen BIOS-Optionen finden Sie in der Dokumentation des Herstellers.

Überprüfen Sie die von VMware zertifizierten TPM 2.0-Chips unter

https://www.vmware.com/resources/compatibility/search.php

Wenn Sie einen ESXi-Host mit installiertem TPM 2.0-Chip starten, überwacht vCenter Server den Status des Host-Integritätsnachweises. Der vSphere Client zeigt den Status der Hardwarevertrauenswürdigkeit in vCenter Server auf der Registerkarte **Übersicht** unter **Sicherheit** mit den folgenden Alarmen an:

- Grün: Normaler Status, zeigt uneingeschränkte Vertrauenswürdigkeit an.
- Rot: Integritätsnachweis ist fehlgeschlagen.

Hinweis Wenn Sie einen TPM 2.0-Chip zu einem ESXi-Host hinzufügen, der von vCenter Server bereits verwaltet wird, müssen Sie zuerst den Host trennen und dann erneut verbinden. Informationen zum Trennen und Wiederverbinden von Hosts finden Sie in der *vCenter Server und Hostverwaltung*-Dokumentation.

 (Demonstration der ESXi- und Trusted Platform Module 2.0-Funktionen)

Überprüfen des Integritätsnachweis-Status eines ESXi-Hosts

Wenn einem ESXi-Host ein Trusted Platform Module 2.0-kompatibler Chip hinzugefügt wurde, bescheinigt dieser die Integrität der Plattform. Sie können den Integritätsnachweis-Status des Hosts im vSphere Client anzeigen. Sie können auch den Intel TXT-Status (Trusted Execution Technology) anzeigen.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Navigieren Sie zu einem Datencenter und klicken Sie auf die Registerkarte **Überwachen**.
3. Klicken Sie auf **Sicherheit**.
4. Überprüfen Sie den Host-Status in der Spalte „Integritätsnachweis“ und lesen Sie die begleitende Nachricht in der Spalte **Nachricht**.
5. Wenn es sich bei diesem Host um einen vertrauenswürdigen Host handelt, finden Sie weitere Informationen unter Anzeigen des Nachweisstatus des vertrauenswürdigen Clusters.

Nächste Schritte

Informationen zur Fehlerbehandlung bei einem Integritätsnachweis-Status „Fehlgeschlagen“ oder „Warnung“ finden Sie unter Beheben von Problemen beim ESXi-Hostnachweis. Weitere Informationen zu vertrauenswürdigen Hosts finden Sie unter Beheben von Problemen beim Nachweis des vertrauenswürdigen Hosts.

Beheben von Problemen beim ESXi-Hostnachweis

Wenn Sie ein Trusted Platform Module (TPM)-Gerät auf einem ESXi-Host installieren, kann der Host möglicherweise keinen Nachweis erbringen. Sie können die möglichen Ursachen für dieses Problem beheben.

Verfahren

1. Sehen Sie sich den Alarmstatus des ESXi-Hosts und die begleitende Fehlermeldung an. Weitere Informationen hierzu finden Sie unter Überprüfen des Integritätsnachweis-Status eines ESXi-Hosts.
2. Wenn die Fehlermeldung `Sicherer Start des Hosts wurde deaktiviert` lautet, müssen Sie den sicheren Start erneut aktivieren, um das Problem zu beheben.
3. Wenn der Beglaubigungsstatus des Hosts fehlgeschlagen ist, überprüfen Sie die vCenter Server-Datei `vpxd.log` auf folgende Meldung:

   ```
   Kein gecachter Identitätsschlüssel, Laden von der DB
   ```

   Diese Meldung zeigt an, dass Sie einen TPM 2.0-Chip zu einem ESXi-Host hinzufügen, der von vCenter Server bereits verwaltet wird. Sie müssen zuerst die Verbindung zum Host trennen und dann erneut verbinden. Informationen zum Trennen und Wiederverbinden von Hosts finden Sie in der *vCenter Server und Hostverwaltung*-Dokumentation.

   Weitere Informationen zu vCenter Server-Protokolldateien, einschließlich Speicherort und Protokollrotation, finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/1021804.
4. Wenden Sie sich bei allen anderen Fehlermeldungen an den Kunden-Support.

ESXi-Protokolldateien

Protokolldateien sind eine wichtige Komponente bei der Fehlersuche nach Angriffen und für die Suche nach Informationen über Sicherheitsverletzungen. Das Protokollieren auf einem sicheren, zentralen Protokollserver kann die Manipulation von Protokollen verhindern. Die Remoteprotokollierung bietet auch eine Möglichkeit zur Führung langfristiger Prüfungsaufzeichnungen.

Treffen Sie folgende Maßnahmen, um die Sicherheit des Hosts zu erhöhen.

- Konfigurieren Sie die dauerhafte Protokollierung in einem Datenspeicher. Standardmäßig werden die Protokolldateien auf ESXi-Hosts im speicherresidenten Dateisystem gespeichert. Sie gehen daher verloren, wenn Sie den Host neu starten, und Protokolldaten werden nur für 24 Stunden gespeichert. Wenn Sie die dauerhafte Protokollierung aktivieren, verfügen Sie über eine dedizierte Aufzeichnung der Aktivitäten für den Host.
- Mithilfe der Remoteprotokollierung auf einem zentralen Host können Sie Protokolldateien auf einem zentralen Host speichern. Über diesen Host können Sie alle Hosts mit einem einzigen Tool überwachen, zusammenfassende Analysen durchführen und Protokolldaten durchsuchen. Diese Vorgehensweise vereinfacht die Überwachung und macht Informationen zu koordinierten Angriffen auf mehreren Hosts verfügbar.
- Konfigurieren Sie das Remotesicherheits-Syslog auf ESXi-Hosts mithilfe von ESXCLI oder PowerCLI oder mithilfe eines API-Clients.

- Führen Sie eine Abfrage der Syslog-Konfiguration durch, um sicherzustellen, dass der Syslog-Server und der Port gültig sind.

In der Dokumentation *vSphere-Überwachung und -Leistung* finden Sie Informationen zum Syslog-Setup sowie zusätzliche Informationen zu ESXi-Protokolldateien.

Konfiguration von Syslog auf ESXi-Hosts

Sie können vSphere Client oder den Befehl `esxcli system syslog` zum Konfigurieren des Syslog-Dienstes verwenden.

Informationen zur Verwendung des `esxcli system syslog`-Befehls und anderen ESXCLI-Befehlen finden Sie unter *Erste Schritte mit ESXCLI*.

Verfahren

1. Navigieren Sie zum Host im Navigator von vSphere Client.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter „System“ auf **Erweiterte Systemeinstellungen**.
4. Klicken Sie auf **Bearbeiten**.
5. Filter für **`syslog`**.
6. Zum Einrichten einer globalen Protokollierung wählen Sie die zu ändernde Einstellung aus und geben Sie den Wert ein.

Option	Beschreibung
Syslog.global.defaultRotate	Maximale Anzahl der beizubehaltenden Archive. Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen.
Syslog.global.defaultSize	Standardgröße des Protokolls in KB, bevor das System eine Rotation der Protokolle durchführt. Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen.
Syslog.global.LogDir	Verzeichnis, in dem Protokolle gespeichert werden. Das Verzeichnis kann sich auf gemounteten NFS- oder VMFS-Volumes befinden. Nur das Verzeichnis `/scratch` auf dem lokalen Dateisystem bleibt nach einem Neustart konsistent. Geben Sie das Verzeichnis im Format [*Datenspeichername*] *Pfad_zur_Datei* an, wobei sich der Pfad auf das Stammverzeichnis des Volumes bezieht, in dem sich das Backing für den Datenspeicher befindet. Beispielsweise ist der Pfad `[storage1] /systemlogs` dem Pfad `/vmfs/volumes/storage1/systemlogs` zuzuordnen.

Option	Beschreibung
Syslog.global.logDirUnique	Durch die Auswahl dieser Option wird ein Unterverzeichnis mit dem Namen des ESXi-Hosts im von **Syslog.global.LogDir** angegebenen Verzeichnis erstellt. Ein eindeutiges Verzeichnis ist nützlich, wenn dasselbe NFS-Verzeichnis von mehreren ESXi-Hosts verwendet wird.
Syslog.global.LogHost	Remotehost, mit dem Syslog-Meldungen weitergeleitet werden, und Port, auf dem der Remotehost Syslog-Meldungen empfängt. Sie können das Protokoll und den Port einbeziehen, z. B. `ssl://Hostname1:1514`. UDP (nur an Port 514), TCP und SSL werden unterstützt. Beim Remotehost muss syslog installiert und ordnungsgemäß konfiguriert sein, damit die weitergeleiteten Syslog-Meldungen empfangen werden. Weitere Informationen zur Konfiguration des Remote-Hosts finden Sie in der Dokumentation für den auf dem Remote-Host installierten Syslog-Dienst. Sie können eine unbegrenzte Anzahl von Remote-Hosts verwenden, um Syslog-Server-Meldungen zu erhalten.

7 (Optional) So überschreiben Sie die Standardprotokollgröße und die Rotationsangaben für ein Protokoll:

   a Klicken Sie auf den Namen des Protokolls, das Sie anpassen möchten.

   b Geben Sie die Anzahl der Rotationen und die gewünschte Protokollgröße ein.

8 Klicken Sie auf **OK**.

Ergebnisse

Änderungen an der syslog-Option werden sofort wirksam.

Speicherorte der ESXi-Protokolldateien

ESXi zeichnet die Hostaktivität in Protokolldateien mithilfe eines syslog-Hilfsprogramms auf.

Tabelle 3-8. Speicherorte der ESXi-Protokolldateien

Komponente	Speicherort	Zweck
Authentifizierung	`/var/log/auth.log`	Enthält alle Ereignisse, die sich auf die Authentifizierung für das lokale System beziehen.
ESXi-Hostagenten-Protokoll	`/var/log/hostd.log`	Enthält Informationen zum Agenten, mit dem der ESXi-Host und seine virtuellen Maschinen verwaltet und konfiguriert werden.
Shell-Protokoll	`/var/log/shell.log`	Enthält einen Datensatz mit allen Befehlen, die in die ESXi-Shell eingegeben wurden, und Shell-Ereignisse (z. B. Zeitpunkt der Aktivierung der Shell).

Tabelle 3-8. Speicherorte der ESXi-Protokolldateien (Fortsetzung)

Komponente	Speicherort	Zweck
Systemmeldungen	`/var/log/syslog.log`	Enthält alle allgemeinen Protokollmeldungen und kann zur Fehlerbehebung verwendet werden. Diese Informationen befanden sich vorher in der Protokolldatei „messages“.
Protokoll des vCenter Server-Agenten	`/var/log/vpxa.log`	Enthält Informationen zu dem Agenten, der mit vCenter Server kommuniziert (wenn der Host von vCenter Server verwaltet wird).
virtuelle Maschinen	Dasselbe Verzeichnis wie für die Konfigurationsdateien der jeweiligen virtuellen Maschine mit der Bezeichnung `vmware.log` und `vmware*.log`. Beispiel: `/vmfs/volumes/datastore/virtual machine/vwmare.log`	Enthält Ereignisse der virtuellen Maschine, Informationen zum Systemausfall, den Status und die Aktivitäten von Tools, die Uhrzeitsynchronisierung, Änderungen an der virtuellen Hardware, vMotion-Migrationen, Maschinen-Klonvorgänge usw.
VMkernel	`/var/log/vmkernel.log`	Zeichnet Aktivitäten in Verbindung mit virtuellen Maschinen und ESXi auf.
VMkernel-Übersicht	`/var/log/vmksummary.log`	Wird verwendet, um die Betriebszeit und die Verfügbarkeitsstatistiken für ESXi (kommagetrennt) zu bestimmen.
VMkernel-Warnungen	`/var/log/vmkwarning.log`	Zeichnet Aktivitäten in Verbindung mit virtuellen Maschinen auf.
Schnellstart	`/var/log/loadESX.log`	Enthält alle Ereignisse bezüglich des Neustarts eines ESXi-Hosts mithilfe des Schnellstarts.
Agent der vertrauenswürdigen Infrastruktur	`/var/run/log/kmxa.log`	Zeichnet Aktivitäten im Zusammenhang mit dem Client-Dienst auf dem vertrauenswürdigen ESXi-Host auf.
Schlüsselanbieterdienst	`/var/run/log/kmxd.log`	Zeichnet Aktivitäten im Zusammenhang mit dem vSphere Trust Authority-Schlüsselanbieterdienst auf.
Bestätigungsdienst	`/var/run/log/attestd.log`	Zeichnet Aktivitäten im Zusammenhang mit dem vSphere Trust Authority-Bestätigungsdienst auf.

Tabelle 3-8. Speicherorte der ESXi-Protokolldateien (Fortsetzung)

Komponente	Speicherort	Zweck
ESX-Token-Dienst	`/var/run/log/esxtokend.log`	Zeichnet Aktivitäten im Zusammenhang mit dem vSphere Trust Authority-ESX-Token-Dienst auf.
ESX-API-Weiterleitung	`/var/run/log/esxapiadapter.log`	Zeichnet Aktivitäten im Zusammenhang mit der vSphere Trust Authority-API-Weiterleitung auf.

Sichern des Fault Tolerance-Protokollierungsdatenverkehrs

VMware Fault Tolerance (FT) erfasst Eingaben und Ereignisse einer primären virtuellen Maschine und sendet sie an eine sekundäre virtuelle Maschine, die auf einem anderen Host ausgeführt wird.

Dieser Datenverkehr für die Protokollierung zwischen den primären und sekundären virtuelle Maschinen erfolgt unverschlüsselt und enthält Gastnetzwerk- und Storage I/O-Daten sowie die Speicherinhalte des Gastbetriebssystems. Dieser Datenverkehr enthält möglicherweise vertrauliche Daten, wie z. B. Kennwörter im Klartext. Um zu verhindern, dass solche Daten preisgegeben werden, stellen Sie sicher, dass dieses Netzwerk gesichert ist, insbesondere gegen sogenannte „Man-in-the-middle“-Angriffe. Verwenden Sie z. B. ein privates Netzwerk für den Datenverkehr für die Fault Toleranceprotokollierung.

Aktivieren der Fault Tolerance-Vverschlüsselung

Sie können den Fault Tolerance-Protokolldatenverkehr verschlüsseln.

vSphere Fault Tolerance führt häufige Prüfungen zwischen einer primären und einer sekundären VM durch, damit die sekundäre VM vom letzten erfolgreichen Prüfpunkt aus schnell fortgesetzt werden kann. Der Prüfpunkt enthält den VM-Status, der seit dem vorherigen Prüfpunkt geändert wurde. Sie können den Fault Tolerance-Protokolldatenverkehr verschlüsseln.

Wenn Sie Fault Tolerance aktivieren, ist die FT-Verschlüsselung standardmäßig auf **Opportunistisch** festgelegt. Dies bedeutet, dass die Verschlüsselung nur aktiviert wird, wenn sowohl der primäre als auch der sekundäre Host verschlüsselt werden können. Befolgen Sie dieses Verfahren, wenn Sie den FT-Verschlüsselungsmodus manuell ändern müssen.

Hinweis Fault Tolerance unterstützt vSphere Virtual Machine Encryption mit vSphere 7.0 Update 2 und höher. Gastinterne und Array-basierte Verschlüsselung sind nicht von der VM-Verschlüsselung abhängig und stören sie nicht. Bei Verwendung mehrerer Verschlüsselungsschichten werden zusätzliche Computing-Ressourcen verwendet, was sich auf die Leistung der virtuellen Maschine auswirken kann. Die Auswirkung variiert je nach Hardware sowie der Menge und dem Typ der E/A, aber die Auswirkungen auf die Gesamtleistung sind für die meisten Arbeitslasten vernachlässigbar. Die Effektivität und Kompatibilität von Back-End-Speicherfunktionen wie Deduplizierung, Komprimierung und Replizierung kann auch von der VM-Verschlüsselung betroffen sein.

Voraussetzungen

Die FT-Verschlüsselung erfordert SMP-FT. Eine Verschlüsselung auf Legacy FT (Record-Replay FT) wird nicht unterstützt.

Verfahren

1 Wählen Sie die VM und dann **Einstellungen bearbeiten** aus.

2 Wählen Sie unter **VM-Optionen** das Dropdown-Menü **Verschlüsselte FT** aus.

3 Wählen Sie eine der folgenden Optionen aus:

Option	Beschreibung
Deaktiviert	Schalten Sie die verschlüsselte Fault Tolerance-Protokollierung nicht ein.
Opportunistisch	Aktivieren Sie die Verschlüsselung nur, wenn beide Seiten dazu in der Lage sind. Eine Fault Tolerance-VM kann auf einen ESXi-Host verschoben werden, der keine verschlüsselte Fault Tolerance-Protokollierung unterstützt.
Erforderlich	Wählen Sie Hosts für die primäre und sekundäre Fault Tolerance aus, die beide die verschlüsselte FT-Protokollierung unterstützen.

Hinweis Während die VM-Verschlüsselung aktiviert ist, ist der FT-Verschlüsselungsmodus standardmäßig auf **Erforderlich** festgelegt und kann nicht geändert werden.

Wenn der FT-Verschlüsselungsmodus auf **Erforderlich** festgelegt ist:

- Wenn Sie FT aktivieren, werden nur Hosts für die Platzierung der sekundären FT-Verschlüsselung aufgelistet, welche die FT-Verschlüsselung unterstützen.
- FT-Failover kann nur auf den von der FT-Verschlüsselung unterstützten Hosts erfolgen.

4 Klicken Sie auf **OK**.

Verwalten von ESXi-Überwachungsdatensätzen

Überwachungsdatensätze entsprechen RFC 5424 und enthalten Informationen zu Ereignissen in Bezug auf Elemente wie Zeit, Status, Beschreibung und Benutzerinformationen, die für Ereignisse protokolliert wurden, die bei Aktionen auf ESXi-Hosts aufgetreten sind. Sowohl lokale als auch Remote-Überwachungsdatensätze sind verfügbar. Die Aufbewahrung von Überwachungsdatensätzen ist standardmäßig deaktiviert. Sie müssen den lokalen und den Remoteüberwachungsmodus manuell aktivieren.

Das lokale ESXi-Überwachungsprotokoll fungiert als Puffer mit fester Größe für kürzlich ausgegebene Überwachungsmeldungen. Wenn der Puffer mit Meldungen gefüllt ist, werden die ältesten Datensätze von neuen Datensätzen überschrieben. Das Remote-Überwachungsprotokoll leitet denselben Stream von Überwachungsdatensätzen entweder unverschlüsselt oder verschlüsselt (RFC 5425) in einem Syslog-Standardformat (RFC 3164) an einen Remoteserver weiter. Überwachungsmeldungen entsprechen RFC 5424, allgemeine Syslog-Meldungen entsprechen jedoch nur RFC 3164. Das System sendet eine generierte Überwachungsmeldung gleichzeitig an den lokalen Speicher und den Remotespeicher.

Während des Verlusts der Verbindung zwischen dem Host und dem Remotespeicher löscht der Remotespeicher alle generierten Überwachungsmeldungen. Bei einer erneuten Verbindung generiert das System eine Überwachungsmeldung, die auf einen potenziellen Verlust von Meldungen hinweist.

Konfigurieren von Überwachungsdatensätzen

Sie konfigurieren die lokale Aufbewahrung von Überwachungsdatensätzen mithilfe von ESXCLI. Weitere Informationen finden Sie in *ESXCLI – Referenz* unter https://code.vmware.com/.

Anzeigen von Überwachungsdatensätzen

Sie können die Überwachungsdatensätze wie folgt anzeigen.

- Lokal: Verwenden Sie die ESXi-Anwendung `/bin/viewAudit`.
- Remote: Konfigurieren Sie mithilfe von ESXCLI einen Remote-Überwachungsserver.

Sie können auch die FetchAuditRecords-API (im verwalteten DiagnosticsManager-Objekt) verwenden, um Überwachungsdatensätze anzuzeigen.

Sichern der ESXi-Konfiguration

Ab der vSphere 7.0 Update 2 ist die ESXi-Konfiguration durch Verschlüsselung geschützt. Wenn ein ESXi-Host optional durch ein TPM geschützt ist, wird der Verschlüsselungsschlüssel für die ESXi-Konfiguration durch das TPM versiegelt.

Viele ESXi-Dienste speichern geheime Schlüssel in ihren Konfigurationsdateien. Diese Konfigurationen werden in einer Startbank des ESXi-Hosts als archivierte Datei beibehalten. Ab vSphere 7.0 Update 2 ist diese archivierte Datei verschlüsselt. Dies führt dazu, dass Angreifer diese Datei nicht direkt lesen oder ändern können, selbst wenn sie physischen Zugriff auf den Speicher des ESXi-Hosts haben.

Zusätzlich zur Verhinderung des Zugriffs eines Angreifers auf geheime Schlüssel kann eine sichere ESXi-Konfiguration bei Verwendung eines TPM die Verschlüsselungsschlüssel der virtuellen Maschine über Neustarts hinweg speichern. Daher können verschlüsselte Arbeitslasten weiterhin funktionieren, wenn ein Schlüsselserver nicht verfügbar oder nicht erreichbar ist. Weitere Informationen hierzu finden Sie unter Schlüsselpersistenz – Übersicht.

Sichern der ESXi-Konfiguration – Übersicht

Sie müssen die Verschlüsselung der ESXi-Konfiguration nicht manuell aktivieren. Wenn Sie vSphere 7.0 Update 2 oder höher installieren oder aktualisieren, ist die archivierte ESXi-Konfigurationsdatei verschlüsselt.

Vor vSphere 7.0 Update 2 ist die archivierte ESXi-Konfigurationsdatei nicht verschlüsselt. In vSphere 7.0 Update 2 und höher ist die archivierte Konfigurationsdatei verschlüsselt. Wenn der ESXi-Host mit einem Trusted Platform Module (TPM) konfiguriert ist, wird das TPM zum „Versiegeln“ der Konfiguration für den Host verwendet, was eine starke Sicherheitsgarantie bietet.

ESXi-Konfigurationsdateien vor vSphere 7.0 Update 2 – Übersicht

Die Konfiguration eines ESXi-Hosts besteht aus Konfigurationsdateien für jeden Dienst, der auf dem Host ausgeführt wird. Die Konfigurationsdateien befinden sich in der Regel im Verzeichnis `/etc/`, aber sie können sich auch in anderen Namespaces befinden. Die Konfigurationsdateien enthalten Laufzeitinformationen über den Status der Dienste. Im Laufe der Zeit können sich die Standardwerte in den Konfigurationsdateien ändern, z. B. wenn Sie Einstellungen auf dem ESXi-Host ändern. Ein Cron-Auftrag sichert die ESXi-Konfigurationsdateien regelmäßig, oder wenn ESXi ordnungsgemäß heruntergefahren wird, oder bei Bedarf, und erstellt eine archivierte Konfigurationsdatei in der Startbank. Wenn ESXi neu startet, wird die archivierte Konfigurationsdatei gelesen und der Zustand wird wiederhergestellt, in dem sich ESXi befand, als die Sicherung erstellt wurde. Vor vSphere 7.0 Update 2 ist die archivierte Konfigurationsdatei unverschlüsselt. Dies führt dazu, dass ein Angreifer, der Zugriff auf den physischen ESXi-Speicher hat, diese Datei lesen und ändern kann, während das System offline ist.

Sichere ESXi-Konfiguration – Übersicht

Beim ersten Start nach der Installation oder dem Upgrade des ESXi-Hosts auf vSphere 7.0 Update 2 oder höher tritt Folgendes auf:

- Wenn der ESXi-Host über ein TPM verfügt und in der Firmware aktiviert ist, wird die archivierte Konfigurationsdatei mit einem im TPM gespeicherten Verschlüsselungsschlüssel verschlüsselt. Ab diesem Zeitpunkt wird die Konfiguration des Hosts durch das TPM versiegelt.
- Wenn der ESXi-Host nicht über ein TPM verfügt, verwendet ESXi eine Schlüsselableitungsfunktion (Key Derivation Function, KDF), um einen sicheren Verschlüsselungsschlüssel für die Konfiguration der archivierten Konfigurationsdatei zu generieren. Die Eingaben für KDF werden auf der Festplatte in der Datei `encryption.info` gespeichert.

Hinweis Wenn ein ESXi-Host über ein aktiviertes TPM-Gerät verfügt, erhalten Sie zusätzlichen Schutz.

Wenn der ESXi-Host nach dem ersten Start neu gestartet wird, tritt Folgendes auf:

- Wenn der ESXi-Host über ein TPM verfügt, muss der Host den Verschlüsselungsschlüssel vom TPM für diesen spezifischen Host abrufen. Wenn die TPM-Messungen der Versiegelungsrichtlinie entsprechen, die beim Erstellen des Verschlüsselungsschlüssels verwendet wurde, erhält der Host den Verschlüsselungsschlüssel vom TPM.
- Wenn der ESXi-Host nicht über ein TPM verfügt, liest ESXi Informationen aus der Datei `encryption.info` um die sichere Konfiguration zu entsperren.

Anforderungen für die sichere ESXi-Konfiguration

- ESXi 7.0 Update 2 oder höher
- TPM 2.0 für Konfigurationsverschlüsselung und die Möglichkeit, eine Versiegelungsrichtlinie zu verwenden

Wiederherstellungsschlüssel für die sichere ESXi-Konfiguration

Eine sichere ESXi-Konfiguration beinhaltet einen Wiederherstellungsschlüssel. Wenn Sie die sichere ESXi-Konfiguration wiederherstellen müssen, verwenden Sie einen Wiederherstellungsschlüssel, dessen Inhalt Sie als Befehlszeilen-Startoption eingeben. Sie können den Wiederherstellungsschlüssel auflisten, um eine Sicherung des Wiederherstellungsschlüssels zu erstellen. Sie können den Wiederherstellungsschlüssel auch im Rahmen Ihrer Sicherheitsanforderungen rotieren.

Die Sicherung des Wiederherstellungsschlüssels ist ein wichtiger Bestandteil der Verwaltung Ihrer sicheren ESXi-Konfiguration. vCenter Server generiert einen Alarm, um Sie daran zu erinnern, den Wiederherstellungsschlüssel zu sichern.

Alarm für Wiederherstellungsschlüssel

Die Sicherung des Wiederherstellungsschlüssels ist ein wichtiger Bestandteil der Verwaltung Ihrer sicheren ESXi-Konfiguration. Wenn ein ESXi-Host im TPM-Modus mit dem vCenter Server verbunden oder erneut verbunden wird, generiert vCenter Server einen Alarm, um Sie daran zu erinnern, den Wiederherstellungsschlüssel zu sichern. Wenn Sie den Alarm zurücksetzen, wird er nicht erneut ausgelöst, es sei denn, die Bedingungen ändern sich.

Empfohlene Vorgehensweisen für die sichere ESXi-Konfiguration

Befolgen Sie diese empfohlenen Vorgehensweisen für den Wiederherstellungsschlüssel:

- Wenn Sie einen Wiederherstellungsschlüssel auflisten, wird er vorübergehend in einer nicht vertrauenswürdigen Umgebung angezeigt und befindet sich im Arbeitsspeicher. Entfernen Sie Ablaufverfolgungen des Schlüssels.
  - Durch den Neustart des Hosts wird der verbleibende Schlüssel im Arbeitsspeicher entfernt.
  - Für erweiterten Schutz können Sie den Verschlüsselungsmodus auf dem Host aktivieren. Weitere Informationen hierzu finden Sie unter Explizites Aktivieren des Hostverschlüsselungsmodus.
- Vorgehensweise beim Durchführen einer Wiederherstellung:
  - Um Ablaufverfolgungen des Wiederherstellungsschlüssels in einer nicht vertrauenswürdigen Umgebung zu eliminieren, starten Sie den Host neu.
  - Um die Sicherheit zu verbessern, rotieren Sie den Wiederherstellungsschlüssel, um einen neuen Schlüssel zu verwenden, nachdem Sie den Schlüssel einmal wiederhergestellt haben.

Übersicht über TPM-Versiegelungsrichtlinien

In vSphere 7.0 Update 2 und höher verwendet ein ESXi-Host das TPM, um die Konfiguration des Hosts mit einer Richtlinie für das Platform Configuration Register (PCR) zu versiegeln. Die PCR-Richtlinie kann so konfiguriert werden, dass UEFI Secure Boot und andere Einstellungen erzwungen werden.

Ein TPM kann mithilfe von PCR-Messungen (Platform Configuration Register) Richtlinien implementieren, die den nicht autorisierten Zugriff auf vertrauliche Daten beschränken. Wenn Sie einen ESXi-Host mit einem TPM installieren oder ein Upgrade auf vSphere 7.0 Update 2 und höher durchführen, versiegelt das TPM die vertraulichen Informationen mithilfe einer Richtlinie, die die Einstellung für den sicheren Start enthält. Diese Richtlinie überprüft, dass, wenn der sichere Start aktiviert war, als Daten zum ersten Mal mit dem TPM versiegelt wurden, der sichere Start immer noch aktiviert sein muss, wenn versucht wird, die Daten bei einem nachfolgenden Start zu entsiegeln.

Secure Boot (sicherer Start) ist Bestandteil des UEFI-Firmwarestandards. Bei aktiviertem UEFI Secure Boot lädt ein Host einen UEFI-Treiber oder -Apps nur, wenn der Bootloader des Betriebssystems über ein gültige digitale Signatur verfügt.

Sie können die UEFI Secure Boot-Erzwingung deaktivieren oder aktivieren. Weitere Informationen hierzu finden Sie unter Aktivieren oder Deaktivieren der Secure Boot-Erzwingung für eine sichere ESXi-Konfiguration.

Hinweis Wenn Sie bei der Installation von oder beim Upgrade auf vSphere 7.0 Update 2 oder höher kein TPM aktivieren, ist dies zu einem späteren Zeitpunkt mithilfe des folgenden Befehls möglich.

```
esxcli system settings encryption set --mode=TPM
```

Nach Aktivierung des TPM können Sie die Einstellung nicht mehr rückgängig machen.

Der Befehl `esxcli system settings encryption set` schlägt auf manchen TPMs selbst dann fehl, wenn das jeweilige TPM für den Host aktiviert ist.

- In vSphere 7.0 Update 2: TPMs von NationZ (NTZ), Infineon Technologies (IFX) und bestimmte neue Modelle (wie NPCT75x) von Nuvoton Technologies Corporation (NTC)
- In vSphere 7.0 Update 3: TPMs von NationZ (NTZ)

Wenn eine Installation oder ein Upgrade von vSphere 7.0 Update 2 das TPM beim ersten Start nicht verwenden kann, wird die Installation oder das Upgrade fortgesetzt, und der Modus wird standardmäßig auf KEINE (d. h. `--mode=NONE`) festgelegt. Das resultierende Verhalten sieht so aus, als ob das TPM nicht aktiviert ist.

Das TPM kann auch die Einstellung für die Startoption „execInstalledOnly“ in der Versiegelungsrichtlinie erzwingen. Die Erzwingung „execInstalledOnly“ ist eine erweiterte ESXi-Startoption, mit der garantiert wird, dass der VMkernel nur Binärdateien ausführt, die ordnungsgemäß verpackt und als Teil eines VIB signiert wurden. Die Startoption „execInstalledOnly“ ist von der Option für den sicheren Start abhängig. Die Erzwingung

des sicheren Starts muss aktiviert sein, bevor Sie die Startoption „execInstalledOnly“ in der Versiegelungsrichtlinie erzwingen können. Weitere Informationen hierzu finden Sie unter Aktivieren oder Deaktivieren der execInstalledOnly-Erzwingung für eine sichere ESXi-Konfiguration.

Verwalten einer sicheren ESXi-Konfiguration

Sie können ESXCLI-Befehle verwenden, um den Wiederherstellungsschlüssel für die sichere ESXi-Konfiguration anzuzeigen, den Wiederherstellungsschlüssel zu rotieren und die TPM-Richtlinien zu ändern (z. B. Erzwingen von UEFI Secure Boot).

Auflisten der Inhalte des Wiederherstellungsschlüssels für die sichere ESXi-Konfiguration

Sie können ESXCLI verwenden, um den Inhalt des Wiederherstellungsschlüssels für die sichere ESXi-Konfiguration anzuzeigen.

Diese Aufgabe gilt nur für einen ESXi-Host, der über ein TPM verfügt. Im Allgemeinen listen Sie den Inhalt des Wiederherstellungsschlüssels für die sichere ESXi-Konfiguration auf, um eine Sicherung zu erstellen, oder als Teil der rotierenden Wiederherstellungsschlüssel.

Voraussetzungen

- Zugriff auf den ESXCLI-Befehlssatz. Sie können ESXCLI-Befehle remote oder in der ESXi-Shell ausführen.
- Notwendige Berechtigung zur Verwendung der eigenständigen ESXCLI-Version oder über PowerCLI: **Host.Config.Settings**

Verfahren

1. Führen Sie den folgenden Befehl auf dem ESXi-Host aus.

   ```
   esxcli system settings encryption recovery list
   ```

2. Speichern Sie die Ausgabe an einem sicheren Remotespeicherort als Sicherung, falls Sie die sichere Konfiguration wiederherstellen müssen.

Ergebnisse

Die Wiederherstellungsschlüssel-ID und der Schlüssel werden angezeigt.

Beispiel: Auflisten des Wiederherstellungsschlüssels für die sichere ESXi-Konfiguration

```
[root@host1] esxcli system settings encryption recovery list

Recovery ID                              Key
---------------------------------------  ---
{2DDD5424-7F3F-406A-8DA8-D62630F6C8BC}
478269-039194-473926-430939-686855-231401-642208-184477-602511
-225586-551660-586542-338394-092578-687140-267425
```

Rotieren des Wiederherstellungsschlüssels für die sichere ESXi-Konfiguration

Sie können ESXCLI verwenden, um den Wiederherstellungsschlüssel für die sichere ESXi-Konfiguration zu rotieren.

Diese Aufgabe gilt nur für einen ESXi-Host, der über ein TPM verfügt. Sie können den Wiederherstellungsschlüssel für die sichere ESXi-Konfiguration im Rahmen der Best Practices für die Sicherheit rotieren.

Voraussetzungen

- Zugriff auf den ESXCLI-Befehlssatz. Sie können ESXCLI-Befehle remote oder in der ESXi-Shell ausführen.
- Notwendige Berechtigung zur Verwendung der eigenständigen ESXCLI-Version oder über PowerCLI: **Host.Config.Settings**

Verfahren

1. Listet den Wiederherstellungsschlüssel auf.

   Weitere Informationen hierzu finden Sie unter Auflisten der Inhalte des Wiederherstellungsschlüssels für die sichere ESXi-Konfiguration.

2. Führen Sie den folgenden Befehl aus.

   ```
   esxcli system settings encryption recovery rotate [-k keyID] -u uuid
   ```

   In diesem Befehl ist die optionale *keyID* die Schlüssel-ID im VMkernel-Schlüssel-Cache und *uuid* die Wiederherstellungs-ID (erhalten über den Befehl `esxcli system settings encryption recovery list`). Wenn Sie die optionale Schlüssel-ID nicht angeben, ersetzt ESXi den alten Wiederherstellungsschlüssel durch einen neuen, der zufällig generiert wird.

Ergebnisse

Der Wiederherstellungsschlüssel ist jetzt auf den Inhalt des Schlüssels festgelegt, auf den die Schlüssel-ID verweist (sofern sie bereitgestellt wurde). Andernfalls stellt ESXi eine neue Schlüssel-ID bereit.

Fehlerbehebung und Wiederherstellung der sicheren ESXi-Konfiguration

Sie können Probleme beim Starten beheben und wiederherstellen, die bei einer sicheren ESXi-Konfiguration auftreten können.

Wenn Sie ein TPM löschen (d. h. die Seed-Werte im TPM werden zurückgesetzt) oder wenn ein TPM fehlschlägt, müssen Sie Schritte zum Wiederherstellen der sicheren ESXi-Konfiguration durchführen. Sie müssen über den Wiederherstellungsschlüssel verfügen, um die Konfiguration wiederherstellen zu können. Bis Sie die Konfiguration wiederherstellen, kann der ESXi-Host nicht gestartet werden. Weitere Informationen hierzu finden Sie unter Wiederherstellen der sicheren ESXi-Konfiguration.

Obwohl es eher ungewöhnlich ist, ist es möglich, dass ein ESXi-Host die sichere Konfiguration nicht wiederherstellen oder entschlüsseln kann, was dazu führen kann, dass der Host nicht gestartet wird. Mögliche Situationen:

- Zur Einstellung für sicheren Start (oder andere Richtlinie) wechseln
- Tatsächliche Manipulation
- Der Wiederherstellungsschlüssel ist nicht verfügbar

Weitere Informationen zur Fehlerbehebung bei diesen Bedingungen finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/kb/81446.

Wiederherstellen der sicheren ESXi-Konfiguration

Wenn ein TPM fehlschlägt oder wenn Sie ein TPM löschen, müssen Sie die sichere ESXi-Konfiguration wiederherstellen. Bis Sie die Konfiguration wiederherstellen, kann der ESXi-Host nicht gestartet werden.

Die Wiederherstellung der ESXi-Konfiguration bezieht sich auf die folgenden Situationen:

- Sie haben das TPM gelöscht (d. h., die Speicher im TPM wurden zurückgesetzt).
- Das TPM ist fehlgeschlagen.

Informationen zur Behebung anderer Probleme bei der sicheren ESXi-Konfiguration finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/kb/81446.

Führen Sie eine manuelle Wiederherstellung aus. Führen Sie die Wiederherstellung nicht als Teil eines Installations- oder Upgrade-Skripts durch.

Voraussetzungen

Rufen Sie Ihren Wiederherstellungsschlüssel ab. Sie sollten zuvor den Wiederherstellungsschlüssel aufgelistet und gespeichert haben. Weitere Informationen hierzu finden Sie unter Auflisten der Inhalte des Wiederherstellungsschlüssels für die sichere ESXi-Konfiguration.

Verfahren

1. (Optional) Wenn das TPM fehlgeschlagen ist, verschieben Sie die Festplatte (mit der Startbank) auf einen anderen Host mit einem TPM.
2. Starten Sie den ESXi-Host.
3. Wenn das ESXi-Installationsprogramms angezeigt wird, drücken Sie Umschalt+O, um die Startoptionen zu bearbeiten.
4. Geben Sie an der Eingabeaufforderung die Startoption zum Wiederherstellen der Konfiguration ein.

   ```
   encryptionRecoveryKey=recovery_key
   ```

   Die sichere ESXi-Konfiguration wird wiederhergestellt, und der ESXi-Host wird gestartet.

5 Geben Sie zum Beibehalten der Änderung den folgenden Befehl ein:

```
/sbin/auto-backup.sh
```

Nächste Schritte

Wenn Sie den Wiederherstellungsschlüssel eingeben, wird er vorübergehend in einer nicht vertrauenswürdigen Umgebung angezeigt und befindet sich im Arbeitsspeicher. Damit der Schlüssel vollständig aus dem Arbeitsspeicher entfernt wird, empfiehlt es sich als Best Practice (nicht erforderlich), den Host neu zu starten. Sie können den Link auch rotieren. Weitere Informationen hierzu finden Sie unter Rotieren des Wiederherstellungsschlüssels für die sichere ESXi-Konfiguration.

Aktivieren oder Deaktivieren der Secure Boot-Erzwingung für eine sichere ESXi-Konfiguration

Sie können UEFI Secure Boot-Erzwingung aktivieren oder eine zuvor aktivierte UEFI Secure Boot-Erzwingung deaktivieren. Sie müssen ESXCLI verwenden, um die Einstellung im TPM auf dem ESXi-Host zu ändern.

Diese Aufgabe gilt nur für ESXi-Hosts, die über ein TPM verfügen. Bei UEFI Secure Boot handelt es sich um eine Firmware-Einstellung, mit der sichergestellt wird, dass die von der Firmware gestartete Software vertrauenswürdig ist. Die Aktivierung von UEFI Secure Boot kann bei jedem Start mithilfe des TPM erzwungen werden.

Voraussetzungen

- Zugriff auf den ESXCLI-Befehlssatz. Sie können ESXCLI-Befehle remote oder in der ESXi-Shell ausführen.
- Notwendige Berechtigung zur Verwendung der eigenständigen ESXCLI-Version oder über PowerCLI: **Host.Config.Settings**

Verfahren

1 Listen Sie die aktuellen Einstellungen auf dem ESXi-Host auf.

```
esxcli system settings encryption get
   Mode: TPM
   Require Executables Only From Installed VIBs: false
   Require Secure Boot: true
```

Bei aktivierter Secure Boot-Erzwingung wird „True“ für „Secure Boot anfordern“ angezeigt. Bei deaktivierter Secure Boot-Erzwingung wird „False“ für „Secure Boot anfordern“ angezeigt.

Wenn als Modus KEINE angezeigt wird, müssen Sie das TPM in der Firmware des Hosts aktivieren und den Modus durch Ausführen des folgenden Befehls festlegen:

```
esxcli system settings encryption set --mode=TPM
```

2 Aktivieren oder deaktivieren Sie Secure Boot-Erzwingung.

Option	Beschreibung

Aktivieren	a Fahren Sie den Host ordnungsgemäß herunter.
	Beispiel: Klicken Sie mit der rechten Maustaste auf den ESXi-Host im vSphere Client und wählen Sie **Betrieb > Herunterfahren** aus.
	b Aktivieren Sie „Secure Boot“ in der Firmware des Hosts.
	Weitere Informationen finden Sie in der Hardwaredokumentation Ihres Anbieters.
	c Starten Sie den Host neu.
	d Führen Sie den folgenden ESXCLI-Befehl aus.
	`esxcli system settings encryption set --require-secure-boot=T`
	e Überprüfen Sie die Änderung.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: true`
	Bestätigen Sie, dass „True“ für „Secure Boot anfordern“ angezeigt wird.
	f Führen Sie zum Speichern der Einstellung folgenden Befehl aus:
	`/sbin/auto-backup.sh`

Deaktivieren	a Führen Sie den folgenden ESXCLI-Befehl aus.
	`esxcli system settings encryption set --require-secure-boot=F`
	b Überprüfen Sie die Änderung.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: false`
	Bestätigen Sie, dass „False“ für „Secure Boot anfordern“ angezeigt wird.
	c Führen Sie zum Speichern der Einstellung folgenden Befehl aus:
	`/sbin/auto-backup.sh`
	Sie können „Secure Boot“ in der Firmware des Hosts deaktivieren. Zum gegenwärtigen Zeitpunkt besteht die Abhängigkeit zwischen der Firmware-Einstellung und der TPM-Erzwingung jedoch nicht mehr.

Ergebnisse

Der ESXi-Host wird je nach Benutzerauswahl mit aktivierter oder deaktivierter Secure Boot-Erzwingung ausgeführt.

Hinweis Wenn Sie bei der Installation von oder beim Upgrade auf vSphere 7.0 Update 2 oder höher kein TPM aktivieren, ist dies zu einem späteren Zeitpunkt mithilfe des folgenden Befehls möglich.

```
esxcli system settings encryption set --mode=TPM
```

Nach Aktivierung des TPM können Sie die Einstellung nicht mehr rückgängig machen.

Der Befehl `esxcli system settings encryption set` schlägt auf manchen TPMs selbst dann fehl, wenn das jeweilige TPM für den Host aktiviert ist.

- In vSphere 7.0 Update 2: TPMs von NationZ (NTZ), Infineon Technologies (IFX) und bestimmte neue Modelle (wie NPCT75x) von Nuvoton Technologies Corporation (NTC)
- In vSphere 7.0 Update 3: TPMs von NationZ (NTZ)

Wenn eine Installation oder ein Upgrade von vSphere 7.0 Update 2 das TPM beim ersten Start nicht verwenden kann, wird die Installation oder das Upgrade fortgesetzt, und der Modus wird standardmäßig auf KEINE (d. h. `--mode=NONE`) festgelegt. Das resultierende Verhalten sieht so aus, als ob das TPM nicht aktiviert ist.

Aktivieren oder Deaktivieren der execInstalledOnly-Erzwingung für eine sichere ESXi-Konfiguration

Sie können execInstalledOnly-Erzwingung aktivieren oder eine zuvor aktivierte execInstalledOnly-Erzwingung deaktivieren. Sie müssen ESXCLI verwenden, um die Einstellung im TPM auf dem ESXi-Host zu ändern. UEFI Secure Boot-Erzwingung muss aktiviert sein. Erst dann kann die execInstalledOnly-Erzwingung aktiviert werden.

Diese Aufgabe gilt nur für ESXi-Hosts, die über ein TPM verfügen. Unter der Voraussetzung, dass die erweiterte ESXi-Startoption „execInstalledOnly“ auf TRUE festgelegt ist, wird garantiert, dass der VMkernel nur diejenigen Binärdateien ausführt, die als Teil des VIB gepackt und signiert wurden. Die Aktivierung dieser Startoption kann bei jedem Start mithilfe des TPM erzwungen werden.

Voraussetzungen

- Zum Aktivieren der execInstalledOnly-Erzwingung müssen Sie zuerst die UEFI Secure Boot-Erzwingung aktivieren. Die execInstalledOnly-Erzwingung baut auf der UEFI Secure Boot-Erzwingung auf. Weitere Informationen hierzu finden Sie unter Aktivieren oder Deaktivieren der Secure Boot-Erzwingung für eine sichere ESXi-Konfiguration.
- Zugriff auf den ESXCLI-Befehlssatz. Sie können ESXCLI-Befehle remote oder in der ESXi-Shell ausführen.

- Notwendige Berechtigung zur Verwendung der eigenständigen ESXCLI-Version oder über PowerCLI: **Host.Config.Settings**

Verfahren

1 Listen Sie die aktuellen Einstellungen auf dem ESXi-Host auf.

```
esxcli system settings encryption get
   Mode: TPM
   Require Executables Only From Installed VIBs: false
   Require Secure Boot: true
```

Bei aktivierter execInstalledOnly-Erzwingung wird „True“ für „Ausführbare Dateien nur aus installierten VIBs anfordern“ angezeigt. Bei deaktivierter execInstalledOnly-Erzwingung wird „False“ für „Ausführbare Dateien nur aus installierten VIBs anfordern“ angezeigt. Zum Aktivieren der execInstalledOnly-Erzwingung muss die Secure Boot-Erzwingung aktiviert sein, und „Secure Boot anfordern“ ist in diesem Fall auf „True“ festgelegt.

Wenn als Modus KEINE angezeigt wird, müssen Sie das TPM in der Firmware des Hosts aktivieren und den Modus durch Ausführen des folgenden Befehls festlegen:

```
esxcli system settings encryption set --mode=TPM
```

Wenn „Secure Boot anfordern“ auf „False“ festgelegt ist, finden Sie unter Aktivieren oder Deaktivieren der Secure Boot-Erzwingung für eine sichere ESXi-Konfiguration Informationen zum Aktivieren der Erzwingung.

2 Aktivieren oder deaktivieren Sie execInstalledOnly-Erzwingung.

Option	Beschreibung

Aktivieren	a Stellen Sie sicher, dass die Secure Boot-Option erzwungen wird.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: true`
	Bestätigen Sie, dass „True“ für „Secure Boot anfordern“ angezeigt wird. Falls nicht, finden Sie weitere Informationen unter Aktivieren oder Deaktivieren der Secure Boot-Erzwingung für eine sichere ESXi-Konfiguration.
	b Um den Laufzeitwert der execInstalledOnly-Startoption auf TRUE zu setzen, führen Sie den folgenden ESXCLI-Befehl aus.
	`esxcli system settings kernel set -s execInstalledOnly -v TRUE`
	c Fahren Sie den Host ordnungsgemäß herunter.
	Beispiel: Klicken Sie mit der rechten Maustaste auf den ESXi-Host im vSphere Client und wählen Sie **Betrieb > Herunterfahren** aus.
	d Starten Sie den Host neu.
	e Führen Sie zum Festlegen der execInstalledOnly-Erzwingung den folgenden ESXCLI-Befehl aus.
	`esxcli system settings encryption set --require-exec-installed-only=T`
	f Überprüfen Sie die Änderung.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: true`
	`Require Secure Boot: true`
	Vergewissern Sie sich, dass „Ausführbare Dateien nur aus installierten VIBs anfordern“ auf „true“ festgelegt ist.
	g Führen Sie zum Speichern der Einstellung folgenden Befehl aus:
	`/sbin/auto-backup.sh`

Deaktivieren	a Führen Sie den folgenden ESXCLI-Befehl aus.
	`esxcli system settings encryption set --require-exec-installed-only=F`
	b Überprüfen Sie die Änderung.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: true`
	Vergewissern Sie sich, dass „Ausführbare Dateien nur aus installierten VIBs anfordern“ auf „false“ festgelegt ist.

Option	Beschreibung
	c Führen Sie zum Speichern der Einstellung folgenden Befehl aus: `/sbin/auto-backup.sh` Das TPM erzwingt die execInstalledOnly-Startoption nicht mehr.

Ergebnisse

Der ESXi-Host wird je nach Benutzerauswahl mit aktivierter oder deaktivierter execInstalledOnly-Erzwingung ausgeführt.

Sichern von vCenter Server-Systemen

4

Für die vCenter Server-Sicherung muss gewährleistet werden, dass der Host gesichert wird, auf dem vCenter Server läuft, indem Best Practices für die Zuweisung von Berechtigungen und Rollen verwendet werden und die Integrität der Clients überprüft wird, die sich mit vCenter Server verbinden.

Dieses Kapitel enthält die folgenden Themen:

Empfohlene Vorgehensweisen für die vCenter Server-Sicherheit

Durch die Befolgung der empfohlenen Vorgehensweisen für die vCenter Server-Sicherheit können Sie zum Schutz der Integrität Ihrer vSphere-Umgebung beitragen.

Best Practices für die vCenter Server-Zugriffssteuerung

Steuern Sie den Zugriff auf die einzelnen vCenter Server-Komponenten streng, um die Systemsicherheit zu erhöhen.

Die folgenden Richtlinien tragen dazu bei, die Sicherheit Ihrer Umgebung zu sichern.

Verwenden von benannten Konten

- Gewähren Sie die Administratorrolle nur Administratoren, die diese Rolle benötigen. Sie können benutzerdefinierte Rollen erstellen oder die Rolle „Kein Kryptografie-Administrator“ für Administratoren mit eingeschränkteren Rechten verwenden. Wenden Sie diese Rolle nicht auf eine Gruppe an, deren Mitgliedschaft nicht streng kontrolliert wird.
- Vergewissern Sie sich, dass die Anwendungen eindeutige Dienstkonten verwenden, wenn sie eine Verbindung zu einem vCenter Server-System herstellen.

Überwachen der Rechte von vCenter Server-Administratorbenutzern

Nicht alle Administratorbenutzer benötigen die Administratorrolle. Stattdessen können Sie eine benutzerdefinierte Rolle mit den geeigneten Rechten erstellen und diese den anderen Administratoren zuweisen.

Benutzer mit der vCenter Server-Administratorrolle haben Rechte für alle Objekte in der Hierarchie. Standardmäßig ermöglicht z. B. die Administratorrolle Benutzern die Interaktion mit Dateien und Programmen innerhalb des Gastbetriebssystems einer virtuellen Maschine. Wenn diese Rolle zu vielen Benutzern zugewiesen wird, kann dies die Vertraulichkeit, Verfügbarkeit oder Integrität der Daten auf der virtuellen Maschine beeinträchtigen. Erstellen Sie eine Rolle, die den Administratoren die benötigten Rechte zuweist, aber entfernen Sie einige der Verwaltungsrechte für die virtuelle Maschine.

Minimieren des Zugriffs

Sorgen Sie dafür, dass sich keine Benutzer direkt bei der vCenter Server-Hostmaschine anmelden können. Benutzer, die bei der vCenter Server-Hostmaschine angemeldet sind, können absichtlich oder unabsichtlich Schaden anrichten, indem sie Einstellungen und Prozesse ändern. Diese Benutzer haben auch potenziell Zugriff auf vCenter-Anmeldedaten wie das SSL-Zertifikat. Erlauben Sie nur Benutzern mit legitimen Aufgaben, sich beim System anzumelden, und vergewissern Sie sich, dass diese Anmeldeereignisse überprüft werden.

Gewähren von minimalen Rechten für vCenter Server-Datenbankbenutzer

Der Datenbankbenutzer benötigt nur bestimmte Rechte für den Datenbankzugriff.

Einige Rechte sind nur für die Installation und das Upgrade erforderlich. Nach der Installation bzw. dem Upgrade von vCenter Server können Sie diese Rechte für den Datenbankadministrator entfernen.

Beschränken des Zugriffs auf den Datenspeicherbrowser

Weisen Sie das Recht **Datenspeicher.Datenspeicher durchsuchen** nur Benutzern oder Gruppen zu, die tatsächlich diese Rechte benötigen. Benutzer mit diesem Recht können über den Webbrowser oder den vSphere Client Dateien in Datenspeichern, die der vSphere-Bereitstellung zugeordnet sind, anzeigen, hochladen oder herunterladen.

Beschränken der Ausführung von Befehlen durch Benutzer innerhalb einer virtuellen Maschine

Standardmäßig kann ein Benutzer mit der vCenter Server-Administratorrolle mit Dateien und Programmen innerhalb des Gastbetriebssystems einer virtuellen Maschine interagieren. Erstellen Sie eine benutzerdefinierte Rolle ohne das Recht **Gastvorgänge**, um das Sicherheitsrisiko für die Vertraulichkeit, Verfügbarkeit und Integrität des Gastbetriebssystems zu verringern. Weitere Informationen hierzu finden Sie unter Beschränken der Ausführung von Befehlen durch Benutzer innerhalb einer virtuellen Maschine.

Ändern der Kennwortrichtlinie für vpxuser

Standardmäßig ändert vCenter Server das vpxuser-Kennwort automatisch alle 30 Tage. Stellen Sie sicher, dass diese Einstellung die Unternehmensrichtlinien erfüllt, oder konfigurieren Sie andernfalls die vCenter Server-Kennwortrichtlinie. Weitere Informationen hierzu finden Sie unter Festlegen der vCenter Server-Kennwortrichtlinie.

Hinweis Vergewissern sie sich, dass die Kennwortablaufrichtlinie nicht zu kurz festgelegt ist.

Überprüfen von Rechten nach einem vCenter Server-Neustart

Überprüfen Sie die erneute Zuweisung von Rechten, wenn Sie vCenter Server neu starten. Wenn der Benutzer oder die Gruppe mit der Administratorrolle für den Stammordner während eines Neustarts nicht überprüft werden kann, wird die Rolle für diesen Benutzer bzw. diese Gruppe entfernt. Stattdessen gewährt vCenter Server dem vCenter Single Sign On-Administrator (administrator@vsphere.local) standardmäßig die Administratorrolle. Dieses Konto kann dann als vCenter Server-Administrator fungieren.

Richten Sie erneut ein benanntes Administratorkonto ein und weisen Sie diesem Konto die Administratorrolle zu, um die Verwendung des anonymen vCenter Single Sign On-Administratorkontos (standardmäßig administrator@vsphere.local) zu vermeiden.

Verwenden von hohen RDP-Verschlüsselungsstufen

Vergewissern Sie sich, dass auf jedem Windows-Computer in der Infrastruktur die Einstellungen für die Remote Desktop Protocol-Hostkonfiguration (RDP) festgelegt sind, um den für Ihre Umgebung geeigneten höchsten Grad der Verschlüsselung sicherzustellen.

Überprüfen der vSphere Client-Zertifikate

Weisen Sie Benutzer des vSphere Client oder anderer Clientanwendungen an, Zertifikatverifizierungswarnungen zu beachten. Ohne Zertifikatverifizierung kann der Benutzer Ziel eines MiTM-Angriffs werden.

Festlegen der vCenter Server-Kennwortrichtlinie

Standardmäßig ändert vCenter Server das vpxuser-Kennwort automatisch alle 30 Tage. Sie können diesen Wert über den vSphere Client ändern.

Verfahren

1. Melden Sie sich beim vCenter Server-System mit dem vSphere Client an.
2. Wählen Sie in der Objekthierarchie das vCenter Server-System aus.
3. Klicken Sie auf **Konfigurieren**.
4. Klicken Sie auf **Erweiterte Einstellungen** und auf **Einstellungen bearbeiten**.
5. Klicken Sie auf das Symbol **Filter** und geben Sie **`VimPasswordExpirationInDays`** ein.
6. Legen Sie `VirtualCenter.VimPasswordExpirationInDays` entsprechend Ihren Anforderungen fest.

Entfernen abgelaufener oder widerrufener Zertifikate und Protokolle fehlgeschlagener Installationen

Wenn Sie abgelaufene oder widerrufene Zertifikate oder Installationsprotokolle für eine fehlgeschlagene Installation von vCenter Server auf Ihrem vCenter Server-System beibehalten, kann dies Ihre Umgebung beeinträchtigen.

Aus den folgenden Gründen müssen abgelaufene oder widerrufene Zertifikate entfernt werden:

- Wenn abgelaufene oder widerrufene Zertifikate nicht vom vCenter Server-System entfernt werden, wird die Umgebung anfällig für Man-in-the-Middle-Angriffe (MITM).
- In bestimmten Fällen wird eine Protokolldatei, die das Datenbankkennwort als normalen Text enthält, auf dem System erstellt, wenn die Installation von vCenter Server fehlschlägt. Ein Angreifer, der in das vCenter Server eindringt, könnte sich Zugriff auf dieses Kennwort verschaffen und zugleich auf die vCenter Server-Datenbank zugreifen.

Begrenzen der vCenter Server-Netzwerkkonnektivität

Zur Erhöhung der Sicherheit sollten Sie das vCenter Server-System nur im Verwaltungsnetzwerk bereitstellen und sicherstellen, dass für den Verwaltungsdatenverkehr von vSphere ein begrenztes Netzwerk verwendet wird. Durch Einschränkung der Netzwerkkonnektivität begrenzen Sie bestimmte Angriffsarten.

vCenter Server benötigt den Zugang nur zu einem Verwaltungsnetzwerk. Stellen Sie das vCenter Server-System möglichst nicht in anderen Netzwerken wie Ihrem Produktionsnetzwerk oder Speichernetzwerk bzw. einem Netzwerk mit Zugang zum Internet bereit. vCenter Server benötigt keinen Zugriff auf das Netzwerk, in dem vMotion ausgeführt wird.

vCenter Server benötigt Netzwerkkonnektivität zu den folgenden Systemen:

- Allen ESXi-Hosts.
- Der vCenter Server-Datenbank.
- Andere vCenter Server-Systeme (wenn die vCenter Server-Systeme Teil einer gemeinsamen vCenter Single Sign On-Domäne zum Replizieren von Tags, Berechtigungen usw. sind).
- Systemen, die Verwaltungsclients ausführen dürfen. Beispielsweise der vSphere Client, ein Windows-System, in dem Sie PowerCLI verwenden, oder ein anderer SDK-basierter Client.
- Infrastrukturdiensten wie DNS, Active Directory und PTP oder NTP.
- Anderen Systemen, auf denen Komponenten laufen, die für die Funktionen des vCenter Server-Systems wesentlich sind.

Verwenden Sie die Firewall auf dem vCenter Server. Beziehen Sie IP-basierte Zugriffsbeschränkungen ein, damit nur notwendige Komponenten mit dem vCenter Server-System kommunizieren können.

Bewerten der Verwendung von Linux-Clients mit CLIs und SDKs

Die Kommunikation zwischen Clientkomponenten und einem vCenter Server-System oder ESXi-Hosts wird standardmäßig durch eine SSL-Verschlüsselung geschützt. Bei den Linux-Versionen dieser Komponenten findet keine Zertifikatvalidierung statt. Daher sollten Sie die Verwendung dieser Clients einschränken.

Um die Sicherheit zu verbessern, können Sie die VMCA-signierten Zertifikate auf dem vCenter Server-System und auf den ESXi-Hosts durch Zertifikate ersetzen, die von einer Unternehmens- oder Drittanbieter-Zertifizierungsstelle signiert sind. Allerdings wären bestimmte Kommunikationen mit Linux-Clients immer noch anfällig für Machine-in-the-Middle-Angriffe. Die folgenden Komponenten sind anfällig, wenn sie auf einem Linux-Betriebssystem laufen.

- ESXCLI-Befehle
- vSphere SDK for Perl-Skripts
- Mit vSphere Web Services SDK geschriebene Programme

Sie können die Einschränkungen bei Linux-Clients lockern, wenn Sie geeignete Kontrollen erzwingen.

- Beschränken Sie den Zugriff zum Verwaltungsnetzwerk auf autorisierte Systeme.
- Verwenden Sie Firewalls, um sicherzustellen, dass nur autorisierte Hosts die Berechtigung haben, auf vCenter Server zuzugreifen.
- Verwenden Sie Bastionhosts (Jump-Box-Systeme), um sicherzustellen, dass Linux-Clients sich hinter dem „Jump“ befinden.

Untersuchen der Client-Plug-Ins

vSphere Client-Erweiterungen werden auf der Berechtigungsstufe ausgeführt, mit der der Benutzer angemeldet ist. Eine bösartige Erweiterung kann als nützliches Plug-In maskiert sein und schädliche Vorgänge ausführen, etwa Anmeldedaten stehlen oder die Systemkonfiguration ändern. Verwenden Sie zur Verbesserung der Sicherheit eine Installation, die ausschließlich autorisierte Erweiterungen vertrauenswürdiger Quellen enthält.

Eine vCenter-Installation enthält ein Erweiterbarkeits-Framework für den vSphere Client. Sie können dieses Framework verwenden, um den Client mit Menüauswahlen oder Symbolleistensymbolen zu erweitern. Die Erweiterungen können Zugriff auf vCenter-Add-On-Komponenten oder externe, webbasierte Funktionen bereitstellen.

Die Verwendung des erweiterbaren Frameworks birgt das Risiko, ungewollte Funktionen zu installieren. Wenn beispielsweise ein Administrator ein Plug-In in einer Instanz des vSphere Client installiert, kann das Plug-In auf der Berechtigungsstufe dieses Administrators beliebige Befehle ausführen.

Zum Schutz vor einer möglichen Manipulation des vSphere Client überprüfen Sie alle installierten Plug-Ins in regelmäßigen Abständen und stellen Sie sicher, dass jedes Plug-In aus einer vertrauenswürdigen Quelle stammt.

Voraussetzungen

Für den Zugriff auf den vCenter Single Sign On-Dienst benötigen Sie entsprechende Rechte. Diese Berechtigungen weichen von den Berechtigungen für vCenter Server ab.

Verfahren

1. Melden Sie sich beim vSphere Client als „administrator@vsphere.local“ oder als Benutzer mit vCenter Single Sign On-Rechten an.
2. Wählen Sie auf der Homepage die Option **Verwaltung** und dann unter **Lösungen** die Option **Client-Plug-Ins** aus.
3. Prüfen Sie die Liste der Client-Plug-Ins.

Empfohlene Vorgehensweisen für die Sicherheit von vCenter Server

Verwenden Sie alle empfohlenen Vorgehensweisen zum Absichern eines vCenter Server-Systems. Mit zusätzlichen Schritten können Sie die Sicherheit Ihres vCenter Server verbessern.

PTP oder NTP konfigurieren

Stellen Sie sicher, dass alle Systeme dieselbe relative Zeitquelle verwenden. Diese Zeitquelle muss mit einem vereinbarten Zeitstandard wie z. B. der koordinierten Weltzeit (Coordinated Universal Time, UTC) synchronisiert sein. Synchronisierte Systeme sind für die Zertifikatsvalidierung wesentlich. PTP und NTP vereinfachen auch die Erkennung von Eindringungsversuchen in den Protokolldateien. Bei falschen Zeiteinstellungen ist es schwierig, Protokolldateien zur Suche nach Angriffen zu untersuchen und abzugleichen. Dies führt zu ungenauen Ergebnissen beim Audit. Weitere Informationen hierzu finden Sie unter Synchronisieren der Uhrzeit in vCenter Server mit einem NTP-Server.

Beschränken des vCenter Server-Netzwerkzugriffs

Beschränken Sie den Zugriff auf Komponenten, die für die Kommunikation mit der vCenter Server erforderlich sind. Das Blockieren des Zugriffs von unnötigen Systemen reduziert das Risiko von Angriffen auf das Betriebssystem.

Eine Liste aller unterstützten Ports und Protokolle in VMware, einschließlich vSphere und vSAN, finden Sie im Tool VMware Ports and Protocols™ unter https://ports.vmware.com/. Sie können Ports nach VMware-Produkt durchsuchen, eine benutzerdefinierte Portliste erstellen und Portlisten drucken oder speichern.

Konfigurieren eines Bastionhosts

Zum Schutz Ihrer Assets konfigurieren Sie einen Bastionhost (auch als „Jump Box“ bezeichnet), um Verwaltungsaufgaben mit erhöhten Rechten durchzuführen. Ein Bastionhost ist ein spezieller Computer, der eine minimale Anzahl an administrativen Anwendungen hostet. Alle anderen unnötigen Dienste werden entfernt. Der Host befindet sich in der Regel im Verwaltungsnetzwerk. Ein Bastionhost erhöht den Schutz von Assets, da er die Anmeldung auf

wichtige Personen beschränkt, für den Anmeldevorgang Firewallregeln erfordert und durch Audit-Tools eine zusätzliche Überwachung stattfindet.

Kennwortanforderungen und Sperrverhalten für vCenter

Beim Verwalten der vSphere-Umgebung müssen Sie die vCenter Single Sign On-Kennwortrichtlinie, die vCenter Server-Kennwörter und das Sperrverhalten berücksichtigen.

Dieser Abschnitt befasst sich mit vCenter Single Sign-On-Kennwörtern. Unter Kennwörter und Kontosperrung für ESXi werden Kennwörter von lokalen ESXi-Benutzern besprochen.

vCenter Single Sign On-Administratorkennwort

Das Kennwort für den vCenter Single Sign On-Administrator, standardmäßig „administrator@vsphere.local“, wird in den vCenter Single Sign On-Kennwortrichtlinien angegeben. Standardmäßig muss dieses Kennwort die folgenden Anforderungen erfüllen:

- Mindestens 8 Zeichen
- Mindestens einen Kleinbuchstaben
- Mindestens ein numerisches Zeichen
- Mindestens ein Sonderzeichen

Das Kennwort für diesen Benutzer darf nicht mehr als 20 Zeichen lang sein. Nicht-ASCII-Zeichen sind zulässig. Administratoren können die Standard-Kennwortrichtlinien ändern. Informationen finden Sie in der Dokumentation *vSphere-Authentifizierung*.

vCenter Server-Kennwörter

In vCenter Server werden die Kennwortanforderungen von vCenter Single Sign On oder einer konfigurierten Identitätsquelle vorgegeben, z. B. Active Directory oder OpenLDAP.

Sperrverhalten von vCenter Single Sign-On

Benutzer werden nach einer vorher festgelegten Anzahl von aufeinanderfolgenden Fehlversuchen gesperrt. Standardmäßig werden Benutzer nach fünf aufeinanderfolgenden Fehlerversuchen innerhalb von drei Minuten gesperrt. Ein gesperrtes Konto wird automatisch nach fünf Minuten wieder entsperrt. Sie können diese Standardeinstellungen mithilfe der vCenter Single Sign-On-Sperrrichtlinie ändern. Informationen finden Sie in der Dokumentation *vSphere-Authentifizierung*.

Der vCenter Single Sign On-Domänenadministrator, standardmäßig „administrator@vsphere.local“, ist von der Sperrrichtlinie nicht betroffen. Die Kennwortrichtlinie betrifft den Benutzer.

Kennwortänderungen

Wenn Sie Ihr Kennwort kennen, können Sie es mithilfe des Befehls `dir-cli password change` ändern. Falls Sie Ihr Kennwort vergessen haben, kann ein vCenter Single Sign-On-Administrator es mithilfe des Befehls `dir-cli password reset` zurücksetzen.

Suchen Sie in der VMware-Knowledgebase nach Informationen über das Ablaufen von Kennwörtern in verschiedenen Versionen von vSphere sowie nach verwandten Themen.

Überprüfen der Fingerabdrücke bei Legacy-ESXi-Hosts

In vSphere 6.0 und höher werden den Hosts standardmäßig VMCA-Zertifikate zugewiesen. Wenn Sie den Zertifikatmodus zu Fingerabdruck ändern, können Sie für Legacy-Hosts auch weiterhin den Fingerabdruckmodus verwenden. Die Fingerabdrücke werden im vSphere Client überprüft.

Hinweis Standardmäßig bleiben die Zertifikate bei Upgrades erhalten.

Verfahren

1. Navigieren Sie zum vCenter Server in der Bestandsliste des vSphere Client.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter **Einstellungen** auf **Allgemein**.
4. Klicken Sie auf **Bearbeiten**.
5. Klicken Sie auf **SSL-Einstellungen**.
6. Falls einer Ihrer Hosts aus ESXi 5.5 oder früher eine manuelle Validierung erfordert, vergleichen Sie die für die Hosts aufgeführten Fingerabdrücke mit den Fingerabdrücken in der Hostkonsole.

   Verwenden Sie die Benutzerschnittstelle der direkten Konsole (DCUI), um den Fingerabdruck des Hosts abzurufen.

   a. Melden Sie sich bei der direkten Konsole an und drücken Sie F2, um das Menü für die Systemanpassung aufzurufen.

   b. Wählen Sie **Support-Informationen anzeigen**.

      Der Fingerabdruck des Hosts wird in der Spalte auf der rechten Seite angezeigt.
7. Stimmen die Fingerabdrücke überein, wählen Sie das Kontrollkästchen **Überprüfen** neben dem Host aus.

   Hosts, die nicht ausgewählt sind, werden getrennt, nachdem Sie auf **OK** klicken.
8. Klicken Sie auf **Speichern**.

Erforderliche Ports für vCenter Server

Das vCenter Server-System muss in der Lage sein, Daten an jeden verwalteten Host zu senden und Daten vom vSphere Client zu erhalten. Die Quell- und Zielhosts müssen Daten über vorab festgelegte TCP- und UDP-Ports miteinander austauschen können, um Migrations- und Bereitstellungsaktivitäten zwischen verwalteten Hosts zu ermöglichen.

Der Zugriff auf vCenter Server erfolgt über vorab festgelegte TCP- und UDP-Ports. Wenn Netzwerkkomponenten, die außerhalb einer Firewall liegen, verwaltet werden müssen, muss ggf. die Firewall neu konfiguriert werden, damit auf die entsprechenden Ports zugegriffen werden kann. Eine Liste aller unterstützten Ports und Protokolle in vSphere finden Sie im Tool VMware Ports and Protocols™ unter https://ports.vmware.com.

Wenn während der Installation ein Port verwendet wird oder mittels einer Sperrliste gesperrt ist, zeigt das Installationsprogramm für vCenter Server eine Fehlermeldung an. Sie müssen eine andere Portnummer verwenden, um mit der Installation fortfahren zu können. Es gibt interne Ports, die nur für den Datenaustausch zwischen Prozessen verwendet werden.

Für die Kommunikation verwendet VMware festgelegte Ports. Zudem überwachen die verwalteten Hosts die festgelegten Ports auf Daten von vCenter Server. Wenn zwischen diesen Elementen eine integrierte Firewall vorhanden ist, öffnet das Installationsprogramm die Ports während der Installation bzw. des Upgrades. Für benutzerdefinierte Firewalls müssen die erforderlichen Ports manuell geöffnet werden. Wenn sich eine Firewall zwischen zwei von verwalteten Hosts befindet und Sie Quell- oder Zielaktivitäten wie z. B. eine Migration oder einen Klonvorgang ausführen möchten, muss der verwaltete Host Daten empfangen können.

Wenn das vCenter Server-System einen anderen Port zum Empfangen von vSphere Client-Daten verwenden soll, lesen Sie die Dokumentation *vCenter Server und Hostverwaltung*.

Sichern von virtuellen Maschinen 5

Das Gastbetriebssystem, das in der virtuellen Maschine läuft, ist denselben Sicherheitsrisiken ausgesetzt wie ein physisches System. Sichern Sie virtuelle Maschinen genauso wie physische Maschinen und halten Sie sich an die in diesem Dokument und im *Security Configuration Guide* (Handbuch für die Sicherheitskonfiguration – früher bekannt als *Handbuch für Hardening*) besprochenen Best Practices.

Das *Handbuch für die Sicherheitskonfiguration* finden Sie unter https://core.vmware.com/security.

Dieses Kapitel enthält die folgenden Themen:

- Aktivieren oder Deaktivieren von UEFI Secure Boot für eine virtuelle Maschine
- Beschränken informativer Meldungen von virtuellen Maschinen auf VMX-Dateien
- Virtuelle Maschine – Empfohlene Vorgehensweisen für die Sicherheit
- Sichern von virtuellen Maschinen mit Intel Software Guard-Erweiterungen
- Sichern von virtuellen Maschinen mit AMD Secure Encrypted Virtualization-Encrypted State

Aktivieren oder Deaktivieren von UEFI Secure Boot für eine virtuelle Maschine

UEFI Secure Boot ist ein Sicherheitsstandard, mit dem sichergestellt werden kann, dass ein PC nur über Software gestartet wird, die durch den entsprechenden PC-Hersteller als vertrauenswürdig eingestuft wird. Für bestimmte Hardwareversionen und Betriebssysteme von virtuellen Maschinen können Sie einen sicheren Start in der gleichen Weise wie für physische Maschinen aktivieren.

In einem Betriebssystem, das UEFI Secure Boot unterstützt, ist jedes Element der Boot-Software signiert, einschließlich dem Bootloader, dem Betriebssystem-Kernel und den Betriebssystem-Treibern. Zur Standardkonfiguration der virtuellen Maschine gehören verschiedene Code-Signaturzertifikate.

- Ein Microsoft-Zertifikat, das nur für den Start von Windows verwendet wird.
- Ein Microsoft-Zertifikat, das für Drittanbieter-Code verwendet wird, welcher von Microsoft signiert ist, wie beispielsweise Linux-Bootloader.

- Ein VMware-Zertifikat, das nur für den Start von ESXi innerhalb einer virtuellen Maschine verwendet wird.

Zur Standardkonfiguration der virtuellen Maschine gehört ein Zertifikat für Authentifizierungsanforderungen, um die Konfiguration des sicheren Starts zu ändern. Dazu gehört auch die Widerrufsliste für den sicheren Start von innerhalb der virtuellen Maschine. Dies ist ein Microsoft KEK-Zertifikat (Key Exchange Key, Schlüsselaustauschschlüssel).

In nahezu allen Fällen ist es nicht notwendig, die vorhandenen Zertifikate zu ersetzen. Wenn Sie die Zertifikate ersetzen möchten, informieren Sie sich im VMware-Kowledgebase-System.

VMware Tools Version 10.1 oder höher ist für virtuelle Maschinen erforderlich, die UEFI Secure Boot verwenden. Sie können diese virtuellen Maschinen auf eine höhere Version von VMware Tools aktualisieren, wenn diese verfügbar ist.

Bei Linux-basierten virtuellen Maschinen wird das VMware Host-Gast-Dateisystem im sicheren Startmodus nicht unterstützt. Entfernen Sie das VMware Host-Gast-Dateisystem aus den VMware Tools, bevor Sie den sicheren Start aktivieren.

Hinweis Wenn Sie den sicheren Start für eine virtuelle Maschine aktivieren, können Sie nur signierte Treiber in diese virtuelle Maschine laden.

In dieser Aufgabe wird beschrieben, wie der sichere Start für eine virtuelle Maschine mithilfe von vSphere Client aktiviert und deaktiviert wird. Sie können auch Skripte schreiben, um die Einstellungen für virtuelle Maschinen zu verwalten. Sie können beispielsweise das Ändern der Firmware von BIOS zu EFI für virtuelle Maschinen mit dem folgenden PowerCLI-Code automatisieren:

```
$vm = Get-VM TestVM

$spec = New-Object VMware.Vim.VirtualMachineConfigSpec
$spec.Firmware = [VMware.Vim.GuestOsDescriptorFirmwareType]::efi
$vm.ExtensionData.ReconfigVM($spec)
```

Weitere Informationen finden Sie im *VMware PowerCLI-Benutzerhandbuch*.

Voraussetzungen

Sie können einen sicheren Start nur aktivieren, wenn alle Voraussetzungen erfüllt sind. Wenn die Voraussetzungen nicht erfüllt sind, wird das Kontrollkästchen nicht im vSphere Client angezeigt.

- Stellen Sie sicher, dass das Betriebssystem und die Firmware der virtuellen Maschine UEFI Secure Boot unterstützen.
  - EFI-Firmware
  - Virtuelle Hardwareversion 13 oder höher.

- Betriebssystem, das UEFI Secure Boot unterstützt.

Hinweis Manche Gastbetriebssysteme unterstützten das Wechseln vom BIOS-Start zum UEFI-Start ohne Änderungen des Gastbetriebssystems nicht. Lesen Sie in der Dokumentation zum Gastbetriebssystem nach, bevor Sie einen Wechsel zum UEFI-Start vornehmen. Wenn Sie eine virtuelle Maschine, für die bereits der UEFI-Start verwendet wird, auf ein Betriebssystem aktualisieren, das UEFI Secure Boot unterstützt, können Sie den sicheren Start für diese virtuelle Maschine aktivieren.

- Schalten Sie die virtuelle Maschine aus. Wenn die virtuelle Maschine ausgeführt wird, ist das Kontrollkästchen abgeblendet.

Verfahren

1. Navigieren Sie zur virtuellen Maschine in der Bestandsliste des vSphere Client.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
3. Klicken Sie auf die Registerkarte **VM-Optionen** und erweitern Sie **Startoptionen**.
4. Stellen Sie sicher, dass unter **Startoptionen** die Firmware auf **EFI** festgelegt ist.
5. Wählen Sie Ihre Aufgabe.
   - Aktivieren Sie das Kontrollkästchen **Sicherer Start**, um den sicheren Start zu aktivieren.
   - Deaktivieren Sie das Kontrollkästchen **Sicherer Start**, um den sicheren Start zu deaktivieren.
6. Klicken Sie auf **OK**.

Ergebnisse

Wenn die virtuelle Maschine gestartet wird, werden nur Komponenten mit gültigen Signaturen zugelassen. Der Startvorgang wird angehalten, und es wird ein Fehler angezeigt, wenn eine Komponente mit einer fehlenden oder ungültigen Signatur festgestellt wird.

Beschränken informativer Meldungen von virtuellen Maschinen auf VMX-Dateien

Begrenzen Sie informelle Meldungen der virtuellen Maschine auf die VMX-Datei, um zu vermeiden, dass der Datenspeicher voll wird und einen Denial of Service (DoS) bewirkt. Ein Denial of Service (DoS) kann auftreten, wenn Sie die Größe der VMX-Datei einer virtuellen Maschine nicht kontrollieren und die Informationsmenge die Kapazität des Datenspeichers überschreitet.

Der Grenzwert für die Konfigurationsdatei der virtuellen Maschine (VMX-Datei) beträgt standardmäßig 1 MB. Diese Kapazität ist in der Regel ausreichend. Dieser Wert kann jedoch bei Bedarf geändert werden. Beispielsweise können Sie den Grenzwert erhöhen, wenn Sie große Mengen benutzerdefinierter Informationen in der Datei speichern.

Hinweis Wägen Sie sorgfältig ab, wie viele Informationen Sie benötigen. Wenn die Datenmenge die Kapazität des Datenspeichers überschreitet, kann dies einen Denial of Service (DoS) zur Folge haben.

Das Standardlimit von 1 MB wird auch dann angewendet, wenn der Parameter `tools.setInfo.sizeLimit` in den erweiterten Optionen nicht aufgeführt wird.

Verfahren

1. Navigieren Sie zur virtuellen Maschine in der Bestandsliste des vSphere Client.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie auf **Einstellungen bearbeiten**.
3. Wählen Sie **VM-Optionen**.
4. Klicken Sie auf **Erweitert** und anschließend auf **Konfiguration bearbeiten**.
5. Fügen Sie den Parameter `tools.setInfo.sizeLimit` hinzu bzw. bearbeiten Sie ihn.

Virtuelle Maschine – Empfohlene Vorgehensweisen für die Sicherheit

Die Einhaltung der empfohlenen Vorgehensweisen für die Sicherheit in Bezug auf virtuelle Maschinen ist eine wichtige Maßnahme zur Wahrung der Integrität Ihrer vSphere-Umgebung.

- Allgemeiner Schutz für virtuelle Maschinen

  Eine virtuelle Maschine ist nahezu mit einem physischen Server äquivalent. Wenden Sie in virtuellen Maschinen die gleichen Sicherheitsmaßnahmen wie für physische Systeme an.

- Verwendung von Vorlagen zum Bereitstellen von virtuellen Maschinen

  Wenn Sie Gastbetriebssysteme und Anwendungen auf einer virtuellen Maschine manuell installieren, besteht das Risiko einer fehlerhaften Konfiguration. Mithilfe einer Vorlage zum Erfassen eines abgesicherten Basisbetriebssystem-Images ohne installierte Anwendungen können Sie sicherstellen, dass alle virtuellen Maschinen mit einem bekannten Baseline-Sicherheitsniveau erstellt werden.

- Beschränken der Verwendung der VM-Konsole auf ein Minimum

  Die VM-Konsole bietet für eine virtuelle Maschine dieselbe Funktionalität wie ein Monitor auf einem physischen Server. Benutzer mit Zugriff auf die VM-Konsole haben Zugriff auf die Energieverwaltung der virtuellen Maschine und auf Konnektivitätssteuerelemente von Wechselmedien. Der Zugriff auf die Konsole kann deshalb einen bösartigen Angriff auf eine virtuelle Maschine ermöglichen.

- Verhindern, dass virtuelle Maschinen Ressourcen in Besitz nehmen

  Wenn eine virtuelle Maschine so viele Hostressourcen verbraucht, dass andere virtuelle Maschinen auf dem Host ihre Funktionen nicht mehr erfüllen können, kann es zur Dienstverweigerung (Denial of Service, DoS) kommen. Um zu verhindern, dass eine virtuelle Maschine DoS verursacht, verwenden Sie Funktionen der Hostressourcenverwaltung, beispielsweise die Einrichtung von Anteilen und die Verwendung von Ressourcenpools.

- Deaktivieren unnötiger Funktionen innerhalb von virtuellen Maschinen

  Jeder Dienst, der in einer virtuellen Maschine ausgeführt wird, ist ein potenzielles Angriffsziel. Indem Sie Systemkomponenten deaktivieren, die zur Ausführung der Anwendung bzw. des Dienstes auf dem System nicht benötigt werden, verringern Sie das Angriffsrisiko.

Allgemeiner Schutz für virtuelle Maschinen

Eine virtuelle Maschine ist nahezu mit einem physischen Server äquivalent. Wenden Sie in virtuellen Maschinen die gleichen Sicherheitsmaßnahmen wie für physische Systeme an.

Befolgen Sie diese empfohlenen Vorgehensweisen zum Schutz Ihrer virtuellen Maschine:

Patches und sonstiger Schutz

Halten Sie alle Sicherheitsmaßnahmen immer auf dem neuesten Stand, und wenden Sie immer die entsprechenden Patches an. Es ist besonders wichtig, auch die Updates für inaktive virtuelle Maschinen zu beachten, die ausgeschaltet sind, weil diese leicht vergessen werden können. Vergewissern Sie sich beispielsweise, dass Schutzmechanismen wie Virenschutzsoftware, Anti-Spyware, Erkennung von Eindringversuchen usw. für jede virtuelle Maschine der virtuellen Infrastruktur aktiviert sind. Sie sollten außerdem sicherstellen, das ausreichend Speicherplatz für die Protokolle der virtuellen Maschinen vorhanden ist.

Virenschutzprüfungen

Da auf jeder virtuellen Maschine ein gewöhnliches Betriebssystem ausgeführt wird, müssen Sie es durch die Installation von Virenschutzsoftware vor Viren schützen. Je nach Verwendungszweck der virtuellen Maschine sollte ggf. auch eine Firewall installiert werden.

Planen Sie die Virenprüfungen zeitlich versetzt, insbesondere in Implementierungen mit vielen virtuellen Maschinen. Die Leistung der Systeme in Ihrer Umgebung wird entscheidend verringert, wenn alle virtuellen Maschinen gleichzeitig geprüft werden. Softwarefirewalls und Antivirensoftware können die Virtualisierungsleistung beeinflussen. Sie können die beiden Sicherheitsmaßnahmen gegen Leistungsvorteile abwägen, insbesondere wenn Sie sich sicher sind, dass sich die virtuellen Maschinen in einer vollständig vertrauenswürdigen Umgebung befinden.

Serielle Ports

Über serielle Schnittstellen können Peripheriegeräte an die virtuelle Maschine angeschlossen werden. Bei physischen Systemen dienen sie häufig für direkte Low-Level-Verbindungen mit einer Serverkonsole. Virtuelle serielle Schnittstellen haben genau den gleichen Zweck bei virtuellen Maschinen. Da über serielle Schnittstellen meist nur Low-Level-Verbindungen hergestellt werden, bestehen hier kaum starke Zugangskontrollen, etwa bei der Protokollierung oder bei Berechtigungen.

Verwendung von Vorlagen zum Bereitstellen von virtuellen Maschinen

Wenn Sie Gastbetriebssysteme und Anwendungen auf einer virtuellen Maschine manuell installieren, besteht das Risiko einer fehlerhaften Konfiguration. Mithilfe einer Vorlage zum Erfassen eines abgesicherten Basisbetriebssystem-Images ohne installierte Anwendungen können Sie sicherstellen, dass alle virtuellen Maschinen mit einem bekannten Baseline-Sicherheitsniveau erstellt werden.

Sie können Vorlagen verwenden, die ein abgesichertes, gepatchtes und korrekt konfiguriertes Betriebssystem enthalten, um andere, anwendungsspezifische Vorlagen zu erstellen, oder mithilfe der Anwendungsvorlage virtuelle Maschinen bereitstellen.

Verfahren

- Stellen Sie Vorlagen für die Erstellung von virtuellen Maschinen bereit, die abgesicherte, gepatchte und korrekt konfigurierte Betriebssystembereitstellungen enthalten.

  Wenn möglich, stellen Sie auch Anwendungen in Vorlagen bereit. Achten Sie darauf, dass die Anwendungen nicht von Informationen abhängen, die spezifisch für eine virtuelle Maschine sind, die bereitgestellt werden soll.

Nächste Schritte

Weitere Informationen zu Vorlagen finden Sie in der Dokumentation *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Beschränken der Verwendung der VM-Konsole auf ein Minimum

Die VM-Konsole bietet für eine virtuelle Maschine dieselbe Funktionalität wie ein Monitor auf einem physischen Server. Benutzer mit Zugriff auf die VM-Konsole haben Zugriff auf die Energieverwaltung der virtuellen Maschine und auf Konnektivitätssteuerelemente von Wechselmedien. Der Zugriff auf die Konsole kann deshalb einen bösartigen Angriff auf eine virtuelle Maschine ermöglichen.

Verfahren

1. Verwenden Sie native Remoteverwaltungsdienste wie etwa Terminaldienste und SSH für die Interaktion mit virtuellen Maschinen.

   Gewähren Sie nur dann Zugriff auf die VM-Konsole, wenn dies erforderlich ist.

2 Beschränken Sie die Verbindungen auf die VM-Konsole.

   Beschränken Sie beispielsweise in einer Hochsicherheitsumgebung die Verbindungen auf eine. In manchen Umgebungen können Sie den Grenzwert erhöhen, wenn mehrere gleichzeitige Verbindungen für reguläre Aufgaben erforderlich sind.

   a Schalten Sie die virtuelle Maschine im vSphere Client aus.

   b Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.

   c Klicken Sie auf die Registerkarte **VM-Optionen** und erweitern Sie **Optionen der VMware-Remotekonsole**.

   d Geben Sie die maximale Anzahl der Sitzungen ein, z. B. **2**.

   e Klicken Sie auf **OK**.

Verhindern, dass virtuelle Maschinen Ressourcen in Besitz nehmen

Wenn eine virtuelle Maschine so viele Hostressourcen verbraucht, dass andere virtuelle Maschinen auf dem Host ihre Funktionen nicht mehr erfüllen können, kann es zur Dienstverweigerung (Denial of Service, DoS) kommen. Um zu verhindern, dass eine virtuelle Maschine DoS verursacht, verwenden Sie Funktionen der Hostressourcenverwaltung, beispielsweise die Einrichtung von Anteilen und die Verwendung von Ressourcenpools.

Standardmäßig haben alle virtuellen Maschinen auf einem ESXi-Host gleiche Anteile an den Ressourcen. Sie können mithilfe von Anteilen und Ressourcenpools einen Denial-of-Service-Angriff verhindern, der bewirkt, dass eine virtuelle Maschine so viele Ressourcen des Hosts beansprucht, dass andere virtuelle Maschinen auf demselben Host ihre beabsichtigten Funktionen nicht ausführen können.

Legen Sie Grenzwerte erst fest bzw. verwenden Sie Ressourcenpools erst, wenn Sie die Auswirkungen vollständig verstanden haben.

Verfahren

1 Stellen Sie für jede virtuelle Maschine gerade genug Ressourcen (CPU und Arbeitsspeicher) bereit, sodass sie ordnungsgemäß arbeitet.

2 Verwenden Sie Anteile, um Ressourcen für kritische virtuelle Maschinen zu garantieren.

3 Gruppieren Sie virtuelle Maschinen mit ähnlichen Anforderungen in Ressourcenpools.

4 Behalten Sie in jedem Ressourcenpool die Standardwerte für Anteile bei, um sicherzustellen, dass jeder virtuellen Maschine im Pool ungefähr dieselbe Ressourcenpriorität zugeordnet ist.

   Mit dieser Einstellung kann eine einzelne virtuelle Maschine nicht mehr Ressourcen als andere virtuelle Maschinen im Ressourcenpool verwenden.

Nächste Schritte

Informationen über Ressourcenanteile und Grenzwerte finden Sie in der Dokumentation *Handbuch zur vSphere-Ressourcenverwaltung*.

Deaktivieren unnötiger Funktionen innerhalb von virtuellen Maschinen

Jeder Dienst, der in einer virtuellen Maschine ausgeführt wird, ist ein potenzielles Angriffsziel. Indem Sie Systemkomponenten deaktivieren, die zur Ausführung der Anwendung bzw. des Dienstes auf dem System nicht benötigt werden, verringern Sie das Angriffsrisiko.

Für virtuelle Maschinen werden in der Regel weniger Dienste bzw. Funktionen benötigt als für physische Server. Wenn Sie ein System virtualisieren, prüfen Sie, ob bestimmte Dienste oder Funktionen erforderlich sind.

Hinweis Installieren Sie Gastbetriebssysteme gegebenenfalls mit den Installationsmodi „Minimal“ oder „Kern“, um die Größe, Komplexität und Angriffsfläche der Gastbetriebssysteme zu verringern.

Verfahren

- Deaktivieren Sie nicht verwendete Dienste im Betriebssystem.

  Wenn auf dem System beispielsweise ein Dateiserver ausgeführt wird, deaktivieren Sie die Webdienste.
- Trennen Sie nicht verwendete physische Geräte wie CD/DVD-Laufwerke, Diskettenlaufwerke und USB-Adapter.
- Deaktivieren Sie nicht verwendete Funktionen, wie etwa nicht verwendete Anzeigefunktionen oder VMware-Ordnerfreigaben, mit denen die Freigabe von Hostdateien an die virtuelle Maschine (Host-Gastdateisystem) aktiviert wird.
- Deaktivieren Sie Bildschirmschoner.
- Führen Sie das X Window-System auf Linux-, BSD- oder Solaris-Gastbetriebssystemen nur aus, wenn es erforderlich ist.

Entfernen ungenutzter Hardwaregeräte

Ein aktiviertes oder verbundenes Gerät stellt einen potenziellen Kanal für einen Angriff dar. Benutzer und Prozesse mit Berechtigungen für die virtuelle Maschine können Hardwaregeräte wie Netzwerkadapter oder CD-ROM-Laufwerke einbinden oder trennen. Angreifer können diese Fähigkeit nutzen, um die Sicherheit einer virtuellen Maschine zu gefährden. Das Entfernen überflüssiger Hardwaregeräte kann Angriffe verhindern.

Ein Angreifer mit Zugriff auf eine virtuelle Maschine kann ein getrenntes Hardwaregerät verbinden und auf die vertraulichen Informationen eines verbleibenden Mediums auf einem Hardwaregerät zugreifen. Der Angreifer könnte einen Netzwerkadapter trennen, um die virtuelle Maschine vom Netzwerk zu isolieren, was zu einem Denial-of-Service-Fehler führt.

- Verbinden Sie keine unzulässigen Geräte mit der virtuellen Maschine.
- Entfernen Sie Hardwaregeräte, die nicht benötigt oder nicht verwendet werden.
- Deaktivieren Sie nicht benötigte virtuelle Geräte in einer virtuellen Maschine.

- Stellen Sie sicher, dass nur erforderliche Geräte mit einer virtuellen Maschine verbunden sind. Virtuelle Maschinen verwenden selten serielle oder parallele Ports. In der Regel werden CD/DVD-Laufwerke nur während der Softwareinstallation temporär verbunden.

Verfahren

1. Navigieren Sie zur virtuellen Maschine in der Bestandsliste des vSphere Client.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie auf **Einstellungen bearbeiten**.
3. Deaktivieren Sie Hardwaregeräte, die nicht benötigt werden.

   Prüfen Sie insbesondere auch die folgenden Geräte:

   - Serielle Ports
   - Parallele Schnittstellen
   - USB-Controller
   - CD-ROM-Laufwerke

   Hinweis Sie müssen PowerCLI-Befehle verwenden, um Diskettenlaufwerke in vSphere 7.0 und höher zu verwalten.

Deaktivieren nicht verwendeter Anzeigefunktionen

Angreifer können sich nicht verwendete Anzeigefunktionen zunutze machen, um Schadcode in Ihre Umgebung einzuschleusen. Deaktivieren Sie daher alle Funktionen, die Sie in Ihrer Umgebung nicht nutzen.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1. Navigieren Sie zur virtuellen Maschine in der Bestandsliste des vSphere Client.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie auf **Einstellungen bearbeiten**.
3. Wählen Sie **VM-Optionen**.
4. Klicken Sie auf **Erweitert** und anschließend auf **Konfiguration bearbeiten**.

5 Fügen Sie ggf. die folgenden Parameter hinzu bzw. bearbeiten Sie sie.

Option	Beschreibung
svga.vgaonly	Wenn Sie diesen Parameter auf TRUE setzen, werden erweiterte Grafikfunktionen deaktiviert. Legen Sie diesen Parameter bei modernen Gastbetriebssystemen nicht auf TRUE fest, da sie nicht ordnungsgemäß funktionieren. Wenn `svga.vgaonly` auf TRUE festgelegt ist, ist nur der Textkonsolenmodus verfügbar. Bei dieser Einstellung bleibt der Parameter `mks.enable3d` wirkungslos. **Hinweis** Wenden Sie diese Einstellung nur auf virtuelle Maschinen an, die keine virtualisierte Grafikkarte benötigen.
mks.enable3d	Auf virtuellen Maschinen, die keine 3D-Funktion benötigen, können Sie diesen Parameter auf FALSE setzen.

Deaktivieren nicht freigelegter Funktionen

Virtuelle VMware-Maschinen können in einer vSphere-Umgebung und auf gehosteten Virtualisierungsplattformen wie VMware Workstation und VMware Fusion verwendet werden. Bestimmte VM-Parameter müssen nicht aktiviert werden, wenn eine virtuelle Maschine in einer vSphere-Umgebung ausgeführt wird. Deaktivieren Sie diese Parameter, um potenzielle Schwachstellen zu vermeiden.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1 Navigieren Sie zur virtuellen Maschine in der Bestandsliste des vSphere Client.

2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie auf **Einstellungen bearbeiten**.

3 Wählen Sie **VM-Optionen**.

4 Klicken Sie auf **Erweitert** und anschließend auf **Konfiguration bearbeiten**.

5 Setzen Sie die folgenden Parameter durch Bearbeiten oder Hinzufügen auf TRUE.

- `isolation.tools.memSchedFakeSampleStats.disable`
- `isolation.tools.getCreds.disable`
- `isolation.bios.bbs.disable`
- `isolation.tools.hgfsServerSet.disable`

6 Klicken Sie auf **OK**.

Deaktivieren der Freigabe von Hostdateien durch VMware-Ordnerfreigaben an die virtuelle Maschine

In Umgebungen mit hohen Sicherheitsanforderungen können Sie bestimmte Komponenten deaktivieren und damit das Risiko minimieren, dass ein Angreifer mithilfe des Host-Gastdateisystems (HGFS) Dateien innerhalb des Gastbetriebssystems übertragen kann.

Die Änderung der in diesem Abschnitt beschriebenen Parameter wirkt sich ausschließlich auf die Funktion „Ordnerfreigaben“ aus, nicht jedoch auf den HGFS-Server, der als Teil der Tools auf den virtuellen Gastmaschinen ausgeführt wird. Diese Parameter wirken sich außerdem nicht auf die automatischen Upgrade- und VIX-Befehle aus, die die Dateiübertragungen des Tools verwenden.

Verfahren

1. Navigieren Sie zur virtuellen Maschine in der Bestandsliste des vSphere Client.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie auf **Einstellungen bearbeiten**.
3. Wählen Sie **VM-Optionen**.
4. Klicken Sie auf **Erweitert** und anschließend auf **Konfiguration bearbeiten**.
5. Vergewissern Sie sich, dass der Parameter `isolation.tools.hgfsServerSet.disable` auf TRUE gesetzt ist.

   Die Einstellung TRUE verhindert, dass der VMX-Prozess eine Benachrichtigung von den Dienst-, Daemon- oder Upgrade-Prozessen jedes Tools über seine HGFS-Serverfunktionalität erhält.
6. (Optional) Vergewissern Sie sich, dass der Parameter `isolation.tools.hgfs.disable` auf TRUE gesetzt ist.

   Die Einstellung TRUE deaktiviert die nicht verwendeten VMware-Ordnerfreigaben für die Freigabe von Hostdateien an die virtuelle Maschine.

Deaktivieren von Kopier- und Einfügevorgängen zwischen Gastbetriebssystem und Remotekonsole

Kopier- und Einfügevorgänge zwischen dem Gastbetriebssystem und der Remotekonsole sind standardmäßig deaktiviert. Behalten Sie aus Gründen der Umgebungssicherheit die Standardeinstellung bei. Falls Sie Kopier- und Einfügevorgänge benötigen, müssen Sie diese im vSphere Client aktivieren.

Die Standardwerte für diese Optionen werden festgelegt, um eine sichere Umgebung zu gewährleisten. Sie müssen sie jedoch explizit auf „true“ festlegen, wenn Überwachungstools in der Lage sein sollen, die Korrektheit der Einstellung zu überprüfen.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1 Navigieren Sie zur virtuellen Maschine in der Bestandsliste des vSphere Client.

2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie auf **Einstellungen bearbeiten**.

3 Wählen Sie **VM-Optionen**.

4 Klicken Sie auf **Erweitert** und anschließend auf **Konfiguration bearbeiten**.

5 Stellen Sie sicher, dass in den Spalten „Name“ und „Wert“ die folgenden Werte enthalten sind, oder fügen Sie diese hinzu.

Name	Wert
`isolation.tools.copy.disable`	`true`
`isolation.tools.paste.disable`	`true`
`isolation.tools.setGUIOptions.enable`	`false`

Diese Optionen heben die Einstellungen in der Systemsteuerung von VMware Tools auf dem Gastbetriebssystem auf.

6 Klicken Sie auf **OK**.

7 (Optional) Starten Sie die virtuelle Maschine neu, wenn Sie Änderungen an den Konfigurationsparametern vornehmen.

Begrenzen der Offenlegung vertraulicher Daten, die in die Zwischenablage kopiert wurden

Kopier- und Einfügevorgänge sind für Hosts standardmäßig deaktiviert, um die Offenlegung vertraulicher Daten durch das Kopieren in die Zwischenablage zu verhindern.

Wenn Kopier- und Einfügevorgänge auf einer virtuellen Maschine aktiviert sind, auf der VMware Tools ausgeführt wird, können Sie Kopier- und Einfügevorgänge zwischen dem Gastbetriebssystem und der Remotekonsole ausführen. Wenn sich das Konsolenfenster im Vordergrund befindet, können auf der virtuellen Maschine ausgeführte Prozesse und nicht berechtigte Benutzer auf die Zwischenablage der VM-Konsole zugreifen. Wenn ein Benutzer vor der Verwendung der Konsole vertrauliche Daten in die Zwischenablage kopiert, macht der Benutzer unter Umständen vertrauliche Daten auf der virtuellen Maschine zugänglich. Um dies zu verhindern, sind Kopier- und Einfügevorgänge für das Gastbetriebssystem standardmäßig deaktiviert.

Bei Bedarf ist es möglich, Kopier- und Einfügevorgänge für virtuelle Maschinen zu aktivieren.

Beschränken der Ausführung von Befehlen durch Benutzer innerhalb einer virtuellen Maschine

Standardmäßig kann ein Benutzer mit der vCenter Server-Administratorrolle mit Dateien und Anwendungen innerhalb des Gastbetriebssystems einer virtuellen Maschine interagieren. Erstellen

Sie eine Rolle ohne das Recht **Gastvorgänge**, um das Sicherheitsrisiko für die Vertraulichkeit, Verfügbarkeit und Integrität des Gastbetriebssystems zu verringern. Weisen Sie diese Rolle Administratoren zu, die keinen Zugriff auf Dateien virtueller Maschinen benötigen.

Seien Sie beim Zulassen des Zugriffs auf das virtuelle Datencenter aus Sicherheitsgründen so restriktiv wie beim physischen Datencenter. Wenden Sie eine benutzerdefinierte Rolle, mit der der Gastzugriff deaktiviert wird, auf Benutzer an, die Administratorberechtigungen benötigen, die aber nicht mit Dateien und Anwendungen des Gastbetriebssystems interagieren dürfen.

Beispielsweise könnte eine Konfiguration eine virtuelle Maschine in der Infrastruktur mit vertraulichen Daten enthalten.

Wenn für Aufgaben wie die Migration mit vMotion Datencenter-Administratoren Zugriff auf die virtuelle Maschine benötigen, deaktivieren Sie einige Remote-Gastbetriebssystemvorgänge, um sicherzustellen, dass diese Administratoren keinen Zugriff auf vertrauliche Informationen haben.

Voraussetzungen

Stellen Sie sicher, dass Sie im vCenter Server-System, auf dem Sie die Rolle erstellen, über das **Administrator**-Recht verfügen.

Verfahren

1. Melden Sie sich beim vSphere Client als Benutzer mit **Administratorrechten** in dem vCenter Server-System an, in dem Sie die Rolle erstellen möchten.
2. Wählen Sie **Verwaltung** aus und klicken Sie auf **Rollen**.
3. Klicken Sie auf die Rolle „Administrator“ und dann auf das Symbol **Rollenaktion klonen**.
4. Geben Sie einen Namen und eine Beschreibung für die Rolle ein und klicken Sie auf **OK**.

   Geben Sie beispielsweise **`Administrator ohne Gastzugriff`** ein.
5. Wählen Sie die geklonte Rolle aus und klicken Sie auf das Symbol **Rollenaktion bearbeiten**.
6. Deaktivieren Sie unter der Berechtigung **Virtuelle Maschine** die Option **Gastvorgänge** und klicken Sie auf **Weiter**.
7. Klicken Sie auf **Beenden**.

Nächste Schritte

Wählen Sie das vCenter Server-System oder den Host aus und weisen Sie eine Berechtigung zu, die den Benutzer bzw. die Gruppe, der/die über die neuen Berechtigungen verfügen soll, mit der neu erstellten Rolle verknüpft. Entfernen Sie diese Benutzer aus der Administratorrolle.

Verhindern, dass ein Benutzer oder Prozess auf einer virtuellen Maschine die Verbindung zu Geräten trennt

Benutzer und Prozesse ohne Root- oder Administratorberechtigungen innerhalb virtueller Maschinen können Geräte verbinden oder trennen, wie z. B. Netzwerkadapter und CD-ROM-Laufwerke, und Geräteeinstellungen ändern. Entfernen Sie diese Geräte, um die Sicherheit der virtuellen Maschinen zu verstärken.

Sie können VM-Benutzer im Gastbetriebssystem sowie auf dem Gastbetriebssystem ausgeführte Prozesse daran hindern, Änderungen an den Geräten vorzunehmen, indem Sie die erweiterten Einstellungen der virtuellen Maschine ändern.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1. Navigieren Sie zur virtuellen Maschine in der Bestandsliste des vSphere Client.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie auf **Einstellungen bearbeiten**.
3. Wählen Sie **VM-Optionen**.
4. Klicken Sie auf **Erweitert** und anschließend auf **Konfiguration bearbeiten**.
5. Stellen Sie sicher, dass in den Spalten „Name“ und „Wert“ die folgenden Werte enthalten sind, oder fügen Sie diese hinzu.

Name	Wert
isolation.device.connectable.disable	Wahr
isolation.device.edit.disable	Wahr

   Diese Einstellungen wirken sich nicht auf die Fähigkeit eines vSphere-Administrators aus, die mit der virtuellen Maschine verbundenen Geräte zu verbinden oder zu trennen.
6. Klicken Sie auf **OK**, um das Dialogfeld „Konfigurationsparameter“ zu schließen, und klicken Sie erneut auf **OK**.

Verhindern, dass Gastbetriebssystemprozesse Konfigurationsnachrichten an den Host senden

Um sicherzustellen, dass das Gastbetriebssystem keine Konfigurationseinstellungen ändert, können Sie verhindern, dass diese Prozesse Name-Werte-Paare in die Konfigurationsdatei schreiben.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1. Navigieren Sie zur virtuellen Maschine in der Bestandsliste des vSphere Client.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie auf **Einstellungen bearbeiten**.
3. Wählen Sie **VM-Optionen**.
4. Klicken Sie auf **Erweitert** und anschließend auf **Konfiguration bearbeiten**.

5 Klicken Sie auf **Konfigurationsparameter hinzufügen** und geben Sie die folgenden Werte in den Spalten „Name“ und „Wert“ ein.

Spalte	Wert
Name	`isolation.tools.setinfo.disable`
Wert	`true`

6 Klicken Sie auf **OK**, um das Dialogfeld „Konfigurationsparameter“ zu schließen, und klicken Sie erneut auf **OK**.

Vermeiden der Verwendung von unabhängigen, nicht-dauerhaften Festplatten

Wenn Sie unabhängige, nicht dauerhafte Festplatten verwenden, können erfolgreiche Angreifer Beweise, dass die Maschine manipuliert wurde, durch Herunterfahren oder Neustarten des Systems beseitigen. Ohne eine dauerhafte Aufzeichnung der Aktivitäten auf einer virtuellen Maschine registrieren Administratoren einen Angriff möglicherweise überhaupt nicht. Deshalb sollten Sie die Verwendung unabhängiger, nicht dauerhafter Festplatten vermeiden.

Verfahren

- Stellen Sie sicher, dass die Aktivitäten der virtuellen Maschine auf einem separaten Server per Remoteprotokollierung aufgezeichnet werden, beispielsweise auf einem Syslog-Server oder einem gleichwertigen Windows-basierten Ereignis-Collector.

  Falls die Remoteprotokollierung von Ereignissen und Aktivitäten nicht für den Gast konfiguriert ist, sollte für „scsiX:Y.mode“ eine der folgenden Einstellungen verwendet werden:

  - Nicht vorhanden
  - Nicht eingestellt auf unabhängig, nicht dauerhaft

Ergebnisse

Wenn der nicht dauerhafte Modus nicht aktiviert ist, können Sie für eine virtuelle Maschine kein Rollback auf einen bekannten Status ausführen, wenn Sie das System neu starten.

Sichern von virtuellen Maschinen mit Intel Software Guard-Erweiterungen

Mithilfe von vSphere können Sie Virtual Intel® Software Guard Extensions (vSGX) für virtuelle Maschinen konfigurieren. Indem Sie vSGX verwenden, können Sie zusätzliche Sicherheit für Ihre Arbeitslasten bereitstellen.

Einige moderne Intel-CPUs implementieren eine Sicherheitserweiterung namens Intel® Software Guard Extensions (Intel® SGX). Intel SGX ist eine prozessorspezifische Technologie für Anwendungsentwickler, die den ausgewählten Code und die ausgewählten Daten vor Offenlegung oder Änderung schützen möchten. Mit Intel SGX kann Code auf Benutzerebene private Arbeitsspeicherbereiche definieren, die als Enklaven bezeichnet werden. Der Inhalt der Enklave wird so geschützt, dass außerhalb der Enklave ausgeführter Code nicht auf den Inhalt der Enklave zugreifen kann.

vSGX ermöglicht virtuellen Maschinen die Verwendung der Intel SGX-Technologie, sofern diese auf der Hardware verfügbar ist. Um vSGX zu verwenden, muss der ESXi-Host auf einer SGX-fähigen CPU installiert sein, und SGX muss im BIOS des ESXi-Hosts aktiviert sein. Sie können den vSphere Client verwenden, um SGX für eine virtuelle Maschine zu aktivieren.

vSGX-Übersicht

Virtuelle Maschinen können die Intel SGX-Technologie verwenden, sofern diese auf der Hardware verfügbar ist.

Voraussetzungen für vSGX

Zur Verwendung von vSGX muss die vSphere-Umgebung folgende Voraussetzungen erfüllen:

- Anforderungen an virtuelle Maschinen:
  - EFI-Firmware
  - Ab Hardwareversion 17
- Anforderungen an Komponenten:
  - vCenter Server 7.0 und höher
  - ESXi 7.0 und höher
- Unterstützung folgender Gastbetriebssysteme:
  - Linux
  - Windows Server 2016 (64 Bit) und höher
  - Windows 10 (64 Bit) und höher

Intel-Hardware

Informationen zur unterstützten Intel-Hardware für vSGX finden Sie im vSphere-Kompatibilitätshandbuch unter https://www.vmware.com/resources/compatibility/search.php.

Möglicherweise müssen Sie Hyper-Threading auf bestimmten CPUs ausschalten, um SGX auf dem ESXi-Host zu aktivieren. Weitere Informationen finden Sie im VMware Knowledge Base-Artikel unter https://kb.vmware.com/s/article/71367.

Nicht unterstützte VMware-Funktionen auf vSGX

Die folgenden Funktionen auf einer virtuellen Maschine werden nicht unterstützt, wenn vSGX aktiviert ist:

- vMotion/DRS-Migration
- Anhalten und Fortsetzen einer virtuellen Maschine
- VM-Snapshots (VM-Snapshots werden unterstützt, wenn Sie keinen Snapshot für den Arbeitsspeicher der virtuellen Maschine erstellen.)
- Fault Tolerance
- Gastintegrität (GI, Plattformgrundlage für VMware AppDefense™ 1.0)

Hinweis Diese VMware-Funktionen werden aufgrund der Funktionsweise der Intel SGX-Architektur nicht unterstützt. Diese fehlende Unterstützung ist nicht auf Mängel bei VMware zurückzuführen.

Aktivieren von vSGX auf einer virtuellen Maschine

Sie können vSGX auf einer virtuellen Maschine aktivieren, während Sie eine virtuelle Maschine erstellen.

Voraussetzungen

Der ESXi-Host muss auf einer SGX-fähigen CPU installiert und SGX muss im BIOS des Hosts aktiviert sein. Weitere Informationen zu unterstützten Intel-CPUs finden Sie unter vSGX-Übersicht.

Erstellen Sie eine virtuelle Maschine, für die Hardwareversion 17 oder höher und eines der folgenden unterstützten Gastbetriebssysteme verwendet wird:

- Linux
- Windows 10 (64 Bit) und höher
- Windows Server 2016 (64 Bit) und höher

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Wählen Sie in der Bestandsliste ein Objekt aus, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, beispielsweise einen ESXi-Host oder einen Cluster.
3. Klicken Sie mit der rechten Maustaste auf das Objekt, wählen Sie **Neue virtuelle Maschine** aus und befolgen Sie die Anweisungen zum Erstellen einer virtuellen Maschine.

Option	Aktion
Erstellungstyp auswählen	Erstellen Sie eine virtuelle Maschine.
Namen und Ordner auswählen	Legen Sie einen Namen und einen Zielspeicherort fest.

Option	Aktion
Computing-Ressource auswählen	Geben Sie ein Objekt an, für das Sie über Rechte zum Erstellen von virtuellen Maschinen verfügen.
Speicher auswählen	Wählen Sie in der VM-Speicherrichtlinie die entsprechende Speicherrichtlinie aus. Wählen Sie einen kompatiblen Datenspeicher aus.
Kompatibilität auswählen	Stellen Sie sicher, dass **ESXi 7.0 und höher** ausgewählt ist.
Gastbetriebssystem auswählen	Wählen Sie entweder Linux, Windows 10 (64 Bit) oder Windows Server 2016 (64 Bit) aus.
Hardware anpassen	Aktivieren Sie unter „Sicherheitsgeräte“ das Kontrollkästchen **Aktivieren** für SGX. Stellen Sie unter **VM-Optionen > Startoptionen > Firmware** sicher, dass EFI ausgewählt ist. Geben Sie die EPC-Größe (Enclave Page Cache) ein und wählen Sie den FLC-Modus (Flexible Launch Control) entsprechend aus.
Bereit zum Abschließen	Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

Aktivieren von vSGX auf einer vorhandenen virtuellen Maschine

Sie können vSGX auf einer vorhandenen virtuellen Maschine aktivieren.

Sie können vSGX für virtuelle Maschinen unter vSphere 7.0 und höher aktivieren.

Voraussetzungen

- Der ESXi-Host muss auf einer SGX-fähigen CPU installiert und SGX muss im BIOS des Hosts aktiviert sein. Weitere Informationen zu unterstützten Intel-CPUs finden Sie unter vSGX-Übersicht.
- Als Gastbetriebssystem muss Linux oder Windows Server 2016 (64 Bit) oder höher bzw. Windows 10 (64 Bit) oder höher verwendet werden.
- Die in Ihrer Umgebung ausgeführten ESXi-Hosts müssen ESXi 7.0 oder höher aufweisen.
- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.
- Die virtuelle Maschine muss EFI-Firmware nutzen.
- Die virtuelle Maschine muss die Hardwareversion 17 oder höher verwenden.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Klicken Sie mit der rechten Maustaste auf die zu ändernde virtuelle Maschine in der Bestandsliste und wählen Sie **Einstellungen bearbeiten** aus.
3. Aktivieren Sie im Dialogfeld **Einstellungen bearbeiten** unter **Sicherheitsgeräte** das Kontrollkästchen **Aktivieren** für SGX.
4. Geben Sie die EPC-Größe (Enclave Page Cache) ein und wählen Sie den FLC-Modus (Flexible Launch Control) entsprechend aus.
5. Stellen Sie unter **VM-Optionen > Startoptionen > Firmware** sicher, dass EFI ausgewählt ist.

6 Klicken Sie auf **OK**.

Entfernen von vSGX von einer virtuellen Maschine

Sie können vSGX von einer virtuellen Maschine entfernen.

Verfahren

1 Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.

2 Klicken Sie mit der rechten Maustaste auf die zu ändernde virtuelle Maschine in der Bestandsliste und wählen Sie **Einstellungen bearbeiten** aus.

3 Deaktivieren Sie im Dialogfeld **Einstellungen bearbeiten** unter **Sicherheitsgeräte** das Kontrollkästchen **Aktivieren** für SGX.

4 Klicken Sie auf **OK**.

Stellen Sie sicher, dass der vSGX-Eintrag nicht mehr auf der Registerkarte **Übersicht** der virtuellen Maschine im Bereich **VM-Hardware** angezeigt wird.

Sichern von virtuellen Maschinen mit AMD Secure Encrypted Virtualization-Encrypted State

Secure Encrypted Virtualization-Encrypted State (SEV-ES) ist eine in neueren AMD-CPUs aktivierte Hardwarefunktion, mit der der Arbeitsspeicher und das Register des Gastbetriebssystems zustandsverschlüsselt gehalten und gegen Zugriff vom Hypervisor geschützt werden.

Sie können SEV-ES für Ihre virtuellen Maschinen als zusätzliche Sicherheitsfunktion hinzufügen. SEV-ES verhindert, dass CPU-Register Informationen aus Registern an Komponenten wie den Hypervisor weitergeben. SEV-ES kann auch böswillige Änderungen an einem CPU-Registerzustand erkennen.

Übersicht über AMD-SEV-ES (Secure Encrypted Virtualization-Encrypted State)

In vSphere 7.0 Update 1 und höher können Sie Secure Encrypted Virtualization-Encrypted State (SEV-ES) auf unterstützten AMD-CPUs und Gastbetriebssystemen aktivieren.

Aktuell unterstützt SEV-ES nur AMD EPYC 7xx2- (Codename „Rome“) und höhere CPUs sowie ausschließlich Versionen von Linux-Kerneln, die spezifische Unterstützung für SEV-ES enthalten.

SEV-ES-Komponenten und -Architektur

Die SEV-ES-Architektur besteht aus den folgenden Komponenten.

- AMD-CPU, insbesondere der speziell der Platform Security Processor (PSP), der Verschlüsselungsschlüssel verwaltet und Verschlüsselung verarbeitet.

- Optimiertes Betriebssystem, d. h., ein Betriebssystem, das vom Gast initiierte Aufrufe an den Hypervisor verwendet.
- Virtual Machine Monitor (VMM) und Virtual Machine Executable (VMX) zum Initialisieren eines verschlüsselten VM-Status beim Einschalten der VM sowie zum Verarbeiten von Aufrufen des Gastbetriebssystems.
- Der VMkernel-Treiber zum Kommunizieren unverschlüsselter Daten zwischen dem Hypervisor und dem Gastbetriebssystem.

Implementieren und Verwalten von SEV-ES auf ESXi

Sie müssen SEV-ES zuerst in der BIOS-Konfiguration eines Systems aktivieren. In der Systemdokumentation finden Sie weitere Informationen zum Zugriff auf die BIOS-Konfiguration Nach dem Aktivieren von SEV-ES im BIOS des Systems können Sie SEV-ES einer virtuellen Maschine hinzufügen.

Sie verwenden entweder den vSphere Client (ab vSphere 7.0 Update 2) oder PowerCLI-Befehle zum Aktivieren und Deaktivieren von SEV-ES auf virtuellen Maschinen. Sie können neue virtuelle Maschinen mit SEV-ES erstellen oder SEV-ES auf vorhandenen virtuellen Maschinen aktivieren. Berechtigungen zum Verwalten virtueller Maschinen, die mit SEV-ES aktiviert sind, entsprechen denjenigen zum Verwalten regulärer VMs.

Nicht unterstützte VMware-Funktionen in SEV-ES

Die folgenden Funktionen werden nicht unterstützt, wenn SEV-ES aktiviert ist.

- Systemverwaltungsmodus
- vMotion
- Eingeschaltete Snapshots (Snapshots ohne Arbeitsspeicher hingegen werden unterstützt)
- CPU oder Arbeitsspeicher im laufenden Betrieb hinzufügen oder entfernen
- Anhalten/fortsetzen
- VMware Fault Tolerance
- Klone und Instant Clones
- Gastintegrität
- UEFI Secure Boot

Hinzufügen von AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) zu einer virtuellen Maschine mit dem vSphere Client

In vSphere 7.0 Update 2 und höher können Sie SEV-ES mithilfe des vSphere Client zu einer virtuellen Maschine hinzufügen, um verbesserte Sicherheitseinstellungen für das Gastbetriebssystem zur Verfügung zu stellen.

Sie können SEV-ES virtuellen Maschinen unter ESXi 7.0 Update 1 oder höher hinzufügen.

Voraussetzungen

- Das System muss mit einer AMD EPYC 7xx2- (Codename „Rome“) oder höheren CPU und einem unterstützenden BIOS installiert werden.
- SEV-ES muss im BIOS aktiviert sein.
- Die Anzahl der SEV-ES-VMs pro ESXi-Host wird vom BIOS gesteuert. Geben Sie bei Aktivierung von SEV-ES im BIOS einen Wert für die Einstellung **Mindestanzahl SEV-Nicht-ES-ASID** ein, der der Anzahl an virtuellen SEV-ES-Maschinen plus eins entspricht. Wenn beispielsweise 12 virtuelle Maschinen gleichzeitig ausgeführt werden sollen, geben Sie **13** ein.

  Hinweis vSphere 7.0 Update 1 bietet Unterstützung für 16 SEV-ES-fähige VMs pro ESXi-Host. Die Verwendung einer höheren Einstellung im BIOS verhindert nicht, dass SEV-ES funktioniert. Der Grenzwert von 16 gilt jedoch weiterhin. vSphere 7.0 Update 2 bietet Unterstützung für 480 SEV-ES-fähige VMs pro ESXi-Host.
- Die in Ihrer Umgebung ausgeführten ESXi-Hosts müssen ESXi 7.0 Update 1 oder höher aufweisen.
- Der vCenter Server muss unter vSphere 7.0 Update 2 oder höher ausgeführt werden.
- Das Gastbetriebssystem muss SEV-ES unterstützen.

  Aktuell werden nur Linux-Kernel mit spezifischer Unterstützung für SEV-ES unterstützt.
- Die virtuelle Maschine muss die Hardwareversion 18 oder höher aufweisen.
- Für die virtuelle Maschine muss die Option **Gesamten Gastarbeitsspeicher reservieren** aktiviert sein, andernfalls kann die VM nicht eingeschaltet werden.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Wählen Sie in der Bestandsliste ein Objekt aus, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, beispielsweise einen ESXi-Host oder einen Cluster.
3. Klicken Sie mit der rechten Maustaste auf das Objekt, wählen Sie **Neue virtuelle Maschine** aus und befolgen Sie die Anweisungen zum Erstellen einer virtuellen Maschine.

Option	Aktion
Erstellungstyp auswählen	Erstellen Sie eine virtuelle Maschine.
Namen und Ordner auswählen	Legen Sie einen Namen und einen Zielspeicherort fest.
Computing-Ressource auswählen	Geben Sie ein Objekt an, für das Sie über Rechte zum Erstellen von virtuellen Maschinen verfügen.
Speicher auswählen	Wählen Sie in der VM-Speicherrichtlinie die entsprechende Speicherrichtlinie aus. Wählen Sie einen kompatiblen Datenspeicher aus.
Kompatibilität auswählen	Stellen Sie sicher, dass **ESXi 7.0 und höher** ausgewählt ist.
Gastbetriebssystem auswählen	Wählen Sie Linux und eine Linux-Version mit spezieller Unterstützung für SEV-ES aus.

Option	Aktion
Hardware anpassen	Stellen Sie unter **VM-Optionen > Startoptionen > Firmware** sicher, dass EFI ausgewählt ist. Wählen Sie unter **VM-Optionen > Verschlüsselung** das Kontrollkästchen **Aktivieren** für AMD SEV-ES aus.
Bereit zum Abschließen	Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

Ergebnisse

Die virtuelle Maschine wird mit SEV-ES erstellt.

Hinzufügen von AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) zu einer virtuellen Maschine

Sie können SEV-ES einer virtuellen Maschine hinzufügen, um verbesserte Sicherheitseinstellungen für das Gastbetriebssystem zur Verfügung zu stellen.

Sie können SEV-ES virtuellen Maschinen unter ESXi 7.0 Update 1 oder höher hinzufügen.

Voraussetzungen

- Das System muss mit einer AMD EPYC 7xx2- (Codename „Rome“) oder höheren CPU und einem unterstützenden BIOS installiert werden.
- SEV-ES muss im BIOS aktiviert sein.
- Die Anzahl der SEV-ES-VMs pro ESXi-Host wird vom BIOS gesteuert. Geben Sie bei Aktivierung von SEV-ES im BIOS einen Wert für die Einstellung **Mindestanzahl SEV-Nicht-ES-ASID** ein, der der Anzahl an virtuellen SEV-ES-Maschinen plus eins entspricht. Wenn beispielsweise 12 virtuelle Maschinen gleichzeitig ausgeführt werden sollen, geben Sie **13** ein.

  Hinweis vSphere 7.0 Update 1 bietet Unterstützung für 16 SEV-ES-fähige VMs pro ESXi-Host. Die Verwendung einer höheren Einstellung im BIOS verhindert nicht, dass SEV-ES funktioniert. Der Grenzwert von 16 gilt jedoch weiterhin. vSphere 7.0 Update 2 bietet Unterstützung für 480 SEV-ES-fähige VMs pro ESXi-Host.
- Die in Ihrer Umgebung ausgeführten ESXi-Hosts müssen ESXi 7.0 Update 1 oder höher aufweisen.
- Das Gastbetriebssystem muss SEV-ES unterstützen.

  Aktuell werden nur Linux-Kernel mit spezifischer Unterstützung für SEV-ES unterstützt.
- Die virtuelle Maschine muss die Hardwareversion 18 oder höher aufweisen.
- Für die virtuelle Maschine muss die Option **Gesamten Gastarbeitsspeicher reservieren** aktiviert sein, andernfalls kann die VM nicht eingeschaltet werden.
- PowerCLI 12.1.0 oder höher muss auf einem System mit Zugriff auf Ihre Umgebung installiert sein.

Verfahren

1 Führen Sie in einer PowerCLI-Sitzung das Cmdlet `Connect-VIServer` aus, um als Administrator eine Verbindung mit dem vCenter Server herzustellen, der den ESXi-Host verwaltet, auf dem Sie eine virtuelle Maschine mit SEV-ES hinzufügen möchten.

```
Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
```

2 Erstellen Sie die virtuelle Maschine mit dem Cmdlet `New-VM` und geben Sie `-SEVEnabled $true` an.

Beispiel: Weisen Sie die Hostinformationen zuerst zu einer Variable zu und erstellen Sie dann die virtuelle Maschine.

```
$vmhost = Get-VMHost -Name 10.193.25.83
New-VM -Name MyVM1 $vmhost -NumCPU 2 -MemoryMB 4 -DiskMB 4 -SEVEnabled $true
```

Wenn Sie die Version der virtuelle Hardware angeben müssen, führen Sie das Cmdlet `New-VM` mit dem Parameter `-HardwareVersion vmx-18` aus. Beispiel:

```
New-VM -Name MyVM1 $vmhost -NumCPU 2 -MemoryMB 4 -DiskMB 4 -SEVEnabled $true
-HardwareVersion vmx-18
```

Ergebnisse

Die virtuelle Maschine wird mit SEV-ES erstellt.

Aktivieren von AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) auf einer vorhandenen virtuellen Maschine mit dem vSphere Client

In vSphere 7.0 Update 2 und höher können Sie SEV-ES mithilfe des vSphere Client zu einer vorhandenen virtuellen Maschine hinzufügen, um verbesserte Sicherheitseinstellungen für das Gastbetriebssystem zur Verfügung zu stellen.

Sie können SEV-ES virtuellen Maschinen unter ESXi 7.0 Update 1 oder höher hinzufügen.

Voraussetzungen

- Das System muss mit einer AMD EPYC 7xx2- (Codename „Rome“) oder höheren CPU und einem unterstützenden BIOS installiert werden.
- SEV-ES muss im BIOS aktiviert sein.

- Die Anzahl der SEV-ES-VMs pro ESXi-Host wird vom BIOS gesteuert. Geben Sie bei Aktivierung von SEV-ES im BIOS einen Wert für die Einstellung **Mindestanzahl SEV-Nicht-ES-ASID** ein, der der Anzahl an virtuellen SEV-ES-Maschinen plus eins entspricht. Wenn beispielsweise 12 virtuelle Maschinen gleichzeitig ausgeführt werden sollen, geben Sie **13** ein.

  Hinweis vSphere 7.0 Update 1 bietet Unterstützung für 16 SEV-ES-fähige VMs pro ESXi-Host. Die Verwendung einer höheren Einstellung im BIOS verhindert nicht, dass SEV-ES funktioniert. Der Grenzwert von 16 gilt jedoch weiterhin. vSphere 7.0 Update 2 bietet Unterstützung für 480 SEV-ES-fähige VMs pro ESXi-Host.

- Die in Ihrer Umgebung ausgeführten ESXi-Hosts müssen ESXi 7.0 Update 1 oder höher aufweisen.
- Der vCenter Server muss unter vSphere 7.0 Update 2 oder höher ausgeführt werden.
- Das Gastbetriebssystem muss SEV-ES unterstützen.

  Aktuell werden nur Linux-Kernel mit spezifischer Unterstützung für SEV-ES unterstützt.
- Die virtuelle Maschine muss die Hardwareversion 18 oder höher aufweisen.
- Für die virtuelle Maschine muss die Option **Gesamten Gastarbeitsspeicher reservieren** aktiviert sein, andernfalls kann die VM nicht eingeschaltet werden.
- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Klicken Sie mit der rechten Maustaste auf die zu ändernde virtuelle Maschine in der Bestandsliste und wählen Sie **Einstellungen bearbeiten** aus.
3. Stellen Sie unter **VM-Optionen > Startoptionen > Firmware** sicher, dass EFI ausgewählt ist.
4. Aktivieren Sie im Dialogfeld **Einstellungen bearbeiten** unter **VM-Optionen > Verschlüsselung** das Kontrollkästchen **Aktivieren** für AMD SEV-ES.
5. Klicken Sie auf **OK**.

Ergebnisse

SEV-ES wird der virtuellen Maschine hinzugefügt.

Aktivieren von AMD-SEV-ES (Secure Encrypted Virtualization-Encrypted State) auf einer vorhandenen virtuellen Maschine

Sie können einer vorhandenen virtuellen Maschine SEV-ES hinzufügen, um verbesserte Sicherheitseinstellungen für das Gastbetriebssystem zur Verfügung zu stellen.

Sie können SEV-ES virtuellen Maschinen unter ESXi 7.0 Update 1 oder höher hinzufügen.

Voraussetzungen

- Das System muss mit einer AMD EPYC 7xx2- (Codename „Rome“) oder höheren CPU und einem unterstützenden BIOS installiert werden.
- SEV-ES muss im BIOS aktiviert sein.
- Die Anzahl der SEV-ES-VMs pro ESXi-Host wird vom BIOS gesteuert. Geben Sie bei Aktivierung von SEV-ES im BIOS einen Wert für die Einstellung **Mindestanzahl SEV-Nicht-ES-ASID** ein, der der Anzahl an virtuellen SEV-ES-Maschinen plus eins entspricht. Wenn beispielsweise 12 virtuelle Maschinen gleichzeitig ausgeführt werden sollen, geben Sie **13** ein.

  Hinweis vSphere 7.0 Update 1 bietet Unterstützung für 16 SEV-ES-fähige VMs pro ESXi-Host. Die Verwendung einer höheren Einstellung im BIOS verhindert nicht, dass SEV-ES funktioniert. Der Grenzwert von 16 gilt jedoch weiterhin. vSphere 7.0 Update 2 bietet Unterstützung für 480 SEV-ES-fähige VMs pro ESXi-Host.
- Die in Ihrer Umgebung ausgeführten ESXi-Hosts müssen ESXi 7.0 Update 1 oder höher aufweisen.
- Das Gastbetriebssystem muss SEV-ES unterstützen.

  Aktuell werden nur Linux-Kernel mit spezifischer Unterstützung für SEV-ES unterstützt.
- Die virtuelle Maschine muss die Hardwareversion 18 oder höher aufweisen.
- Für die virtuelle Maschine muss die Option **Gesamten Gastarbeitsspeicher reservieren** aktiviert sein, andernfalls kann die VM nicht eingeschaltet werden.
- PowerCLI 12.1.0 oder höher muss auf einem System mit Zugriff auf Ihre Umgebung installiert sein.
- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.

Verfahren

1. Führen Sie in einer PowerCLI-Sitzung das Cmdlet `Connect-VIServer` aus, um als Administrator eine Verbindung mit dem vCenter Server herzustellen, der den ESXi-Host mit der virtuellen Maschine verwaltet, der SEV-ES hinzugefügt werden soll.

   Beispiel:

   ```
   Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
   ```
2. Aktivieren Sie SEV-ES auf der virtuellen Maschine mit dem Cmdlet `Set-VM` und geben Sie `-SEVEnabled $true` an.

   Beispiel:

   ```
   $vmhost = Get-VMHost -Name 10.193.25.83
   Set-VM -Name MyVM2 $vmhost -SEVEnabled $true
   ```

Wenn Sie die Version der virtuelle Hardware angeben müssen, führen Sie das Cmdlet `Set-VM` mit dem Parameter `-HardwareVersion vmx-18` aus. Beispiel:

```
Set-VM -Name MyVM2 $vmhost -SEVEnabled $true -HardwareVersion vmx-18
```

Ergebnisse

SEV-ES wird der virtuellen Maschine hinzugefügt.

Deaktivieren von AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) auf einer virtuellen Maschine mit dem vSphere Client

In vSphere 7.0 Update 2 und höher können Sie den vSphere Client zum Deaktivieren von SEV-ES auf einer virtuellen Maschine verwenden.

Voraussetzungen

- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Klicken Sie mit der rechten Maustaste auf die zu ändernde virtuelle Maschine in der Bestandsliste und wählen Sie **Einstellungen bearbeiten** aus.
3. Deaktivieren Sie im Dialogfeld **Einstellungen bearbeiten** unter **VM-Optionen > Verschlüsselung** das Kontrollkästchen **Aktivieren** für AMD SEV-ES.
4. Klicken Sie auf **OK**.

Ergebnisse

SEV-ES ist auf der virtuellen Maschine deaktiviert.

Deaktivieren von AMD-SEV-ES (Secure Encrypted Virtualization-Encrypted State) auf einer virtuellen Maschine

Sie können SEV-ES auf einer virtuellen Maschine deaktivieren.

Voraussetzungen

- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.
- PowerCLI 12.1.0 oder höher muss auf einem System mit Zugriff auf Ihre Umgebung installiert sein.

Verfahren

1 Führen Sie in einer PowerCLI-Sitzung das Cmdlet `Connect-VIServer` aus, um als Administrator eine Verbindung mit dem vCenter Server herzustellen, der den ESXi-Host mit der virtuellen Maschine verwaltet, von der SEV-ES entfernt werden soll.

   Beispiel:

   ```
   Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
   ```

2 Deaktivieren Sie SEV-ES auf der virtuellen Maschine mit dem Cmdlet `Set-VM` und geben Sie `-SEVEnabled $false` an.

   Beispiel: Weisen Sie die Hostinformationen zuerst einer Variablen zu und deaktivieren Sie SEV-ES dann für die virtuelle Maschine.

   ```
   $vmhost = Get-VMHost -Name 10.193.25.83
   Set-VM -Name MyVM2 $vmhost -SEVEnabled $false
   ```

Ergebnisse

SEV-ES ist auf der virtuellen Maschine deaktiviert.

Verschlüsselung virtueller Maschinen

6

Mit der vSphere-VM-Verschlüsselung können Sie vertrauliche Arbeitslasten noch sicherer verschlüsseln. Der Zugriff auf Verschlüsselungsschlüssel kann davon abhängig gemacht werden, ob sich der ESXi-Host in einem vertrauenswürdigen Zustand befindet.

Bevor Sie mit den Verschlüsselungsaufgaben für virtuelle Maschinen beginnen können, müssen Sie einen Schlüsselanbieter einrichten. Die folgenden Schlüsselanbietertypen sind verfügbar.

Tabelle 6-1. vSphere-Schlüsselanbieter

Schlüsselanbieter	Beschreibung	Für weitere Informationen.
Standardschlüsselanbieter	Der Standardschlüsselanbieter ist in vSphere 6.5 und höher verfügbar und verwendet vCenter Server, um Schlüssel von einem externen Schlüsselserver anzufordern. Der Schlüsselserver generiert und speichert die Schlüssel und leitet sie an vCenter Server zur Verteilung weiter.	Weitere Informationen hierzu finden Sie unter Kapitel 7 Konfigurieren und Verwalten eines Standardschlüsselanbieters.
Vertrauenswürdiger Schlüsselanbieter	Der in vSphere 7.0 und höher verfügbare vertrauenswürdige vSphere Trust Authority-Schlüsselanbieter ermöglicht den Zugriff auf die Verschlüsselungsschlüssel abhängig vom Bestätigungsstatus eines Arbeitslastclusters. Für vSphere Trust Authority ist ein externer Schlüsselserver erforderlich.	Weitere Informationen hierzu finden Sie unter Kapitel 9 vSphere Trust Authority.
VMware vSphere® Nativer Schlüsselanbieter™	vSphere Native Key Provider ist ab vSphere 7.0 Update 2 verfügbar und in allen vSphere-Editionen enthalten. Dafür ist kein externer Schlüsselserver erforderlich.	Weitere Informationen hierzu finden Sie unter Kapitel 8 Konfigurieren und Verwalten eines vSphere Native Key Providers.

Dieses Kapitel enthält die folgenden Themen:

- vSphere Virtual Machine Encryption-Komponenten
- Prozessablauf bei der Verschlüsselung
- Verschlüsseln von virtuellen Festplatten
- Fehler bei der Verschlüsselung von virtuellen Maschinen
- Voraussetzungen und erforderliche Berechtigungen für die Verschlüsselung
- Verschlüsseltes vSphere vMotion
- Empfohlene Vorgehensweisen für die Verschlüsselung, Einschränkungen und Interoperabilität
- Schlüsselpersistenz – Übersicht

Vergleich von vSphere-Schlüsselanbietern

Mithilfe einer allgemeinen Übersicht über die Funktionen der vSphere-Schlüsselanbieter können Sie Ihre Verschlüsselungsstrategie planen.

Im Allgemeinen gibt es im Regelbetrieb der einzelnen Schlüsselanbieter nur geringe Unterschiede bei den unterstützten Funktionen und Produkten. Trotz des ähnlichen Aussehens und Verhaltens der verschiedenen Schlüsselanbieter müssen bei der Auswahl eines Schlüsselanbieters unter Umständen Anforderungen und Bestimmungen berücksichtigt werden. Diese werden in der folgenden Tabelle dargestellt:

Tabelle 6-2. Überlegungen zu Schlüsselanbietern

Schlüsselanbieter	Externer Schlüsselserver erforderlich?	Schnelle Einrichtung?	Funktioniert nur mit vSphere?
Standardschlüsselanbieter	Ja	Nein	Nein
Vertrauenswürdiger Schlüsselanbieter	Ja	Nein	Nein
vSphere Native Key Provider	Nein	Ja	Ja

Verschlüsselungsfunktionen

Die folgenden Verschlüsselungsfunktionen werden von jedem Schlüsselanbietertyp unterstützt.

- Erneute Schlüsselerstellung mithilfe desselben oder eines anderen Schlüsselanbieters
- Schlüssel rotieren
- Virtuelles Trusted Platform Module (vTPM)
- Festplattenverschlüsselung
- Verschlüsselung virtueller vSphere-Maschinen
- Koexistenz mit anderen Schlüsselanbietern
- Upgrade auf einen anderen Schlüsselanbieter

vSphere-Funktionen

Im Folgenden wird die Unterstützung der Schlüsselanbieter für bestimmte wichtige vSphere-Funktionen beschrieben.

- Verschlüsselte vSphere vMotion: Wird von allen Schlüsselanbietertypen unterstützt. Derselbe Schlüsselanbieter muss auf dem Zielhost verfügbar sein. Weitere Informationen hierzu finden Sie unter Verschlüsseltes vSphere vMotion.
- Dateibasierte Sicherung und Wiederherstellung in vCenter Server: Standardschlüsselanbieter und vSphere Native Key Provider unterstützen dateibasierte Sicherung und Wiederherstellung in vCenter Server. Da die meisten vSphere Trust Authority-Konfigurationsinformationen auf den ESXi-Hosts gespeichert werden, erfolgt keine Sicherung dieser Informationen durch den dateibasierten Sicherungsmechanismus in vCenter Server. Um sicherzustellen, dass die Konfigurationsinformationen für Ihre vSphere Trust Authority-Bereitstellung gespeichert werden, finden Sie Informationen unter Sichern der vSphere Trust Authority-Konfiguration.

VMware Produkte

In der folgenden Tabelle wird die Schlüsselanbieterunterstützung für bestimmte VMware-Produkte verglichen.

Tabelle 6-3. Vergleich der Unterstützung für VMware-Produkte

Schlüsselanbieter	vSAN	Site Recovery Manager	vSphere Replication
Standardschlüsselanbieter	Ja	Ja	Ja
Vertrauenswürdiger Schlüsselanbieter	Ja	Ja Wenn dieselbe Konfiguration der vSphere Trust Authority-Dienste auf der Wiederherstellungsseite verfügbar ist, wird SRM mit Array-basierter Replizierung unterstützt.	Nein
vSphere Native Key Provider	Ja	Ja	Ja

Notwendige Hardware

In der folgenden Tabelle werden bestimmte Mindestanforderungen an die Hardware des Schlüsselanbieters verglichen.

Tabelle 6-4. Vergleich der notwendigen Hardware

Schlüsselanbieter	TPM auf ESXi-Host
Standardschlüsselanbieter	Nicht erforderlich
Vertrauenswürdiger Schlüsselanbieter	Erforderlich auf vertrauenswürdigen Hosts (Hosts im vertrauenswürdigen Cluster). **Hinweis** Aktuell benötigen die ESXi-Hosts im Trust Authority-Cluster kein TPM. Es empfiehlt sich jedoch, neue ESXi-Hosts mit TPMs zu installieren.
vSphere Native Key Provider	Nicht erforderlich Die Verfügbarkeit des vSphere Native Key Providers kann optional auf Hosts mit einem TPM beschränkt werden.

Benennung des Schlüsselanbieters

vSphere verwendet den Schlüsselanbieternamen, um einen Schlüsselbezeichner zu suchen. Wenn zwei Schlüsselanbieter denselben Namen haben, geht vSphere davon aus, dass sie äquivalent sind und Zugriff auf dieselben Schlüssel haben. Jeder logische Schlüsselanbieter muss unabhängig von seinem Typ (Standard-, vertrauenswürdiger und nativer Schlüsselanbieter) über einen eindeutigen Namen in allen vCenter Server-Systemen verfügen.

In einigen Fällen konfigurieren Sie denselben Schlüsselanbieter über mehrere vCenter Server-Systeme hinweg, z. B. den folgenden:

- Migrieren verschlüsselter virtueller Maschinen zwischen vCenter Server-Systemen
- Einrichten eines vCenter Servers als Notfallwiederherstellungsort

Wie vSphere Virtual Machine Encryption Ihre Umgebung schützt

Unabhängig davon, welchen Schlüsselanbieter Sie verwenden, können Sie mit vSphere Virtual Machine Encryption verschlüsselte virtuelle Maschinen erstellen und vorhandene virtuelle Maschinen verschlüsseln. Da alle Dateien der virtuellen Maschine, die vertrauliche Informationen enthalten, verschlüsselt werden, ist die virtuelle Maschine geschützt. Nur Administratoren mit Berechtigungen zum Verschlüsseln können Verschlüsselungs- und Entschlüsselungsaufgaben durchführen.

Welcher Speicher wird von vSphere Virtual Machine Encryption unterstützt

vSphere Virtual Machine Encryption funktioniert mit allen unterstützten Speichertypen (NFS, iSCSI, Fibre Channel, direkt angeschlossener Speicher usw.), einschließlich VMware vSAN. Weitere Informationen zur Verwendung von Verschlüsselung auf einem vSAN-Cluster finden Sie unter *Verwalten von VMware vSAN*.

vSphere Virtual Machine Encryption und vSAN verwenden dieselben Verschlüsselungsbibliotheken, aber unterschiedliche Profile. Bei der VM-Verschlüsselung handelt es sich um eine Verschlüsselung pro VM, während es sich bei vSAN um eine Verschlüsselung auf Datenspeicherebene handelt.

vSphere-Verschlüsselungsschlüssel und -Schlüsselanbieter

vSphere verwendet zwei Verschlüsselungsebenen in Form eines Schlüsselverschlüsselungsschlüssels (Key Encryption Key, KEK) und eines Datenverschlüsselungsschlüssels (Data Encryption Key, DEK). Kurz gesagt erzeugt ein ESXi-Host einen DEK, um virtuelle Maschinen und Festplatten zu verschlüsseln. Der KEK wird von einem Schlüsselserver bereitgestellt und zur Verschlüsselung (oder „Packung“) des DEK verwendet. Der KEK wird mithilfe des AES256-Algorithmus verschlüsselt und der DEK wird mithilfe des XTS-AES-256-Algorithmus verschlüsselt. Je nach Typ des Schlüsselanbieters werden verschiedene Methoden zum Erstellen und Verwalten des DEK und KEK verwendet.

Der Standardschlüsselanbieter funktioniert wie folgt.

1 Der ESXi-Host generiert und verwendet interne Schlüssel zum Verschlüsseln von virtuellen Maschinen und Festplatten. Diese Schlüssel werden als DEKs verwendet.

2 vCenter Server fordert Schlüssel aus dem Schlüsselserver (KMS) an. Diese Schlüssel werden als KEKs verwendet. vCenter Server speichert nur die ID jedes KEK, nicht jedoch den Schlüssel selbst.

3 ESXi verwendet den KEK zum Verschlüsseln der internen Schlüssel und speichert den verschlüsselten internen Schlüssel auf der Festplatte. ESXi speichert den KEK nicht auf der Festplatte. Wenn ein Host neu gestartet wird, fordert vCenter Server den KEK mit der entsprechenden ID beim Schlüsselserver an und macht ihn für ESXi verfügbar. ESXi kann dann die internen Schlüssel nach Bedarf entschlüsseln.

Der vertrauenswürdige vSphere Trust Authority-Schlüsselanbieter funktioniert folgendermaßen.

1 Der vCenter Server des vertrauenswürdigen Clusters überprüft, ob der ESXi-Host, auf dem die verschlüsselte virtuelle Maschine erstellt werden soll, auf den standardmäßigen vertrauenswürdigen Schlüsselanbieter zugreifen kann.

2 Der vCenter Server des vertrauenswürdigen Clusters fügt dem vertrauenswürdigen Schlüsselanbieter die Konfigurationsspezifikation der virtuellen Maschine hinzu.

3 Die Anforderung zum Erstellen der virtuellen Maschine wird an den ESXi-Host gesendet.

4 Wenn dem ESXi-Host noch kein Bestätigungstoken zur Verfügung steht, wird ein Token beim Bestätigungsdienst angefordert.

5 Der Schlüsselanbieterdienst validiert das Bestätigungstoken und erstellt einen KEK, der an den ESXi-Host gesendet werden soll. Der KEK wird mit dem auf dem Schlüsselanbieter konfigurierten primären Schlüssel verschlüsselt. Sowohl der verschlüsselte KEK-Text als auch der KEK-Klartext werden an den vertrauenswürdigen Host zurückgegeben.

6 Der ESXi-Host erzeugt einen DEK, um die Festplatten der virtuellen Maschine zu verschlüsseln.

7 Der KEK wird zum Verschlüsseln des vom ESXi-Host generierten DEK verwendet und der Verschlüsselungstext des Schlüsselanbieters wird mit den verschlüsselten Daten gespeichert.

8 Die virtuelle Maschine wird verschlüsselt und in den Speicher geschrieben.

Hinweis Wenn Sie eine verschlüsselte virtuelle Maschine löschen oder deren Registrierung aufheben, entfernen der ESXi-Host und der Cluster den KEK aus dem Zwischenspeicher. Der ESXi-Host kann den KEK nicht mehr verwenden. Dieses Verhalten ist für Standardschlüsselanbieter und vertrauenswürdige Schlüsselanbieter identisch.

Der vSphere Native Key Provider funktioniert folgendermaßen.

1 Wenn Sie den Schlüsselanbieter erstellen, generiert vCenter Server einen primären Schlüssel und über gibt ihn an die ESXi-Hosts im Cluster weiter. (Es ist kein externer Schlüsselserver beteiligt.)

2 Die ESXi-Hosts erzeugen bei Bedarf einen DEK.

3 Wenn Sie eine Verschlüsselungsaktivität durchführen, werden die Daten mit dem DEK verschlüsselt.

   Verschlüsselte DEKs werden neben den verschlüsselten Daten gespeichert.

4 Wenn Sie Daten entschlüsseln, wird der primäre Schlüssel verwendet, um den DEK und dann die Daten zu entschlüsseln.

Was wird verschlüsselt?

vSphere Virtual Machine Encryption unterstützt die Verschlüsselung von Dateien der virtuellen Maschine, von virtuellen Festplattendateien und von Core-Dump-Dateien.

Dateien der virtuellen Maschine

Die meisten Dateien der virtuellen Maschine werden verschlüsselt, insbesondere Gastdaten, die nicht in der VMDK-Datei gespeichert werden. Zu diesen Dateien gehören unter anderen die NVRAM-, VSWP- und VMSN-Dateien. Der Schlüssel vom Schlüsselanbieter entsperrt ein verschlüsseltes Paket in der VMX-Datei, die interne Schlüssel und andere Geheimschlüssel enthält. Der Schlüsselabruf funktioniert je nach Schlüsselanbieter wie folgt:

- Standardschlüsselanbieter: vCenter Server verwaltet die Schlüssel vom Schlüsselserver und ESXi-Hosts können nicht direkt auf den Schlüsselanbieter zugreifen. Die Hosts warten, bis vCenter Server die Schlüssel überträgt.
- Vertrauenswürdiger Schlüsselanbieter und vSphere Native Key Provider: Die ESXi-Hosts greifen direkt auf die Schlüsselanbieter zu und rufen die angeforderten Schlüssel entweder direkt vom vSphere Trust Authority-Dienst oder vom vSphere Native Key Provider ab.

Wenn Sie den vSphere Client zum Erstellen einer verschlüsselten virtuellen Maschine verwenden, können Sie virtuelle Festplatten getrennt von VM-Dateien verschlüsseln und entschlüsseln. Alle virtuellen Festplatten sind standardmäßig verschlüsselt. Für andere Verschlüsselungsaufgaben wie das Verschlüsseln einer vorhandenen virtuellen Maschine können Sie virtuelle Festplatten getrennt von Dateien der virtuellen Maschine verschlüsseln und entschlüsseln.

Hinweis Eine verschlüsselte virtuelle Festplatte kann nicht einer unverschlüsselten virtuellen Maschine zugeordnet werden.

Virtuelle Festplattendateien

Daten in einer Datei einer verschlüsselten virtuellen Festplatte (VMDK-Datei) werden nie in Klartext in den Speicher oder auf eine physische Festplatte geschrieben und nie in Klartext über das Netzwerk übertragen. Die VMDK-Deskriptordatei besteht zum größten Teil aus Klartext, enthält jedoch eine Schlüssel-ID für den KEK und den internen Schlüssel (DEK) im verschlüsselten Paket.

Sie können die vSphere API zum Durchführen einer flachen Verschlüsselung mit einem neuen KEK oder einer tiefen Neuverschlüsselung mit einem neuen internen Schlüssel verwenden.

Core-Dumps

Core-Dumps auf einem ESXi-Host, auf dem der Verschlüsselungsmodus aktiviert ist, werden immer verschlüsselt. Weitere Informationen hierzu finden Sie unter vSphere VM-Verschlüsselung und Core-Dumps. Core-Dumps auf dem vCenter Server-System werden nicht verschlüsselt. Schützen Sie den Zugriff auf das vCenter Server-System.

Hinweis Informationen zu Einschränkungen bezüglich Geräten und Funktionen, mit denen vSphere Virtual Machine Encryption interagieren kann, finden Sie unter Interoperabilität bei der Verschlüsselung von virtuellen Maschinen.

Was wird nicht verschlüsselt?

Einige der Dateien, die einer virtuellen Maschine zugeordnet sind, werden nicht oder teilweise verschlüsselt.

Protokolldateien

Protokolldateien werden nicht verschlüsselt, da sie keine vertraulichen Daten enthalten.

Konfigurationsdateien der virtuellen Maschine

Die meisten Informationen zur Konfiguration der virtuellen Maschine (gespeichert in den VMX- und VMSD-Dateien) werden nicht verschlüsselt.

Deskriptordatei der virtuellen Festplatte

Zur Unterstützung der Festplattenverwaltung ohne Schlüssel werden die meisten Deskriptordateien der virtuellen Festplatte nicht verschlüsselt.

Wer darf kryptografische Vorgänge durchführen?

Nur Benutzer die über Berechtigungen für **Kryptografische Vorgänge** verfügen, können kryptografische Vorgänge durchführen. Die Berechtigungen sind fein unterteilt. Die standardmäßige Systemrolle „Administrator“ umfasst alle Berechtigungen für **Kryptografische Vorgänge**. Die Rolle, „Kein Kryptografie-Administrator“ unterstützt alle Administratorberechtigungen mit Ausnahme der Berechtigungen für **Kryptografievorgänge**.

Zusätzlich zur Verwendung der **Cryptographer.***-Berechtigungen kann vSphere Native Key Provider die Berechtigung **Cryptographer.ReadKeyServersInfo** verwenden, die spezifisch für vSphere Native Key Providers ist.

Weitere Informationen hierzu finden Sie unter Rechte für Verschlüsselungsvorgänge.

Sie können zusätzliche benutzerdefinierte Rollen erstellen, um beispielsweise zuzulassen, dass eine Gruppe von Benutzern virtuelle Maschinen verschlüsselt, zugleich aber zu verhindern, dass diese Benutzer virtuelle Maschinen entschlüsseln.

Wie können kryptografische Vorgänge durchgeführt werden?

Der vSphere Client unterstützt viele der kryptografischen Vorgänge. Für andere Aufgaben können Sie die vSphere API verwenden.

Tabelle 6-5. Schnittstellen für das Durchführen von kryptografischen Vorgängen

Schnittstelle	Vorgänge	Informationen
vSphere Client	Erstellen einer verschlüsselten virtuellen Maschine Verschlüsseln und Entschlüsseln virtueller Maschinen	Dieses Handbuch
PowerCLI	Erstellen einer verschlüsselten virtuellen Maschine Verschlüsseln und Entschlüsseln virtueller Maschinen Konfigurieren von vSphere Trust Authority	*Referenz zu VMware PowerCLI-Cmdlets*
vSphere Web Services SDK	Erstellen einer verschlüsselten virtuellen Maschine Verschlüsseln und Entschlüsseln virtueller Maschinen Durchführen einer tiefen Neuverschlüsselung einer virtuellen Maschine (Verwendung eines anderen DEK) Durchführen einer flachen Neuverschlüsselung einer virtuellen Maschine (Verwendung eines anderen KEK)	*Programmierhandbuch zum vSphere Web Services SDK* *vSphere Web Services-API-Referenz*
`crypto-util`	Entschlüsseln verschlüsselter Core-Dumps Prüfen, ob Dateien verschlüsselt sind Führen Sie andere Verwaltungsaufgaben direkt auf dem ESXi-Host durch.	Befehlszeilenhilfe vSphere VM-Verschlüsselung und Core-Dumps

Neuverschlüsselung virtueller Maschinen

Sie können eine virtuelle Maschine mit neuen Schlüsseln neu verschlüsseln, z. B. für den Fall, dass ein Schlüssel abläuft oder manipuliert wird. Die folgenden Optionen sind verfügbar.

- Eine tiefe Neuverschlüsselung, bei der sowohl der Festplattenverschlüsselungsschlüssel (DEK, Disk Encryption Key) als auch der Schlüsselverschlüsselungsschlüssel (KEK, Key Encryption Key) ersetzt wird
- Eine flache Neuverschlüsselung, bei der nur der KEK ersetzt wird

Sie müssen die Neuverschlüsselung einer virtuellen Maschine mithilfe der API durchführen. Weitere Informationen hierzu finden Sie unter *Programmierhandbuch zum vSphere Web Services SDK*.

Bei einer tiefen Neuverschlüsselung muss die virtuelle Maschine ausgeschaltet sein und darf keine Snapshots enthalten. Sie können eine flache Neuverschlüsselung bei eingeschalteter virtueller Maschine durchführen, sofern auf der virtuellen Maschine Snapshots vorhanden sind. Die flache Neuverschlüsselung einer verschlüsselten virtuellen Maschine mit Snapshots ist nur in einem einzelnen Snapshot-Zweig (Festplattenkette) zulässig. Mehrere Snapshot-Zweige werden nicht unterstützt. Darüber hinaus wird eine flache Neuverschlüsselung auf einem verknüpften Klon einer virtuellen Maschine oder Festplatte nicht unterstützt. Wenn die flache Neuverschlüsselung fehlschlägt, bevor alle Verknüpfungen in der Kette mit dem neuen KEK aktualisiert werden, können Sie weiterhin auf die verschlüsselte virtuelle Maschine zugreifen, vorausgesetzt, Sie verfügen über die alten und neuen KEKs. Es erweist sich jedoch am sinnvollsten, die flache Neuverschlüsselung vor dem Durchführen von Snapshot-Vorgängen erneut auszuführen.

vSphere Virtual Machine Encryption-Komponenten

Je nachdem, welchen Schlüsselanbieter Sie verwenden, tragen ein externer Schlüsselserver, das vCenter Server-System und Ihre ESXi-Hosts potenziell zur Verschlüsselungslösung bei.

Die folgenden Komponenten umfassen vSphere Virtual Machine Encryption:

- Einen externen Schlüsselserver, auch als KMS bezeichnet (für vSphere Native Key Provider nicht erforderlich)
- vCenter Server
- ESXi-Hosts

Schlüsselserver

Der Schlüsselserver ist ein KMIP-Verwaltungsserver (Key Management Interoperability Protocol), der einem Schlüsselanbieter zugeordnet ist. Ein Standardschlüsselanbieter und ein vertrauenswürdiger Schlüsselanbieter benötigen einen Schlüsselserver. vSphere Native Key Provider benötigt keinen Schlüsselserver. In der folgenden Tabelle werden die Unterschiede bei der Schlüsselanbieter- und Schlüsselserverinteraktion beschrieben.

Tabelle 6-6. Interaktion zwischen Schlüsselanbietern und Schlüsselservern

Schlüsselanbieter	Interaktion mit Schlüsselservern
Standardschlüsselanbieter	Ein Standardschlüsselanbieter verwendet vCenter Server zum Anfordern von Schlüsseln von einem Schlüsselserver. Der Schlüsselserver generiert und speichert die Schlüssel und leitet sie zur Verteilung an die ESXi-Hosts an vCenter Server weiter.
Vertrauenswürdiger Schlüsselanbieter	Ein vertrauenswürdiger Schlüsselanbieter verwendet einen Schlüsselanbieterdienst, mit dem die vertrauenswürdigen ESXi die Schlüssel direkt abrufen können. Weitere Informationen hierzu finden Sie unter Was ist der vSphere Trust Authority-Schlüsselanbieterdienst?.
vSphere Native Key Provider	vSphere Native Key Provider benötigt keinen Schlüsselserver. vCenter Server Generiert einen primären Schlüssel und über leitet ihn an die ESXi-Hosts weiter. Daraufhin generieren die ESXi-Hosts dann Datenverschlüsselungsschlüssel (auch wenn sie nicht mit dem vCenter Server verbunden sind). Weitere Informationen hierzu finden Sie unter vSphere Native Key Provider – Übersicht.

Sie können den vSphere Client oder die vSphere API verwenden, um Schlüsselanbieterinstanzen zum vCenter Server-System hinzuzufügen. Wenn Sie mehrere Schlüsselanbieterinstanzen in einem Cluster verwenden, müssen alle Instanzen vom selben Anbieter stammen und Schlüssel replizieren.

Wenn in Ihrer Umgebung verschiedene Schlüsselserveranbieter in unterschiedlichen Umgebungen verwendet werden, können Sie einen Schlüsselanbieter für jeden Schlüsselserver hinzufügen und einen Standardschlüsselanbieter angeben. Der erste hinzugefügte Schlüsselanbieter fungiert als Standardschlüsselanbieter. Sie können den Standardcluster auch zu einem späteren Zeitpunkt explizit festlegen.

Als KMIP-Client verwendet vCenter Server das KMIP (Key Management Interoperability Protocol), um eine problemlose Verwendung des Schlüsselservers Ihrer Wahl zu gewährleisten.

vCenter Server

In der folgenden Tabelle wird die Rolle von vCenter Server beim Verschlüsselungsprozess beschrieben.

Tabelle 6-7. Schlüsselanbieter und vCenter Server

Schlüsselanbieter	Rolle von vCenter Server	Wie werden die Rechte überprüft?
Standardschlüsselanbieter	Nur vCenter Server verfügt über die Anmeldedaten für die Anmeldung beim Schlüsselserver. Ihre ESXi-Hosts verfügen nicht über diese Anmeldedaten. vCenter Server ruft Schlüssel vom Schlüsselserver ab und pusht diese an die ESXi-Hosts. Der vCenter Server speichert keine Schlüsselserver-Schlüssel, sondern nur eine Liste mit Schlüssel-IDs.	vCenter Server überprüft die Berechtigungen der Benutzer, die Kryptografie-Vorgänge durchführen.
Vertrauenswürdiger Schlüsselanbieter	Mit vSphere Trust Authority muss vCenter Server nicht länger Schlüssel vom Schlüsselserver anfordern und der Zugriff auf die Verschlüsselungsschlüssel wird somit abhängig vom Bestätigungszustand eines Arbeitslastclusters. Sie müssen getrennte vCenter Server-Systeme für den vertrauenswürdigen Cluster und den Trust Authority Cluster verwenden.	vCenter Server überprüft die Berechtigungen der Benutzer, die Kryptografie-Vorgänge durchführen. Nur Benutzer, die Mitglieder der TrustedAdmins SSO-Gruppe sind, können Verwaltungsvorgänge durchführen.
vSphere Native Key Provider	Der vCenter Server generiert die Schlüssel.	vCenter Server überprüft die Berechtigungen der Benutzer, die Kryptografie-Vorgänge durchführen.

Sie können den vSphere Client zum Zuweisen von Berechtigungen für Kryptografie-Vorgänge oder zum Zuweisen der benutzerdefinierten Rolle **Kein Kryptografie-Administrator** zu Benutzergruppen verwenden. Weitere Informationen hierzu finden Sie unter Voraussetzungen und erforderliche Berechtigungen für die Verschlüsselung.

vCenter Server fügt Kryptografie-Ereignisse zur Ereignisliste hinzu, die Sie über die vSphere Client-Ereigniskonsole anzeigen und exportieren können. Jedes Ereignis enthält den Benutzer, die Uhrzeit, die Schlüssel-ID und den Kryptografie-Vorgang.

Die Schlüssel aus dem Schlüsselserver werden als Schlüssel für Verschlüsselungsschlüssel (KEKs) verwendet.

ESXi-Hosts

ESXi-Hosts sind verantwortlich für einige Aspekte des Verschlüsselungs-Workflows.

Tabelle 6-8. ESXi-Hosts

Schlüsselanbieter	ESXi-Hostaspekte
Standardschlüsselanbieter	■ vCenter Server leitet Schlüssel an den ESXi-Host weiter, wenn dieser einen Schlüssel benötigt. Für den Host muss der Verschlüsselungsmodus aktiviert sein. Die Rolle des aktuellen Benutzers muss Berechtigungen für Kryptografie-Vorgänge enthalten. Weitere Informationen hierzu finden Sie unter Voraussetzungen und erforderliche Berechtigungen für die Verschlüsselung und Rechte für Verschlüsselungsvorgänge. ■ Es wird sichergestellt, dass die Gastdaten für verschlüsselte virtuelle Maschinen beim Speichern auf die Festplatte verschlüsselt werden. ■ Es wird sichergestellt, dass die Gastdaten für verschlüsselte virtuelle Maschinen nicht ohne Verschlüsselung über das Netzwerk weitergeleitet werden.
Vertrauenswürdiger Schlüsselanbieter	Die ESXi-Hosts führen vSphere Trust Authority aus, je nachdem, ob es sich um vertrauenswürdige Hosts oder Trust Authority Hosts handelt. Auf vertrauenswürdigen ESXi-Hosts werden virtuelle Arbeitslastmaschinen ausgeführt, die mithilfe der von den Trust Authority Hosts veröffentlichten Schlüsselanbieter verschlüsselt werden können. Weitere Informationen hierzu finden Sie unter Vertrauenswürdige Infrastruktur – Übersicht.
vSphere Native Key Provider	Die ESXi-Hosts rufen Schlüssel direkt vom vSphere Native Key Provider ab.

Die vom ESXi-Host generierten Schlüssel werden in diesem Dokument als interne Schlüssel bezeichnet. Diese Schlüssel fungieren normalerweise als Schlüssel zur Datenverschlüsselung.

Prozessablauf bei der Verschlüsselung

Nachdem Sie einen Schlüsselanbieter eingerichtet haben, können Benutzer mit den erforderlichen Berechtigungen verschlüsselte virtuelle Maschinen und Festplatten erstellen. Diese Benutzer können auch vorhandene virtuelle Maschinen verschlüsseln und verschlüsselte virtuelle Maschinen entschlüsseln sowie virtuellen Maschinen vTPMs (Virtual Trusted Platform Modules) hinzufügen.

Je nach Typ des Schlüsselanbieters kann der Prozessablauf einen Schlüsselserver, den vCenter Server und den ESXi-Host beinhalten.

Prozessablauf bei der Verschlüsselung des Standardschlüsselanbieters

Während des Verschlüsselungsvorgangs interagieren die unterschiedlichen Komponenten von vSphere folgendermaßen.

1 Wenn eine Benutzer eine Verschlüsselungsaufgabe durchführt, z. B. die Erstellung einer verschlüsselten virtuellen Maschine, fordert der vCenter Server einen neuen Schlüssel vom Standardschlüsselserver an. Dieser Schlüssel wird als KEK verwendet.

2 Der vCenter Server speichert diese Schlüssel-ID und gibt den Schlüssel an den ESXi-Host weiter. Wenn der ESXi-Host zu einem Cluster gehört, sendet der vCenter Server den KEK an jeden Host im Cluster.

   Der Schlüssel selbst wird nicht im vCenter Server-System gespeichert. Nur die Schlüssel-ID ist bekannt.

3 Der ESXi-Host generiert interne Schlüssel (DEKs) für die virtuelle Maschine und deren Festplatten. Es legt die internen Schlüssel nur im Arbeitsspeicher ab und verwendet die KEKs zum Verschlüsseln der internen Schlüssel.

   Nicht verschlüsselte interne Schlüssel werden niemals auf der Festplatte gespeichert. Es werden nur verschlüsselte Daten gespeichert. Da die KEKs vom Schlüsselserver stammen, verwendet der Host weiterhin dieselben KEKs.

4 Der ESXi-Host verschlüsselt die virtuelle Maschine mit dem verschlüsselten internen Schlüssel.

   Jeder Host, der über den KEK verfügt und auf die verschlüsselte Schlüsseldatei zugreifen kann, kann Vorgänge auf der verschlüsselten virtuellen Maschine oder Festplatte ausführen.

Prozessablauf bei der Verschlüsselung des vertrauenswürdigen Schlüsselanbieters

Der Prozessablauf bei der vSphere Trust Authority-Verschlüsselung umfasst die vSphere Trust Authority-Dienste, die vertrauenswürdigen Schlüsselanbieter sowie den vCenter Server und die ESXi-Hosts.

Das Verschlüsseln einer virtuellen Maschine mit einem vertrauenswürdigen Schlüsselanbieter entspricht der Benutzererfahrung bei der VM-Verschlüsselung bei Verwendung eines Standardschlüsselanbieters. Die VM-Verschlüsselung unter vSphere Trust Authority verlässt sich weiterhin entweder auf die Speicherrichtlinien für die Verschlüsselung von virtuellen Maschinen oder auf das Vorhandensein eines vTPM-Geräts, um zu entscheiden, wann eine virtuelle Maschine verschlüsselt werden soll. Sie verwenden weiterhin einen standardmäßig konfigurierten Schlüsselanbieter (in vSphere 6.5 und 6.7 als KMS-Cluster bezeichnet), wenn Sie eine virtuelle Maschine über den vSphere Client verschlüsseln. Darüber hinaus können Sie die APIs immer noch auf ähnliche Weise verwenden, um den Schlüsselanbieter manuell anzugeben. Die vorhandenen Kryptografierechte, die für vSphere 6.5 hinzugefügt wurden, gelten nach wie vor in vSphere 7.0 für vSphere Trust Authority.

Der Verschlüsselungsprozess für den vertrauenswürdigen Schlüsselanbieter weist einige wichtige Unterschiede zum Standardschlüsselanbieter auf:

- Trust Authority-Administratoren geben Informationen nicht direkt an, wenn sie einen Schlüsselserver für eine vCenter Server-Instanz einrichten, und sie legen auch die Vertrauensstellung des Schlüsselservers nicht fest. Stattdessen veröffentlicht vSphere Trust Authority vertrauenswürdige Schlüsselanbieter, die von den vertrauenswürdigen Hosts verwendet werden können.
- vCenter Server überträgt Schlüssel nicht mehr an ESXi-Hosts und kann stattdessen jeden vertrauenswürdigen Schlüsselanbieter als einzelnen Schlüssel der obersten Ebene verarbeiten.
- Nur vertrauenswürdige Hosts können Verschlüsselungsvorgänge von Trust Authority-Hosts anfordern.

Prozessablauf bei der vSphere Native Key Provider-Verschlüsselung

vSphere Native Key Provider ist im Lieferumfang von vSphere ab Version 7.0 Update 2 enthalten. Wenn Sie einen vSphere Native Key Provider konfigurieren, überträgt vCenter Server einen primären Schlüssel an alle ESXi-Hosts im Cluster. Ebenso wird die Änderung an die Hosts im Cluster übertragen, wenn Sie einen vSphere Native Key Provider aktualisieren oder löschen. Der Prozessablauf bei der Verschlüsselung ähnelt der Funktionsweise eines vertrauenswürdigen Schlüsselanbieters. Der Unterschied besteht darin, dass vSphere Native Key Provider die Schlüssel generiert und sie mit dem Primärschlüssel umhüllt und dann zur Verschlüsselung zurückgibt.

Benutzerdefinierte Attribute für Schlüsselserver

Das KMIP-Protokoll (Key Management Interoperability Protocol) bietet Unterstützung beim Hinzufügen benutzerdefinierter Attribute, die für anbieterspezifische Zwecke bestimmt sind. Mit benutzerdefinierten Attributen können Sie die in Ihrem Schlüsselserver gespeicherten Schlüssel genauer angeben. vCenter Server fügt die folgenden benutzerdefinierten Attribute für VM- und Hostschlüssel hinzu.

Tabelle 6-9. Benutzerdefinierte Attribute für die Verschlüsselung virtueller Maschinen

Benutzerdefiniertes Attribut	Wert
`x-Vendor`	VMware, Inc.
`x-Product`	VMware vSphere
`x-Product_Version`	vCenter Server-Version
`x-Component`	Virtuelle Maschine
`x-Name`	Name der virtuellen Maschine (aus ConfigInfo oder ConfigSpec erfasst)
`x-Identifier`	Instanz-UUID der virtuellen Maschine (aus ConfigInfo oder ConfigSpec erfasst)

Tabelle 6-10. Benutzerdefinierte Attribute für die Hostverschlüsselung

Benutzerdefiniertes Attribut	Wert
`x-Vendor`	VMware, Inc.
`x-Product`	VMware vSphere
`x-Product_Version`	vCenter Server-Version
`x-Component`	ESXi-Server
`x-Name`	Hostname
`x-Identifier`	Hardware-UUID des Hosts

vCenter Server fügt die Attribute `x-Vendor`, `x-Product` und `x-Product_Version` hinzu, wenn der Schlüsselserver einen Schlüssel erstellt. Wenn der Schlüssel zum Verschlüsseln einer virtuellen Maschine oder eines Hosts verwendet wird, legt vCenter Server die Attribute `x-Component`, `x-Identifier` und `x-Name` fest. Unter Umständen können Sie diese benutzerdefinierten Attribute auf der Schlüsselserver-Benutzeroberfläche anzeigen. Erkundigen Sie sich bei Ihrem Schlüsselserveranbieter.

Sowohl der Host- als auch der VM-Schlüssel enthalten die sechs benutzerdefinierten Attribute. `x-Vendor`, `x-Product` und `x-Product_Version` sind möglicherweise für beide Schlüssel identisch. Diese Attribute werden beim Erzeugen des Schlüssels festgelegt. Je nachdem, ob der Schlüssel für eine virtuelle Maschine oder einen Host verwendet wird, werden unter Umständen die Attribute `x-Component`, `x-Identifier` und `x-Name` angehängt.

Schlüsselfehler

Wenn beim Senden von Schlüsseln vom Schlüsselserver an einen ESXi-Host ein Fehler auftritt, erzeugt vCenter Server eine Meldung im Ereignisprotokoll für die folgenden Ereignisse:

- Das Hinzufügen von Schlüsseln zum ESXi-Host ist aufgrund von Problemen bei der Hostverbindung oder -unterstützung fehlgeschlagen.
- Das Abrufen von Schlüsseln aus dem Schlüsselserver ist aufgrund eines fehlenden Schlüssels im Schlüsselserver fehlgeschlagen.
- Das Abrufen von Schlüsseln aus dem Schlüsselserver ist aufgrund der Schlüsselserververbindung fehlgeschlagen.

Entschlüsseln verschlüsselter virtueller Maschinen

Wenn Sie später eine verschlüsselte virtuelle Maschine entschlüsseln möchten, ändern Sie deren Speicherrichtlinie. Sie können die Speicherrichtlinie für die virtuelle Maschine und alle Festplatten ändern. Wenn Sie individuelle Komponenten entschlüsseln möchten, entschlüsseln Sie zunächst ausgewählte Festplatten und anschließend die virtuelle Maschine, indem Sie die Speicherrichtlinie für VM-Home ändern. Beide Schlüssel sind für die Entschlüsselung jeder Komponente notwendig. Weitere Informationen hierzu finden Sie unter Entschlüsseln einer verschlüsselten virtuellen Maschine oder virtuellen Festplatte.

Verschlüsseln von virtuellen Festplatten

Wenn Sie eine verschlüsselte virtuelle Maschine anhand des vSphere Client erstellen, können Sie die Festplatten auswählen, die aus der Verschlüsselung ausgeschlossen werden sollen. Sie können später Festplatten hinzufügen und deren Verschlüsselungsrichtlinien festlegen. Sie können keine verschlüsselte Festplatte zu einer unverschlüsselten virtuellen Maschine hinzufügen und Sie können keine Festplatte verschlüsseln, wenn die virtuelle Maschine nicht verschlüsselt ist.

Die Verschlüsselung einer virtuellen Maschine und ihrer Festplatten wird durch Speicherrichtlinien gesteuert. Die Speicherrichtlinie für VM Home regelt die virtuelle Maschine selbst und jede virtuelle Festplatte verfügt über eine zugeordnete Speicherrichtlinie.

- Wenn die Speicherrichtlinien von VM Home auf eine Verschlüsselungsrichtlinie festgelegt werden, wird nur die virtuelle Maschine selbst verschlüsselt.
- Wenn die Speicherrichtlinien von VM Home und allen Festplatten auf eine Verschlüsselungsrichtlinie festgelegt werden, werden alle Komponenten verschlüsselt.

Beachten Sie die folgenden Anwendungsbeispiele.

Tabelle 6-11. Anwendungsbeispiele für die Verschlüsselung von virtuellen Festplatten

Anwendungsfall	Details
Erstellen einer verschlüsselten virtuellen Maschine.	Wenn Sie während der Erstellung einer verschlüsselten virtuellen Maschine Festplatten hinzufügen, werden die Festplatten standardmäßig verschlüsselt. Sie können die Richtlinie so ändern, dass eine oder mehrere Festplatten nicht verschlüsselt werden. Nach Erstellung der virtuellen Maschine können Sie für jede Festplatte explizit die Speicherrichtlinien ändern. Weitere Informationen hierzu finden Sie unter Ändern der Verschlüsselungsrichtlinie für virtuelle Festplatten.
Verschlüsseln einer virtuellen Maschine.	Um eine vorhandene virtuelle Maschine zu verschlüsseln, müssen Sie deren Speicherrichtlinie ändern. Sie können die Speicherrichtlinien für die virtuelle Maschine und alle virtuellen Festplatten ändern. Wenn Sie nur die virtuelle Maschine verschlüsseln möchten, können Sie für VM Home eine Verschlüsselungsrichtlinie und für jede virtuelle Festplatte eine andere Speicherrichtlinie angeben, z. B. Standarddatenspeicher. Weitere Informationen hierzu finden Sie unter Erstellen einer verschlüsselten virtuellen Maschine.
Hinzufügen einer vorhandenen unverschlüsselten Festplatte zu einer verschlüsselten virtuellen Maschine (Speicherrichtlinie für die Verschlüsselung)	Schlägt mit Fehlermeldung fehl. Sie müssen die Festplatte mit der Standard-Speicherrichtlinie hinzufügen, können aber die Speicherrichtlinie später ändern. Weitere Informationen hierzu finden Sie unter Ändern der Verschlüsselungsrichtlinie für virtuelle Festplatten.
Hinzufügen einer vorhandenen unverschlüsselten Festplatte mit einer Speicherrichtlinie zu einer verschlüsselten virtuellen Maschine, die keine Verschlüsselung enthält, z. B. Standarddatenspeicher.	Die Festplatte verwendet die Standard-Speicherrichtlinie. Nach dem Hinzufügen der Festplatte können Sie die Speicherrichtlinie explizit ändern, wenn Sie eine verschlüsselte Festplatte möchten. Weitere Informationen hierzu finden Sie unter Ändern der Verschlüsselungsrichtlinie für virtuelle Festplatten.
Hinzufügen einer verschlüsselten Festplatte zu einer verschlüsselten virtuellen Maschine; Die VM Home-Speicherrichtlinie ist „Verschlüsselung“.	Wenn Sie die Festplatte hinzufügen, bleibt sie verschlüsselt. Der vSphere Client zeigt die Größe und andere Attribute sowie den Verschlüsselungsstatus an.

Tabelle 6-11. Anwendungsbeispiele für die Verschlüsselung von virtuellen Festplatten (Fortsetzung)

Anwendungsfall	Details
Hinzufügen einer vorhandenen verschlüsselten Festplatte zu einer unverschlüsselten virtuellen Maschine	Dieser Anwendungsfall wird nicht unterstützt.
Registrieren einer verschlüsselten virtuellen Maschine	Wenn Sie eine verschlüsselte virtuelle Maschine aus vCenter Server entfernen, aber nicht von der Festplatte löschen, können Sie sie in die vCenter Server-Bestandsliste zurücksetzen, indem Sie die VMX-Datei (Konfiguration der virtuellen Maschine) der VM registrieren. Um die verschlüsselte VM zu registrieren, muss der Benutzer über das Recht **Verschlüsselungsvorgänge.VM registrieren** verfügen. Wenn die VM mithilfe eines Standardschlüsselanbieters verschlüsselt wurde und die verschlüsselte VM registriert ist, überträgt vCenter Server die erforderlichen Schlüssel an den ESXi-Host. Wenn der Benutzer, der die VM registriert, nicht über das Recht **Verschlüsselungsvorgänge.VM registrieren** verfügt, sperrt vCenter Server die VM bei Registrierung, und die VM kann nicht verwendet werden, bis sie entsperrt wird. Wenn die VM mithilfe eines vertrauenswürdigen Schlüsselanbieters oder vSphere Native Key Provider verschlüsselt wurde und die verschlüsselte VM registriert ist, überträgt vCenter Server keine Schlüssel mehr an den ESXi-Host. Stattdessen werden die Schlüssel vom Hosts abgerufen, wenn die VM registriert ist. Wenn der Benutzer, der die VM registriert, nicht über das Recht **Verschlüsselungsvorgänge.VM registrieren** verfügt, lässt vCenter Server den Vorgang nicht zu.

Fehler bei der Verschlüsselung von virtuellen Maschinen

Wenn vCenter Server auf einen kritischen Fehler bei der VM-Verschlüsselung stößt, wird ein Ereignis erstellt. Sie können diese Ereignisse anzeigen, um Verschlüsselungsfehler zu beheben.

vCenter Server erstellt Ereignisse für die folgenden kritischen Fehler bei der VM-Verschlüsselung.

- Fehler beim Generieren eines KEK.
- Nicht genügend Festplattenspeicher auf dem Datenspeicher, um eine verschlüsselte virtuelle Maschine zu erstellen.
- Unzureichende Benutzerberechtigung zum Initiieren des Verschlüsselungsvorgangs.
- Der angegebene Schlüssel fehlt beim Schlüsselanbieter, sodass der ESXi-Hostschlüssel mit einem neuen Schlüssel erneuert wird.
- Beim Schlüsselanbieter mit dem angegebenen Schlüssel ist ein Fehler aufgetreten. Daher wird der ESXi-Hostschlüssel mit einem neuen Schlüssel erneuert.

Voraussetzungen und erforderliche Berechtigungen für die Verschlüsselung

Eine Verschlüsselung ist nur in Umgebungen mit vCenter Server möglich. Zusätzlich muss für die meisten Verschlüsselungsaufgaben bei dem ESXi-Host der Verschlüsselungsmodus aktiviert sein. Der Benutzer, der diese Aufgaben durchführt, muss über die entsprechenden Berechtigungen verfügen. Eine Gruppe von Berechtigungen für **Kryptografievorgänge** ermöglicht eine detaillierte Steuerung. Wenn bei Verschlüsselungsaufgaben für virtuelle Maschinen ein Wechsel in den Hostverschlüsselungsmodus erforderlich ist, sind zusätzliche Berechtigungen erforderlich.

Hinweis vSphere Trust Authority weist zusätzliche Voraussetzungen und notwendige Berechtigungen auf. Weitere Informationen hierzu finden Sie unter Voraussetzungen und notwendige Berechtigungen für vSphere Trust Authority.

Kryptografie-Berechtigungen und -rollen

Standardmäßig verfügt der Benutzer mit der Rolle des vCenter Server-Administrators über alle Berechtigungen. Die Rolle **Kein Kryptografie-Administrator** ist mit den folgenden, für Kryptografie-Vorgänge erforderlichen Berechtigungen ausgestattet.

- Fügen Sie Berechtigungen für **Kryptografievorgänge** hinzu.
- **Global.Diagnose**
- **Host.Bestandsliste.Host zu Cluster hinzufügen**
- **Host.Bestandsliste.Eigenständigen Host hinzufügen**
- **Host.Lokale Vorgänge.Benutzergruppen verwalten**

Sie können die Rolle **Kein Kryptografie-Administrator** vCenter Server-Administratoren zuweisen, die die Berechtigungen **Kryptografievorgänge** nicht benötigen.

Um den Handlungsspielraum der Benutzer weiter einzuschränken, können Sie die Rolle **Kein Kryptografie-Administrator** klonen und eine benutzerdefinierte Rolle erstellen, die nur bestimmte Berechtigungen der **Kryptografievorgänge** umfasst. Sie können beispielsweise eine Rolle erstellen, die Benutzern das Verschlüsseln virtueller Maschinen erlaubt, das Entschlüsseln jedoch nicht. Weitere Informationen hierzu finden Sie unter Verwenden von Rollen zum Zuweisen von Rechten.

Hostverschlüsselungsmodus

Der Hostverschlüsselungsmodus entscheidet darüber, ob ein ESXi-Host bereit ist, kryptografisches Material zum Verschlüsseln virtueller Maschinen und virtueller Festplatten zu akzeptieren. Bevor Kryptografievorgänge auf einem Host stattfinden können, muss der Hostverschlüsselungsmodus aktiviert werden. Der Hostverschlüsselungsmodus wird häufig automatisch aktiviert, wenn er benötigt wird. Sie können ihn jedoch explizit aktivieren. Sie können den aktuellen Hostverschlüsselungsmodus über den vSphere Client oder die vSphere API festlegen.

Wenn der Hostverschlüsselungsmodus aktiviert ist, installiert vCenter Server auf dem Host einen Hostschlüssel, der sicherstellt, dass der Host in kryptografischer Hinsicht „sicher“ ist. Nachdem der Hostschlüssel installiert wurde, können andere Kryptografievorgänge ablaufen, einschließlich des Abrufens von Schlüsseln aus dem Schlüsselanbieter und deren Weitergabe an die ESXi-Hosts seitens vCenter Server.

Im „sicheren“ Modus werden die Core-Dumps von Benutzer-Worlds (d. h. hostd) und verschlüsselten virtuellen Maschinen verschlüsselt. Die Core-Dumps von nicht verschlüsselten virtuellen Maschinen werden nicht verschlüsselt.

Weitere Informationen zu verschlüsselten Core-Dumps und deren Verwendung seitens des technischen Supports von VMware finden Sie im VMware Knowledgebase-Artikel unter http://kb.vmware.com/kb/2147388.

Eine Anleitung dafür finden Sie in Explizites Aktivieren des Hostverschlüsselungsmodus.

Nach der Aktivierung der Hostverschlüsselungsmodus ist dessen einfache Deaktivierung nicht mehr möglich. Weitere Informationen hierzu finden Sie unter Deaktivieren des Hostverschlüsselungsmodus mithilfe der API.

Es werden automatische Änderungen vorgenommen, wenn Verschlüsselungsvorgänge versuchen, den Hostverschlüsselungsmodus zu aktivieren. Angenommen, Sie möchten einem eigenständigen Host eine verschlüsselte virtuelle Maschine hinzufügen. Der Hostverschlüsselungsmodus ist nicht aktiviert. Wenn Sie über die erforderlichen Berechtigungen auf dem Host verfügen, werden Verschlüsselungsmodusänderungen automatisch aktiviert.

Angenommen, ein Cluster umfasst die drei ESXi-Hosts A, B und C. Sie erstellen eine verschlüsselte virtuelle Maschine auf Host A. Was daraufhin geschieht, hängt von mehreren Faktoren ab.

- Wenn für die Hosts A, B und C die Verschlüsselung bereits aktiviert ist, benötigen Sie nur die Berechtigungen **Kryptografievorgänge.Neue verschlüsseln**, um die virtuelle Maschine zu erstellen.
- Wenn für die Hosts A und B Verschlüsselung aktiviert ist und für C nicht, geht das System wie folgt vor.
  - Nehmen wir an, dass Sie auf jedem Host über die Berechtigungen **Kryptografievorgänge.Neue verschlüsseln** und **Kryptografievorgänge.Host registrieren** verfügen. In diesem Fall wird die Verschlüsselung auf Host C durch den Erstellungsprozess für virtuelle Maschinen aktiviert. Der Verschlüsselungsprozess aktiviert den Hostverschlüsselungsmodus auf Host C und verteilt den Schlüssel an alle Hosts im Cluster.

    In diesem Fall können Sie die Hostverschlüsselung auf Host C auch explizit aktiveren.
  - Angenommen, Sie verfügen auf der virtuellen Maschine bzw. dem VM-Ordner nur über die Berechtigungen **Kryptografievorgänge.Neue verschlüsseln**. In diesem Fall gelingt die Erstellung der virtuellen Maschine und der Schlüssel steht auf Host A und Host B zur Verfügung. Host C bleibt für die Verschlüsselung deaktiviert und verfügt nicht über den Schlüssel der virtuellen Maschine.

- Wenn die Verschlüsselung für keinen der Hosts aktiviert ist und Sie auf Host A über die Berechtigungen **Kryptografievorgänge.Host registrieren** verfügen, wird die Hostverschlüsselung auf diesem Host durch den Prozess zum Erstellen der virtuellen Maschine aktiviert. Andernfalls kommt es zu einem Fehler.
- Sie können auch die vSphere API verwenden, um den Verschlüsselungsmodus eines Clusters auf „Aktivierung erzwingen“ festzulegen. Mit „Aktivierung erzwingen“ wird erreicht, dass alle Hosts im Cluster in kryptografischer Hinsicht „sicher“ sind, d. h., vCenter Server hat einen Hostschlüssel auf dem Host installiert. Weitere Informationen hierzu finden Sie unter *Programmierhandbuch zum vSphere Web Services SDK*.

Anforderungen an den Festplattenspeicher

Zur Verschlüsselung einer virtuellen Maschine ist im Vergleich zum bisherigen Speicherbedarf mindestens der doppelte Speicherplatz nötig.

Verschlüsseltes vSphere vMotion

vSphere vMotion verwendet beim Migrieren verschlüsselter virtueller Maschinen immer Verschlüsselung. Bei nicht verschlüsseln virtuellen Maschinen können Sie eine der verschlüsselten vSphere vMotion-Optionen auswählen.

Verschlüsseltes vSphere vMotion sichert die Vertraulichkeit, Integrität und Authentizität der mit vSphere vMotion übertragenen Daten. vSphere unterstützt verschlüsseltes vMotion nicht verschlüsselter und verschlüsselter virtueller Maschinen für vCenter Server-Instanzen.

Was wird verschlüsselt?

Bei verschlüsselten Festplatten werden die übertragenen Daten immer verschlüsselt übertragen. Bei unverschlüsselten Festplatten gilt Folgendes:

- Wenn Festplattendaten innerhalb eines Hosts übertragen werden, also ohne den Host zu ändern, ändern Sie nur den Datenspeicher; die Übertragung wird nicht verschlüsselt.
- Wenn Festplattendaten zwischen Hosts übertragen und verschlüsseltes vMotion verwendet wird, wird die Übertragung verschlüsselt. Wenn verschlüsseltes vMotion nicht verwendet wird, wird die Übertragung unverschlüsselt.

Bei verschlüsselten virtuellen Maschinen wird für die Migration mit vSphere vMotion immer verschlüsseltes vSphere vMotion verwendet. Sie können verschlüsseltes vSphere vMotion für verschlüsselte virtuelle Maschinen nicht deaktivieren.

Zustände von verschlüsseltem vSphere vMotion

Bei nicht verschlüsselten virtuellen Maschinen können Sie für die Verschlüsselung von vSphere vMotion einen der folgenden Zustände festlegen. Der Standard ist „Opportunistisch“.

Deaktiviert

Verschlüsseltes vSphere vMotion wird nicht verwendet.

Opportunistisch

Verschlüsseltes vSphere vMotion wird verwendet, wenn diese Funktion von Quell- und Zielhosts unterstützt wird. Nur ESXi Version 6.5 und höher verwendet verschlüsseltes vSphere vMotion.

Erforderlich

Nur verschlüsseltes vSphere vMotion zulassen. Wenn der Quell- oder Zielhost verschlüsseltes vSphere vMotion nicht unterstützt, ist die Migration mit vSphere vMotion nicht zulässig.

Wenn Sie eine virtuelle Maschine verschlüsseln, speichert die virtuelle Maschine einen Eintrag der aktuellen Verschlüsselungseinstellung von vSphere vMotion. Wenn Sie zu einem späteren Zeitpunkt die Verschlüsselung der virtuellen Maschine deaktivieren, verbleibt die verschlüsselte vMotion-Einstellung im Zustand „Erforderlich“, bis Sie diese Einstellung explizit ändern. Sie können diese Einstellungen über **Einstellungen bearbeiten** ändern.

Weitere Informationen zum Aktivieren und Deaktivieren von verschlüsseltem vSphere vMotion für nicht verschlüsselte virtuelle Maschinen finden Sie in der Dokumentation zu *vCenter Server und Hostverwaltung*.

Hinweis Derzeit müssen Sie die vSphere APIs verwenden, um verschlüsselte virtuelle Maschinen über vCenter Server-Instanzen hinweg zu migrieren oder zu klonen. Weitere Informationen finden Sie unter *Programmierhandbuch zum vSphere Web Services SDK* und *vSphere Web Services-API-Referenz*.

Migrieren oder Klonen verschlüsselter virtueller Maschinen über vCenter Server-Instanzen hinweg

vSphere vMotion bietet Unterstützung für die Migration und das Klonen verschlüsselter virtueller Maschinen über vCenter Server-Instanzen hinweg.

Beim Migrieren oder Klonen verschlüsselter virtueller Maschinen über vCenter Server-Instanzen müssen die Quell- und Zielinstanz von vCenter Server für die gemeinsame Nutzung des Schlüsselanbieters konfiguriert werden, der zum Verschlüsseln der virtuellen Maschine verwendet wurde. Darüber hinaus muss der Name des Schlüsselanbieters sowohl auf der Quell- als auch auf der Zielinstanz in vCenter Server identisch sein und folgende Eigenschaften aufweisen:

- Standardschlüsselanbieter: Derselbe Schlüsselserver (oder mehrere Schlüsselserver) muss sich im Schlüsselanbieter befinden.
- Vertrauenswürdiger Schlüsselanbieter: Derselbe vSphere Trust Authority-Dienst muss auf dem Zielhost konfiguriert werden.
- vSphere Native Key Provider: Muss denselben KDK aufweisen.

Der Ziel-vCenter Server stellt sicher, dass der Verschlüsselungsmodus für den ESXi-Zielhost aktiviert ist. Hiermit wird gewährleistet, dass der Host kryptografisch als „sicher“ gilt.

Die folgenden Rechte sind erforderlich, wenn Sie vSphere vMotion verwenden, um eine verschlüsselte virtuelle Maschine über vCenter Server-Instanzen hinweg zu migrieren oder zu klonen.

- Migrieren: **Kryptografievorgänge.Migrieren** auf der virtuellen Maschine
- Klonen: **Kryptografievorgänge.Klonen** auf der virtuellen Maschine

Außerdem muss der Ziel-vCenter Server die Berechtigung **Kryptografievorgänge.Neue verschlüsseln** aufweisen. Wenn der ESXi-Zielhost nicht im sicheren Modus ausgeführt wird, muss sich die Berechtigung **Kryptografievorgänge.Host registrieren** ebenfalls auf dem Ziel-vCenter Server befinden.

Bestimmte Aufgaben sind nicht zulässig, wenn virtuelle Maschinen (nicht verschlüsselt oder verschlüsselt) auf demselben vCenter Server oder auf mehreren vCenter Server-Instanzen migriert werden.

- Sie können die VM-Speicherrichtlinie nicht ändern.
- Sie können keine Schlüsseländerung vornehmen.

Hinweis Sie können die VM-Speicherrichtlinie beim Klonen virtueller Maschinen ändern.

Mindestanforderungen zum Migrieren oder Klonen verschlüsselter virtueller Maschinen über vCenter Server-Instanzen hinweg

Die Mindestanforderungen an die Version zum Migrieren oder Klonen verschlüsselter virtueller Maschinen des Standardschlüsselanbieters über vCenter Server-Instanzen mithilfe von vSphere vMotion lauten:

- Auf der Quell- und Zielinstanz von vCenter Server muss Version 7.0 oder höher installiert sein.
- Auf dem Quell- und Zielhost von ESXi muss Version 6.7 oder höher installiert sein.

Die Mindestanforderungen an die Version zum Migrieren oder Klonen verschlüsselter virtueller Maschinen des vertrauenswürdigen Schlüsselanbieters über vCenter Server-Instanzen mithilfe von vSphere vMotion lauten:

- Der vSphere Trust Authority-Dienst muss für den Zielhost konfiguriert werden und der Zielhost muss bestätigt sein.
- Die Verschlüsselung kann bei der Migration nicht geändert werden. Eine nicht verschlüsselte Festplatte kann beispielsweise nicht verschlüsselt werden, während die virtuelle Maschine auf den neuen Speicher migriert wird.
- Sie können eine verschlüsselte virtuelle Standardmaschine auf einen vertrauenswürdigen Host migrieren. Der Name des Schlüsselanbieters muss sowohl auf der Quell- als auch auf der Zielinstanz von vCenter Server identisch sein.
- Sie können eine verschlüsselte virtuelle vSphere Trust Authority-Maschine nicht auf einen nicht vertrauenswürdigen Host migrieren.

vMotion des vertrauenswürdigen Schlüsselanbieters und vCenter Server-übergreifendes vMotion

Der vertrauenswürdige Schlüsselanbieter bietet vollständige Unterstützung für vMotion über mehrere ESXi-Hosts hinweg.

vCenter Server übergreifendes vMotion wird mit den folgenden Einschränkungen unterstützt.

1. Der benötigte vertrauenswürdige Dienst muss auf dem Zielhost konfiguriert und der Zielhost muss bestätigt werden.
2. Die Verschlüsselung kann bei der Migration nicht geändert werden. Eine Festplatte kann beispielsweise nicht verschlüsselt werden, während die virtuelle Maschine auf den neuen Speicher migriert wird.

Bei der Durchführung von vCenter Server-übergreifendem vMotion überprüft vCenter Server, ob der vertrauenswürdige Schlüsselanbieter auf dem Zielhost verfügbar ist und ob der Host darauf zugreifen kann.

vMotion des vSphere Native Key Providers und vCenter Server-übergreifendes vMotion

vSphere Native Key Provider unterstützt vMotion und Verschlüsseltes vMotion für ESXi-Hosts. vCenter Server-übergreifendes vMotion wird unterstützt, wenn vSphere Native Key Provider auf dem Zielhost konfiguriert ist.

Empfohlene Vorgehensweisen für die Verschlüsselung, Einschränkungen und Interoperabilität

Sämtliche Empfohlene Vorgehensweisen und Einschränkungen, die für die Verschlüsselung physischer Maschinen gelten, gelten auch für die Verschlüsselung virtueller Maschinen. Für die Verschlüsselungsarchitektur virtueller Maschinen gelten einige zusätzliche Empfehlungen. Berücksichtigen Sie bei der Planung der Verschlüsselungsstrategie für Ihre virtuelle Maschine Einschränkungen in Bezug auf die Interoperabilität.

Hinweis Informationen zur Interoperabilität mit vSphere Trust Authority finden Sie unter vSphere Trust Authority – Best Practices, Einschränkungen und Interoperabilität.

Virtuelle Maschine – Empfohlene Vorgehensweisen für die Verschlüsselung

Die folgenden empfohlenen Vorgehensweisen für die Verschlüsselung von virtuellen Maschinen sollten zwecks Vermeidung späterer Probleme befolgt werden, zum Beispiel wenn Sie ein `vm-support`-Paket erstellen.

Allgemeine empfohlene Vorgehensweisen

Um Probleme zu vermeiden, befolgen Sie diese allgemeinen Best Practices.

- Verschlüsseln Sie keine virtuellen Maschinen der vCenter Server Appliance.
- Wenn Ihr ESXi-Host fehlschlägt, rufen Sie schnellstmöglich das Support-Paket ab. Sie benötigen den Hostschlüssel zum Generieren eines Support-Pakets mit einem Kennwort oder zum Entschlüsseln des Core-Dumps. Wenn der Host neu gestartet wird, ändert sich der Hostschlüssel möglicherweise. Ist dies der Fall, können Sie mit diesem Hostschlüssel kein Support-Paket mehr mit einem Kennwort generieren bzw. keine Core-Dumps im Support-Paket entschlüsseln.
- Verwalten Sie die Namen von Schlüsselanbietern sorgfältig. Wenn sich der Name des Schlüsselanbieters für einen bereits verwendeten Schlüsselserver ändert, wechseln VMs, die mit Schlüsseln aus diesem Schlüsselserver verschlüsselt sind, beim Einschalten oder bei der Registrierung in einen gesperrten Zustand. Entfernen Sie in diesem Fall den Schlüsselserver aus dem vCenter Server und fügen Sie ihn mit dem Schlüsselanbieternamen hinzu, den Sie anfänglich verwendet haben.
- Bearbeiten Sie keine VMX-Dateien und VMDK-Deskriptordateien. Diese Dateien enthalten das Verschlüsselungspaket. Möglicherweise kann die virtuelle Maschine nach Ihren Änderungen nicht mehr wiederhergestellt werden und dieses Wiederherstellungsproblem kann nicht behoben werden.
- Der vSphere-Prozess zur Verschlüsselung virtueller Maschinen verschlüsselt die Daten auf dem Host, bevor die Daten in den Speicher geschrieben werden. Die Effektivität von Back-End-Speicherfunktionen wie Deduplizierung, Komprimierung, Replizierung usw. kann beeinträchtigt werden, wenn virtuelle Maschinen auf diese Weise verschlüsselt werden.
- Wenn Sie mehrere Verschlüsselungsebenen verwenden, z. B. die Verschlüsselung virtueller Maschinen von vSphere und In-Guest-Verschlüsselung (BitLocker, dm-crypt usw.), kann dies die Gesamtleistung der virtuellen Maschinen beeinträchtigen, da die Verschlüsselungsprozesse zusätzliche CPU- und Arbeitsspeicherressourcen verwenden.
- Sorgen Sie dafür, dass replizierte Kopien von virtuellen Maschinen, die über die Verschlüsselung virtueller Maschinen von vSphere verschlüsselt wurden, in der Wiederherstellungs-Site Zugriff auf die Verschlüsselungsschlüssel haben. Für Standardschlüsselanbieter ist dies Teil des Designs des Schlüsselverwaltungssystems außerhalb von vSphere. Stellen Sie für vSphere Native Key Provider sicher, dass eine Sicherungskopie des Schlüssels von Native Key Provider vorhanden ist und vor Verlust geschützt ist. Weitere Informationen finden Sie unter Sichern eines vSphere Native Key Providers.
- Die Verschlüsselung ist CPU-intensiv. Mit AES-NI wird die Verschlüsselungsleistung deutlich gesteigert. Aktivieren Sie AES-NI im BIOS.

Empfohlene Vorgehensweisen für verschlüsselte Core-Dumps

Befolgen Sie diese empfohlenen Vorgehensweisen, damit keine Probleme auftreten, wenn Sie einen Core-Dump zwecks Problemdiagnose untersuchen möchten.

- Erstellen Sie eine Richtlinie bezüglich Core-Dumps. Core-Dumps sind verschlüsselt, da sie vertrauliche Informationen wie etwa Schlüssel enthalten können. Wenn Sie einen Core-Dump entschlüsseln, gehen Sie sehr sorgfältig mit den enthaltenen vertraulichen Informationen um. ESXi- Core-Dumps können Schlüssel für den ESXi-Host und die sich darauf befindlichen virtuellen Maschinen enthalten. Sie sollten den Hostschlüssel ändern und verschlüsselte virtuelle Maschinen erneut verschlüsseln, nachdem Sie einen Core-Dump entschlüsselt haben. Beide Aufgaben können mit der vSphere API durchgeführt werden.

  Weitere Informationen finden Sie unter vSphere VM-Verschlüsselung und Core-Dumps.

- Verwenden Sie immer ein Kennwort, wenn Sie ein `vm-support`-Paket erfassen. Sie können das Kennwort angeben, wenn Sie das Support-Paket vom vSphere Client generieren oder den `vm-support`-Befehl verwenden.

  Das Kennwort verschlüsselt Core-Dumps erneut, die interne Schlüssel zur Verwendung von auf diesem Kennwort basierenden Schlüsseln verwenden. Sie können das Kennwort zu einem späteren Zeitpunkt zum Entschlüsseln und Verschlüsseln von Core-Dumps verwenden, die möglicherweise im Support-Paket enthalten sind. Nicht verschlüsselte Core-Dumps und Protokolle sind bei Verwendung der Kennwortoption nicht betroffen.

- Das von Ihnen während der `vm-support`-Paketerstellung angegebene Kennwort wird in vSphere-Komponenten nicht dauerhaft gespeichert. Sie müssen Ihre Kennwörter für Support-Pakete selbst speichern bzw. diese notieren.

- Bevor Sie den Hostschlüssel ändern, generieren Sie ein `vm-support`-Paket mit einem Kennwort. Sie können das Kennwort später für den Zugriff auf alle Core-Dumps verwenden, die ggf. mit dem alten Hostschlüssel verschlüsselt wurden.

Empfohlene Vorgehensweisen bei der Verwaltung des Lebenszyklus von Schlüsseln

Implementieren Sie empfohlene Vorgehensweisen, die Schlüsselserver-Verfügbarkeit garantieren und Schlüssel auf dem Schlüsselserver überwachen.

- Sie müssen die entsprechenden Richtlinien erstellen und anwenden, die eine Schlüsselserver-Verfügbarkeit sicherstellen.

  Wenn der Schlüsselserver nicht verfügbar ist, sind VM-Vorgänge nicht möglich, bei denen vCenter Server den Schlüssel vom Schlüsselserver abrufen muss. Laufende virtuelle Maschinen werden daher fortwährend ausgeführt und Sie können sie ausschalten, einschalten und neu konfigurieren. Sie können eine virtuelle Maschine jedoch nicht auf einen Host verlagern, der nicht über die Schlüsselinformationen verfügt.

Die meisten Schlüsselserver-Lösungen beinhalten HA (High Availability)-Funktionen. Sie können den vSphere Client oder die API verwenden, um einen Schlüsselanbieter und die verbundenen Schlüsselserver anzugeben.

Hinweis Ab Version 7.0 Update 2 können verschlüsselte virtuelle Maschinen und virtuelle TPMs auch dann weiterhin funktionieren, wenn der Schlüsselserver vorübergehend offline oder nicht verfügbar ist. Die ESXi-Hosts können die Verschlüsselungsschlüssel beibehalten, um die Verschlüsselung und vTPM-Vorgänge fortzusetzen. Weitere Informationen hierzu finden Sie unter Schlüsselpersistenz – Übersicht.

- Sie müssen die Schlüssel speichern und eine Standardisierung durchführen, wenn sich die Schlüssel für vorhandene virtuelle Maschinen nicht im aktiven Zustand befinden.

  Der KMIP-Standard definiert die folgenden Zustände für Schlüssel.

  - Voraktiv
  - Aktiv
  - Deaktiviert
  - Manipuliert
  - Zerstört
  - Zerstört/Manipuliert

  Bei der Verschlüsselung der virtuellen vSphere-Maschinen werden nur aktive Schlüssel verwendet. Wenn ein Schlüssel voraktiv ist, wird dieser über die Funktion „Verschlüsselung der virtuellen vSphere-Maschine“ aktiviert. Wenn der Schlüsselzustand „Deaktiviert“, „Manipuliert“, „Zerstört“ oder „Zerstört/Manipuliert“ ist, können Sie eine virtuelle Maschine oder Festplatte nicht mit diesem Schlüssel verschlüsseln.

  Für Schlüssel, die andere Zustände aufweisen, werden virtuelle Maschinen unter Verwendung dieser Schlüssel weiterhin ausgeführt. Ob ein Klon- oder Migrationsvorgang erfolgreich ist, hängt davon ab, ob sich der Schlüssel bereits auf dem Host befindet.

  - Wenn sich der Schlüssel auf einem Zielhost befindet, wird der Vorgang erfolgreich ausgeführt, auch wenn der Schlüssel auf dem Schlüsselserver nicht aktiv ist.
  - Wenn sich die erforderlichen Schlüssel für die virtuellen Maschinen und die virtuellen Festplatten nicht auf dem Zielhost befinden, muss vCenter Server die Schlüssel vom Schlüsselserver abrufen. Wenn es sich bei dem Schlüsselzustand um „Deaktiviert“, „Manipuliert“, „Zerstört“ oder „Zerstört/Manipuliert“ handelt, zeigt vCenter Server eine Fehlermeldung an und der Vorgang wird nicht erfolgreich durchgeführt.

  Ein Klon- oder Migrationsvorgang wird erfolgreich durchgeführt, wenn sich der Schlüssel bereits auf dem Host befindet. Der Vorgang schlägt fehl, wenn vCenter Server die Schlüssel vom Schlüsselserver abruft.

Wenn ein Schlüssel nicht aktiv ist, führen Sie eine erneute Verschlüsselung unter Verwendung der API durch. Weitere Informationen finden Sie im *Programmierhandbuch zum vSphere Web Services SDK*.

- Entwickeln Sie Richtlinien für die Schlüsselrotation, sodass Schlüssel nach einer bestimmten Zeit stillgelegt und ein Rollover durchgeführt wird.
  - Vertrauenswürdiger Schlüsselanbieter: Ändern Sie den primären Schlüssel eines vertrauenswürdigen Schlüsselanbieters.
  - vSphere Native Key Provider: Ändern Sie die `key_id` eines vSphere Native Key Provider.

Empfohlene Vorgehensweisen für das Sichern und Wiederherstellen

Erstellen Sie Richtlinien für Sicherungs- und Wiederherstellungsvorgänge.

- Es werden nicht alle Sicherungsarchitekturen unterstützt. Weitere Informationen hierzu finden Sie unter Interoperabilität bei der Verschlüsselung von virtuellen Maschinen.
- Erstellen Sie Richtlinien für Wiederherstellungsvorgänge. Da die Sicherung immer auf Klartextdaten beruht, sollten Sie virtuelle Maschinen direkt nach Beendigung der Wiederherstellung verschlüsseln. Sie können angeben, dass die virtuelle Maschine als Teil des Wiederherstellungsvorgangs verschlüsselt wird. Wenn möglich, verschlüsseln Sie die virtuelle Maschine als Teil des Wiederherstellungsvorgangs, um die Offenlegung von vertraulichen Informationen zu vermeiden. Um die Verschlüsselungsrichtlinie für Festplatten zu ändern, die mit der virtuellen Maschine verbunden sind, ändern Sie die Speicherrichtlinie für diese Festplatte.
- Da die VM-Home-Dateien verschlüsselt sind, stellen Sie sicher, dass die Verschlüsselungsschlüssel zum Zeitpunkt der Wiederherstellung verfügbar sind.

Empfohlene Vorgehensweisen für die Leistung

- Die Verschlüsselungsleistung richtet sich nach der CPU- und Speicherkapazität.
- Die Verschlüsselung von vorhandenen virtuellen Maschinen nimmt mehr Zeit in Anspruch als die Verschlüsselung einer virtuellen Maschine bei deren Erstellung. Verschlüsseln Sie also eine virtuelle Maschine wenn möglich bei deren Erstellung.

Empfohlene Vorgehensweisen für Speicherrichtlinien

Ändern Sie nicht die im Paket enthaltene Beispielspeicherrichtlinie für die VM-Verschlüsselung. Klonen Sie stattdessen die Richtlinie und bearbeiten Sie den Klon.

Hinweis Die Zurücksetzung der VM-Verschlüsselungsrichtlinie auf ihre ursprünglichen Einstellungen ist nicht möglich.

Details zur Anpassung von Speicherrichtlinien finden Sie in der *vSphere-Speicher*-Dokumentation.

Entfernen von Verschlüsselungsschlüsseln – Best Practices

Um sicherzustellen, dass Verschlüsselungsschlüssel aus einem Cluster entfernt werden, starten Sie nach dem Löschen, Aufheben der Registrierung oder Verschieben der verschlüsselten virtuellen Maschine in einen anderen vCenter Server die ESXi-Hosts im Cluster neu.

Vorbehalte bei der Verschlüsselung von virtuellen Maschinen

Machen Sie sich mit den Vorbehalten bei der Verschlüsselung von virtuellen Maschinen vertraut, um möglicherweise später auftretende Probleme zu vermeiden.

Informationen darüber, welche Geräte und Funktionen nicht bei der Verschlüsselung von virtuellen Maschinen verwendet werden können, finden Sie unter Interoperabilität bei der Verschlüsselung von virtuellen Maschinen.

Einschränkungen

Beachten Sie die folgenden Vorbehalte bei der Planung Ihrer Strategie zur Verschlüsselung von virtuellen Maschinen.

- Wenn Sie eine verschlüsselte Maschine klonen oder einen Storage vMotion-Vorgang durchführen, können Sie versuchen, das Festplattenformat zu ändern. Diese Konvertierungen sind jedoch nicht immer erfolgreich. Wenn Sie beispielsweise eine virtuelle Maschine klonen und versuchen, das Festplattenformat von „lazy-zeroed thick“ in „thin“ zu ändern, behält die Festplatte der virtuellen Maschine das Format „lazy-zeroed thick“ bei.
- Wenn Sie eine Festplatte von einer virtuellen Maschine trennen, werden die Informationen der Speicherrichtlinie für die virtuelle Festplatte nicht gespeichert.
  - Wenn die virtuelle Festplatte verschlüsselt ist, müssen Sie die Speicherrichtlinie explizit auf „VM-Speicherrichtlinie“ oder auf eine Speicherrichtlinie festlegen, die Verschlüsselung enthält.
  - Wenn die virtuelle Festplatte nicht verschlüsselt ist, können Sie die Speicherrichtlinie ändern, wenn Sie die Festplatte zu einer virtuellen Maschine hinzufügen.

  Weitere Informationen finden Sie unter Verschlüsseln von virtuellen Festplatten.
- Entschlüsseln Sie Core-Dumps, bevor Sie eine virtuelle Maschine auf einen anderen Cluster verschieben.

  Der vCenter Server speichert keine KMS-Schlüssel, sondern nur die Schlüssel-IDs. vCenter Server speichert daher den ESXi-Hostschlüssel nicht dauerhaft.

  Unter gewissen Umständen, zum Beispiel beim Verschieben des ESXi-Hosts auf einen anderen Cluster und beim Neustart des Hosts weist vCenter Server dem Host einen neuen Hostschlüssel zu. Sie können keine vorhandenen Core-Dumps mit dem neuen Hostschlüssel entschlüsseln.
- OVF-Export wird für eine verschlüsselte virtuelle Maschine nicht unterstützt.
- Die Verwendung des VMware Host Client zum Registrieren einer verschlüsselten virtuellen Maschine wird nicht unterstützt.

Virtuelle Maschine im gesperrten Zustand

Wenn der Schlüssel für eine virtuelle Maschine oder mindestens ein Schlüssel für die virtuellen Festplatten fehlt, wechselt die virtuelle Maschine in einen gesperrten Zustand. In einem gesperrten Zustand können Sie keine Vorgänge für die virtuelle Maschine durchführen.

- Wenn Sie eine virtuelle Maschine und deren Festplatten über den vSphere Client verschlüsseln, wird derselbe Schlüssel für beide Vorgänge verwendet.
- Wenn Sie die Verschlüsselung mit der API durchführen, können Sie verschiedene Verschlüsselungsschlüssel für die virtuelle Maschine und deren Festplatten verwenden. Wenn Sie in diesem Fall versuchen, eine virtuelle Maschine einzuschalten, und einer der Festplattenschlüssel fehlt, schlägt das Einschalten fehl. Wenn Sie die virtuelle Festplatte entfernen, können Sie die virtuelle Maschine einschalten.

Vorschläge zur Fehlerbehebung finden Sie unter Beheben von Problemen in Bezug auf fehlende Schlüssel.

Interoperabilität bei der Verschlüsselung von virtuellen Maschinen

vSphere Virtual Machine Encryption weist einige Einschränkungen in Bezug auf Geräte und Funktionen auf, mit denen Interoperabilität möglich ist.

Die folgenden Einschränkungen und Anmerkungen beziehen sich auf die Verwendung von vSphere Virtual Machine Encryption. Ähnliche Informationen zur Verwendung der vSAN-Verschlüsselung finden Sie in der Dokumentation *Verwalten von VMware vSAN*.

Einschränkungen bei bestimmten Verschlüsselungsaufgaben

Für die Durchführung bestimmter Aufgaben auf einer verschlüsselten virtuellen Maschine gelten einige Einschränkungen.

- Sie können die meisten Verschlüsselungsvorgänge nicht auf einer eingeschalteten virtuellen Maschine durchführen. Die virtuelle Maschine muss ausgeschaltet sein. Sie können eine verschlüsselte virtuelle Maschine klonen und beim Einschalten der virtuellen Maschine eine oberflächliche erneute Verschlüsselung vornehmen.
- Auf einer virtuellen Maschine mit Snapshots kann keine tiefe Neuverschlüsselung durchgeführt werden. Auf einer virtuellen Maschine mit Snapshots kann eine flache Neuverschlüsselung durchgeführt werden.

Virtual Trusted Platform Module-Geräte und vSphere Virtual Machine Encryption

Ein vTPM (Virtual Trusted Platform Module) ist eine softwarebasierte Darstellung eines physischen Trusted Platform Module 2.0-Chips. Sie können ein vTPM zu einer neuen oder einer vorhandenen virtuellen Maschine hinzufügen. Zum Hinzufügen eines vTPM zu einer virtuellen Maschine müssen Sie einen Schlüsselanbieter in Ihrer vSphere-Umgebung konfigurieren. Wenn

Sie ein vTPM konfigurieren, werden die Home-Dateien der virtuellen Maschine verschlüsselt (Arbeitsspeicherauslagerung, NVRAM-Dateien usw.). Die Festplattendateien oder VMDK-Dateien werden nicht automatisch verschlüsselt. Sie haben die Möglichkeit, Verschlüsselung für die Festplatten der virtuellen Maschine explizit hinzuzufügen.

Vorsicht Durch das Klonen einer virtuellen Maschine wird die gesamte virtuelle Maschine, einschließlich der virtuellen Geräte, wie z. B. eines vTPM, dupliziert. Die im vTPM gespeicherten Informationen, einschließlich der Eigenschaften des vTPM, mit denen die Software die Identität eines Systems ermitteln kann, werden ebenfalls dupliziert.

vSphere Virtual Machine Encryption sowie Zustand „Angehalten“ und Snapshots

Sie können eine im angehaltenen Zustand befindliche verschlüsselte virtuelle Maschine fortsetzen oder einen Arbeitsspeicher-Snapshot einer verschlüsselten Maschine wiederherstellen. Sie können eine im angehaltenen Zustand befindliche verschlüsselte virtuelle Maschine mit einem Arbeitsspeicher-Snapshot zwischen ESXi-Hosts migrieren.

vSphere Virtual Machine Encryption und IPv6

Sie können vSphere Virtual Machine Encryption im reinen IPv6- oder gemischten Modus verwenden. Sie können den Schlüsselserver mit IPv6-Adressen konfigurieren. Sie können sowohl den vCenter Server als auch den Schlüsselserver nur mit IPv6-Adressen konfigurieren.

Einschränkungen beim Klonen in vSphere Virtual Machine Encryption

Bestimmte Klonfunktionen können mit vSphere Virtual Machine Encryption nicht ausgeführt werden.

- Bei einem Standardschlüsselanbieter wird das Klonen bedingt unterstützt.
  - Vollständige Klone werden unterstützt. Der Klon erbt den übergeordneten Verschlüsselungszustand und alle Schlüssel. Sie können den vollständigen Klon verschlüsseln, ihn zur Verwendung neuer Schlüssel erneut verschlüsseln oder entschlüsseln.

    Verknüpfte Klone werden unterstützt und der Klon erbt den übergeordneten Verschlüsselungsstatus einschließlich der Schlüssel. Sie können den verknüpften Klon nicht entschlüsseln oder einen verknüpften Klon nicht mit unterschiedlichen Schlüsseln erneut verschlüsseln.

    Hinweis Überprüfen Sie, ob andere Anwendungen verknüpfte Klone unterstützen. Beispiel: VMware Horizon® 7 unterstützt sowohl vollständige Klone als auch Instant Clones, aber keine verknüpften Klone.

- Bei einem vertrauenswürdigen Schlüsselanbieter oder einem vSphere Native Key Provider wird das Klonen unterstützt, aber Verschlüsselungsschlüssel können beim Klonen nicht geändert werden. Dieses Verhalten steht im Gegensatz zur Standardverschlüsselung, bei der Sie Schlüssel beim Erstellen eines Klons ändern können. Die folgenden Vorgänge werden von vSphere Trust Authority oder einem vSphere Native Key Provider beim Klonen einer virtuellen Maschine nicht unterstützt:
  - Durchführen eines Klonvorgangs von einer nicht verschlüsselten virtuellen Maschine in eine verschlüsselte virtuelle Maschine
  - Durchführen eines Klonvorgangs von einer verschlüsselten virtuellen Maschine und Ändern der Verschlüsselungsschlüssel
  - Durchführen eines Klonvorgangs von einer verschlüsselten virtuellen Maschine in eine unverschlüsselte virtuelle Maschine
- Instant Clone wird von allen Schlüsselanbietertypen unterstützt. Verschlüsselungsschlüssel können beim Klonen jedoch nicht geändert werden.

Nicht unterstützte Festplattenkonfigurationen bei vSphere Virtual Machine Encryption

Bestimmte Konfigurationstypen von VM-Festplatten werden mit vSphere Virtual Machine Encryption nicht unterstützt.

- RDM (Raw Device Mapping). vSphere Virtual Volumes (vVols) werden jedoch unterstützt.
- Multiwriter- oder freigegebene Festplatten (MSCS, WSFC oder Oracle RAC). Verschlüsselte VM-Home-Dateien werden bei Multiwriter-Festplatten unterstützt. Verschlüsselte virtuelle Festplatten werden bei Multiwriter-Festplatten nicht unterstützt. Wenn Sie versuchen, Multiwriter auf der Seite **Einstellungen bearbeiten** der virtuellen Maschine mit verschlüsselten virtuellen Festplatten auszuwählen, ist die Schaltfläche **OK** deaktiviert.

Verschiedene Einschränkungen bei vSphere Virtual Machine Encryption

Zu den anderen Funktionen, die nicht mit vSphere Virtual Machine Encryption funktionieren, gehören:

- vSphere ESXi Dump Collector
- Inhaltsbibliothek
  - Inhaltsbibliotheken unterstützen zwei Arten von Vorlagen: OVF- und VM-Vorlagen. Sie können eine verschlüsselte virtuelle Maschine nicht in den OVF-Vorlagentyp exportieren. Das OVF-Tool unterstützt keine verschlüsselten virtuellen Maschinen. Sie können verschlüsselte VM-Vorlagen mithilfe des VM-Vorlagentyps erstellen. Weitere Informationen finden Sie im *Administratorhandbuch für vSphere Virtual Machine*.

- Software zum Sichern verschlüsselter virtueller Festplatten muss die VMware vSphere Storage API - Data Protection (VADP) verwenden, damit die Festplatten entweder im Hot-Add-Modus oder im NBD-Modus bei aktiviertem SSL gesichert werden können. Es werden jedoch nicht alle Sicherungslösungen unterstützt, die VADP für die Sicherung virtueller Festplatten verwenden. Weitere Informationen erhalten Sie von Ihrem Backupanbieter.
  - Lösungen für den VADP-SAN-Transportmodus werden für die Sicherung verschlüsselter virtueller Festplatten nicht unterstützt.
  - VADP-Hot-Add-Lösungen werden für verschlüsselte virtuelle Festplatten unterstützt. Die Sicherungssoftware muss die Verschlüsselung der Proxy-VM, die als Teil des Hot-Add-Sicherungsworkflows verwendet wird, unterstützen. Der Anbieter muss über die Rechte für **Verschlüsselungsvorgänge.Virtuelle Maschine verschlüsseln** verfügen.
  - Sicherungslösungen mithilfe der NBD-SSL-Transportmodi werden für die Sicherung verschlüsselter virtueller Festplatten unterstützt. Die Anwendung des Anbieters muss über die Rechte für **Verschlüsselungsvorgänge.Direkter Zugriff** verfügen.
- Sie können keine Ausgabe von einer verschlüsselten virtuellen Maschine an einen seriellen oder parallelen Port senden. Selbst wenn die Konfiguration scheinbar erfolgreich ist, wird die Ausgabe an eine Datei gesendet.
- vSphere Virtual Machine Encryption wird in VMware Cloud on AWS nicht unterstützt. Einzelheiten finden Sie unter *Verwalten des VMware Cloud on AWS-Datencenters.*

Schlüsselpersistenz – Übersicht

In vSphere 7.0 Update 2 und höher können verschlüsselte virtuelle Maschinen und virtuelle TPMs auch dann weiterhin optional funktionieren, wenn der Schlüsselserver vorübergehend offline oder nicht verfügbar ist. Die ESXi-Hosts können die Verschlüsselungsschlüssel beibehalten, um die Verschlüsselung und vTPM-Vorgänge fortzusetzen.

Vor vSphere 7.0 Update 2 ist es für verschlüsselte virtuelle Maschinen und vTPMs erforderlich, dass der Schlüsselserver immer verfügbar ist. In vSphere 7.0 Update 2 und höher können verschlüsselte Geräte auch dann funktionieren, wenn der Zugriff auf einen Schlüsselserver unterbrochen ist.

Ab vSphere 7.0 Update 3 können verschlüsselte vSAN-Cluster auch dann funktionieren, wenn der Zugriff auf einen Schlüsselanbieter unterbrochen ist.

Hinweis Schlüsselpersistenz ist nicht erforderlich, wenn vSphere Native Key Provider verwendet wird. vSphere Native Key Provider ist sofort einsatzbereit und kann ohne Zugriff auf einen Schlüsselserver ausgeführt werden. Weitere Informationen finden Sie im folgenden Abschnitt „Schlüsselpersistenz und vSphere Native Key Provider“.

Schlüsselpersistenz auf dem ESXi-Host

Bei Verwendung eines Standardschlüsselanbieters verlässt sich der ESXi-Host auf vCenter Server, um Verschlüsselungsschlüssel zu verwalten. Wenn Sie einen vertrauenswürdigen Schlüsselanbieter verwenden, verlässt sich der ESXi-Host direkt auf die Trust Authority-Hosts für Schlüssel und vCenter Server ist nicht beteiligt.

Unabhängig vom Typ des Schlüsselanbieters erhält der ESXi-Host die Schlüssel anfänglich und behält sie im Schlüssel-Cache bei. Wenn der ESXi-Host neu gestartet wird, verliert er seinen Schlüssel-Cache. Der ESXi-Host fordert die Schlüssel dann erneut an, entweder vom Schlüsselserver (Standardschlüsselanbieter) oder vom Trust Authority-Host (vertrauenswürdiger Schlüsselanbieter). Wenn der ESXi-Host versucht, Schlüssel abzurufen, und der Schlüsselserver offline oder nicht erreichbar ist, können vTPMs und die Arbeitslastverschlüsselung nicht funktionieren. Bei Bereitstellungen im Edge-Stil, bei denen ein Schlüsselserver normalerweise nicht vor Ort bereitgestellt wird, kann ein Verlust der Konnektivität mit einem Schlüsselserver zu unnötigen Ausfallzeiten für verschlüsselte Arbeitslasten führen.

In vSphere 7.0 Update 2 und höher können verschlüsselte Arbeitslasten auch dann weiterhin funktionieren, wenn der Schlüsselserver offline oder nicht erreichbar ist. Wenn der ESXi-Host über ein TPM verfügt, werden die Verschlüsselungsschlüssel im TPM über Neustarts hinweg beibehalten. Selbst wenn ein ESXi-Host neu gestartet wird, muss der Host keine Verschlüsselungsschlüssel anfordern. Darüber hinaus können Verschlüsselungs- und Entschlüsselungsvorgänge fortgesetzt werden, wenn der Schlüsselserver nicht verfügbar ist, da die Schlüssel im TPM beibehalten wurden. Wenn also entweder der Schlüsselserver oder die Trust Authority-Hosts nicht verfügbar sind, können Sie verschlüsselte Arbeitslasten weiterhin „ohne Schlüsselserver“ ausführen. Darüber hinaus können vTPMs auch dann weiterhin funktionieren, wenn der Schlüsselserver nicht erreichbar ist.

Schlüsselpersistenz und vSphere Native Key Provider

Wenn Sie einen vSphere Native Key Provider verwenden, generiert vSphere Verschlüsselungsschlüssel und es ist kein Schlüsselserver erforderlich. Die ESXi-Hosts erhalten einen Schlüsselschlüssel (KDK), der zum Ableiten anderer Schlüssel verwendet wird. Nach dem Empfang des KDK und dem Generieren weiterer Schlüssel benötigen die ESXi-Hosts keinen Zugriff auf vCenter Server, um Verschlüsselungsvorgänge durchzuführen. Im Prinzip wird ein vSphere Native Key Provider immer „ohne Schlüsselserver“ ausgeführt.

Der KDK bleibt nach einem Neustart standardmäßig auf einem ESXi-Host erhalten, auch wenn vCenter Server nach dem Neustart des Hosts nicht verfügbar ist.

Sie können Schlüsselpersistenz mithilfe des vSphere Native Key Provider aktivieren, dies ist jedoch normalerweise nicht erforderlich. Die ESXi-Hosts haben vollständigen Zugriff auf vSphere Native Key Provider, weshalb zusätzliche Schlüsselpersistenz redundant ist. Ein Anwendungsfall für die Aktivierung der Schlüsselpersistenz mit vSphere Native Key Provider besteht dann, wenn Sie auch einen Standardschlüsselanbieter (externen KMIP-Server) konfiguriert haben.

Vorgehensweise zum Einrichten von Schlüsselpersistenz

Informationen zum Aktivieren oder Deaktivieren der Schlüsselpersistenz finden Sie unter Aktivieren und Deaktivieren von Schlüsselpersistenz auf einem ESXi-Host.

Konfigurieren und Verwalten eines Standardschlüsselanbieters

7

Die Verwendung eines Standardschlüsselanbieters in Ihrer vSphere-Umgebung muss vorbereitet werden. Wenn Sie Ihre Umgebung eingerichtet haben, können Sie verschlüsselte virtuelle Maschinen und virtuelle Festplatten erstellen und vorhandene virtuelle Maschinen und Festplatten verschlüsseln.

Wenn Sie Ihre Umgebung für einen Standardschlüsselanbieter eingerichtet haben, können Sie mithilfe des vSphere Client verschlüsselte virtuelle Maschinen und virtuelle Festplatten erstellen und vorhandene virtuelle Maschinen und Festplatten verschlüsseln. Weitere Informationen hierzu finden Sie unter Kapitel 10 Verwenden von Verschlüsselung in Ihrer vSphere-Umgebung.

Unter Verwendung der API und der crypto-util-Befehlszeilenschnittstelle können Sie zusätzliche Aufgaben ausführen. Die API-Dokumentation finden Sie im *Programmierhandbuch zum vSphere Web Services SDK*. Informationen zu diesem Tool finden Sie der `crypto-util`-Befehlszeilenhilfe.

Dieses Kapitel enthält die folgenden Themen:

Standardschlüsselanbieter – Übersicht

Sie können einen Standardschlüsselanbieter verwenden, um Verschlüsselungsaufgaben für virtuelle Maschinen durchzuführen.

Was ist ein Standardschlüsselanbieter?

In vSphere ruft ein Standardschlüsselanbieter die Verschlüsselungsschlüssel direkt von einem Schlüsselserver ab, und der vCenter Server verteilt die Schlüssel an die notwendigen ESXi-Hosts in einem Datencenter.

Sie können separate Standardschlüsselanbieter für verschiedene Benutzer hinzufügen und den Standardschlüsselanbieter festlegen.

Anforderungen an den vSphere-Standardschlüsselanbieter

- vSphere 6.5 oder höher

- Ein externer Schlüsselserver (KMS)

Der Schlüsselverwaltungsserver muss den KMIP 1.1-Standard (KMIP = Key Management Interoperability Protocol) unterstützen. Weitere Informationen finden Sie unter *vSphere-Kompatibilitätstabellen*.

Informationen über von VMware zertifizierte KMS-Anbieter finden Sie im VMware-Kompatibilitätshandbuch unter „Plattform und Computing“. Wenn Sie „Kompatibilitätshandbücher“ auswählen, können Sie die KMS-Kompatibilitätsdokumentation öffnen. Diese Dokumentation wird häufig aktualisiert.

Standardschlüsselanbieter – Berechtigungen

Standardschlüsselanbieter verwenden **Cryptographer.***-Berechtigungen Weitere Informationen hierzu finden Sie unter Rechte für Verschlüsselungsvorgänge.

Einrichten des Standardschlüsselanbieters

Bevor Sie mit den Verschlüsselungsaufgaben für virtuelle Maschinen beginnen können, müssen Sie den Standardschlüsselanbieter einrichten.

Zum Einrichten eines Standardschlüsselanbieters gehört das Hinzufügen des Schlüsselanbieters und das Einrichten einer Vertrauensstellung mit dem Schlüsselserver. Wenn Sie einen Schlüsselanbieter hinzufügen, werden Sie aufgefordert, ihn als Standardwert festzulegen. Sie können den Standardschlüsselanbieter explizit ändern. vCenter Server stellt Schlüssel über den Standardschlüsselanbieter bereit.

Hinweis Was zuvor in vSphere 6.5 und 6.7 als KMS-Cluster bezeichnet wurde, heißt nun Schlüsselanbieter.

 (Verschlüsselung virtueller Maschinen mit Einrichtung eines Standardschlüsselanbieters)

Hinzufügen eines Standardschlüsselanbieters mithilfe des vSphere Client

Sie können Ihrem vCenter Server-System über den vSphere Client oder über die öffentliche API einen Standardschlüsselanbieter hinzufügen.

Mithilfe des vSphere Client können Sie Ihrem vCenter Server-System einen Standardschlüsselanbieter hinzufügen und eine Vertrauensstellung zwischen dem Schlüsselserver und vCenter Server einrichten.

- Sie können mehrere Schlüsselserver desselben Anbieters hinzufügen.
- Wenn Ihre Umgebung Lösungen anderer Anbieter unterstützt, können Sie mehrere Schlüsselanbieter hinzufügen.

- Wenn Ihre Umgebung mehrere Schlüsselanbieter enthält und Sie den Standardschlüsselanbieter löschen, müssen Sie explizit einen anderen Standardschlüsselanbieter festlegen.
- Sie können den Schlüsselserver mit IPv6-Adressen konfigurieren.
  - Das vCenter Server-System und der Schlüsselserver können nur mit IPv6-Adressen konfiguriert werden.

Voraussetzungen

- Stellen Sie sicher, dass der Schlüsselserver (KMS) im *VMware-Kompatibilitätshandbuch für Schlüsselverwaltungsserver (KMS)* aufgeführt und mit KMIP 1.1 kompatibel ist und dass er als Foundry und Server für symmetrische Schlüssel dienen kann.
- Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen verfügen: **Verschlüsselungsvorgänge.Schlüsselserver verwalten**
- Stellen Sie Hochverfügbarkeit für den Schlüsselserver sicher. Bei einem Abbruch der Verbindung zum Schlüsselserver, beispielsweise bei einem Stromausfall oder einer Notfallwiederherstellung, ist ein Zugriff auf verschlüsselte virtuelle Maschinen nicht mehr möglich.

  Hinweis Ab vSphere 7.0 Update 2 können verschlüsselte virtuelle Maschinen und virtuelle TPMs auch dann weiterhin funktionieren, wenn der Schlüsselserver vorübergehend offline oder nicht verfügbar ist. Weitere Informationen hierzu finden Sie unter Schlüsselpersistenz – Übersicht.
- Führen Sie eine sorgfältige Prüfung der Infrastrukturabhängigkeiten auf dem Schlüsselserver durch. Bestimmte KMS-Lösungen werden als virtuelle Appliances bereitgestellt, wodurch eine Abhängigkeitsschleife oder ein anderes Verfügbarkeitsproblem aufgrund einer schlechten Platzierung der KMS-Appliance auftreten kann.

Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server-System an.
2. Durchsuchen Sie die Bestandsliste und wählen Sie die vCenter Server-Instanz aus.
3. Klicken Sie auf **Konfigurieren** und unter **Sicherheit** auf **Schlüsselanbieter**.
4. Klicken Sie auf **Standardschlüsselanbieter hinzufügen** und geben Sie die Daten des Schlüsselanbieters ein.

Option	Wert
Name	Name des Schlüsselanbieters. Jeder logische Schlüsselanbieter muss unabhängig von seinem Typ (Standard-, vertrauenswürdiger und nativer Schlüsselanbieter) über einen eindeutigen Namen in allen vCenter Server-Systemen verfügen. Weitere Informationen finden Sie unter Benennung des Schlüsselanbieters.
KMS	Alias für den Schlüsselserver (KMS).

Option	Wert
Adresse	IP-Adresse oder FQDN des Schlüsselservers.
Port	Port, auf dem vCenter Server eine Verbindung zum Schlüsselserver herstellt.
Proxyserver	Optionale Proxyserveradresse für die Verbindung mit dem Schlüsselserver.
Proxyport	Optionaler Proxyport für die Verbindung mit dem Schlüsselserver.
Benutzername	Bestimmte Schlüsselserveranbieter lassen zu, dass Benutzer Verschlüsselungsschlüssel isolieren, die von verschiedenen Benutzern oder Gruppen verwendet werden, indem sie einen Benutzernamen und ein Kennwort angeben. Geben Sie nur dann einen Benutzernamen an, wenn Ihr Schlüsselserver diese Funktion unterstützt und Sie die Funktion verwenden möchten.
Kennwort	Bestimmte Schlüsselserveranbieter lassen zu, dass Benutzer Verschlüsselungsschlüssel isolieren, die von verschiedenen Benutzern oder Gruppen verwendet werden, indem sie einen Benutzernamen und ein Kennwort angeben. Geben Sie nur dann ein Kennwort an, wenn Ihr Schlüsselserver diese Funktion unterstützt und Sie die Funktion verwenden möchten.

Sie können auf **KMS hinzufügen** klicken, um weitere Schlüsselserver hinzuzufügen.

5 Klicken Sie auf **Schlüsselanbieter hinzufügen**.

6 Klicken Sie auf **Vertrauenswürdigkeit**.

vCenter Server fügt den Schlüsselanbieter hinzu und zeigt den Status als „Verbunden“ an.

Nächste Schritte

Weitere Informationen hierzu finden Sie unter Herstellen einer vertrauenswürdigen Standardschlüsselanbieter-Verbindung durch den Austausch von Zertifikaten.

Herstellen einer vertrauenswürdigen Standardschlüsselanbieter-Verbindung durch den Austausch von Zertifikaten

Nach dem Hinzufügen des Standardschlüsselanbieters zum vCenter Server-System können Sie eine vertrauenswürdige Verbindung herstellen. Der spezifische Prozess hängt von den Zertifikaten, die der Schlüsselanbieter akzeptiert, sowie von der Unternehmensrichtlinie ab.

Voraussetzungen

Fügen Sie den Standardschlüsselanbieter hinzu.

Verfahren

1 Navigieren Sie zum vCenter Server.

2 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.

3 Wählen Sie den Schlüsselanbieter aus.

Der KMS für den Schlüsselanbieter wird angezeigt.

4 Wählen Sie den KMS aus.

5 Wählen Sie im Dropdown-Menü **Vertrauensstellung herstellen** die Option **KMS für vCenter vertrauenswürdig machen** aus.

6 Wählen Sie die entsprechende Option für den Server aus und befolgen Sie die entsprechenden Schritte.

Option	Informationen hierzu finden Sie unter
CA-Root-Zertifikat von vCenter Server	Verwenden der Option „Root-CA-Zertifikat“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters.
vCenter Server-Zertifikat	Verwenden der Zertifikatsoption zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters.
Zertifikat und privaten Schlüssel hochladen	Verwenden der Option „Zertifikat und privaten Schlüssel hochladen“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters.
Neue Zertifikatssignieranforderung	Verwenden der Option „Neue Zertifikatssignieranforderung“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters.

Verwenden der Option „Root-CA-Zertifikat“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters

Bestimmte KMS-Anbieter (Key Management Server) verlangen, dass Sie das Root-CA-Zertifikat auf den KMS hochladen. Alle von Ihrer Root-Zertifizierungsstelle signierten Zertifikate werden dann von diesem KMS als vertrauensvoll angesehen.

Das von der vSphere VM-Verschlüsselung verwendete Root-CA-Zertifikat ist ein selbst signiertes Zertifikat, das in einem separaten Speicher im VECS (VMware Endpoint Certificate Store) auf dem vCenter Server-System gespeichert wird.

Hinweis Generieren Sie ein Root-CA-Zertifikat nur dann, wenn Sie vorhandene Zertifikate ersetzen möchten. Wenn Sie das tun, werden andere von dieser Root-Zertifizierungsstelle signierten Zertifikate ungültig. Sie können ein neues Root-CA-Zertifikat als Teil dieses Workflows generieren.

Verfahren

1 Navigieren Sie zum vCenter Server.

2 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.

3 Wählen Sie den Schlüsselanbieter aus, mit dem Sie eine vertrauenswürdige Verbindung herstellen möchten.

   Der KMS für den Schlüsselanbieter wird angezeigt.

4 Wählen Sie im Dropdown-Menü **Vertrauensstellung herstellen** die Option **KMS für vCenter vertrauenswürdig machen** aus.

5 Wählen Sie **vCenter-Zertifikat der Stammzertifizierungsstelle herunterladen** aus und klicken Sie auf **Weiter**.

   Im Dialogfeld „Root-CA-Zertifikat herunterladen“ steht bereits das Root-Zertifikat, das vCenter Server zur Verschlüsselung verwendet. Dieses Zertifikat wird in VECS gespeichert.

6 Kopieren Sie das Zertifikat in die Zwischenablage oder laden Sie das Zertifikat als Datei herunter.

7 Folgen Sie den Anweisungen des KMS-Anbieters, um das Zertifikat auf sein System hochzuladen.

   Hinweis Einige KMS-Anbieter verlangen, dass der KMS-Anbieter den KMS neu startet, um das von Ihnen hochgeladene Root-Zertifikat abzuholen.

Nächste Schritte

Schließen Sie den Zertifikatsaustausch ab. Weitere Informationen hierzu finden Sie unter Einrichten einer vertrauenswürdigen Verbindung für einen Standardschlüsselanbieter.

Verwenden der Zertifikatsoption zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters

Bestimmte KMS-Anbieter (Key Management Server) verlangen, dass Sie das vCenter Server-Zertifikat auf den KMS hochladen. Nach dem Upload akzeptiert der KMS den Datenverkehr, der von einem System mit diesem Zertifikat stammt.

vCenter Server generiert ein Zertifikat, um Verbindungen mit dem KMS zu schützen. Das Zertifikat wird in einem getrennten Keystore im VMware Endpoint Certificate Store (VECS) auf dem vCenter Server-System gespeichert.

Verfahren

1 Navigieren Sie zum vCenter Server.

2 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.

3 Wählen Sie den Schlüsselanbieter aus, mit dem Sie eine vertrauenswürdige Verbindung herstellen möchten.

   Der KMS für den Schlüsselanbieter wird angezeigt.

4 Wählen Sie im Dropdown-Menü **Vertrauensstellung herstellen** die Option **KMS für vCenter vertrauenswürdig machen** aus.

5 Wählen Sie **vCenter-Zertifikat** aus und klicken Sie auf **Weiter**.

   Im Dialogfeld „Zertifikat herunterladen“ steht bereits das Root-Zertifikat, das vCenter Server zur Verschlüsselung verwendet. Dieses Zertifikat wird in VECS gespeichert.

   Hinweis Generieren Sie kein neues Zertifikat, es sei denn, Sie möchten vorhandene Zertifikate ersetzen.

6 Kopieren Sie das Zertifikat in die Zwischenablage oder laden Sie es als Datei herunter.

7 Folgen Sie den Anweisungen des KMS-Anbieters, um das Zertifikat auf den KMS hochzuladen.

Nächste Schritte

Schließen Sie die Vertrauensbeziehung ab. Weitere Informationen hierzu finden Sie unter Einrichten einer vertrauenswürdigen Verbindung für einen Standardschlüsselanbieter.

Verwenden der Option „Zertifikat und privaten Schlüssel hochladen“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters

Bestimmte KMS-Anbieter (Key Management Server) verlangen, dass Sie das KMS-Serverzertifikat und den privaten Schlüssel in das vCenter Server-System hochladen.

Einige KMS-Anbieter generieren ein Zertifikat und einen privaten Schlüssel für die Verbindung und stellen Ihnen diese zur Verfügung. Sobald Sie die Dateien hochgeladen haben, wird Ihre vCenter Server-Instanz vom KMS für vertrauenswürdig erachtet.

Voraussetzungen

- Fordern Sie ein Zertifikat und einen privaten Schlüssel vom KMS-Anbieter an. Bei den Dateien handelt es sich um X509-Dateien im PEM-Format.

Verfahren

1 Navigieren Sie zum vCenter Server.

2 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.

3 Wählen Sie den Schlüsselanbieter aus, mit dem Sie eine vertrauenswürdige Verbindung herstellen möchten.

   Der KMS für den Schlüsselanbieter wird angezeigt.

4 Wählen Sie im Dropdown-Menü **Vertrauensstellung herstellen** die Option **KMS für vCenter vertrauenswürdig machen** aus.

5 Wählen Sie **KMS-Zertifikat und privater Schlüssel** aus und klicken Sie auf **Weiter**.

6 Fügen Sie das Zertifikat, das Sie vom KMS-Anbieter erhalten haben, in das obere Textfeld ein oder klicken Sie auf **Datei hochladen**, um die Zertifikatsdatei hochzuladen.

7 Fügen Sie die Schlüsseldatei in das untere Textfeld ein oder klicken Sie auf **Datei hochladen**, um die Schlüsseldatei hochzuladen.

8 Klicken Sie auf **Vertrauenswürdige Verbindung einrichten**.

Nächste Schritte

Schließen Sie die Vertrauensbeziehung ab. Weitere Informationen hierzu finden Sie unter Einrichten einer vertrauenswürdigen Verbindung für einen Standardschlüsselanbieter.

Verwenden der Option „Neue Zertifikatssignieranforderung“ zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters

Bestimmte KMS-Anbieter (Key Management Server) verlangen, dass vCenter Server eine Zertifikatssignieranforderung (CSR) generiert und an den KMS übermittelt. Der KMS signiert die Zertifikatsignierungsanforderung und sendet das signierte Zertifikat zurück. Sie können das signierte Zertifikat auf den vCenter Server hochladen.

Bei der Verwendung der Option **Neue Zertifikatsignierungsanforderung** handelt es sich um einen Vorgang mit zwei Schritten. Zuerst generieren Sie die Zertifikatsignierungsanforderung und senden diese an den KMS-Anbieter. Anschließend laden Sie das signierte Zertifikat, das Sie vom KMS-Anbieter erhalten, auf den vCenter Server hoch.

Verfahren

1. Navigieren Sie zum vCenter Server.
2. Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.
3. Wählen Sie den Schlüsselanbieter aus, mit dem Sie eine vertrauenswürdige Verbindung herstellen möchten.

   Der KMS für den Schlüsselanbieter wird angezeigt.
4. Wählen Sie im Dropdown-Menü **Vertrauensstellung herstellen** die Option **KMS für vCenter vertrauenswürdig machen** aus.
5. Wählen Sie **Neue Zertifikatssignieranforderung (CSR)** aus und klicken Sie auf **Weiter**.
6. Im Dialogfeld kopieren Sie das vollständige Zertifikat aus dem Textfeld in die Zwischenablage oder laden es als Datei herunter.

   Klicken Sie auf die Schaltfläche **Neue CSR generieren** des Dialogfelds nur dann, wenn Sie explizit eine Zertifikatsignierungsanforderung generieren möchten. Durch die Verwendung dieser Option werden alle signierten Zertifikate ungültig, die auf der alten Zertifikatsignierungsanforderung basieren.
7. Folgen Sie den Anweisungen Ihres KMS-Anbieters zum Einreichen der Zertifikatsignierungsanforderung.
8. Wenn Sie das signierte Zertifikat vom KMS-Anbieter erhalten, klicken Sie erneut auf **Schlüsselanbieter**, wählen den Schlüsselanbieter aus und wählen dann im Dropdown-Menü **Vertrauensstellung herstellen** die Option **Signiertes CSR-Zertifikat hochladen** aus.
9. Fügen Sie das signierte Zertifikat in das untere Textfeld ein oder klicken Sie auf **Datei hochladen** und laden Sie die Datei hoch. Klicken Sie anschließend auf **Hochladen**.

Nächste Schritte

Schließen Sie die Vertrauensbeziehung ab. Weitere Informationen hierzu finden Sie unter Einrichten einer vertrauenswürdigen Verbindung für einen Standardschlüsselanbieter.

Festlegen des Standardschlüsselanbieters

Sie müssen den Standardschlüsselanbieter festlegen, wenn Sie nicht den ersten Schlüsselanbieter als Standardschlüsselanbieter verwenden oder wenn in Ihrer Umgebung mehrere Schlüsselanbieter verwendet werden und der Standardschlüsselanbieter von Ihnen entfernt wird.

Voraussetzungen

Als Best Practice stellen Sie sicher, dass auf der Registerkarte **Schlüsselanbieter** der Verbindungsstatus „Verbunden“ mit einem grünen Häkchen angezeigt wird.

Verfahren

1. Navigieren Sie zum vCenter Server.
2. Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.
3. Wählen Sie den Schlüsselanbieter aus.
4. Klicken Sie auf **Als Standard festlegen**.

   Ein Bestätigungsdialogfeld wird angezeigt.
5. Klicken Sie auf **Als Standard festlegen**.

   Der Schlüsselanbieter wird als aktueller Standardschlüsselanbieter angezeigt.

Einrichten einer vertrauenswürdigen Verbindung für einen Standardschlüsselanbieter

Sofern Sie im Dialogfeld **Standardschlüsselanbieter hinzufügen** nicht aufgefordert wurden, eine vertrauenswürdige Verbindung mit dem KMS herzustellen, müssen Sie die vertrauenswürdige Verbindung nach erfolgtem Zertifikatsaustausch explizit einrichten.

Eine vertrauenswürdige Verbindung zwischen vCenter Server und dem KMS-Server können Sie einrichten, indem Sie entweder den KMS-Server als vertrauenswürdig einstufen oder ein KMS-Zertifikat hochladen. Die folgenden beiden Möglichkeiten stehen zur Verfügung:

- Legen Sie das Zertifikat mithilfe der Option **KMS-Zertifikat hochladen** explizit als vertrauenswürdig fest.
- Laden Sie ein untergeordnetes KMS-Zertifikat oder das KMS-CA-Zertifikat in vCenter Server hoch, indem Sie die Option **vCenter für KMS vertrauenswürdig machen** verwenden.

Hinweis Wenn Sie das CA-Root-Zertifikat oder das Zwischen-CA-Zertifikat hochladen, vertraut vCenter Server allen Zertifikaten, die von dieser Zertifizierungsstelle signiert wurden. Um hohe Sicherheit zu gewährleisten, laden Sie ein untergeordnetes Zertifikat oder ein Zwischen-CA-Zertifikat hoch, das vom KMS-Anbieter kontrolliert wird.

Verfahren

1. Navigieren Sie zum vCenter Server.
2. Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.

3 Wählen Sie den Schlüsselanbieter aus, mit dem Sie eine vertrauenswürdige Verbindung herstellen möchten.

   Der KMS für den Schlüsselanbieter wird angezeigt.

4 Wählen Sie den KMS aus.

5 Wählen Sie eine der folgenden Optionen im Dropdown-Menü **Vertrauensstellung herstellen** aus.

Option	Aktion
vCenter für KMS vertrauenswürdig machen	Klicken Sie im daraufhin angezeigten Dialogfeld auf **Vertrauenswürdigkeit**.
KMS-Zertifikat hochladen	a Fügen Sie im angezeigten Dialogfeld entweder das Zertifikat ein oder klicken Sie auf **Datei hochladen** und navigieren Sie zur Zertifikatsdatei. b Klicken Sie auf **Hochladen**.

Einrichten separater Schlüsselanbieter für verschiedene Benutzer

Sie können in Ihrer Umgebung mehrere Schlüsselanbieter für verschiedene Benutzer der gleichen KMS-Instanz einrichten. Mehrere Schlüsselanbieter sind hilfreich, wenn Sie beispielsweise verschiedenen Abteilungen in Ihrem Unternehmen Zugriff auf unterschiedliche Sätze von Verschlüsselungsschlüsseln erteilen möchten.

Sie können mehrere Schlüsselanbieter für denselben KMS verwenden, um Schlüssel zu trennen. Das Vorhandensein getrennter Schlüsselsätze ist im Fall verschiedener Geschäftsbereiche oder Kunden entscheidend.

Hinweis Nicht alle KMS-Anbieter unterstützen mehrere Benutzer.

Voraussetzungen

Richten Sie die Verbindung mit dem KMS ein.

Verfahren

1 Erstellen Sie zwei Benutzer mit entsprechenden Benutzernamen und Kennwörtern im KMS, z. B. C1 und C2.

2 Melden Sie sich bei vCenter Server an und erstellen Sie den ersten Schlüsselanbieter.

3 Wenn Sie zur Eingabe eines Benutzernamens und Kennworts aufgefordert werden, geben Sie Informationen an, die für den ersten Benutzer eindeutig sind.

4 Erstellen Sie einen zweiten Schlüsselanbieter und fügen Sie den gleichen KMS hinzu, aber verwenden Sie den zweiten Benutzernamen und das zweite Kennwort (C2).

Ergebnisse

Die beiden Schlüsselanbieter haben unabhängige Verbindungen zum KMS und verwenden unterschiedliche Schlüsselsätze.

Konfigurieren und Verwalten eines vSphere Native Key Providers

8

Die Verwendung eines VMware vSphere® Native Key Providers™ in Ihrer vSphere-Umgebung muss vorbereitet werden. Nach dem Konfigurieren des vSphere Native Key Providers können Sie vTPMs (virtual Trusted Platform Modules) auf Ihren virtuellen Maschinen erstellen.

Nach der Einrichtung Ihrer Umgebung für einen vSphere Native Key Provider können Sie den vSphere Client und die API zum Erstellen von vTPMs verwenden. Bei Erwerb der VMware vSphere® Enterprise Plus Edition™ können Sie auch virtuelle Maschinen und Festplatten sowie vorhandene virtuelle Maschinen und Festplatten verschlüsseln.

 (Konfigurieren eines vSphere Native Key Providers)

Dieses Kapitel enthält die folgenden Themen:

- vSphere Native Key Provider – Übersicht
- vSphere Native Key Provider – Prozessablauf
- Konfigurieren eines vSphere Native Key Providers
- Sichern eines vSphere Native Key Providers
- Importieren eines vSphere Native Key Providers in eine Konfiguration mit erweitertem verknüpftem Modus
- Wiederherstellen eines vSphere Native Key Providers
- Aktualisieren eines vSphere Native Key Providers
- Löschen eines vSphere Native Key Providers

vSphere Native Key Provider – Übersicht

In vSphere 7.0 Update 2 und höher können Sie den integrierten vSphere Native Key Provider verwenden, um Verschlüsselungstechnologien wie virtuelle TPMs (vTPM) zu aktivieren.

vSphere Native Key Provider ist in allen vSphere Editionen enthalten und benötigt keinen externen Schlüsselserver – in der Branche auch als Schlüsselmanagementserver (Key Management Server oder KMS) bezeichnet. Sie können auch vSphere Native Key Provider für vSphere Virtual Machine Encryption verwenden. Dazu müssen Sie jedoch die VMware vSphere® Enterprise Plus Edition™ erwerben.

Was ist vSphere Native Key Provider?

Bei einem Standardschlüsselanbieter oder vertrauenswürdigen Schlüsselanbieter müssen Sie einen externen Schlüsselserver konfigurieren. In einer Standardschlüsselanbieter-Konfiguration ruft vCenter Server Schlüssel vom externen Schlüsselserver ab und verteilt sie an die ESXi-Hosts. In der Konfiguration eines vertrauenswürdigen Schlüsselanbieters (vSphere Trust Authority) rufen die vertrauenswürdigen ESXi-Hosts die Schlüssel direkt ab.

Mit vSphere Native Key Provider benötigen Sie keinen externen Schlüsselserver mehr. vCenter Server generiert einen primären Schlüssel, den so genannten Key Derivation Key (KDK), und leitet ihn an alle ESXi-Hosts im Cluster weiter. Daraufhin generieren die ESXi-Hosts Datenverschlüsselungsschlüssel (auch wenn sie nicht mit vCenter Server verbunden sind), um Sicherheitsfunktionalität wie vTPMs zu aktivieren. Die vTPM-Funktionalität ist in allen vSphere Editionen enthalten. Um einen vSphere Native Key Provider für vSphere Virtual Machine Encryption zu verwenden, müssen Sie die vSphere Enterprise Plus Edition erwerben. vSphere Native Key Provider kann mit einer vorhandenen Schlüsselserverinfrastruktur koexistieren.

vSphere Native Key Provider:

- Aktiviert die Verwendung von vTPMs, vSphere Virtual Machine Encryption und die vSAN-Verschlüsselung ruhender Daten, wenn Sie keinen externen Schlüsselserver benötigen oder möchten.
- Funktioniert nur mit VMware-Infrastrukturprodukten.
- Bietet keine externe Interoperabilität, KMIP-Unterstützung, Hardware-Sicherheitsmodule oder andere Funktionen, die ein herkömmlicher, externer Schlüsselserver von Drittanbietern für die Interoperabilität oder die Einhaltung behördlicher Auflagen anbieten kann. Wenn Ihre Organisation diese Funktionalität für Nicht-VMware-Produkte und -Komponenten benötigt, installieren Sie den herkömmlichen Schlüsselserver eines Drittanbieters.
- Hilft bei der Abwicklung der Anforderungen von Organisationen, die einen externen Schlüsselserver entweder nicht verwenden können oder nicht verwenden möchten.
- Verbessert die Methoden der Datenbereinigung und der Systemwiederverwendung, indem die frühere Verwendung von Verschlüsselungstechnologien auf schwer zu bereinigenden Medien wie Flash und SSD aktiviert wird.
- Stellt einen Übergangspfad zwischen Schlüsselanbietern bereit. vSphere Native Key Provider ist mit dem VMware-Standardschlüsselanbieter und dem vertrauenswürdigen vSphere Trust Authority-Schlüsselanbieter kompatibel.
- Funktioniert mit mehreren vCenter Server-Systemen, die eine Konfiguration im erweiterten verknüpften Modus oder eine vCenter Server-Hochverfügbarkeitskonfiguration verwenden.

- Kann verwendet werden, um vTPM in allen Editionen von vSphere zu aktivieren und virtuelle Maschinen mit dem Kauf der vSphere Enterprise Plus Edition zu verschlüsseln, die vSphere Virtual Machine Encryption enthält. vSphere Virtual Machine Encryption funktioniert mit vSphere Native Key Provider wie bei VMware und vertrauenswürdigen Schlüsselanbietern.
- Kann verwendet werden, um vSAN-Verschlüsselung ruhender Daten mithilfe einer entsprechenden vSAN-Lizenz zu aktivieren.
- Kann ein Trusted Platform Module (TPM) 2.0 verwenden, um die Sicherheit zu erhöhen, wenn eins auf einem ESXi-Host installiert ist. Sie können vSphere Native Key Provider auch so konfigurieren, dass er nur für Hosts verfügbar ist, auf denen ein TPM 2.0 installiert ist.

Hinweis Ein ESXi-Host benötigt kein TPM 2.0 zur Verwendung eines vSphere Native Key Providers. Ein TPM 2.0 bietet jedoch erweiterte Sicherheit.

Wie bei allen Sicherheitslösungen sollten Sie das Systemdesign, Implementierungsüberlegungen und Konflikte bei der Verwendung des nativen Schlüsselanbieters berücksichtigen. Beispielsweise vermeidet ESXi-Schlüsselpersistenz die Abhängigkeit von einem Schlüsselserver, der immer verfügbar ist. Da die Schlüsselpersistenz jedoch die kryptografischen Informationen des nativen Schlüsselanbieters auf den Clusterhosts speichert, sind Sie weiterhin gefährdet, wenn böswillige Akteure die ESXi-Hosts selbst stehlen. Da sich Umgebungen unterscheiden, bewerten und implementieren Sie Ihre Sicherheitskontrollen gemäß den regulatorischen und Sicherheitsanforderungen Ihrer Organisation, den operativen Anforderungen und der Toleranz gegenüber Risiken.

Weitere Informationen zum vSphere Native Key Provider finden Sie unter https://core.vmware.com/native-key-provider.

vSphere Native Key Provider – Anforderungen

Um vSphere Native Key Provider zu verwenden, müssen Sie Folgendes ausführen:

- Stellen Sie sicher, dass sowohl das vCenter Server-System als auch ESXi-Hosts vSphere 7.0 Update 2 oder höher ausführen.
- Konfigurieren Sie die ESXi-Hosts in einem Cluster. Obwohl dies nicht erforderlich ist, wird empfohlen, möglichst identische ESXi-Hosts zu verwenden, einschließlich TPMs. Clusterverwaltung und Funktionsaktivierung werden durch identische Clusterhosts stark vereinfacht.
- Konfigurieren Sie die dateibasierte vCenter Server-Sicherung und -Wiederherstellung und speichern Sie die Backups auf sichere Weise, da sie den KDK (Key Derivation Key) enthalten. Weitere Informationen finden Sie im Thema zur vCenter Server-Sicherung und -Wiederherstellung in *Installation und Einrichtung von vCenter Server*.

Um vSphere Virtual Machine Encryption oder vSAN-Verschlüsselung mit vSphere Native Key Provider durchführen zu können, müssen Sie diejenigen Editionen dieser Produkte erwerben, die die entsprechende Lizenz enthalten.

vSphere Native Key Provider und erweiterter verknüpfter Modus

Sie können einen einzelnen vSphere Native Key Provider konfigurieren, der über vCenter Server-Systeme hinweg gemeinsam nutzbar ist, die in einer Konfiguration des erweiterten verknüpften Modus konfiguriert sind. Die allgemeinen Schritte in diesem Szenario:

1 Erstellen des vSphere Native Key Providers auf einem der vCenter Server-Systeme

2 Sichern des nativen Schlüsselanbieters auf dem vCenter Server, auf dem er erstellt wurde

3 Exportieren des nativen Schlüsselanbieters

4 Importieren des nativen Schlüsselanbieters in die anderen vCenter Server-Systeme in der Konfiguration des erweiterten verknüpften Modus

Weitere Informationen finden Sie unter Importieren eines vSphere Native Key Providers in eine Konfiguration mit erweitertem verknüpftem Modus.

vSphere Native Key Provider – Rechte

Wie bei Standardschlüsselanbietern und vertrauenswürdigen Schlüsselanbietern verwendet vSphere Native Key Provider den **Cryptographer.***-Berechtigungen Darüber hinaus verwendet vSphere Native Key Provider zum Auflisten der vSphere Native Key Provider das Recht **Cryptographer.ReadKeyServersInfo**, das speziell für vSphere Native Key Provider gilt. Weitere Informationen hierzu finden Sie unter Rechte für Verschlüsselungsvorgänge.

vSphere Native Key Provider – Alarme

Sie müssen einen vSphere Native Key Provider sichern. Wenn ein vSphere Native Key Provider nicht gesichert wird, generiert vCenter Server einen Alarm. Wenn Sie den vSphere Native Key Provider, für den ein Alarm generiert wurde, sichern, setzt vCenter Server den Alarm zurück. Standardmäßig überprüft vCenter Server einmal täglich, ob vSphere Native Key Provider gesichert wurden. Sie können das Prüfintervall ändern, indem Sie die Option `vpxd.KMS.backupCheckInterval` ändern.

vSphere Native Key Provider – regelmäßige Standardisierungsprüfung

vCenter Server Prüft regelmäßig, ob die vSphere Native Key Provider-Konfiguration auf den vCenter Server- und ESXi-Hosts übereinstimmt. Wenn sich ein Hoststatus ändert, z. B. wenn Sie einen Host zum Cluster hinzufügen, weicht die Konfiguration des Schlüsselanbieters auf dem Cluster von der Konfiguration auf dem Host ab. Wenn die Konfiguration (keyID) auf dem Host abweicht, aktualisiert vCenter Server die Konfiguration des Hosts automatisch. Es ist kein manueller Eingriff erforderlich.

Standardmäßig überprüft vCenter Server die Konfiguration alle fünf Minuten. Sie können das Intervall mit der Option `vpxd.KMS.remediationInterval` ändern.

Verwenden von vSphere Native Key Provider mit einer Site für die Notfallwiederherstellung

Sie können vSphere Native Key Provider mit einer Site für die Notfallwiederherstellung als Backup verwenden. Durch Importieren des vSphere Native Key Provider-Backups von der primären Site auf den vCenter Server der Site für die Notfallwiederherstellung kann dieser Cluster die verschlüsselten virtuellen Maschinen entschlüsseln und ausführen.

Testen Sie immer Ihre Notfallwiederherstellungslösung. Verlassen Sie sich nicht darauf, dass Ihre Lösung funktioniert, ohne testweise eine Wiederherstellung durchzuführen. Stellen Sie sicher, dass eine Kopie der vSphere Native Key Provider-Sicherung auch für Ihre DR-Site verfügbar ist.

vSphere Native Key Provider – Prozessablauf

Das Verstehen der vSphere Prozessabläufe von vSphere Native Key Provider ist wichtig, um zu erfahren, wie Sie Ihren vSphere Native Key Provider konfigurieren und verwalten können.

Sie können den integrierten vSphere Native Key Provider verwenden, um verschlüsselungsbasierte virtuelle TPMs (vTPM) zu aktivieren. vSphere Native Key Provider ist in allen vSphere Editionen enthalten und erfordert keinen externen Schlüsselserver (KMS). Um einen vSphere Native Key Provider für vSphere Virtual Machine Encryption zu verwenden, müssen Sie die vSphere Enterprise+ Edition erwerben.

Konfigurieren von vSphere Native Key Provider

Die Konfiguration von vSphere Native Key Provider umfasst die folgenden grundlegenden Vorgänge:

1. Ein Benutzer mit den entsprechenden Administratorrechten generiert mit vSphere Client einen vSphere Native Key Provider auf einem vCenter Server.
2. Daraufhin konfiguriert vCenter Server dann den vSphere Native Key Provider für alle ESXi-Host-Cluster.

   In diesem Schritt pusht vCenter Server einen primären Schlüssel an alle ESXi-Hosts im Cluster. Ebenso wird die Änderung an die Hosts im Cluster übertragen, wenn Sie einen vSphere Native Key Provider aktualisieren oder löschen.
3. Benutzer mit den entsprechenden kryptografischen Rechten erstellen vTPMs und verschlüsselte virtuelle Maschinen (vorausgesetzt, Sie haben die vSphere Enterprise+ Edition erworben).

   Weitere Informationen finden Sie unter Kapitel 11 Sichern von virtuellen Maschinen mit Virtual Trusted Platform Module und Kapitel 10 Verwenden von Verschlüsselung in Ihrer vSphere-Umgebung.

Prozessablauf bei der vSphere Native Key Provider-Verschlüsselung

Informationen dazu, wie verschiedene Komponenten interagieren, um eine Verschlüsselungsaufgabe mit vSphere Native Key Provider durchzuführen, finden Sie unter Prozessablauf bei der Verschlüsselung.

Konfigurieren eines vSphere Native Key Providers

Bevor Sie mit den Verschlüsselungsaufgaben beginnen, müssen Sie einen vSphere Native Key Provider auf dem vCenter Server konfigurieren.

vSphere 7.0 Update 2 und höhere Versionen enthalten einen Schlüsselanbieter mit der Bezeichnung „vSphere Native Key Provider“. vSphere Native Key Provider ermöglicht die Verwendung verschlüsselungsbezogener Funktionen, ohne dass ein externer Schlüsselserver (KMS) erforderlich ist. vCenter Server ist zunächst nicht mit einem vSphere Native Key Provider konfiguriert. Sie müssen einen vSphere Native Key Provider manuell konfigurieren.

Ein ESXi-Host benötigt kein TPM 2.0 zur Verwendung eines vSphere Native Key Providers. Ein TPM 2.0 bietet jedoch erweiterte Sicherheit.

Hinweis Wenn Sie einen vSphere Native Key Provider konfigurieren, stehen die Schlüsselanbieter auf allen Clustern für den vCenter Server zur Verfügung, auf dem Sie sie konfigurieren. Folglich haben alle mit dem vCenter Server verbundenen Hosts Zugriff auf alle von Ihnen konfigurierten vSphere Native Key Provider.

Voraussetzungen

Notwendige Berechtigung: **Kryptografievorgänge.Schlüsselserver verwalten**

Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server-System an.
2. Durchsuchen Sie die Bestandsliste und wählen Sie die vCenter Server-Instanz aus.
3. Klicken Sie auf **Konfigurieren** und unter **Sicherheit** auf **Schlüsselanbieter**.
4. Klicken Sie auf **Hinzufügen** und dann auf **Nativen Schlüsselanbieter hinzufügen**.
5. Geben Sie einen Namen für den vSphere Native Key Provider ein.

   Jeder logische Schlüsselanbieter muss unabhängig von seinem Typ (Standard-, vertrauenswürdiger und nativer Schlüsselanbieter) über einen eindeutigen Namen in allen vCenter Server-Systemen verfügen.

   Weitere Informationen finden Sie unter Benennung des Schlüsselanbieters.

6 Wenn dieser vSphere Native Key Provider nur von Hosts mit einem TPM 2.0 verwendet werden soll, aktivieren Sie das Kontrollkästchen **Schlüsselanbieter nur mit TPM-geschützten ESXi-Hosts verwenden**.

   Bei aktiviertem Kontrollkästchen steht der vSphere Native Key Provider nur auf Hosts mit einem TPM 2.0 zur Verfügung.

7 Klicken Sie auf **Schlüsselanbieter hinzufügen**.

   Hinweis Es dauert etwa fünf Minuten, bis alle geclusterten ESXi-Hosts in einem Datencenter den Schlüsselanbieter erhalten und der Cache des vCenter Server aktualisiert ist. Aufgrund der Art und Weise der Informationsweiterleitung müssen Sie unter Umständen einige Minuten warten, bis Sie den Schlüsselanbieter für wichtige Vorgänge auf bestimmten Hosts verwenden können.

Ergebnisse

Der vSphere Native Key Provider wird hinzugefügt und im Bereich **Schlüsselanbieter** angezeigt. Zu diesem Zeitpunkt wird der vSphere Native Key Provider nicht gesichert. Sie müssen den vSphere Native Key Provider sichern, bevor Sie ihn verwenden können.

Nächste Schritte

Weitere Informationen hierzu finden Sie unter Sichern eines vSphere Native Key Providers.

Sichern eines vSphere Native Key Providers

Wenn Sie die Konfiguration eines Schlüsselanbieters wiederherstellen müssen, ist die Sicherung eines vSphere Native Key Providers im Rahmen eines Notfallwiederherstellungsszenarios erforderlich. Sie können den vSphere Client, die PowerCLI oder API verwenden, um den vSphere Native Key Provider zu sichern.

Der vSphere Native Key Provider wird im Rahmen der dateibasierten vCenter Server-Sicherung gesichert. Sie müssen den vSphere Native Key Provider jedoch mindestens einmal sichern, bevor Sie ihn verwenden können. Wenn Sie einen vSphere Native Key Provider erstellen, wird dieser nicht gesichert.

Eine Sicherung ist dann notwendig, wenn die Konfiguration wiederhergestellt werden muss. Informationen zum Wiederherstellen eines vSphere Native Key Providers finden Sie unter Wiederherstellen eines vSphere Native Key Providers mithilfe des vSphere Client.

Speichern Sie die Sicherungsdatei an einem sicheren Ort. Sie können die Sicherung beim Erstellen mit einem Kennwort schützen. Die Sicherungsdatei liegt im Format PKCS#12 vor.

vCenter Server erstellt einen Alarm, wenn ein vSphere Native Key Provider nicht gesichert wurde. Sie können den Alarm zwar bestätigen, bis zur Sicherung des vSphere Native Key Providers wird dieser jedoch alle 24 Stunden erneut angezeigt.

Voraussetzungen

Notwendige Berechtigung: **Kryptografievorgänge.Schlüsselserver verwalten**

Hinweis In einer Konfiguration mit erweitertem verknüpftem Modus müssen Sie die Sicherung auf dem vCenter Server durchführen, zu dem der Schlüsselanbieter gehört.

Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server-System an.
2. Durchsuchen Sie die Bestandsliste und wählen Sie die vCenter Server-Instanz aus.
3. Klicken Sie auf **Konfigurieren** und unter **Sicherheit** auf **Schlüsselanbieter**.
4. Wählen Sie den zu sichernden vSphere Native Key Provider aus.

   Für nicht gesicherte Schlüsselanbieter wird der Status „Nicht gesichert“ angezeigt.
5. Klicken Sie auf **Sichern**.
6. Zum Schützen der Sicherung mit einem Kennwort aktivieren Sie das Kontrollkästchen **Daten des nativen Kennwortanbieters mit Kennwort schützen**.
   a. Geben Sie ein Kennwort ein und speichern Sie es an einem sicheren Ort.
   b. Aktivieren Sie das Kontrollkästchen **Ich habe das Kennwort an einem sicheren Ort gespeichert**, um anzugeben, dass Sie das Kennwort an einem sicheren Ort gespeichert haben.
7. Klicken Sie auf **Schlüsselanbieter sichern**.

   Die Sicherungsdatei liegt im Format PKCS#12 vor.
8. Speichern Sie die Sicherungsdatei an einem sicheren Ort.

Ergebnisse

Der Status des vSphere Native Key Provider ändert sich von „Nicht gesichert“ in „Warnung“ und „Aktiv“. Mit „Warnung“ wird angegeben, dass der vCenter Server die Informationen weiterhin an alle ESXi-Hosts im Datencenter überträgt. „Aktiv“ bedeutet, dass die Informationen an alle Hosts übertragen wurden.

Nächste Schritte

Informationen zum Hinzufügen von vTPMs zu Ihren ESXi-Hosts finden Sie unter Kapitel 11 Sichern von virtuellen Maschinen mit Virtual Trusted Platform Module. Informationen zum Verschlüsseln virtueller Maschinen finden Sie unter Kapitel 10 Verwenden von Verschlüsselung in Ihrer vSphere-Umgebung.

Importieren eines vSphere Native Key Providers in eine Konfiguration mit erweitertem verknüpftem Modus

Nachdem Sie einen nativen Schlüsselanbieter auf einem vCenter Server in einer Konfiguration mit erweitertem verknüpftem Modus erstellt haben, können Sie den vSphere Client verwenden, um ihn in einen anderen vCenter Server in der Konfiguration zu importieren.

Sie können einen einzelnen vSphere Native Key Provider konfigurieren, der über vCenter Server-Systeme hinweg gemeinsam nutzbar ist, die in einer Konfiguration des erweiterten verknüpften Modus konfiguriert sind. Sie erstellen den vSphere Native Key Provider auf einem vCenter Server-System in der Konfiguration mit erweitertem verknüpftem Modus und verwenden dann die Funktion **Wiederherstellen**, um die verschlüsselte Schlüsseldatei in die anderen ELM-verbundenen vCenter Server-Systeme zu importieren.

Voraussetzungen

- Notwendige Berechtigung: **Kryptografievorgänge.Schlüsselserver verwalten**
- Erstellen Sie den vSphere Native Key Provider auf einem Ihrer vCenter Server-Systeme in der Konfiguration mit erweitertem verknüpftem Modus. Weitere Informationen finden Sie unter Konfigurieren eines vSphere Native Key Providers.
- Sichern Sie den vSphere Native Key Provider und laden Sie die verschlüsselte Schlüsseldatei für die Sicherung herunter. Weitere Informationen hierzu finden Sie unter Sichern eines vSphere Native Key Providers. Speichern Sie die verschlüsselte Schlüsseldatei für die Sicherung an einem sicheren Ort, auf den Sie beim Importieren zugreifen können.

Verfahren

1. Melden Sie sich beim vSphere Client bei einem vCenter Server in der Konfiguration mit erweitertem verknüpftem Modus an, in den Sie den vSphere Native Key Provider importieren möchten.
2. Durchsuchen Sie die Bestandsliste und wählen Sie die vCenter Server-Instanz aus.
3. Klicken Sie auf **Konfigurieren** und unter **Sicherheit** auf **Schlüsselanbieter**.
4. Klicken Sie auf **Wiederherstellen**.
5. Wechseln Sie zum Dateispeicherort, in dem Sie die verschlüsselte Schlüsseldatei für die Sicherung des vSphere Native Key Providers gespeichert haben.

   Die Datei wurde im PKCS#12-Format gespeichert.
6. Wählen Sie die Datei aus.
7. (Optional) Wenn die Datei kennwortgeschützt ist, geben Sie das Kennwort ein.
8. Klicken Sie auf **Weiter**.
9. (Optional) Wenn Sie sich entschieden haben, diesen Schlüsselanbieter nur mit TPM-geschützten ESXi-Hosts zu verwenden, aktivieren Sie das Kontrollkästchen.

10 Klicken Sie auf **Beenden**.

Ergebnisse

Der vSphere Native Key Provider wird in den vCenter Server importiert. Um den vSphere Native Key Provider für Verschlüsselungsaufgaben zu verwenden, stellen Sie sicher, dass Sie ihn zuerst im Bereich **Schlüsselanbieter** auswählen und auf **Als Standard festlegen** klicken.

Nächste Schritte

Wiederholen Sie diese Schritte für andere vCenter Server-Systeme in Ihrer Konfiguration mit erweitertem verknüpftem Modus, denen Sie den vSphere Native Key Provider hinzufügen möchten.

Wiederherstellen eines vSphere Native Key Providers

Sie können den vSphere Native Key Provider entweder über den -vSphere Client oder über die vCenter Server Appliance wiederherstellen.

Bei Bedarf können Sie einen vSphere Native Key Provider auf folgende Arten wiederherstellen.

1 Wenn Sie Ihre vCenter Server Appliance nicht neu erstellen müssen, verwenden Sie den vSphere Client, um den Schlüsselanbieter wiederherzustellen. Weitere Informationen hierzu finden Sie unter Wiederherstellen eines vSphere Native Key Providers mithilfe des vSphere Client.

2 Wenn Sie Ihre vCenter Server Appliance neu erstellen müssen, müssen Sie den Schlüsselanbieter aus Ihrer vCenter Server Appliance-Sicherung wiederherstellen. Wenn Sie eine vCenter Server Appliance-Sicherung durchführen, wird der native Schlüsselanbieter gespeichert. Unter https://blogs.vmware.com/vsphere/2018/05/vcenter-server-appliance-6-7-file-based-backup-and-restore-walkthroughs.html finden Sie Informationen zum Wiederherstellen von vCenter Server Appliance aus der Sicherung.

Wiederherstellen eines vSphere Native Key Providers mithilfe des vSphere Client

Sie können den vSphere Client zum Wiederherstellen des vSphere Native Key Providers verwenden.

Sie können einen nativen Schlüsselanbieter wiederherstellen, falls er versehentlich gelöscht wurde oder wenn Sie eine Notfallwiederherstellung durchführen müssen.

Wenn Sie einen vSphere Native Key Provider wiederherstellen, müssen Sie den Schlüsselanbieter nicht erneut sichern. Die anfängliche Sicherung ist nicht ausreichend. Verwalten Sie die Sicherungsdatei weiterhin an einem sicheren Ort.

Voraussetzungen

- Notwendige Berechtigung: **Kryptografievorgänge.Schlüsselserver verwalten**
- Die Sicherungsdatei des Schlüsselanbieters.

- Das Kennwort für die Schlüsselanbieterdatei, sofern Sie eines beim Sichern des Schlüsselanbieters eingegeben haben.

Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server-System an.
2. Durchsuchen Sie die Bestandsliste und wählen Sie die vCenter Server-Instanz aus.
3. Klicken Sie auf **Konfigurieren** und unter **Sicherheit** auf **Schlüsselanbieter**.
4. Wählen Sie den vSphere Native Key Provider aus und klicken Sie auf **Wiederherstellen**.
5. Navigieren Sie zum Dateispeicherort und wählen Sie die verschlüsselte Schlüsseldatei für die Sicherung aus.

   Die Datei wurde im PKCS#12-Format gespeichert.
6. (Optional) Wenn die Datei kennwortgeschützt ist, geben Sie das Kennwort ein.
7. Klicken Sie auf **Weiter**.
8. (Optional) Wenn Sie sich entschieden haben, diesen Schlüsselanbieter nur mit TPM-geschützten ESXi-Hosts zu verwenden, aktivieren Sie das Kontrollkästchen.
9. Klicken Sie auf **Beenden**.

Ergebnisse

Der vSphere Native Key Provider wird wiederhergestellt.

Aktualisieren eines vSphere Native Key Providers

Im Rahmen Ihrer regelmäßigen Schlüsselrotationspläne können Sie PowerCLI verwenden, um einen vSphere Native Key Provider zu aktualisieren.

Wenn Sie über eine Richtlinie für die Schlüsselrotation verfügen, können Sie den vSphere Native Key Provider aktualisieren und erneut Schlüssel für die virtuellen Maschinen erstellen, die Sie mit diesem Schlüsselanbieter verschlüsselt haben. Sie müssen PowerCLI verwenden, um den vSphere Native Key Provider zu aktualisieren. Sie können auch erneut Schlüssel für die virtuellen Maschinen erstellen, ohne den Schlüsselanbieter zu aktualisieren. In diesem Fall werden nur die Schlüssel der virtuellen Maschinen geändert. Informationen zur erneuten Schlüsselerstellung für eine virtuelle Maschine finden Sie unter Erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine mithilfe des vSphere Client.

Voraussetzungen

- Notwendige Berechtigung: **Kryptografievorgänge.Schlüsselserver verwalten**
- PowerCLI 12.3.0

Verfahren

1 Führen Sie in einer PowerCLI-Sitzung das Cmdlet `Connect-VIServer` aus, um als Administratorbenutzer eine Verbindung mit dem vCenter Server herzustellen, auf dem Sie den zu aktualisierenden vSphere Native Key Provider konfiguriert haben.

```
Connect-VIServer -server VC_ip_address -User admin_user -Password 'password'
```

2 Zum Abrufen der vSphere Native Key Provider-Namen führen Sie das Cmdlet `Get-KeyProvider` mit dem optionalen Parameter `Type` aus.

```
Get-KeyProvider -Type NativeKeyProvider
```

3 Zum Aktualisieren des Schlüsselanbieters führen Sie das Cmdlet `Set-KeyProvider` aus und geben Sie den Namen des Schlüsselanbieters und die GUID an.

Sie können die zu verwendende GUID generieren, indem Sie das Cmdlet `New-Guid` ausführen.

```
Set-KeyProvider -KeyProvider KeyProvider_name -KeyId Guid
```

Es wird eine Warnung zum Sichern der Konfiguration angezeigt.

4 Um den Schlüsselanbieter zu sichern, führen Sie das Cmdlet `Export-KeyProvider` aus.

```
Export-KeyProvider -KeyProvider KeyProvider_name -FilePath path_file_name
```

Sie können den Schlüsselanbieter auch mithilfe des vSphere Client sichern. Weitere Informationen finden Sie unter Sichern eines vSphere Native Key Providers.

Ergebnisse

Wenn ein Schlüsselanbieter aktualisiert wird, ändert sich sein Status in „Nicht gesichert“. Nachdem Sie den Schlüsselanbieter gesichert haben, ändert sich sein Status in „Aktiv“.

Löschen eines vSphere Native Key Providers

Sie können einen vSphere Native Key Provider aus vCenter Server löschen.

Nachdem Sie einen vSphere Native Key Provider gelöscht haben, werden virtuelle Maschinen, die über vTPMs verfügen oder verschlüsselt sind, weiterhin ausgeführt. Wenn Sie den ESXi-Host neu starten, wechseln die zugehörigen verschlüsselten VMs in den gesperrten Modus. Nachdem Sie die Registrierung dieser virtuellen Maschinen aufgehoben haben, wechseln sie in den gesperrten Modus, wenn Sie versuchen, sie erneut zu registrieren. Die einzige Möglichkeit zum Entsperren der virtuellen Maschinen besteht in der Wiederherstellung des vorherigen vSphere Native Key Providers.

Voraussetzungen

Notwendige Berechtigung: **Kryptografievorgänge.Schlüsselserver verwalten**

Verschlüsseln Sie vor dem Löschen eines vSphere Native Key Providers alle verschlüsselten virtuellen Maschinen und Datenspeicher, die mithilfe dieses Schlüsselanbieters verschlüsselt wurden, erneut mit einem anderen Schlüsselanbieter. Weitere Informationen finden Sie unter Erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine mithilfe des vSphere Client.

Behalten Sie zudem eine Sicherung des vSphere Native Key Providers für den Fall bei, dass Sie eine verschlüsselte virtuelle Maschine nach dem Löschen des Schlüsselanbieters erneut verschlüsseln müssen.

Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server-System an.
2. Durchsuchen Sie die Bestandsliste und wählen Sie die vCenter Server-Instanz aus.
3. Klicken Sie auf **Konfigurieren** und unter **Sicherheit** auf **Schlüsselanbieter**.
4. Wählen Sie den Schlüsselanbieter aus, den Sie löschen möchten.
5. Klicken Sie auf **Löschen**.
6. Lesen Sie die Warnmeldung und ziehen Sie den Schieberegler ganz nach rechts.
7. Klicken Sie auf **Löschen**.

Ergebnisse

Der vSphere Native Key Provider wird aus dem vCenter Server entfernt.

vSphere Trust Authority

9

Mit vSphere ab Version 7.0 können Sie die Vorteile von VMware® vSphere Trust Authority™ nutzen. vSphere Trust Authority ist eine grundlegende Technologie zur Verbesserung der Sicherheit von Arbeitslasten. vSphere Trust Authority schafft ein größeres Maß an Vertrauen in Ihrer Organisation, indem Sie den Hardware-Root of Trust eines ESXi-Hosts mit der Arbeitslast selbst verknüpfen.

Dieses Kapitel enthält die folgenden Themen:

vSphere Trust Authority – Konzepte und Funktionen

vSphere Trust Authority schützt Ihr SDDC vor böswilligen Angriffen, indem die Vertrauenswürdigkeit einer vertrauenswürdigen Computing-Basis auf die gesamte Computing-Infrastruktur Ihres Unternehmens ausgeweitet wird. vSphere Trust Authority verwendet Remotebestätigung und kontrollierten Zugriff auf erweiterte Kryptografiefunktionen.

vSphere Trust Authority ist ein Satz von Diensten, der hohe Sicherheitsanforderungen erfüllt. Mit vSphere Trust Authority können Sie eine sichere Infrastruktur einrichten und verwalten. Sie können sicherstellen, dass vertrauliche Arbeitslasten nur auf ESXi-Hosts ausgeführt werden, auf denen nachweislich Originalsoftware gestartet wurde.

So schützt vSphere Trust Authority Ihre Umgebung

Sie konfigurieren vSphere Trust Authority-Dienste zum Bestätigen Ihrer ESXi-Hosts, die dann vertrauenswürdige Kryptografievorgänge durchführen können.

vSphere Trust Authority verwendet Remotebestätigungen für ESXi-Hosts, um die Echtheit der gestarteten Software zu bestätigen. Mithilfe von Bestätigungen wird sichergestellt, dass auf den ESXi-Hosts echte VMware-Software oder von VMware signierte Partnersoftware verwendet wird. Bestätigungen greifen auf Messungen zurück, die sich in einem TPM 2.0-Chip (Trusted Platform Module) befinden, der auf dem ESXi-Host installiert ist. In vSphere Trust Authority kann ein ESXi-Host nur dann auf Verschlüsselungsschlüssel zugreifen und Kryptografievorgänge durchführen, wenn er bestätigt wurde.

vSphere Trust Authority-Glossar

vSphere Trust Authority führt bestimmte wichtige Begriffe und Definitionen ein.

Tabelle 9-1. vSphere Trust Authority-Glossar

Begriff	Definition
VMware vSphere® Trust Authority™	Gibt einen Satz von Diensten an, die eine vertrauenswürdige Infrastruktur ermöglichen. Stellt sicher, dass auf ESXi-Hosts vertrauenswürdige Software ausgeführt wird und dass Verschlüsselungsschlüssel nur für vertrauenswürdige ESXi-Hosts freigegeben werden.
vSphere Trust Authority-Komponenten	Zu den vSphere Trust Authority-Komponenten gehören: ■ Bestätigungsdienst ■ Schlüsselanbieterdienst
Bestätigungsdienst	Bestätigt den Status eines ESXi-Remotehosts. Verwendet TPM 2.0 zum Aufbau eines Hardware-Root of Trust und überprüft Software-Messungen anhand einer Liste mit ESXi-Versionen, die vom Administrator genehmigt wurden.
Schlüsselanbieterdienst	Schließt einen oder mehrere Schlüsselserver ein und macht vertrauenswürdige Schlüsselanbieter verfügbar, die beim Verschlüsseln von virtuellen Maschinen angegeben werden können. Derzeit sind Schlüsselserver auf das KMIP-Protokoll beschränkt.
Vertrauenswürdige Infrastruktur	Eine vertrauenswürdige Infrastruktur besteht aus Folgendem: ■ Ein Trust Authority-vCenter Server ■ Ein Arbeitslast-vCenter Server ■ Mindestens ein vSphere Trust Authority-Cluster (konfiguriert als Teil des Trust Authority-vCenter Server) ■ Mindestens ein vertrauenswürdiger Cluster (konfiguriert als Teil des Arbeitslast-vCenter Server) ■ Verschlüsselte Arbeitslast-VMs, die im vertrauenswürdigen Cluster ausgeführt werden ■ Mindestens ein KMIP-konformer Schlüsselverwaltungsserver **Hinweis** Sie müssen getrennte vCenter Server-Systeme für den Trust Authority- und den vertrauenswürdigen Cluster verwenden.
Trust Authority-Cluster	Besteht aus einem vCenter Server-Cluster mit ESXi-Hosts, auf denen die vSphere Trust Authority-Komponenten (Bestätigungs- und Schlüsselanbieterdienst) ausgeführt werden.
Trust Authority-Host	Ein ESXi-Host, auf dem vSphere Trust Authority-Komponenten (Bestätigungs- und Schlüsselanbieterdienst) ausgeführt werden.
Vertrauenswürdiger Cluster	Besteht aus einem vCenter Server-Cluster mit vertrauenswürdigen ESXi-Hosts, die remote vom Trust Authority-Cluster bestätigt wurden. Obwohl dies nicht unbedingt erforderlich ist, erhöht ein konfigurierter Schlüsselanbieterdienst den von einem vertrauenswürdigen Cluster bereitgestellten Wert erheblich.
Vertrauenswürdiger Host	Ein ESXi-Host, dessen Software vom Bestätigungsdienst des Trust Authority-Clusters überprüft wurde. Dieser Host führt Arbeitslast-VMs aus, die mithilfe von Schlüsselanbietern verschlüsselt werden können, die vom Schlüsselanbieterdienst des Trust Authority-Clusters veröffentlicht wurden.

Tabelle 9-1. vSphere Trust Authority-Glossar (Fortsetzung)

Begriff	Definition
vSphere Encryption für virtuelle Maschinen	Mit vSphere Virtual Machine Encryption können Sie verschlüsselte virtuelle Maschinen erstellen und vorhandene virtuelle Maschinen verschlüsseln. ■ Ab vSphere 6.5 fordert vCenter Server Schlüssel bei einem externen Schlüsselserver an. Der Schlüsselserver generiert und speichert die Schlüssel und leitet sie zur Verteilung an vCenter Server weiter. ■ Ab vSphere 7.0 kann die vertrauenswürdige Verbindung zwischen vSphere Trust Authority und einem Schlüsselserver eingerichtet werden. In diesem Setup müssen der vCenter Server und die ESXi-Arbeitslasthosts keine direkten Schlüsselserver-Anmeldedaten anfordern. Darüber hinaus ermöglicht dieses Setup eine zusätzliche Sicherheitsebene zur Verteidigung in der Tiefe (Defense-in-Depth).
Vertrauenswürdiger Schlüsselanbieter	Ein Schlüsselanbieter, der einen einzelnen Verschlüsselungsschlüssel auf einem Schlüsselserver kapselt. Für den Zugriff auf den Verschlüsselungsschlüssel muss vom Bestätigungsdienst bestätigt werden, dass die ESXi-Software auf dem vertrauenswürdigen Host verifiziert wurde.
Standardschlüsselanbieter	Ein Schlüsselanbieter, der Verschlüsselungsschlüssel direkt von einem Schlüsselserver abruft und Schlüssel an die notwendigen Hosts in einem Datencenter verteilt. Wurde zuvor in vSphere als KMS-Cluster bezeichnet.
Schlüsselserver	Ein KMIP-KMS (Key Management Server), der einem Schlüsselanbieter zugeordnet ist.
Arbeitslast-vCenter Server	Der vCenter Server, der einen oder mehrere vertrauenswürdige Cluster verwaltet und zu deren Konfiguration verwendet wird.

Grundlegendes zu vSphere Trust Authority

Mit vSphere Trust Authority können Sie folgende Aufgaben durchführen:

- Bereitstellen von ESXi-Hosts mit einem Hardware-Root of Trust und Funktionen für die Remotebestätigung
- Einschränken der Verschlüsselungsschlüsselverwaltung, indem Schlüssel nur für bestätigte ESXi-Hosts freigegeben werden
- Erstellen einer sichereren Verwaltungsumgebung für die Verwaltung von Vertrauensstellungen
- Zentrale Verwaltung mehrerer Schlüsselserver
- Weitere Durchführung von Kryptografievorgängen auf virtuellen Maschinen, jedoch mit erweiterter Verschlüsselungsschlüsselverwaltung.

In vSphere 6.5 und 6.7 ist die VM-Verschlüsselung auf vCenter Server angewiesen, um Verschlüsselungsschlüssel aus einem Schlüsselserver abzurufen und gegebenenfalls an ESXi-Hosts weiterzugeben. vCenter Server authentifiziert sich beim Schlüsselserver unter Verwendung von Client- und Serverzertifikaten, die in VMware Endpoint Certificate Store (VECS) gespeichert sind. Vom Schlüsselserver gesendete Verschlüsselungsschlüssel geben vCenter Server-Arbeitsspeicher an die erforderlichen ESXi-Hosts weiter (mit Datenverschlüsselung, die von TLS über das Netzwerk bereitgestellt wird). Darüber hinaus ist vSphere auf

Berechtigungsprüfungen in vCenter Server angewiesen, um Benutzerberechtigungen zu validieren und Schlüsselserver-Zugriffsbeschränkungen zu erzwingen. Diese Architektur ist zwar sicher, berücksichtigt aber nicht die Gefahren durch einen manipulierten vCenter Server, einen böswilligen vCenter Server-Administrator oder einen Verwaltungs- bzw. Konfigurationsfehler, der dazu führen kann, dass geheime Schlüssel manipuliert oder gestohlen werden.

In vSphere 7.0 werden diese Probleme mithilfe von vSphere Trust Authority behoben. Sie können eine vertrauenswürdige Computerbasis (Trusted Computing Base) erstellen, die aus einem sicheren, verwaltbaren Satz von ESXi-Hosts besteht. vSphere Trust Authority implementiert einen Remotebestätigungsdienst für die ESXi-Hosts, die Sie als vertrauenswürdig einstufen möchten. Darüber hinaus bietet vSphere Trust Authority verbesserte Unterstützung für TPM 2.0-Bestätigungen (ab Version 6.7 zu vSphere hinzugefügt), um Zugriffsbeschränkungen für Verschlüsselungsschlüssel zu implementieren und somit besseren Schutz für die geheimen Schlüssel der Arbeitslast-VM bereitzustellen. Darüber hinaus erlaubt vSphere Trust Authority nur autorisierten Trust Authority-Administratoren, vSphere Trust Authority-Dienste und Trust Authority-Hosts zu konfigurieren. Der Trust Authority-Administrator kann mit dem vSphere-Administratorbenutzer übereinstimmen oder ein separater Benutzer sein.

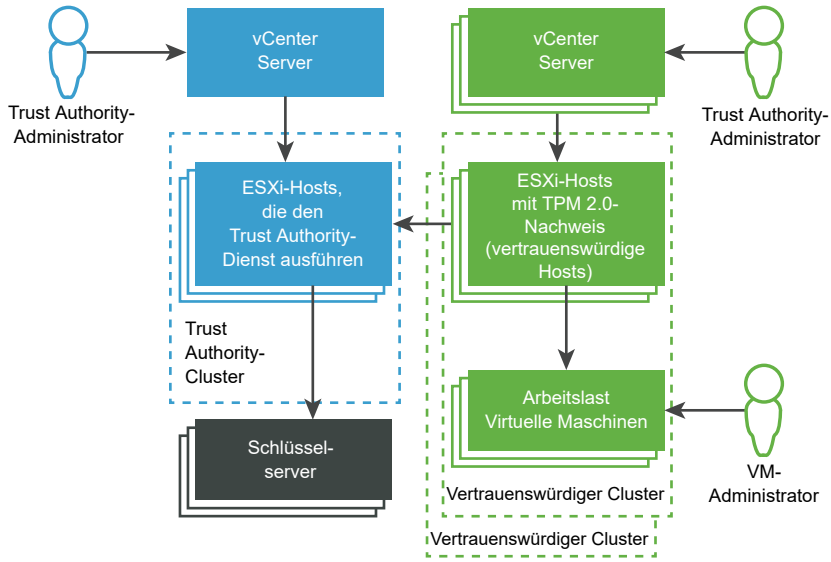
Schließlich können Sie Ihre Arbeitslasten mithilfe von vSphere Trust Authority in einer sichereren Umgebung ausführen, indem Sie:

- Manipulationen erkennen
- Nicht autorisierte Änderungen verweigern
- Malware und Änderungen verhindern
- Vertrauliche Arbeitslasten ausschließlich mit verifizierter, sicherer Hardware und Software ausführen

vSphere Trust Authority – Architektur

Die folgende Abbildung zeigt eine vereinfachte Darstellung der vSphere Trust Authority-Architektur.

Abbildung 9-1. vSphere Trust Authority – Architektur



In dieser Abbildung:

1 vCenter Server-Systeme

Der Trust Authority-Cluster und die vertrauenswürdigen Cluster werden in separaten vCenter Server-Systemen verwaltet.

2 Trust Authority-Cluster

Besteht aus den ESXi-Hosts, die die vSphere Trust Authority-Komponenten ausführen.

3 Schlüsselserver

Speichern Sie Verschlüsselungsschlüssel, die beim Durchführen von Verschlüsselungsvorgängen vom Schlüsselanbieterdienst verwendet werden. Die Schlüsselserver befinden sich außerhalb von vSphere Trust Authority.

4 Vertrauenswürdige Cluster

Bestehen aus den vertrauenswürdigen ESXi-Hosts, die remote mit einem TPM bestätigt wurden und die verschlüsselte Arbeitslasten ausführen.

5 Trust Authority-Administrator

Administrator, der Mitglied der vCenter Server-Gruppe „TrustedAdmins“ ist und die vertrauenswürdige Infrastruktur konfiguriert.

vSphere Trust Authority ermöglicht Flexibilität beim Festlegen von Trust Authority-Administratoren. Bei den Trust Authority-Administratoren in der Abbildung kann es sich um separate Benutzer handeln. Die Trust Authority-Administratoren können aber auch derselbe Benutzer sein, wobei Anmeldedaten verwendet werden, die über die vCenter Server-Systeme hinweg verknüpft sind. In diesem Fall handelt es sich um denselben Benutzer und dieselbe TrustedAdmins-Gruppe.

6 VM-Administrator

Administrator, dem Berechtigungen zum Verwalten der verschlüsselten Arbeitslast-VMs auf den vertrauenswürdigen Hosts erteilt wurden.

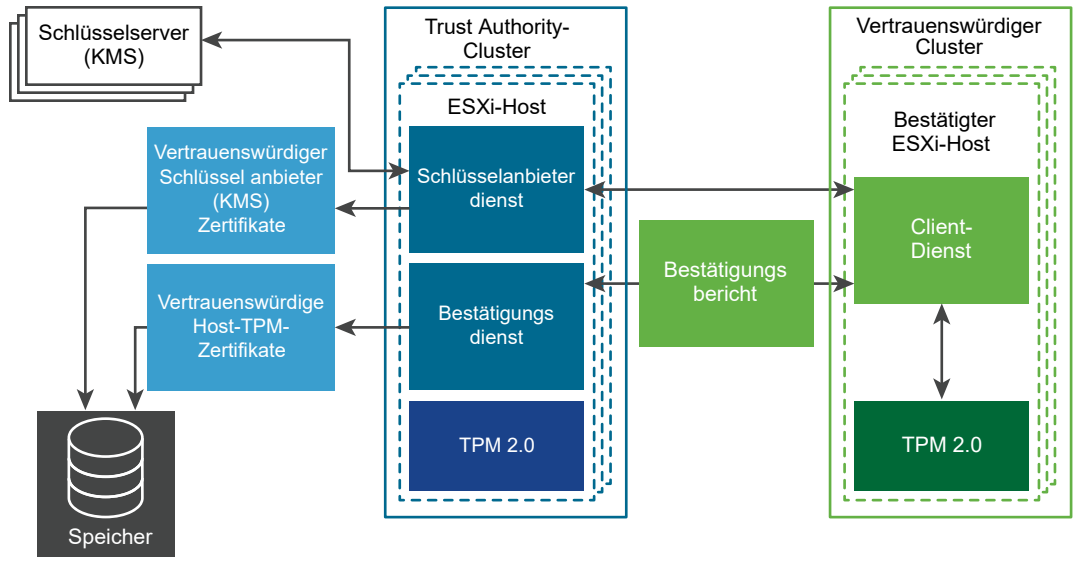
Vertrauenswürdige Infrastruktur – Übersicht

Die vertrauenswürdige Infrastruktur setzt sich aus vSphere Trust Authority-Diensten, mindestens einem KMIP-kompatiblen Schlüsselserver, den vCenter Server-Systemen und Ihren ESXi-Hosts zusammen.

Was ist eine vertrauenswürdige Infrastruktur?

Eine vertrauenswürdige Infrastruktur besteht aus mindestens einem vSphere Trust Authority-Cluster, mindestens einem vertrauenswürdigen Cluster und mindestens einem externen KMIP-kompatiblen Schlüsselserver. Jeder Cluster enthält ESXi-Hosts, auf denen bestimmte vSphere Trust Authority-Dienste ausgeführt werden (siehe folgende Abbildung).

Abbildung 9-2. vSphere Trust Authority-Dienste



Durch die Konfiguration des Trust Authority-Clusters werden zwei Dienste aktiviert:

- Bestätigungsdienst
- Schlüsselanbieterdienst

Wenn Sie vSphere Trust Authority konfigurieren, kommunizieren die ESXi-Hosts im vertrauenswürdigen Cluster mit dem Bestätigungsdienst. Der Schlüsselanbieterdienst befindet sich zwischen den vertrauenswürdigen Hosts und einem oder mehreren vertrauenswürdigen Schlüsselanbietern.

Hinweis Aktuell benötigen die ESXi-Hosts im Trust Authority-Cluster kein TPM. Es empfiehlt sich jedoch, neue ESXi-Hosts mit TPMs zu installieren.

Informationen zum vSphere Trust Authority-Bestätigungsdienst

Der Bestätigungsdienst erzeugt ein signiertes Dokument, das Assertionen enthält, die den Binär- und Konfigurationsstatus der ESXi-Remotehosts im vertrauenswürdigen Cluster beschreiben. Der Bestätigungsdienst bescheinigt den Status der ESXi-Hosts unter Verwendung eines TPM 2.0-Chips (Trusted Platform Module) als Basis für Softwaremessungen und Berichterstellung. Das TPM auf dem ESXi-Remotehost misst den Software-Stack und sendet die Konfigurationsdaten an den Bestätigungsdienst. Der Bestätigungsdienst stellt sicher, dass die Signatur der Softwaremessung einem zuvor konfigurierten vertrauenswürdigen TPM-Endorsement Key (EK) zugewiesen werden kann. Der Bestätigungsdienst stellt außerdem sicher, dass die Softwaremessung mit einem von mehreren zuvor angegebenen ESXi-Images übereinstimmt. Der Bestätigungsdienst signiert ein JSON-Web-Token (JWT), das er an den ESXi-Host ausgibt, indem er die Assertionen über die Identität, Gültigkeit und Konfiguration des ESXi-Hosts bereitstellt.

Was ist der vSphere Trust Authority-Schlüsselanbieterdienst?

Aufgrund des Schlüsselanbieterdiensts benötigen die vCenter Server- und ESXi-Hosts keine direkten Anmeldedaten für den Schlüsselserver. Damit in vSphere Trust Authority ein ESXi-Host auf einen Verschlüsselungsschlüssel zugreifen kann, muss sich der Host beim Schlüsselanbieterdienst authentifizieren.

Der Trust Authority-Administrator muss eine vertrauenswürdige Verbindung konfigurieren, damit der Schlüsselanbieterdienst eine Verbindung zu einem Schlüsselanbieter herstellen kann. Für die meisten KMIP-kompatiblen Server umfasst die Einrichtung einer vertrauenswürdigen Verbindung das Konfigurieren von Client- und Serverzertifikaten.

Um sicherzustellen, dass die Schlüssel nur für vertrauenswürdige ESXi-Hosts freigegeben werden, fungiert der Schlüsselanbieterdienst als Gatekeeper für die Schlüsselserver. Der Schlüsselanbieterdienst verbirgt die Schlüsselserverspezifikationen vor dem verbleibenden Software-Stack des Datencenters, indem er das Konzept eines vertrauenswürdigen Schlüsselanbieters verwendet. Jeder vertrauenswürdige Schlüsselanbieter verfügt über einen einzelnen konfigurierten primären Verschlüsselungsschlüssel und verweist auf einen oder mehrere Schlüsselserver. Der Schlüsselanbieterdienst kann mehrere konfigurierte vertrauenswürdige Schlüsselanbieter enthalten. Beispiel: Angenommen, Sie benötigen einen separaten vertrauenswürdigen Schlüsselanbieter für jede Abteilung in einer Organisation. Jeder vertrauenswürdige Schlüsselanbieter verwendet einen anderen primären Schlüssel, kann aber auf denselben unterstützenden Schlüsselserver zurückgreifen.

Nach der Erstellung eines vertrauenswürdigen Schlüsselanbieters kann der Schlüsselanbieterdienst Anforderungen von den vertrauenswürdigen ESXi-Hosts akzeptieren, um kryptografische Vorgänge für diesen vertrauenswürdigen Schlüsselanbieter auszuführen.

Wenn ein vertrauenswürdiger ESXi-Host Vorgänge für einen vertrauenswürdigen Schlüsselanbieter anfordert, stellt der Schlüsselanbieterdienst sicher, dass der ESXi-Host, der den Verschlüsselungsschlüssel anfordert, bestätigt wird. Nach Durchlaufen aller Prüfungen nimmt der vertrauenswürdige ESXi-Host Verschlüsselungsschlüssel vom Schlüsselanbieterdienst entgegen.

Welche Ports werden von vSphere Trust Authority verwendet?

Die vSphere Trust Authority-Dienste überwachen Verbindungen hinter dem Reverse-Proxy des ESXi-Hosts. Die gesamte Kommunikation erfolgt über HTTPS auf Port 443.

Was sind vertrauenswürdige vSphere Trust Authority-Hosts?

Die vertrauenswürdigen ESXi-Hosts sind so konfiguriert, dass sie vertrauenswürdige Schlüsselanbieter zum Durchführen kryptografischer Vorgänge verwenden. Die vertrauenswürdigen ESXi-Hosts führen wichtige Vorgänge durch, indem sie mit dem Schlüsselanbieter- und dem Bestätigungsdienst kommunizieren. Zur Authentifizierung und Autorisierung verwenden die vertrauenswürdigen ESXi-Hosts ein Token, das sie vom Bestätigungsdienst erhalten haben. Um ein gültiges Token zu erhalten, muss der vertrauenswürdige ESXi-Host den Bestätigungsdienst erfolgreich bestätigen. Das Token enthält bestimmte Beanspruchungen, anhand derer ermittelt werden kann, ob der vertrauenswürdige ESXi-Host für den Zugriff auf einen vertrauenswürdigen Schlüsselanbieter autorisiert ist.

vSphere Trust Authority und Schlüsselserver

vSphere Trust Authority erfordert die Verwendung mindestens eines Schlüsselservers. In früheren vSphere-Versionen wurde ein Schlüsselserver als Schlüsselverwaltungsserver oder KMS bezeichnet. Derzeit bietet die vSphere Virtual Machine Encryption-Lösung Unterstützung für KMIP 1.1-kompatible Schlüsselserver.

Wie speichert vSphere Trust Authority Konfigurations- und Statusinformationen?

vCenter Server fungiert hauptsächlich als Passthrough-Dienst für Informationen zu vSphere Trust Authority-Konfiguration und -Status. Die meisten vSphere Trust Authority-Konfigurations- und -Statusinformationen werden auf den ESXi-Hosts in der ConfigStore-Datenbank gespeichert. Bestimmte Statusinformationen werden auch in der vCenter Server-Datenbank gespeichert.

Hinweis Da die meisten vSphere Trust Authority-Konfigurationsinformationen auf den ESXi-Hosts gespeichert werden, sichert der dateibasierte vCenter Server-Sicherungsmechanismus diese Informationen nicht. Um sicherzustellen, dass die Konfigurationsinformationen für Ihre vSphere Trust Authority-Bereitstellung gespeichert werden, finden Sie Informationen unter Sichern der vSphere Trust Authority-Konfiguration.

Vorgehensweise zum Integrieren von vSphere Trust Authority in vCenter Server

Sie konfigurieren separate vCenter Server-Instanzen, um den Trust Authority-Cluster und den vertrauenswürdigen Cluster zu verwalten. Weitere Informationen hierzu finden Sie unter Konfigurieren von vSphere Trust Authority.

In einem vertrauenswürdigen Cluster verwaltet der vCenter Server die API-Aufrufe der Trust Authority und übergibt sie an die ESXi-Hosts. Der vCenter Server repliziert die API-Aufrufe auf allen ESXi-Hosts im vertrauenswürdigen Cluster.

Nachdem Sie vSphere Trust Authority erstmals konfiguriert haben, können Sie ESXi-Hosts zu einem Trust Authority- oder vertrauenswürdigen Cluster hinzufügen oder daraus entfernen. Weitere Informationen hierzu finden Sie unter Hinzufügen und Entfernen von vSphere Trust Authority-Hosts.

vSphere Trust Authority – Prozessabläufe

Sie müssen sich mit den Prozessabläufen in vSphere Trust Authority vertraut machen, um Ihre vertrauenswürdige Infrastruktur konfigurieren und verwalten zu können.

Vorgehensweise zum Konfigurieren von vSphere Trust Authority

vSphere Trust Authority ist standardmäßig nicht aktiviert. Sie müssen vSphere Trust Authority in Ihrer Umgebung manuell konfigurieren. Weitere Informationen hierzu finden Sie unter Konfigurieren von vSphere Trust Authority.

Wenn Sie vSphere Trust Authority konfigurieren, müssen Sie angeben, welche Versionen der ESXi-Software vom Bestätigungsdienst akzeptiert werden und welche TPMs (Trusted Platform Modules) vertrauenswürdig sind.

TPM und Bestätigung

In diesem Handbuch werden die folgenden Definitionen zur Erläuterung von TPMs und Bestätigung verwendet.

Tabelle 9-2. TPM und Bestätigung – Glossar

Begriff	Definition
Endorsement Key (EK)	Ein TPM wird mit einem öffentlichen/privaten RSA-Schlüsselpaar hergestellt, das in die Hardware eingebaut ist und als Endorsement Key (EK) bezeichnet wird. Der EK ist für ein bestimmtes TPM eindeutig.
EK – Öffentlicher Schlüssel	Der öffentliche Teil des EK-Schlüsselpaars.
EK – Privater Schlüssel	Der private Teil des EK-Schlüsselpaars.
EK-Zertifikat	Der öffentliche EK-Schlüssel, der von einer Signatur umschlossen wird. Das EK-Zertifikat wird vom TPM-Hersteller erstellt, der den privaten Schlüssel seiner Zertifizierungsstelle verwendet, um den öffentlichen EK-Schlüssel zu signieren. Nicht alle TPMs enthalten ein EK-Zertifikat. In diesem Fall ist der öffentliche EK-Schlüssel nicht signiert.
TPM-Bestätigung	Die Fähigkeit des Bestätigungsdiensts, die auf einem Remotehost ausgeführte Software zu überprüfen. Die TPM-Bestätigung erfolgt über kryptografische Messungen, die vom TPM während des Starts des Remotehosts durchgeführt werden, und wird auf Anforderung an den Bestätigungsdienst weitergeleitet. Der Bestätigungsdienst stellt über den öffentlichen EK-Schlüssel oder das EK-Zertifikat eine Vertrauensstellung für das TPM her.

Konfigurieren der TPM-Vertrauensstellung auf den vertrauenswürdigen Hosts

Ein vertrauenswürdiger ESXi-Host muss ein TPM enthalten. Ein TPM wird mit einem öffentlichen/privaten Schlüsselpaar hergestellt, das in die Hardware eingebaut ist und als Endorsement Key (EK) bezeichnet wird. Obwohl TPM 2.0 viele Schlüssel/Zertifikat-Paare zulässt, wird am häufigsten ein RSA-2048-Schlüsselpaar verwendet. Wenn der öffentliche Schlüssel eines TPM von einer Zertifizierungsstelle signiert wird, entsteht ein EK-Zertifikat. Der TPM-Hersteller stellt in der Regel mindestens einen EK bereit, signiert den öffentlichen Schlüssel mit einer Zertifizierungsstelle und bettet das signierte Zertifikat in den nicht flüchtigen Arbeitsspeicher des TPM ein.

Sie können den Bestätigungsdienst so konfigurieren, dass TPMs wie folgt als vertrauenswürdig eingestuft werden:

- Stufen Sie alle CA-Zertifikate als vertrauenswürdig ein, mit denen der Hersteller das TPM signiert hat (öffentlicher EK-Schlüssel). Die Standardeinstellung für den Bestätigungsdienst besteht darin, CA-Zertifikate als vertrauenswürdig einzustufen. Bei dieser Vorgehensweise werden zahlreiche ESXi-Hosts vom selben CA-Zertifikat abgedeckt, wodurch der Verwaltungsaufwand reduziert wird.
- Stufen Sie das TPM-CA-Zertifikat und den öffentlichen EK-Schlüssel des ESXi-Hosts als vertrauenswürdig ein. Letzterer kann entweder das EK-Zertifikat oder der öffentliche EK-Schlüssel sein. Obwohl diese Vorgehensweise mehr Sicherheit bietet, ist es notwendig, Informationen zu jedem vertrauenswürdigen Host zu konfigurieren.
- Bestimmte TPMs enthalten kein EK-Zertifikat. In diesem Fall stufen Sie den öffentlichen EK-Schlüssel als vertrauenswürdig ein.

Die Entscheidung, allen TPM-CA-Zertifikaten zu vertrauen, erweist sich aus betrieblicher Sicht als praktisch. Sie können neue Zertifikate nur konfigurieren, wenn Sie eine neue Hardwareklasse zum Datencenter hinzufügen. Indem Sie einzelne EK-Zertifikate als vertrauenswürdig einstufen, können Sie den Zugriff auf bestimmte ESXi-Hosts einschränken.

Sie können sich auch gegen die Einstufung von TPM-CA-Zertifikaten als vertrauenswürdig entscheiden. Obwohl eine solche Konfiguration eher ungewöhnlich ist, können Sie sie verwenden, wenn ein EK nicht von einer Zertifizierungsstelle signiert ist. Derzeit ist diese Funktion nicht vollständig implementiert.

Hinweis Bestimmte TPMs enthalten keine EK-Zertifikate. Wenn Sie einzelne ESXi-Hosts als vertrauenswürdig einstufen möchten, muss das TPM ein EK-Zertifikat enthalten.

Bestätigen von TPMs

Zum Starten des Bestätigungsvorgangs sendet der vertrauenswürdige ESXi-Host im vertrauenswürdigen Cluster den vorkonfigurierten öffentlichen EK-Schlüssel und das EK-Zertifikat an den Bestätigungsdienst im Trust Authority-Cluster. Wenn der Bestätigungsdienst die Anfrage erhält, sucht er nach dem EK in seiner Konfiguration, wobei es sich je nach Konfiguration um den öffentlichen EK-Schlüssel und/oder das EK-Zertifikat handeln kann. Wenn keiner dieser Fälle zutrifft, lehnt der Bestätigungsdienst die Bestätigungsanfrage ab.

Da der EK nicht direkt für die Signierung verwendet wird, wird ein Bestätigungsschlüssel (AK oder AIK) ausgehandelt. Das Aushandlungsprotokoll stellt sicher, dass ein neu erstellter AK an den zuvor überprüften EK gebunden ist, um Man-in-the-Middle-Angriffe oder Angriffe mit gefälschten Identitäten zu verhindern. Nachdem ein AK ausgehandelt wurde, wird dieser in zukünftigen Bestätigungsanfragen wiederverwendet, statt jedes Mal neu generiert zu werden.

Der vertrauenswürdige ESXi-Host liest die Angebots- und PCR-Werte aus dem TPM. Das Angebot wird vom AK signiert. Der vertrauenswürdige ESXi-Host liest auch das TCG-Ereignisprotokoll, das alle Ereignisse enthält, die zum aktuellen PCR-Zustand geführt haben. Diese TPM-Informationen werden zur Überprüfung an den Bestätigungsdienst gesendet. Der Bestätigungsdienst überprüft die PCR-Werte mithilfe des Ereignisprotokolls.

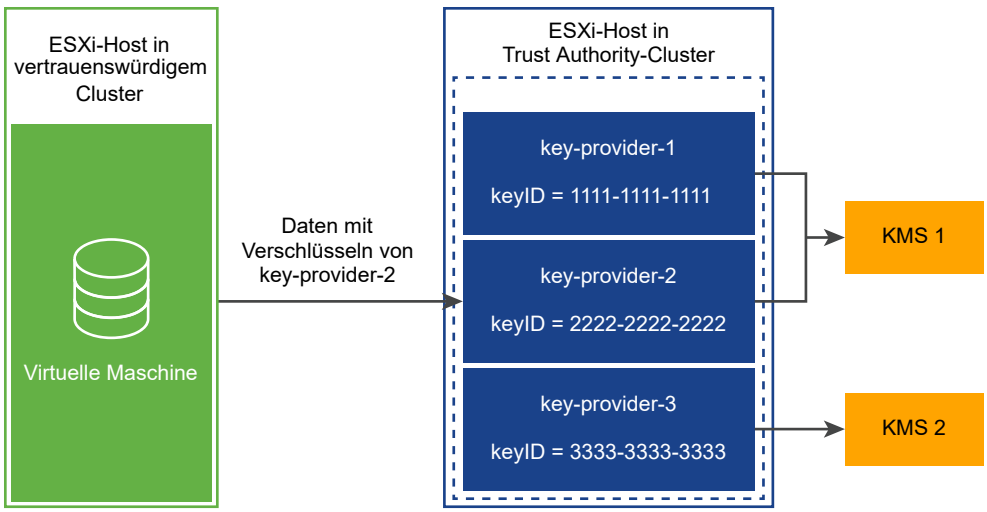
Funktionsweise von Schlüsselanbietern mit Schlüsselservern

Der Schlüsselanbieterdienst verwendet das Konzept eines vertrauenswürdigen Schlüsselanbieters, um die Besonderheiten des Schlüsselservers vor der restlichen Datencenter-Software zu verbergen. Jeder vertrauenswürdige Schlüsselanbieter verfügt über einen einzelnen konfigurierten primären Verschlüsselungsschlüssel und verweist auf einen oder mehrere Schlüsselserver. Der primäre Verschlüsselungsschlüssel befindet sich auf den Schlüsselservern. Im Rahmen der vSphere Trust Authority-Konfiguration müssen Sie den primären Schlüssel als separate Aktivität bereitstellen und aktivieren. Der Schlüsselanbieterdienst kann mehrere konfigurierte vertrauenswürdige Schlüsselanbieter enthalten. Jeder vertrauenswürdige Schlüsselanbieter verwendet einen anderen primären Schlüssel, kann aber auf denselben unterstützenden Schlüsselserver zurückgreifen.

Wenn ein neuer vertrauenswürdiger Schlüsselanbieter hinzugefügt wird, muss der Trust Authority-Administrator den Schlüsselserver und einen vorhandenen Schlüsselbezeichner auf diesem Schlüsselserver angeben.

Die folgende Abbildung zeigt die Beziehung zwischen dem Schlüsselanbieterdienst und den Schlüsselservern.

Abbildung 9-3. Schlüsselanbieter und Schlüsselserver



Nachdem Sie einen vertrauenswürdigen Schlüsselanbieter für einen vertrauenswürdigen Cluster konfiguriert haben, kann der Schlüsselanbieterdienst Anfragen zum Ausführen von Kryptografievorgängen für diesen vertrauenswürdigen Schlüsselanbieter akzeptieren. In dieser Abbildung werden beispielsweise drei vertrauenswürdige Schlüsselanbieter konfiguriert, zwei für KMS-1 und einer für KMS-2. Der vertrauenswürdige Host fordert einen Verschlüsselungsvorgang für key-provider-2 an. Der vertrauenswürdige Host fordert einen Verschlüsselungsschlüssel an, der generiert und zurückgegeben werden soll, und verwendet diesen Verschlüsselungsschlüssel zur Durchführung von Verschlüsselungsvorgängen.

Der Schlüsselanbieterdienst verwendet den über key-provider-2 referenzierten primären Schlüssel, um die angegebenen Klartextdaten zu verschlüsseln und den entsprechenden verschlüsselten Text zurückzugeben. Später kann der vertrauenswürdige Host denselben verschlüsselten Text für einen Entschlüsselungsvorgang bereitstellen und den ursprünglichen Klartext abrufen.

vSphere Trust Authority-Authentifizierung und -Autorisierung

vSphere Trust Authority-Verwaltungsvorgänge benötigen einen Benutzer, der Mitglied der TrustedAdmins-Gruppe ist. Nur Trust Authority-Administratorrechte reichen nicht aus, um alle Verwaltungsvorgänge durchzuführen, die die ESXi-Hosts beinhalten. Weitere Informationen finden Sie unter Voraussetzungen und notwendige Berechtigungen für vSphere Trust Authority.

Hinzufügen eines vertrauenswürdigen Hosts zu einem vertrauenswürdigen Cluster

Die Schritte zum erstmaligen Hinzufügen von ESXi-Hosts zum vertrauenswürdigen Cluster werden in Konfigurieren von vSphere Trust Authority beschrieben.

Wenn Sie ESXi-Hosts zu einem späteren Zeitpunkt zum vertrauenswürdigen Cluster hinzufügen möchten, muss ein anderer Workflow verwendet werden. Weitere Informationen hierzu finden Sie unter Hinzufügen und Entfernen von vSphere Trust Authority-Hosts.

Wenn Sie ESXi-Hosts erstmals zum vertrauenswürdigen Cluster hinzufügen, müssen Sie folgende Informationen zusammenstellen:

- TPM-Zertifikat für jeden Hardwaretyp im Cluster
- ESXi-Image für jede Version von ESXi im Cluster
- Informationen zum vCenter Server-Prinzipal

Wenn Sie ESXi-Hosts zu einem späteren Zeitpunkt zu einem vertrauenswürdigen Cluster hinzufügen, müssen Sie möglicherweise einige zusätzliche Informationen erfassen. Das heißt, wenn sich die neuen ESXi-Hosts in der Hardware- oder ESXi-Version von den ursprünglichen Hosts unterscheiden, müssen Sie die Informationen des neuen ESXi-Hosts zusammenstellen und in den Trust Authority-Cluster importieren. Sie müssen die Informationen zum vCenter Server-Prinzipal nur einmal pro vCenter Server-System erfassen.

vSphere Trust Authority – Topologie

vSphere Trust Authority benötigt separate vCenter Server-Systeme für den Trust Authority-Cluster und den vertrauenswürdigen Cluster.

Der Trust Authority-Cluster wird auf einem unabhängigen, isolierten vCenter Server konfiguriert und verwaltet. Der vCenter Server des Trust Authority-Clusters kann nicht gleichzeitig der vCenter Server des vertrauenswürdigen Clusters sein. Der vertrauenswürdige Cluster muss über einen eigenen, separaten vCenter Server verfügen. Ein einzelner vCenter Server kann mehrere vertrauenswürdige Cluster verwalten. Mehrere vCenter Server-Systeme für vertrauenswürdige Cluster können am erweiterten verknüpften Modus teilnehmen. Der vCenter Server für den Trust Authority-Cluster kann nicht mit anderen vCenter Server-Systemen des Trust Authority-Clusters oder mit vCenter Server-Systemen des vertrauenswürdigen Clusters am erweiterten verknüpften Modus teilnehmen.

Der Trust Authority-Administrator verwaltet den Trust Authority-Cluster und den zugehörigen vCenter Server unabhängig von anderen vCenter Server-Instanzen, da diese Vorgehensweise optimale Sicherheitsisolierung bietet.

Der Trust Authority-Administrator dokumentiert oder veröffentlicht die Hostnamen und SSL-Zertifikate, die von Administratoren vertrauenswürdiger Cluster zum Konfigurieren ihrer Cluster verwendet werden. Der Trust Authority-Administrator stellt auch vertrauenswürdige Schlüsselanbieter für das Unternehmen und seine Abteilungen oder sogar für einzelne Administratoren bereit.

Sie können vSphere Trust Authority-Dienste nicht direkt auf dem vertrauenswürdigen Cluster bereitstellen, der vom Arbeitslast-vCenter Server verwaltet wird, da der Arbeitslastadministrator über weitreichende Zugriffsrechte auf die ESXi-Hosts verfügt. Bei diesem Bereitstellungstyp wird die erforderliche Rollentrennung nicht erreicht, die zum Erfüllen der Sicherheitsziele von vSphere Trust Authority notwendig ist.

Voraussetzungen und notwendige Berechtigungen für vSphere Trust Authority

Bei der Konfiguration von vSphere Trust Authority müssen Sie die Hardware- und Softwareanforderungen berücksichtigen. Zur Verwendung von Verschlüsselung müssen Sie Kryptografieberechtigungen und -rollen festlegen. Der Benutzer, der vSphere Trust Authority-Aufgaben durchführt, muss über die entsprechenden Berechtigungen verfügen.

Anforderungen für vSphere Trust Authority

Zur Verwendung von vSphere Trust Authority muss die vSphere-Umgebung folgende Voraussetzungen erfüllen:

- Hardwareanforderungen für vertrauenswürdigen ESXi-Host:
  - TPM 2.0
  - Sicherer Start muss aktiviert sein

  - EFI-Firmware
- Anforderungen an Komponenten:
  - vCenter Server 7.0 oder höher
  - Ein dediziertes vCenter Server-System für den vSphere Trust Authority-Cluster und ESXi-Hosts
  - Ein separates vCenter Server-System für den vertrauenswürdigen Cluster und vertrauenswürdige ESXi-Hosts
  - Ein Schlüsselserver (in früheren vSphere-Versionen als Schlüsselverwaltungsserver oder KMS bezeichnet)
- Anforderungen an virtuelle Maschinen:
  - EFI-Firmware
  - Sicherer Start ist aktiviert

Hinweis Stellen Sie vor der Konfiguration von vSphere Trust Authority sicher, dass Sie Ihre vCenter Server-Systeme für den Trust Authority- und den vertrauenswürdigen Cluster eingerichtet und jedem Cluster ESXi-Hosts hinzugefügt haben.

Kryptografieberechtigungen

vSphere Trust Authority führt keine neuen Kryptografieberechtigungen ein. Die in Kryptografie-Berechtigungen und -rollen beschriebenen Kryptografieberechtigungen gelten ebenfalls für vSphere Trust Authority.

Hostverschlüsselungsmodus

vSphere Trust Authority führt keine neuen Anforderungen für die Aktivierung des Hostverschlüsselungsmodus auf den vertrauenswürdigen ESXi-Hosts ein. Weitere Informationen zum Hostverschlüsselungsmodus finden Sie unter Voraussetzungen und erforderliche Berechtigungen für die Verschlüsselung.

Informationen zu den vSphere Trust Authority-Rollen und zur TrustedAdmins-Gruppe

vSphere Trust Authority-Vorgänge benötigen einen Benutzer, der Mitglied der TrustedAdmins-Gruppe ist. Dieser Benutzer wird als Trust Authority-Administrator bezeichnet. vSphere-Administratoren müssen sich entweder selbst oder andere Benutzer zur TrustedAdmins-Gruppe hinzufügen, um die Rolle „Administrator der vertrauenswürdigen Infrastruktur“ zu erhalten. Die Rolle „Administrator der vertrauenswürdigen Infrastruktur“ ist für vCenter Server-Autorisierung erforderlich. Die TrustedAdmins-Gruppe wird für die Authentifizierung auf den ESXi-Hosts benötigt, die Teil der vertrauenswürdigen Infrastruktur sind. Benutzer mit der Berechtigung **Kryptografische Vorgänge.Host registrieren** für ESXi-Hosts können den vertrauenswürdigen

Cluster verwalten. Die vCenter Server-Berechtigungen werden nicht an die Trust Authority-Hosts, sondern nur an die vertrauenswürdigen Hosts weitergegeben. Nur Mitgliedern der TrustedAdmins-Gruppe werden Berechtigungen auf den Trust Authority-Hosts erteilt. Die Gruppenmitgliedschaft wird auf dem ESXi-Host selbst überprüft.

Hinweis vSphere-Administratoren und Mitgliedern der Administratorgruppe wird die Rolle „Administrator der vertrauenswürdigen Infrastruktur“ zugewiesen. Diese Rolle allein erlaubt einem Benutzer jedoch nicht, vSphere Trust Authority-Vorgänge durchzuführen. Mitgliedschaft in der TrustedAdmins-Gruppe ist ebenfalls erforderlich.

Nachdem vSphere Trust Authority aktiviert wurde, können Trust Authority-Administratoren vertrauenswürdige Schlüsselanbieter zu vertrauenswürdigen Hosts zuweisen. Diese vertrauenswürdigen Hosts können dann die vertrauenswürdigen Schlüsselanbieter verwenden, um kryptografische Aufgaben durchzuführen.

Neben der Rolle „Administrator der vertrauenswürdigen Infrastruktur“ stellt vSphere Trust Authority die Rolle „Kein Administrator der vertrauenswürdigen Infrastruktur“ bereit, die alle Berechtigungen in vCenter Server enthält, mit Ausnahme derjenigen, die die vSphere Trust Authority-APIs aufrufen.

vSphere Trust Authority-Gruppen, -Rollen und -Benutzer funktionieren folgendermaßen:

- Beim ersten Start erteilt vSphere der TrustedAdmins-Gruppe die Rolle „Administrator der vertrauenswürdigen Infrastruktur“, die über globale Berechtigungen verfügt.
- Bei der Rolle „Administrator der vertrauenswürdigen Infrastruktur“ handelt es sich um eine Systemrolle, die über die erforderlichen Berechtigungen zum Aufrufen der vSphere Trust Authority-APIs (`TrustedAdmin.*`) sowie über die Systemrechte **System.Read**, **System.View** und **System.Anonymous** zum Anzeigen von Bestandslistenobjekten verfügt.
- Die Rolle „Kein Administrator der vertrauenswürdigen Infrastruktur“ ist eine Systemrolle, die alle Berechtigungen in vCenter Server enthält, mit Ausnahme derjenigen, die die vSphere Trust Authority-APIs aufrufen. Wenn Sie neue Berechtigungen zu vCenter Server hinzufügen, werden diese ebenfalls zur Rolle „Kein Administrator der vertrauenswürdigen Infrastruktur“ hinzugefügt. (Die Rolle „Kein Administrator der vertrauenswürdigen Infrastruktur“ ist mit der Rolle „Kein Kryptografie-Administrator“ vergleichbar.)
- Die vSphere Trust Authority-Berechtigungen (`TrustedAdmin.*`-APIs) sind nicht in der Rolle „Kein Kryptografie-Administrator“ enthalten, sodass Benutzer mit dieser Rolle keine vertrauenswürdige Infrastruktur einrichten oder Kryptografievorgänge durchführen können.

Die Anwendungsfälle für diese Benutzer, Gruppen und Rollen werden in der folgenden Tabelle angezeigt.

Tabelle 9-3. vSphere Trust Authority-Benutzer, -Gruppen und -Rollen

Benutzer, Gruppe oder Rolle	Kann vSphere Trust Authority vCenter Server-API aufrufen (enthält Aufrufe an vSphere Trust Authority ESXi-API)	Kann vSphere Trust Authority vCenter Server-API aufrufen (enthält keine Aufrufe an vSphere Trust Authority ESXi-API)	Kann Hostvorgänge im Cluster durchführen, die nicht mit vSphere Trust Authority zusammenhängen	Kommentar
Benutzer in der Gruppe „Administrators@*system.domain*“ und in der Gruppe „TrustedAdmins@*system.domain*“	Ja	Ja	Ja	–
Nur Benutzer in der Gruppe „TrustedAdmins@*system.domain*“	Ja	Ja	Nein	Ein solcher Benutzer kann keine regelmäßigen Clusterverwaltungsvorgänge durchführen.
Nur Benutzer in der Gruppe „Administrators@*system.domain*“	Ja	Nein	Ja	–
Benutzer mit der Rolle „Administrator der vertrauenswürdigen Infrastruktur“, die aber kein Mitglied der Gruppe „TrustedAdmins@*system.domain*“ sind	Ja	Nein	Nein	Der ESXi-Host überprüft die Gruppenmitgliedschaft des Benutzers, um Berechtigungen zu erteilen.
Nur Benutzer mit der Rolle „Kein Administrator der vertrauenswürdigen Infrastruktur“	Nein	Nein	Ja	Ein solcher Benutzer ähnelt einem Administrator, der keine vSphere Trust Authority-Vorgänge durchführen kann.

vSphere Trust Authority – Best Practices, Einschränkungen und Interoperabilität

Aus der vSphere Trust Authority-Architektur ergeben sich einige zusätzliche Empfehlungen. Berücksichtigen Sie bei der Planung Ihrer vSphere Trust Authority-Strategie Einschränkungen bezüglich der Interoperabilität.

Vertrauenswürdige Infrastruktur – Interoperabilität

Für ESXi-Versionen ist der Bestätigungsdienst rückwärts und vorwärts kompatibel. Beispiel: Sie können über einen Cluster aus ESXi-Host verfügen, die unter ESXi 7.0 im vSphere Trust Authority -Cluster ausgeführt werden, und ESXi-Hosts im vertrauenswürdigen Cluster auf eine neuere ESXi-Version upgraden oder patchen. Ebenso können Sie die ESXi-Hosts im Trust Authority-Cluster aktualisieren oder patchen, während für die ESXi-Hosts im vertrauenswürdigen Cluster die aktuelle Version beibehalten wird.

Ein Cluster kann nicht gleichzeitig als Trust Authority- und vertrauenswürdiger Cluster fungieren. Diese Konfiguration wird nicht unterstützt.

Konfigurationseinschränkungen bei vertrauenswürdigen Clustern

Sie können nur einen vertrauenswürdigen Cluster pro Arbeitslast-vCenter Server konfigurieren. Ein vertrauenswürdiger Cluster kann nicht so konfiguriert werden, dass er auf mehrere Trust Authority-Cluster verweist.

Unterstützte Funktionen

vSphere Trust Authority unterstützt Folgendes:

- vCenter High Availability (vCenter HA)
- VMware vSphere High Availability
- DRS
- DPM
- SRM unter folgenden Voraussetzungen:
  - SRM mit Array-basierter Replizierung wird unterstützt, wenn auf der Wiederherstellungsseite dieselbe vSphere Trust Authority-Dienstkonfiguration verfügbar ist.
  - SPPG
- VADP
  - Die Unterstützung entspricht derjenigen bei der Standardverschlüsselung. Die Modi „Hot-Add“ und „NFC“ werden unterstützt, der SAN-Modus jedoch nicht. Sicherungen werden entschlüsselt. VADP-Partner können die gesicherte virtuelle Maschine mit demselben Verschlüsselungsschlüssel wiederherstellen, den sie auch für die ursprüngliche virtuelle Maschine verwenden.
- vSAN
  - VM-Verschlüsselung wird zusätzlich zu vSAN vollständig unterstützt.
- OVF
  - Verschlüsselte virtuelle Maschinen können nicht in OVF exportiert werden. Virtuelle Maschinen können jedoch verschlüsselt werden, während Sie aus einer OVF-Datei importiert werden.

- vVol

Nicht unterstützte Funktionen

Aktuell bietet vSphere Trust Authority keine Unterstützung für Folgendes:

- vSAN-Verschlüsselung
- FCD-Verschlüsselung (First Class Disk)
- vSphere Replication
- vSphere-Hostprofile

vSphere Trust Authority – Lebenszyklus

Die vSphere Trust Authority-Dienste werden als Teil des ESXi-Basis-Image in Paketen zusammengefasst und installiert.

Starten und Beenden von Diensten

Im vSphere Client können Sie die vSphere Trust Authority-Dienste starten, beenden und neu starten, die auf einem ESXi-Host ausgeführt werden. Sie können Dienste im Fall einer Konfigurationsänderung oder bei vermuteten Funktions- oder Leistungsproblemen neu starten. Zum Neustarten des Diensts auf einem vertrauenswürdigen ESXi-Host, müssen Sie sich beim Host anmelden, um den Dienst neu zu starten. Weitere Informationen hierzu finden Sie unter Starten, Stoppen und Neustarten von vSphere Trust Authority-Diensten.

Upgraden und Patchen

Jedes Mal, wenn Sie einen vertrauenswürdigen ESXi-Host upgraden oder patchen, müssen Sie den vSphere Trust Authority-Cluster mit den Informationen der neuen ESXi-Version aktualisieren. Eine Möglichkeit besteht darin, ein Upgrade oder ein Patch für einen ESXi-Testhost durchzuführen, die ESXi-Basisimage-Informationen zu exportieren, die Image-Datei in den Trust Authority-Cluster zu importieren und anschließend die vertrauenswürdigen ESXi-Hosts zu aktualisieren oder zu patchen.

Best Practices für Upgrades

Best Practice für das Upgrade einer vSphere Trust Authority-Infrastruktur bestehen darin, das Upgrade von Trust Authority vCenter Server und der Trust Authority-Hosts zuerst durchzuführen. Auf diese Weise profitieren Sie von den neuesten vSphere Trust Authority-Funktionen. Sie können jedoch getrennte, eigenständige Upgrades von vCenter Server und ESXi-Hosts ausführen, um bestimmte geschäftliche Voraussetzungen zu erfüllen.

Befolgen Sie im Allgemeinen diese Reihenfolge für das Upgrade Ihrer vSphere Trust Authority-Infrastruktur:

1 Führen Sie ein Upgradedes vCenter Servers des Trust Authority Clusters durch.

2 Führen Sie ein Upgrade der Trust Authority-Hosts durch.

3 Führen Sie ein Upgrade des vCenter Servers des vertrauenswürdigen Clusters durch.

4 Führen Sie ein Upgrade der vertrauenswürdigen Hosts durch.

Um einen reibungslosen Ablauf zu gewährleisten, führen Sie das Upgrade der Trust Authority-Hosts und der vertrauenswürdigen Hosts schrittweise durch.

Fehlerbehebung bei Upgrade-Problemen

Führen Sie die folgenden Schritte aus, wenn das Upgrade eines Trust Authority-Hosts nicht erfolgreich war.

1 Entfernen Sie den Trust Authority-Host aus dem vertrauenswürdigen Cluster.

2 Stellen Sie die vorherige Version von ESXi wieder her.

3 Fügen Sie den Trust Authority-Host erneut zum Cluster hinzu, wie im VMware Knowledgebase-Artikel unter https://kb.vmware.com/s/article/77234 beschrieben.

4 Stellen Sie sicher, dass die Konfiguration des Trust Authority-Hosts mit den anderen Trust Authority-Hosts im Trust Authority-Cluster übereinstimmt. Weitere Informationen hierzu finden Sie unter Überprüfen der Integrität des vertrauenswürdigen Clusters.

Wenn Sie ein Upgrade auf eine neue Version von ESXi auf einem vertrauenswürdigen Host durchführen, schlägt der Nachweis fehl, bis Sie den Trust Authority-Cluster mit den neuen ESXi-Basisimage-Informationen aktualisieren. Dieses Verhaltensmuster wird erwartet. Sie können virtuelle Maschinen nicht mehr verschlüsseln und keine vorhandenen virtuellen Maschinen verwenden, die vor dem Upgrade verschlüsselt wurden, bis Sie das Problem beheben. Nachweisfehlermeldungen werden im vSphere Client im Bereich **Kürzlich bearbeitete Aufgaben** und in den Dateien `attestd.log`, `kmxa.log` und `kmxa.log` angezeigt.

Um das Problem zu beheben, gehen Sie folgendermaßen vor.

1 Führen Sie das `Export-VMHostImageDb`-Cmdlet aus, um die ESXi-Basisimages erneut zu exportieren. Weitere Informationen finden Sie in Schritt 5 in Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.

2 Führen Sie das `New-TrustAuthorityVMHostBaseImage`-Cmdlet aus, um das neue Basisimage erneut in den vCenter Server des Trust Authority-Clusters zu importieren. Weitere Informationen finden Sie in Schritt 8 in Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.

3 Wenn Sie die älteren Versionen von ESXi nicht mehr bestätigen müssen (alle vertrauenswürdigen Hosts wurden aktualisiert), führen Sie das `Remove-TrustAuthorityVMHostBaseImage`-Cmdlet aus, um die Versionen zu entfernen. Beispiel:

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
$baseImages = Get-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA
Remove-TrustAuthorityVMHostBaseImage -VMHostBaseImage $baseImages
```

Sichern der vSphere Trust Authority-Konfiguration

Da die meisten vSphere Trust Authority-Konfigurationsinformationen auf den ESXi-Hosts gespeichert werden, erfolgt keine vCenter Server-Sicherung dieser vSphere Trust Authority-Informationen. Weitere Informationen hierzu finden Sie unter Sichern der vSphere Trust Authority-Konfiguration.

Konfigurieren von vSphere Trust Authority

vSphere Trust Authority ist standardmäßig nicht aktiviert. Sie müssen Ihre Umgebung für vSphere Trust Authority konfigurieren, bevor Sie diese nutzen können.

Sie aktivieren die vSphere Trust Authority-Dienste auf einem dedizierten vCenter Server-Cluster, der als vSphere Trust Authority-Cluster bezeichnet wird. Der Trust Authority-Cluster fungiert als eine zentralisierte, sichere Managementplattform. Anschließend aktivieren Sie einen vCenter Server-Cluster als vertrauenswürdigen Cluster. Der vertrauenswürdige Cluster enthält die vertrauenswürdigen ESXi-Hosts.

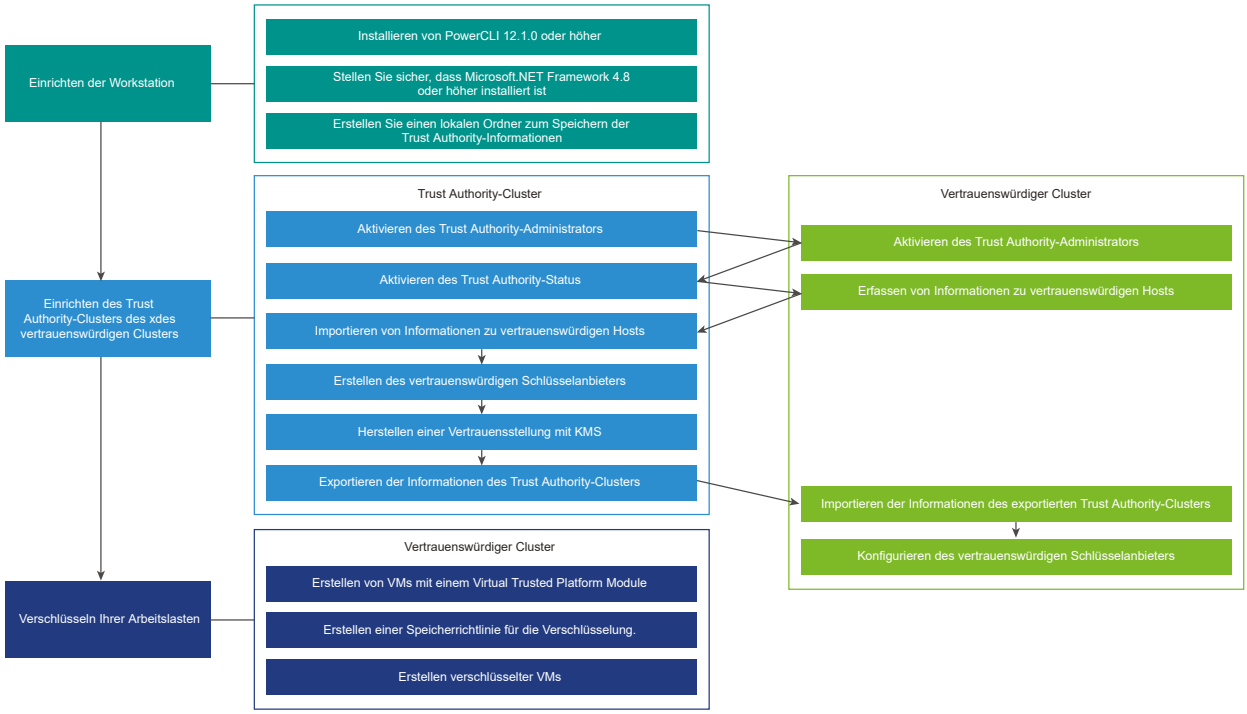
Der Trust Authority-Cluster testet die ESXi-Hosts im vertrauenswürdigen Cluster remote. Der Trust Authority-Cluster gibt Verschlüsselungsschlüssel nur an nachgewiesene ESXi-Hosts im vertrauenswürdigen Cluster frei, um virtuelle Maschinen und virtuelle Festplatten mithilfe vertrauenswürdiger Schlüsselanbieter zu verschlüsseln.

Bevor Sie mit der Konfiguration von vSphere Trust Authority beginnen, finden Sie Informationen zur erforderlichen Einrichtung von vCenter Server-Systemen und ESXi-Hosts unter Voraussetzungen und notwendige Berechtigungen für vSphere Trust Authority.

Sie können verschiedene Aspekte von vSphere Trust Authority auf folgende Arten verwalten.

- Konfigurieren Sie die vSphere Trust Authority-Dienste und vertrauenswürdige Verbindungen mithilfe von PowerCLI-Cmdlets oder vSphere-APIs. Weitere Informationen finden Sie in der *Referenz für VMware PowerCLI-Cmdlets* und im *Programmierhandbuch zu den vSphere Automation SDKs*.
- Verwalten Sie die Konfiguration vertrauenswürdiger Schlüsselanbieter mithilfe der PowerCLI-Cmdlets oder über den vSphere Client.
- Führen Sie Verschlüsselungs-Workflows wie in früheren vSphere-Versionen mit vSphere Client und APIs durch.

Abbildung 9-4. vSphere Trust Authority-Workflow



Zum Konfigurieren und Verwalten von vSphere Trust Authority verwenden Sie VMware PowerCLI, obwohl bestimmte Funktionen im vSphere Client verfügbar sind.

Wenn Sie vSphere Trust Authority konfigurieren, müssen Sie die Einrichtungsaufgaben sowohl für den Trust Authority-Cluster als auch für den vertrauenswürdigen Cluster abschließen. Bei einigen dieser Aufgaben muss eine bestimmte Reihenfolge eingehalten werden. Verwenden Sie die in diesem Handbuch beschriebene Aufgabensequenz.

Hinweis Beim Hinzufügen weiterer ESXi-Hosts zum vertrauenswürdigen Cluster, nachdem Sie die anfängliche vSphere Trust Authority-Einrichtung abgeschlossen haben, müssen Sie möglicherweise die Informationen zum vertrauenswürdigen Host erneut exportieren und importieren. Das heißt, wenn sich die neuen ESXi-Hosts von den ursprünglichen Hosts unterscheiden, müssen Sie die Informationen des neuen ESXi-Hosts zusammenstellen und in den Trust Authority-Cluster importieren. Weitere Informationen hierzu finden Sie unter Hinzufügen und Entfernen von vSphere Trust Authority-Hosts.

Verfahren

1 Einrichten von Workstations

   Um eine vSphere Trust Authority-Bereitstellung zu konfigurieren, müssen Sie zur Vorbereitung zunächst die erforderliche Software auf einer Workstation installieren und diese einrichten.

2 Aktivieren des Trust Authority-Administrators

Zum Aktivieren von vSphere Trust Authority müssen Sie einen Benutzer zur TrustedAdmins-Gruppe in vSphere hinzufügen. Dieser Benutzer übernimmt die Funktion des Trust Authority-Administrators. Sie verwenden den Trust Authority-Administrator für die meisten vSphere Trust Authority-Konfigurationsaufgaben.

3 Aktivieren des Trust Authority-Status

Durch Umwandeln eines vCenter Server-Clusters in einen vSphere Trust Authority-Cluster (auch bezeichnet als Aktivieren des Trust Authority-Status) werden die notwendigen Trust Authority-Dienste auf den ESXi-Hosts im Cluster gestartet.

4 Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server

Zum Aufbau einer Vertrauensstellung benötigt der vSphere Trust Authority-Cluster Informationen über die ESXi-Hosts und den vCenter Server des vertrauenswürdigen Clusters. Sie exportieren diese Informationen als Dateien, die in den Trust Authority-Cluster importiert werden. Sie müssen sicherstellen, dass diese Dateien vertraulich behandelt und sicher übertragen werden.

5 Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster

Sie importieren den exportierten ESXi-Host und die vCenter Server-Informationen in den vSphere Trust Authority-Cluster, um den Trust Authority-Cluster über die zu bestätigenden Hosts zu informieren.

6 Erstellen des Schlüsselanbieters im Trust Authority-Cluster

Damit der Schlüsselanbieterdienst eine Verbindung mit einem Schlüsselanbieter herstellen kann, müssen Sie einen vertrauenswürdigen Schlüsselanbieter erstellen und dann eine vertrauenswürdige Verbindung zwischen dem vSphere Trust Authority-Cluster und dem Schlüsselserver (KMS) konfigurieren. Für die meisten KMIP-kompatiblen Schlüsselserver beinhaltet diese Konfiguration die Einrichtung von Client- und Serverzertifikaten.

7 Exportieren der Informationen des Trust Authority-Clusters

Damit der vertrauenswürdige Cluster eine Verbindung mit dem vSphere Trust Authority-Cluster herstellen kann, müssen Sie die Dienstinformationen des Trust Authority-Clusters in Form einer Datei exportieren und diese Datei dann in den vertrauenswürdigen Cluster importieren. Sie müssen sicherstellen, dass diese Datei vertraulich behandelt und sicher übertragen wird.

8 Importieren der Informationen des Trust Authority-Clusters in die vertrauenswürdigen Hosts

Nachdem Sie die Informationen des vSphere Trust Authority-Clusters in den vertrauenswürdigen Cluster importiert haben, starten die vertrauenswürdigen Hosts den Bestätigungsvorgang mit dem Trust Authority-Cluster.

9 Konfigurieren des vertrauenswürdigen Schlüsselanbieters für vertrauenswürdige Hosts mithilfe des vSphere Client

Sie können den vertrauenswürdigen Schlüsselanbieter mithilfe des vSphere Client konfigurieren.

10 Konfigurieren des vertrauenswürdigen Schlüsselanbieters für vertrauenswürdige Hosts mithilfe der Befehlszeile

Sie können vertrauenswürdige Schlüsselanbieter über die Befehlszeile konfigurieren. Sie können den vertrauenswürdigen Standardschlüsselanbieter für den vCenter Server oder auf Cluster- oder Ordnerebene in der vCenter-Objekthierarchie konfigurieren.

Einrichten von Workstations

Um eine vSphere Trust Authority-Bereitstellung zu konfigurieren, müssen Sie zur Vorbereitung zunächst die erforderliche Software auf einer Workstation installieren und diese einrichten.

Führen Sie auf einer Workstation mit Zugriff auf Ihre vSphere Trust Authority-Umgebung die folgenden Schritte aus.

Verfahren

1 Installieren Sie PowerCLI 12.1.0 oder höher. Weitere Informationen finden Sie im *PowerCLI-Benutzerhandbuch*.

2 Stellen Sie sicher, dass Microsoft .NET Framework 4.8 oder höher installiert ist.

3 Erstellen Sie einen lokalen Ordner, in dem die Trust Authority-Informationen, die Sie als Dateien exportieren, gespeichert werden.

Nächste Schritte

Fahren Sie mit Aktivieren des Trust Authority-Administrators fort.

Aktivieren des Trust Authority-Administrators

Zum Aktivieren von vSphere Trust Authority müssen Sie einen Benutzer zur TrustedAdmins-Gruppe in vSphere hinzufügen. Dieser Benutzer übernimmt die Funktion des Trust Authority-Administrators. Sie verwenden den Trust Authority-Administrator für die meisten vSphere Trust Authority-Konfigurationsaufgaben.

Verwenden Sie einen anderen Benutzer als den vCenter Server-Administrator als Trust Authority-Administrator. Durch Verwendung eines anderen Benutzers wird die Sicherheit Ihrer Umgebung verbessert. Sie müssen einen Trust Authority-Administrator dem Trust Authority-Cluster und dem vertrauenswürdigen Cluster hinzufügen.

Voraussetzungen

Erstellen Sie entweder einen Benutzer oder identifizieren Sie einen vorhandenen Benutzer als Trust Authority-Administrator.

Verfahren

1 Stellen Sie eine Verbindung zum vSphere Client des Trust Authority-Clusters her, indem Sie den vCenter Server verwenden.

2 Melden Sie sich als Administrator an.

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

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

5 Klicken Sie auf **Gruppen** und dann auf die Gruppe **TrustedAdmins**.

   Wenn die Gruppe TrustedAdmins zunächst nicht angezeigt wird, verwenden Sie das **Filter**-Symbol, um nach ihr zu filtern, oder navigieren Sie durch die Gruppen, indem Sie auf den Rechtspfeil am unteren Rand des Fensterspeichers klicken.

6 Klicken Sie im Bereich **Gruppenmitglieder** auf **Mitglieder hinzufügen**.

   Stellen Sie sicher, dass die lokale Identitätsquelle ausgewählt ist („vsphere.local“ ist die Standardeinstellung, aber Sie haben während der Installation möglicherweise eine andere Domäne ausgewählt) und suchen Sie nach dem Mitglied (Benutzer), das Sie der Gruppe als Trust Authority Administrator hinzufügen möchten.

7 Wählen Sie das Mitglied aus.

8 Klicken Sie auf **Speichern**.

9 Wiederholen Sie die Schritte 1 bis 8 für den vCenter Server des vertrauenswürdigen Clusters.

Nächste Schritte

Fahren Sie mit Aktivieren des Trust Authority-Status fort.

Aktivieren des Trust Authority-Status

Durch Umwandeln eines vCenter Server-Clusters in einen vSphere Trust Authority-Cluster (auch bezeichnet als Aktivieren des Trust Authority-Status) werden die notwendigen Trust Authority-Dienste auf den ESXi-Hosts im Cluster gestartet.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.

Verfahren

1 In einer PowerCLI-Sitzung führen Sie das `Connect-VIServer`-Cmdlet aus, um als Administrator der Trust Authority mit dem vCenter Server des Trust Authority-Clusters zu verbinden.

```
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

2 Führen Sie das `Get-TrustAuthorityCluster`-Cmdlet aus, um den aktuellen Status des Clusters zu überprüfen.

   Dieser Befehl zeigt z. B. den Cluster, `vTA Cluster` und dessen Status „deaktiviert“ an.

```
Get-TrustAuthorityCluster

Name                State               Id
----                -----               --
vTA Cluster         Disabled            TrustAuthorityCluster-domain-c8
```

   Die Ausgabe zeigt für jeden gefundenen Cluster entweder „Deaktiviert“ oder „Aktiviert“ in der Spalte „Status“ an. „Deaktiviert“ bedeutet, dass die Trust Authority-Dienste nicht ausgeführt werden.

3 Führen Sie das `Set-TrustAuthorityCluster`-Cmdlet zum Aktivieren des Trust Authority-Clusters aus.

   Mit diesem Befehl wird beispielsweise das Cluster `vTA Cluster` aktiviert.

```
Set-TrustAuthorityCluster -TrustAuthorityCluster 'vTA Cluster' -State Enabled
```

   Das System antwortet mit einer Bestätigungsaufforderung.

```
Confirmation
Setting TrustAuthorityCluster 'vTA Cluster' with new State 'Enabled'. Do you want to
proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

4 Drücken Sie an der Bestätigungsaufforderung die Eingabetaste. (Der Standardwert lautet **Y**.)

   Die Ausgabe zeigt den Status des Clusters an. Folgendes zeigt beispielsweise, dass Cluster `vTA Cluster` aktiviert wurde:

```
Name                State               Id
----                -----               --
vTA Cluster         Enabled             TrustAuthorityCluster-domain-c8
```

Ergebnisse

Zwei Dienste werden auf den ESXi-Hosts im Trust Authority-Cluster gestartet: der Bestätigungsdienst und der Schlüsselanbieterdienst.

Beispiel: Aktivieren des vertrauenswürdigen Status im Trust Authority-Cluster

In diesem Beispiel wird die Verwendung der PowerCLI zum Aktivieren von Diensten im Trust Authority-Cluster veranschaulicht. In der folgenden Tabelle werden die verwendeten Beispielkomponenten und -werte angezeigt.

Tabelle 9-4. Beispiel eines vSphere Trust Authority-Setups

Komponente	Wert
vCenter Server für Trust Authority-Cluster	192.168.210.22
Name des Trust Authority-Clusters	vTA-Cluster
Trust Authority-Administrator	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                 443   VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Get-TrustAuthorityCluster

Name                 State                Id
----                 -----                --
vTA Cluster          Disabled             TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> Set-TrustAuthorityCluster -TrustAuthorityCluster 'vTA
Cluster' -State Enabled

Confirmation
Setting TrustAuthorityCluster 'vTA Cluster' with new State 'Enabled'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

Name                 State                Id
----                 -----                --
vTA Cluster          Enabled              TrustAuthorityCluster-domain-c8
```

Nächste Schritte

Fahren Sie mit Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server fort.

Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server

Zum Aufbau einer Vertrauensstellung benötigt der vSphere Trust Authority-Cluster Informationen über die ESXi-Hosts und den vCenter Server des vertrauenswürdigen Clusters. Sie exportieren diese Informationen als Dateien, die in den Trust Authority-Cluster importiert werden. Sie müssen sicherstellen, dass diese Dateien vertraulich behandelt und sicher übertragen werden.

Mithilfe von vSphere Trust Authority PowerCLI-Cmdlets exportieren Sie die folgenden Informationen als Dateien aus den ESXi-Hosts im vertrauenswürdigen Cluster, damit der Trust Authority-Cluster die vertrauenswürdige Software und Hardware erkennt.

- ESXi-Version

- TPM-Hersteller (CA-Zertifikat)
- (Optional) Einzelnes TPM (EK-Zertifikat)

Hinweis Speichern Sie diese exportierten Dateien an einem sicheren Ort für den Fall, dass Sie die vSphere Trust Authority-Konfiguration wiederherstellen müssen.

Wenn Sie über Hosts desselben Typs und Anbieters verfügen und diese im selben Zeitraum und am selben Ort hergestellt wurden, können Sie unter Umständen alle TPMs als vertrauenswürdig einstufen, indem Sie das CA-Zertifikat nur eines der TPMs abrufen. Um einem einzelnen TPM als vertrauenswürdig einzustufen, rufen Sie das EK-Zertifikat des TPM ab.

Sie müssen auch die Prinzipalinformationen aus dem vCenter Server des vertrauenswürdigen Clusters abrufen. Die Prinzipalinformationen enthalten den Lösungsbenutzer „vpxd“ sowie dessen Zertifikatskette. Mithilfe der Prinzipalinformationen kann der vCenter Server des vertrauenswürdigen Clusters die verfügbaren vertrauenswürdigen Schlüsselanbieter ermitteln, die im Trust Authority-Cluster konfiguriert sind.

Für die erstmalige Konfiguration von vSphere Trust Authority müssen Sie die ESXi-Version und die TPM-Informationen erfassen. Sie müssen auch die ESXi-Version bei jeder Bereitstellung einer neuen Version von ESXi erfassen, so auch beim Upgraden oder Anwenden eines Patches.

Sie erfassen die Informationen des vCenter Server-Prinzipals nur einmal pro vCenter Server-System.

Voraussetzungen

- Geben Sie die ESXi-Versionen und TPM-Hardwaretypen an, die sich im vertrauenswürdigen Cluster befinden, und legen Sie fest, ob Sie alle TPM-Hardwaretypen, nur bestimmte oder einzelne Hosts als vertrauenswürdig einstufen möchten.
- Erstellen Sie auf der Maschine, von der aus Sie die PowerCLI ausführen, einen lokalen Ordner, in dem die Informationen, die Sie als Dateien exportieren, gespeichert werden sollen.
- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.

Verfahren

1. Führen Sie in einer PowerCLI-Sitzung die folgenden Befehle aus, um alle bestehenden Verbindungen zu trennen und als Root-Benutzer eine Verbindung zu einem der ESXi-Hosts im vertrauenswürdigen Cluster herzustellen.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server host_ip_address -User root -Password 'password'
   ```

2. Starten Sie das `Get-VMHost`-Cmdlet, um den ESXi-Host zu bestätigen.

   ```
   Get-VMHost
   ```

   Die Hostinformationen werden angezeigt.

3 Weisen Sie `Get-VMHost` einer Variable zu.

Beispiel:

```
$vmhost = Get-VMHost
```

4 Führen Sie das `Export-Tpm2CACertificate`-Cmdlet aus, um das CA-Zertifikat eines bestimmten TPM-Herstellers zu exportieren.

a Weisen Sie `Get-Tpm2EndorsementKey -VMHost $vmhost` einer Variable zu.

Mit diesem Befehl wird beispielsweise `Get-Tpm2EndorsementKey -VMHost $vmhost` der Variable `$tpm2` zugewiesen.

```
$tpm2 = Get-Tpm2EndorsementKey -VMHost $vmhost
```

b Führen Sie das `Export-Tpm2CACertificate`-cmdlet aus.

Mit diesem Befehl wird beispielsweise das TPM-Zertifikat in die Datei `cacert.zip` exportiert. Stellen Sie vor dem Ausführen des Befehls sicher, dass das Zielverzeichnis bereits vorhanden ist.

```
Export-Tpm2CACertificate -Tpm2EndorsementKey $tpm2 -FilePath C:\vta\cacert.zip
```

Die Datei wird erstellt.

c Wiederholen Sie den Vorgang für jeden TPM-Hardwaretyp im Cluster, den Sie als vertrauenswürdig einstufen möchten. Verwenden Sie einen anderen Dateinamen für jeden TMP-Hardwaretyp, sodass Sie eine zuvor exportierte Datei nicht überschreiben.

5 Führen Sie das `Export-VMHostImageDb`-Cmdlet aus, um die Beschreibung der Software des ESXi-Hosts (das ESXi-Image) zu exportieren.

Mit diesem Befehl werden beispielsweise die Informationen in die Datei `image.tgz` exportiert. Stellen Sie vor dem Ausführen des Befehls sicher, dass das Zielverzeichnis bereits vorhanden ist.

```
Export-VMHostImageDb -VMHost $vmhost -FilePath C:\vta\image.tgz
```

Hinweis Das `Export-VMHostImageDb`-Cmdlet funktioniert auch, wenn Sie sich beim vCenter Server des vertrauenswürdigen Clusters anmelden möchten.

Die Datei wird erstellt.

Wiederholen Sie diese Schritte für jede ESXi-Version im Cluster, den Sie als vertrauenswürdig einstufen möchten. Verwenden Sie für jede Version einen anderen Dateinamen, damit Sie eine zuvor exportierte Datei nicht überschreiben.

6 Exportieren Sie die vCenter Server-Prinzipalinformationen des vertrauenswürdigen Clusters.

a Trennen Sie die Verbindung zum ESXi-Host.

```
Disconnect-VIServer -server * -Confirm:$false
```

b Stellen Sie mithilfe des Trust Authority-Administrators eine Verbindung zum vCenter Server des vertrauenswürdigen Clusters her. (Alternativ können Sie einen Benutzer verwenden, der über **Administrator**-Rechte verfügt.)

```
Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password
'password'
```

c Um die vCenter Server-Prinzipalinformationen des vertrauenswürdigen Clusters zu exportieren, führen Sie das `Export-TrustedPrincipal`-Cmdlet aus.

Mit diesem Befehl werden beispielsweise die Informationen in die Datei `principal.json` exportiert. Stellen Sie vor dem Ausführen des Befehls sicher, dass das Zielverzeichnis bereits vorhanden ist.

```
Export-TrustedPrincipal -FilePath C:\vta\principal.json
```

Die Datei wird erstellt.

7 (Optional) Wenn Sie einen einzelnen Host als vertrauenswürdig einstufen möchten, müssen Sie das TPM-Zertifikat des öffentlichen EK-Schlüssels exportieren.

Weitere Informationen hierzu finden Sie unter Exportieren und Importieren eines TPM Endorsement Key-Zertifikats.

Ergebnisse

Die folgenden Dateien werden erstellt:

- CA-Zertifikatsdatei des TPM (Dateierweiterung „zip“)
- ESXi-Image-Datei (Dateierweiterung „tgz“)
- vCenter Server-Prinzipaldatei (Dateierweiterung „json“)

Beispiel: Erfassen von Informationen zu ESXi-Hosts und zum vertrauenswürdigen vCenter Server

In diesem Beispiel wird die Verwendung der PowerCLI zum Exportieren der ESXi-Hostinformationen und der vCenter Server-Prinzipalinformationen erläutert. In der folgenden Tabelle werden die verwendeten Beispielkomponenten und -werte angezeigt.

Tabelle 9-5. Beispiel eines vSphere Trust Authority-Setups

Komponente	Wert
ESXi-Host im vertrauenswürdigen Cluster	192.168.110.51
vCenter Server für vertrauenswürdigen Cluster	192.168.110.22

Tabelle 9-5. Beispiel eines vSphere Trust Authority-Setups (Fortsetzung)

Komponente	Wert
Variable `$vmhost`	`Get-VMHost`
Variable `$tpm2`	`Get-Tpm2EndorsementKey -VMHost $vmhost`
Trust Authority-Administrator	trustedadmin@vsphere.local
Lokales Verzeichnis zum Speichern von Ausgabedateien	`C:\vta`

```
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.51 -User root -Password
'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.51                  443  root

PS C:\Users\Administrator.CORP> Get-VMHost

Name               ConnectionState PowerState NumCpu CpuUsageMhz CpuTotalMhz MemoryUsageGB
MemoryTotalGB Version
----               --------------- ---------- ------ ----------- ----------- -------------
------------- -------
192.168.110.51     Connected       PoweredOn       4         200        9576
1.614         7.999   7.0.0

PS C:\Users\Administrator.CORP> $vmhost = Get-VMHost
PS C:\Users\Administrator.CORP> $tpm2 = Get-Tpm2EndorsementKey -VMHost $vmhost
PS C:\> Export-Tpm2CACertificate -Tpm2EndorsementKey $tpm2 -FilePath C:\vta\cacert.zip

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/8/2019   6:55 PM           1004 cacert.zip

PS C:\Users\Administrator.CORP> Export-VMHostImageDb -VMHost $vmhost -FilePath
C:\vta\image.tgz

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         10/8/2019  11:02 PM           2391 image.tgz

PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.22                  443  VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Export-TrustedPrincipal -FilePath C:\vta\principal.json

Mode                 LastWriteTime         Length Name
```

```
----                 -------------         ------ ----
-a----         10/8/2019  11:14 PM           1873 principal.json
```

Nächste Schritte

Fahren Sie mit Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster fort.

Exportieren und Importieren eines TPM Endorsement Key-Zertifikats

Sie können ein TPM Endorsement Key (EK)-Zertifikat von einem ESXi-Host exportieren und in den vSphere Trust Authority-Cluster importieren. Führen Sie den Vorgang aus, wenn Sie einem einzelnen ESXi-Host im vertrauenswürdigen Cluster vertrauen möchten.

Um ein TPM EK-Zertifikat in den Trust Authority-Cluster zu importieren, müssen Sie den standardmäßigen Nachweistyp des Trust Authority-Clusters ändern, damit dieser die Zertifikate akzeptiert. Der standardmäßige Nachweistyp akzeptiert Zertifikate der TPM-Zertifizierungsstelle (Certificate Authority, CA). Bestimmte TPMs enthalten keine EK-Zertifikate. Wenn Sie einzelne ESXi-Hosts als vertrauenswürdig einstufen möchten, muss das TPM ein EK-Zertifikat enthalten.

Hinweis Speichern Sie die exportierten EK-Zertifikatsdateien an einem sicheren Ort für den Fall, dass Sie die vSphere Trust Authority-Konfiguration wiederherstellen müssen.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.

Verfahren

1. Stellen Sie sicher, dass Sie als Trust Authority-Administrator mit dem vCenter Server des Trust Authority-Clusters verbunden sind.

   Sie können beispielsweise `$global:defaultviservers` eingeben, um alle verbundenen Server anzuzeigen.

2. (Optional) Sie können gegebenenfalls die folgenden Befehle ausführen, um sicherzustellen, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
   -Password 'password'
   ```

3 So ändern Sie den Nachweistyp des Trust Authority-Clusters:

a Führen Sie das `Get-TrustAuthorityCluster`-Cmdlet aus, um die von diesem vCenter Server verwalteten Cluster anzuzeigen.

```
Get-TrustAuthorityCluster
```

Die Cluster werden angezeigt.

b Weisen Sie die `Get-TrustAuthorityCluster`-Informationen einer Variable zu.

Beispiel: Dieser Befehl weist dem Cluster mit dem Namen `vTA Cluster` der Variable `$vTA` zu.

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

c Weisen Sie die `Get-TrustAuthorityTpm2AttestationSettings`-Informationen einer Variable zu.

Beispiel: Dieser Befehl weist die Informationen der Variable `$tpm2Settings` zu.

```
$tpm2Settings = Get-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster $vTA
```

d Starten Sie das `Set-TrustAuthorityTpm2AttestationSettings`-Cmdlet, indem Sie `RequireEndorsementKey` oder `RequireCertificateValidation` oder beides angeben.

Beispiel: Dieser Befehl gibt `RequireEndorsementKey` an.

```
Set-TrustAuthorityTpm2AttestationSettings -Tpm2AttestationSettings $tpm2Settings
-RequireEndorsementKey
```

Das System antwortet mit einer Bestätigungseingabeaufforderung ähnlich der folgenden.

```
Confirmation
Configure the Tpm2AttestationSettings 'TrustAuthorityTpm2AttestationSettings-domain-
c8' with the following parameters:
 RequireCertificateValidation: False
 RequireEndorsementKey: True
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

e Drücken Sie an der Bestätigungsaufforderung die Eingabetaste. (Der Standardwert lautet **`Y`**.)

Die Ausgabe zeigt den Status „true“ für die angegebene Einstellung an. Beispiel: Dieser Status zeigt „true“ für „Endorsement Key anfordern“ und „false“ für „Zertifikatvalidierung anfordern“ an.

```
Name                                    RequireEndorsementKey
RequireCertificateValidation   Health
----                                    ---------------------
---------------------------    ------
TrustAuthorityTpm2AttestationSettings... True
False                          Ok
```

4 So exportieren Sie das TPM EK-Zertifikat:

a Trennen Sie die Verbindung mit dem vCenter Server des Trust Authority-Clusters.

```
Disconnect-VIServer -server * -Confirm:$false
```

b Führen Sie das `Connect-VIServer`-Cmdlet aus, um als Root-Benutzer eine Verbindung zu einem der ESXi-Hosts im vertrauenswürdigen Cluster herzustellen.

```
Connect-VIServer -server host_ip_address -User root -Password 'password'
```

c Starten Sie das `Get-VMHost`-Cmdlet, um den ESXi-Host zu bestätigen.

```
Get-VMHost
```

Die Hostinformationen werden angezeigt.

d Weisen Sie `Get-VMHost` einer Variable zu.

Beispiel:

```
$vmhost = Get-VMHost
```

e Führen Sie das `Export-Tpm2EndorsementKey`-Cmdlet zum Exportieren des EK-Zertifikats des ESXi-Hosts aus.

Beispiel: Mit diesem Befehl wird das EK-Zertifikat in die Datei `tpm2ek.json` exportiert.

```
Export-Tpm2EndorsementKey -VMHost $vmhost -FilePath C:\vta\tpm2ek.json
```

Die Datei wird erstellt.

5 So importieren Sie das TPM EK:

a Trennen Sie die Verbindung mit dem ESXi-Host im vertrauenswürdigen Cluster.

```
Disconnect-VIServer -server * -Confirm:$false
```

b Stellen Sie mithilfe des Trust Authority-Administrators eine Verbindung zum vCenter Server des Trust Authority-Clusters her.

```
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

c Führen Sie das `Get-TrustAuthorityCluster`-cmdlet aus.

```
Get-TrustAuthorityCluster
```

Die Cluster im Trust Authority-Cluster werden angezeigt.

d Weisen Sie die *Cluster*-Informationen von `Get-TrustAuthorityCluster` einer Variable zu.

Beispiel: Dieser Befehl weist die Informationen für Cluster `vTA Cluster` der Variable `$vTA` zu.

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

e Führen Sie das `New-TrustAuthorityTpm2EndorsementKey`-cmdlet aus.

Beispiel: Dieser Befehl verwendet die `tpm2ek`-Datei, die zuvor in Schritt 4 exportiert wurde.

```
New-TrustAuthorityTpm2EndorsementKey -TrustAuthorityCluster $vTA -FilePath
C:\vta\tpm2ek.json
```

Die importierten Endorsement Key-Informationen werden angezeigt.

Ergebnisse

Der Nachweistyp des Trust Authority-Clusters wird geändert, um die EK-Zertifikate zu akzeptieren. Das EK-Zertifikat wird aus dem vertrauenswürdigen Cluster exportiert und in den Trust Authority-Cluster importiert.

Beispiel: Exportieren und Importieren eines TPM EK-Zertifikats

Dieses Beispiel zeigt, wie Sie PowerCLI verwenden können, um den standardmäßigen Nachweistyp des Trust Authority-Clusters zu ändern, um EK-Zertifikate zu akzeptieren, das TPM EK-Zertifikat vom ESXi-Host im vertrauenswürdigen Cluster zu exportieren und es in den Trust Authority-Cluster zu importieren. In der folgenden Tabelle werden die verwendeten Beispielkomponenten und -werte angezeigt.

Tabelle 9-6. Beispiel eines vSphere Trust Authority-Setups

Komponente	Wert
vCenter Server für Trust Authority-Cluster	192.168.210.22
Variable `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
Variable `$tpm2Settings`	`Get-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster $vTA`
Variable `$vmhost`	`Get-VMHost`
ESXi-Host im vertrauenswürdigen Cluster	192.168.110.51
Trust Authority-Administrator	trustedadmin@vsphere.local
Lokales Verzeichnis zum Speichern von Ausgabedateien	`C:\vta`

```
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                 443   VSPHERE.LOCAL\TrustedAdmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                 State               Id
----                 -----               --
vTA Cluster          Enabled             TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster'

PS C:\Users\Administrator> $tpm2Settings = Get-TrustAuthorityTpm2AttestationSettings
-TrustAuthorityCluster $vTA

PS C:\Users\Administrator> Set-TrustAuthorityTpm2AttestationSettings -Tpm2AttestationSettings
$tpm2Settings -RequireEndorsementKey

Confirmation
```

```
Configure the Tpm2AttestationSettings 'TrustAuthorityTpm2AttestationSettings-domain-c8' with
the following parameters:
 RequireCertificateValidation: False
 RequireEndorsementKey: True
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

Name                                    RequireEndorsementKey
RequireCertificateValidation   Health
----                                    ---------------------
----------------------------   ------
TrustAuthorityTpm2AttestationSettings... True
False                          Ok

PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.110.51 -User root -Password
'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.51                 443   root

PS C:\Users\Administrator> Get-VMHost

Name                 ConnectionState PowerState NumCpu CpuUsageMhz CpuTotalMhz
MemoryUsageGB   MemoryTotalGB Version
----                 --------------- ---------- ------ ----------- -----------
-------------   ------------- -------
192.168.110.51       Connected       PoweredOn       4          55        9576
1.230           7.999   7.0.0

PS C:\Users\Administrator> $vmhost = Get-VMHost
PS C:\Users\Administrator> Export-Tpm2EndorsementKey -VMHost $vmhost -FilePath
C:\vta\tpm2ek.json

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        12/3/2019  10:16 PM           2391 tpm2ek.json

PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                 443   VSPHERE.LOCAL\TrustedAdmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                 State               Id
----                 -----               --
vTA Cluster          Enabled             TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster ‘vTA Cluster’
PS C:\Users\Administrator> New-TrustAuthorityTpm2EndorsementKey -TrustAuthorityCluster $vTA
-FilePath C:\vta\tpm2ek.json
```

```
TrustAuthorityClusterId                  Name                                    Health
-----------------------                  ----                                    ------
TrustAuthorityCluster-domain-c8          1a520e42-4db8-1cbb-6dd7-f493fd921ccb    Ok
```

Nächste Schritte

Fahren Sie mit Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster fort.

Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster

Sie importieren den exportierten ESXi-Host und die vCenter Server-Informationen in den vSphere Trust Authority-Cluster, um den Trust Authority-Cluster über die zu bestätigenden Hosts zu informieren.

Während Sie diese Aufgaben in der angegebenen Reihenfolge ausführen, bleiben Sie weiterhin mit dem vCenter Server des Trust Authority-Clusters verbunden.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.
- Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.

Verfahren

1. Stellen Sie sicher, dass Sie als Trust Authority-Administrator mit dem vCenter Server des Trust Authority-Clusters verbunden sind.

   Sie können beispielsweise `$global:defaultviservers` eingeben, um alle verbundenen Server anzuzeigen.

2. (Optional) Sie können gegebenenfalls die folgenden Befehle ausführen, um sicherzustellen, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
   -Password 'password'
   ```

3. Führen Sie zur Anzeige der von diesem vCenter Server verwalteten Cluster das Cmdlet `Get-TrustAuthorityCluster` aus.

   ```
   Get-TrustAuthorityCluster
   ```

   Die Cluster werden angezeigt.

4 Weisen Sie die *Cluster*-Informationen von `Get-TrustAuthorityCluster` einer Variable zu.

Beispiel: Dieser Befehl weist die Informationen für Cluster `vTA Cluster` der Variable `$vTA` zu.

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

5 Führen Sie zum Importieren der vCenter Server-Prinzipalinformationen des vertrauenswürdigen Clusters in den Trust Authority-Cluster das `New-TrustAuthorityPrincipal`-Cmdlet aus.

Mit dem folgenden Befehl wird beispielsweise die Datei `principal.json` importiert, die zuvor in Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server exportiert wurde.

```
New-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA -FilePath C:\vta\principal.json
```

Die Trust Authority-Prinzipalinformationen werden angezeigt.

6 Führen Sie das `Get-TrustAuthorityPrincipal`-Cmdlet aus, um den Import zu überprüfen.

Beispiel:

```
Get-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA
```

Die importierten Trust Authority-Prinzipalinformationen werden angezeigt.

7 Um die Informationen über das TPM-CA-Zertifikat (Trusted Platform Module, Vertrauenswürdiges Plattformmodul) zu importieren, führen Sie das `New-TrustAuthorityTpm2CACertificate`-Cmdlet aus.

Beispiel: Mit dem folgenden Befehl werden die TPM-CA-Zertifikatsinformationen aus der Datei `cacert.zip` importiert, die zuvor nach Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server exportiert wurde.

```
New-TrustAuthorityTpm2CACertificate -TrustAuthorityCluster $vTA -FilePath
C:\vta\cacert.zip
```

Die importierten Zertifikatinformationen werden angezeigt.

8 Um die Basisimage-Informationen des ESXi-Hosts zu importieren, führen Sie das `New-TrustAuthorityVMHostBaseImage`-Cmdlet aus.

Beispiel: Mit dem folgenden Befehl werden die Image-Informationen aus der Datei `image.tgz` importiert, die zuvor nach Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server exportiert wurde.

```
New-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA -FilePath C:\vta\image.tgz
```

Die importierten Bildinformationen werden angezeigt.

Ergebnisse

Der Trust Authority-Cluster kennt die ESXi-Hosts, die er remote bestätigen und denen er somit vertrauen kann.

Beispiel: Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster

Dieses Beispiel zeigt, wie Sie PowerCLI verwenden können, um die vCenter Server-Prinzipalinformationen über den vertrauenswürdigen Cluster sowie die Informationsdateien über den vertrauenswürdigen Host in den Trust Authority-Cluster zu importieren. Es wird davon ausgegangen, dass Sie als Trust Authority-Administrator mit dem vCenter Server des Trust Authority-Clusters verbunden sind. In der folgenden Tabelle werden die verwendeten Beispielkomponenten und -werte angezeigt.

Tabelle 9-7. Beispiel eines vSphere Trust Authority-Setups

Komponente	Wert
Variable `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster1'`
vCenter Server für Trust Authority-Cluster	192.168.210.22
Namen der Trust Authority-Cluster	vTA-Cluster1 (Aktiviert) vTA-Cluster2 (Deaktiviert)
Datei mit Prinzipalinformationen	`C:\vta\principal.json`
TPM-Zertifikatsdatei	`C:\vta\cacert.cer`
ESXi-Basisimage-Datei des Hosts	`C:\vta\image.tgz`
Trust Authority-Administrator	trustedadmin@vsphere.local

```
PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                  443  VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                 State                Id
----                 -----                --
vTA Cluster1         Enabled              TrustAuthorityCluster-domain-c8
vTA Cluster2         Disabled             TrustAuthorityCluster-domain-c26

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster1'

PS C:\Users\Administrator.CORP> New-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA
-FilePath C:\vta\principal.json

Name                                          Domain          Type
```

```
TrustAuthorityClusterId
----                                        ------          ----
-----------------------
vpxd-de207929-0601-43ef-9616-47d0cee0302f    vsphere.local   STS_USER
TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> Get-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA

Name                                        Domain          Type
TrustAuthorityClusterId
----                                        ------          ----
-----------------------
vpxd-de207929-0601-43ef-9616-47d0cee0302f    vsphere.local   STS_USER
TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> New-TrustAuthorityTpm2CACertificate -TrustAuthorityCluster
$vTA -FilePath C:\vta\cacert.cer

TrustAuthorityClusterId                 Name                                    Health
-----------------------                 ----                                    ------
TrustAuthorityCluster-domain-c8         52BDB7B4B2F55C925C047257DED4588A7767D961 Ok

PS C:\Users\Administrator.CORP> New-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA
-FilePath C:\vta\image.tgz

TrustAuthorityClusterId                 VMHostVersion                           Health
-----------------------                 -------------                           ------
TrustAuthorityCluster-domain-c8         ESXi 7.0.0-0.0.14828939                 Ok
```

Nächste Schritte

Fahren Sie mit Erstellen des Schlüsselanbieters im Trust Authority-Cluster fort.

Erstellen des Schlüsselanbieters im Trust Authority-Cluster

Damit der Schlüsselanbieterdienst eine Verbindung mit einem Schlüsselanbieter herstellen kann, müssen Sie einen vertrauenswürdigen Schlüsselanbieter erstellen und dann eine vertrauenswürdige Verbindung zwischen dem vSphere Trust Authority-Cluster und dem Schlüsselserver (KMS) konfigurieren. Für die meisten KMIP-kompatiblen Schlüsselserver beinhaltet diese Konfiguration die Einrichtung von Client- und Serverzertifikaten.

Der KMS-Cluster in vSphere 6.7 wird in vSphere 7.0 als Schlüsselanbieter bezeichnet. Weitere Informationen zu Schlüsselanbietern finden Sie unter Was ist der vSphere Trust Authority-Schlüsselanbieterdienst?.

In einer Produktionsumgebung können Sie mehrere Schlüsselanbieter erstellen. Indem Sie mehrere Schlüsselanbieter erstellen, können Sie festlegen, wie Ihre Bereitstellung basierend auf Unternehmensorganisation, verschiedenen Geschäftsbereichen oder Kunden usw. verwaltet werden soll.

Wenn Sie diese Aufgaben nacheinander ausführen, sind Sie weiterhin mit dem vCenter Server des vSphere Trust Authority-Clusters verbunden.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.
- Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.
- Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.
- Erstellen und aktivieren Sie einen Schlüssel auf dem Schlüsselserver, der der primäre Schlüssel für den vertrauenswürdigen Schlüsselanbieter sein soll. Dieser Schlüssel umhüllt andere Schlüssel und Geheimnisse, die von diesem vertrauenswürdigen Schlüsselanbieter verwendet werden. Weitere Informationen zum Erstellen von Schlüsseln finden Sie in der Dokumentation des Schlüsselserverherstellers.

Verfahren

1. Stellen Sie sicher, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind. Sie können beispielsweise `$global:defaultviservers` eingeben, um alle verbundenen Server anzuzeigen.
2. (Optional) Sie können gegebenenfalls die folgenden Befehle ausführen, um sicherzustellen, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
   -Password 'password'
   ```

3. Um einen vertrauenswürdigen Schlüsselanbieter zu erstellen, führen Sie das `New-TrustAuthorityKeyProvider`-Cmdlet aus.

   Dieser Befehl verwendet beispielsweise `1` für die PrimaryKeyID und den Namen `clkp`. Wenn Sie diese Aufgaben nacheinander ausführen, haben Sie die `Get-TrustAuthorityCluster`-Informationen zuvor einer Variable zugewiesen (z. B. `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

   ```
   New-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA -PrimaryKeyId 1 -Name clkp
   -KmipServerAddress ip_address
   ```

   Die PrimaryKeyID ist in der Regel eine Schlüssel-ID, die in Form einer UUID aus dem Schlüsselserver stammt. Verwenden Sie für PrimaryKeyID nicht den Schlüsselnamen. Der PrimaryKeyID-Wert ist vom Anbieter abhängig. Informationen finden Sie in der Dokumentation des Schlüsselservers. Das `New-TrustAuthorityKeyProvider`-Cmdlet kann andere Optionen wie z. B. `KmipServerPort`, `ProxyAddress` und `ProxyPort` nutzen. Weitere Informationen finden Sie im `New-TrustAuthorityKeyProvider`-Hilfesystem.

   Jeder logische Schlüsselanbieter muss unabhängig von seinem Typ (Standard-, vertrauenswürdiger und nativer Schlüsselanbieter) über einen eindeutigen Namen in allen vCenter Server-Systemen verfügen.

Weitere Informationen finden Sie unter Benennung des Schlüsselanbieters.

Hinweis Um dem Schlüsselanbieter mehrere Schlüsselserver hinzuzufügen, verwenden Sie das `Add-TrustAuthorityKeyProviderServer`-Cmdlet.

Informationen zum Schlüsselanbieter werden angezeigt.

4 Stellen Sie die vertrauenswürdige Verbindung sicher, sodass der Schlüsselserver dem vertrauenswürdigen Schlüsselanbieter vertraut. Der genaue Prozess hängt von den Zertifikaten, die vom Schlüsselserver akzeptiert werden, sowie von der Unternehmensrichtlinie ab. Wählen Sie die entsprechende Option für den Server aus und schließen Sie die Schritte ab.

Option	Informationen hierzu finden Sie unter
Clientzertifikat hochladen	Hochladen des Clientzertifikats zum Herstellen einer vertrauenswürdigen Verbindung des vertrauenswürdigen Schlüsselanbieters.
KMS-Zertifikat und privaten Schlüssel hochladen	Zertifikat und privaten Schlüssel zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters hochladen.
Neue Zertifikatssignieranforderung	Eine Zertifikatssignieranforderung zum Herstellen einer vertrauenswürdigen Schlüsselanbieter-Verbindung erstellen.

5 Schließen Sie das Trust-Setup ab, indem Sie ein Schlüsselserverzertifikat hochladen, damit der vertrauenswürdige Schlüsselanbieter dem Schlüsselserver vertraut.

a Weisen Sie die `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA-` Informationen einer Variable zu.

Beispiel:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

Diese Variable erhält die vertrauenswürdigen Schlüsselanbieter im Trust Authority-Cluster, in diesem Fall `$vTA`.

Hinweis Wenn Sie über mehrere vertrauenswürdige Schlüsselanbieter verfügen, verwenden Sie Befehle ähnlich den folgenden, um den gewünschten Anbieter auszuwählen:

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

Mit `Select-Object -Last 1` wird der letzte vertrauenswürdige Schlüsselanbieter in der Liste angezeigt.

b Führen Sie den Befehl `Get-TrustAuthorityKeyProviderServerCertificate` aus, um das Serverzertifikat des Schlüsselservers abzurufen.

Beispiel:

```
Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer
$kp.KeyProviderServers
```

Die Serverzertifikatinformationen werden angezeigt. Anfänglich ist das Zertifikat nicht als vertrauenswürdig eingestuft, d. h., der vertrauenswürdige Zustand lautet „False“. Wenn Sie mehr als einen Schlüsselserver konfiguriert haben, wird eine Zertifikatsliste zurückgegeben. Überprüfen Sie jedes Zertifikat und fügen Sie jedes davon hinzu, indem Sie die folgenden Anweisungen befolgen.

c Bevor Sie dem Zertifikat vertrauen, weisen Sie die Informationen aus `Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer $kp.KeyProviderServers` einer Variablen zu (z. B. `cert`), führen Sie den Befehl `$cert.Certificate.ToString()` aus und überprüfen Sie die Ausgabe.

Beispiel:

```
$cert = Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer
$kp.KeyProviderServers
$cert.Certificate.ToString()
```

Die Zertifikatsinformationen werden angezeigt, einschließlich Thema, Aussteller und sonstiger Informationen.

d Um dem vertrauenswürdigen Schlüsselanbieter das KMIP-Serverzertifikat hinzuzufügen, führen Sie `Add-TrustAuthorityKeyProviderServerCertificate` aus.

Beispiel:

```
Add-TrustAuthorityKeyProviderServerCertificate -ServerCertificate $cert
```

Die Zertifikatsinformationen werden angezeigt und der vertrauenswürdige Zustand lautet nun „True“.

6 Überprüfen Sie den Status des Schlüsselanbieters.

a Um den Schlüsselanbieterstatus zu aktualisieren, weisen Sie die `$kp`-Variable neu zu.

Beispiel:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

Hinweis Wenn Sie über mehrere vertrauenswürdige Schlüsselanbieter verfügen, verwenden Sie Befehle ähnlich den folgenden, um den gewünschten Anbieter auszuwählen:

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

Mit `Select-Object -Last 1` wird der letzte vertrauenswürdige Schlüsselanbieter in der Liste angezeigt.

b Führen Sie den Befehl `$kp.Status` aus, um den Schlüsselanbieterstatus anzuzeigen.

Beispiel:

```
$kp.Status
```

Hinweis Die Statusaktualisierung kann einige Minuten dauern. Um den Status anzuzeigen, weisen Sie die Variable `$kp` erneut zu und führen Sie den Befehl `$kp.Status` erneut aus.

Ein Systemzustand von „OK“ weist darauf hin, dass der Schlüsselanbieter ordnungsgemäß ausgeführt wird.

Ergebnisse

Der vertrauenswürdige Schlüsselanbieter wurde erstellt und hat eine vertrauenswürdige Verbindung mit dem Schlüsselserver hergestellt.

Beispiel: Erstellen des Schlüsselanbieters im Trust Authority-Cluster

Dieses Beispiel zeigt, wie Sie den vertrauenswürdigen Schlüsselanbieter mithilfe der PowerCLI im Trust Authority-Cluster erstellen können. Es wird davon ausgegangen, dass Sie als Trust Authority-Administrator mit dem vCenter Server des Trust Authority-Clusters verbunden sind. Zudem wird ein Zertifikat verwendet, das vom Schlüsselserveranbieter signiert wurde, nachdem eine CSR an den Anbieter übermittelt wurde.

In der folgenden Tabelle werden die verwendeten Beispielkomponenten und -werte angezeigt.

Tabelle 9-8. Beispiel eines vSphere Trust Authority-Setups

Komponente	Wert
Variable `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
Variable `$kp`	`Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA`
Variable `$cert`	`Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer $kp.KeyProviderServers`
vCenter Server für Trust Authority-Cluster	192.168.210.22
KMIP-kompatibler Schlüsselserver	192.168.110.91
KMIP-konformer Schlüsselserverbenutzer	vcqekmip
Name des Trust Authority-Clusters	vTA-Cluster
Trust Authority-Administrator	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

PS C:\Users\Administrator.CORP> New-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
-PrimaryKeyId 8 -Name clkp -KmipServerAddress 192.168.110.91
Name                 PrimaryKeyId         Type       TrustAuthorityClusterId
----                 ------------         ----       -----------------------
clkp                 8                    KMIP       TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> New-TrustAuthorityKeyProviderClientCertificate -KeyProvider
$kp
<Export the client certificate when you need to use it.>
PS C:\Users\Administrator.CORP> Export-TrustAuthorityKeyProviderClientCertificate
-KeyProvider $kp -FilePath clientcert.pem
```

```
PS C:\Users\Administrator.CORP> $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster
$vTA
PS C:\Users\Administrator.CORP> Get-TrustAuthorityKeyProviderServerCertificate
-KeyProviderServer $kp.KeyProviderServers

Certificate                              Trusted    KeyProviderServerId       KeyProviderId
-----------                              -------    -------------------       -------------
[Subject]...                             False      domain-c8-clkp:192.16.... domain-c8-clkp

PS C:\WINDOWS\system32> $cert.Certificate.ToString()
[Subject]
  E=<domain>, CN=<IP address>, OU=VMware Engineering, O=VMware, L=Palo Alto, S=California,
C=US

[Issuer]
  O=<host>.eng.vmware.com, C=US, DC=local, DC=vsphere, CN=CA

[Serial Number]
  00CEF192BBF9D80C9F

[Not Before]
  8/10/2015 4:16:12 PM

[Not After]
  8/9/2020 4:16:12 PM

[Thumbprint]
  C44068C124C057A3D07F51DCF18720E963604B70

PS C:\Users\Administrator.CORP> $cert = Get-TrustAuthorityKeyProviderServerCertificate
-KeyProviderServer $kp.KeyProviderServers
PS C:\Users\Administrator.CORP> Add-TrustAuthorityKeyProviderServerCertificate
-ServerCertificate $cert

Certificate                              Trusted    KeyProviderServerId       KeyProviderId
-----------                              -------    -------------------       -------------
[Subject]...                             True                                 domain-c8-clkp

PS C:\Users\Administrator.CORP> $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster
$vTA
PS C:\Users\Administrator.CORP> $kp.Status

KeyProviderId Health HealthDetails ServerStatus
------------- ------ ------------- ------------
domain-c8-kp4     Ok {}            {192.168.210.22}
```

Nächste Schritte

Fahren Sie mit Exportieren der Informationen des Trust Authority-Clusters fort.

Hochladen des Clientzertifikats zum Herstellen einer vertrauenswürdigen Verbindung des vertrauenswürdigen Schlüsselanbieters

Bestimmte Schlüsselserver-Anbieter (KMS) fordern, dass Sie das Clientzertifikat des vertrauenswürdigen Schlüsselanbieters auf den Schlüsselserver hochladen. Nach dem Upload akzeptiert der Schlüsselserver den Datenverkehr, der von dem vertrauenswürdigen Schlüsselanbieter stammt.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.
- Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.
- Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.
- Erstellen des Schlüsselanbieters im Trust Authority-Cluster.

Verfahren

1. Stellen Sie sicher, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind. Sie können beispielsweise `$global:defaultviservers` eingeben, um alle verbundenen Server anzuzeigen.
2. (Optional) Sie können gegebenenfalls die folgenden Befehle ausführen, um sicherzustellen, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
   -Password 'password'
   ```

3. Weisen Sie die `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA`-Informationen einer Variable zu.

   Beispiel:

   ```
   $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
   ```

   Wenn Sie diese Aufgaben nacheinander ausführen, haben Sie die `Get-TrustAuthorityCluster`-Informationen zuvor einer Variable zugewiesen (z. B. `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

Diese Variable erhält die vertrauenswürdigen Schlüsselanbieter im Trust Authority-Cluster, in diesem Fall `$vTA`.

Hinweis Wenn Sie über mehrere vertrauenswürdige Schlüsselanbieter verfügen, verwenden Sie Befehle ähnlich den folgenden, um den gewünschten Anbieter auszuwählen:

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

Mit `Select-Object -Last 1` wird der letzte vertrauenswürdige Schlüsselanbieter in der Liste angezeigt.

4 Um das Clientzertifikat des vertrauenswürdigen Schlüsselanbieters zu erstellen, führen Sie das `New-TrustAuthorityKeyProviderClientCertificate`-Cmdlet aus.

Beispiel:

```
New-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp
```

Der Fingerabdruck wird angezeigt.

5 Um das Clientzertifikat des Schlüsselanbieters zu exportieren, führen Sie das `Export-TrustAuthorityKeyProviderClientCertificate`-Cmdlet aus.

Beispiel:

```
Export-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -FilePath clientcert.pem
```

Das Zertifikat wird in eine Datei exportiert.

6 Laden Sie die Zertifikatsdatei auf den Schlüsselserver hoch.

Weitere Informationen finden Sie in der Dokumentation zum Schlüsselserver.

Ergebnisse

Der vertrauenswürdige Schlüsselanbieter hat eine Vertrauensstellung mit dem Schlüsselserver hergestellt.

Zertifikat und privaten Schlüssel zum Herstellen einer vertrauenswürdigen Verbindung des Standardschlüsselanbieters hochladen

Einige Anbieter von Schlüsselservern (KMS) fordern, dass Sie den vertrauenswürdigen Schlüsselanbieter mit dem Clientzertifikat und dem vom Schlüsselserver bereitgestellten privaten Schlüssel konfigurieren. Nach der Konfiguration des vertrauenswürdigen Schlüsselanbieters akzeptiert der Schlüsselserver den Datenverkehr vom vertrauenswürdigen Schlüsselanbieter.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.

- Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.
- Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.
- Erstellen des Schlüsselanbieters im Trust Authority-Cluster.
- Fordern Sie ein Zertifikat und einen privaten Schlüssel im PEM-Format vom Schlüsselserver-Anbieter an. Wenn das Zertifikat in einem anderen Format als PEM zurückgegeben wird, konvertieren Sie es in PEM. Wenn der private Schlüssel mit einem Kennwort geschützt ist, erstellen Sie eine PEM-Datei mit entferntem Kennwort. Sie können den Befehl `openssl` für beide Vorgänge verwenden. Beispiel:
  - So konvertieren Sie ein Zertifikat vom CRT- in das PEM-Format:

    ```
    openssl x509 -in clientcert.crt -out clientcert.pem -outform PEM
    ```

  - So konvertieren Sie ein Zertifikat vom DER- in das PEM-Format:

    ```
    openssl x509 -inform DER -in clientcert.der -out clientcert.pem
    ```

  - So entfernen Sie das Kennwort aus einem privaten Schlüssel:

    ```
    openssl rsa -in key.pem -out keynopassword.pem
    Enter pass phrase for key.pem:
    writing RSA key
    ```

Verfahren

1. Stellen Sie sicher, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind. Sie können beispielsweise `$global:defaultviservers` eingeben, um alle verbundenen Server anzuzeigen.
2. (Optional) Sie können gegebenenfalls die folgenden Befehle ausführen, um sicherzustellen, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
   -Password 'password'
   ```

3. Weisen Sie die `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA-` Informationen einer Variable zu.

   Beispiel:

   ```
   $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
   ```

   Wenn Sie diese Aufgaben nacheinander ausführen, haben Sie die `Get-TrustAuthorityCluster`-Informationen zuvor einer Variable zugewiesen (z. B. `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

Die `$kp`-Variable erhält die vertrauenswürdigen Schlüsselanbieter im Trust Authority-Cluster, in diesem Fall `$vTA`.

Hinweis Wenn Sie über mehrere vertrauenswürdige Schlüsselanbieter verfügen, verwenden Sie Befehle ähnlich den folgenden, um den gewünschten Anbieter auszuwählen:

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

Mit `Select-Object -Last 1` wird der letzte vertrauenswürdige Schlüsselanbieter in der Liste angezeigt.

4 Laden Sie das Zertifikat und den privaten Schlüssel mithilfe des Befehls `Set-TrustAuthorityKeyProviderClientCertificate` hoch.

Beispiel:

```
Set-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -CertificateFilePath
<path/to/certfile.pem> -PrivateKeyFilePath <path/to/privatekey.pem>
```

Ergebnisse

Der vertrauenswürdige Schlüsselanbieter hat eine Vertrauensstellung mit dem Schlüsselserver hergestellt.

Eine Zertifikatssignieranforderung zum Herstellen einer vertrauenswürdigen Schlüsselanbieter-Verbindung erstellen

Bestimmte Schlüsselserveranbieter (KMS) verlangen, dass eine Zertifikatssignieranforderung (Certificate Signing Request, CSR) generiert und an den Schlüsselserveranbieter übermittelt wird. Der Schlüsselserveranbieter signiert die Zertifikatssignieranforderung und sendet das signierte Zertifikat zurück. Nachdem Sie dieses signierte Zertifikat als Clientzertifikat des vertrauenswürdigen Schlüsselanbieters konfiguriert haben, akzeptiert der Schlüsselserveranbieter den Datenverkehr, der vom vertrauenswürdigen Schlüsselanbieter stammt.

Bei dieser Aufgabe handelt es sich um einen zweistufigen Prozess. Zuerst generieren Sie die Zertifikatssignieranforderung und senden diese an den Schlüsselserveranbieter. Anschließend laden Sie das signierte Zertifikat hoch, das Sie vom Schlüsselserveranbieter erhalten haben.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.
- Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.
- Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.
- Erstellen des Schlüsselanbieters im Trust Authority-Cluster.

Verfahren

1 Stellen Sie sicher, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind. Sie können beispielsweise `$global:defaultviservers` eingeben, um alle verbundenen Server anzuzeigen.

2 (Optional) Sie können gegebenenfalls die folgenden Befehle ausführen, um sicherzustellen, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 Weisen Sie die `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA-` Informationen einer Variable zu.

Beispiel:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

Wenn Sie diese Aufgaben nacheinander ausführen, haben Sie die `Get-TrustAuthorityCluster`-Informationen zuvor einer Variable zugewiesen (z. B. `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

Diese Variable erhält die vertrauenswürdigen Schlüsselanbieter im Trust Authority-Cluster, in diesem Fall `$vTA`.

Hinweis Wenn Sie über mehrere vertrauenswürdige Schlüsselanbieter verfügen, verwenden Sie Befehle ähnlich den folgenden, um den gewünschten Anbieter auszuwählen:

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

Mit `Select-Object -Last 1` wird der letzte vertrauenswürdige Schlüsselanbieter in der Liste angezeigt.

4 Verwenden Sie zum Generieren einer CSR das `New-TrustAuthorityKeyProviderClientCertificateCSR`-Cmdlet.

Beispiel:

```
New-TrustAuthorityKeyProviderClientCertificateCSR -KeyProvider $kp
```

Die CSR wird angezeigt. Sie können auch das `Get-TrustAuthorityKeyProviderClientCertificateCSR -KeyProvider $kp`-Cmdlet verwenden, um die CSR zu erhalten.

5 Um ein signiertes Zertifikat zu erhalten, übermitteln Sie die CSR an Ihren Schlüsselserveranbieter.

Das Zertifikat muss im PEM-Format sein. Wenn das Zertifikat in einem anderen Format als PEM zurückgegeben wird, konvertieren Sie es mithilfe des Befehls `openssl` in PEM. Beispiel:

- So konvertieren Sie ein Zertifikat vom CRT- in das PEM-Format:

```
openssl x509 -in clientcert.crt -out clientcert.pem -outform PEM
```

- So konvertieren Sie ein Zertifikat vom DER- in das PEM-Format:

```
openssl x509 -inform DER -in clientcert.der -out clientcert.pem
```

6 Wenn Sie das signierte Zertifikat vom Schlüsselserveranbieter erhalten, laden Sie das Zertifikat mithilfe des `Set-TrustAuthorityKeyProviderClientCertificate`-Cmdlet auf den Schlüsselserver hoch.

Beispiel:

```
Set-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -CertificateFilePath
<path/tp/certfile.pem>
```

Ergebnisse

Der vertrauenswürdige Schlüsselanbieter hat eine Vertrauensstellung mit dem Schlüsselserver hergestellt.

Exportieren der Informationen des Trust Authority-Clusters

Damit der vertrauenswürdige Cluster eine Verbindung mit dem vSphere Trust Authority-Cluster herstellen kann, müssen Sie die Dienstinformationen des Trust Authority-Clusters in Form einer Datei exportieren und diese Datei dann in den vertrauenswürdigen Cluster importieren. Sie müssen sicherstellen, dass diese Datei vertraulich behandelt und sicher übertragen wird.

Während Sie diese Aufgaben in der angegebenen Reihenfolge ausführen, bleiben Sie weiterhin mit dem vCenter Server des Trust Authority-Clusters verbunden.

Hinweis Speichern Sie die exportierte Datei mit den Dienstinformationen an einem sicheren Ort für den Fall, dass Sie die vSphere Trust Authority-Konfiguration wiederherstellen müssen.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.
- Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.
- Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.
- Erstellen des Schlüsselanbieters im Trust Authority-Cluster.

Verfahren

1. Stellen Sie sicher, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind. Sie können beispielsweise `$global:defaultviservers` eingeben, um alle verbundenen Server anzuzeigen.
2. (Optional) Sie können gegebenenfalls die folgenden Befehle ausführen, um sicherzustellen, dass Sie mit dem vCenter Server des Trust Authority-Clusters verbunden sind.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
   -Password 'password'
   ```

3. Führen Sie das `Export-TrustAuthorityServicesInfo`-Cmdlet aus, um die im Trust Authority-Cluster enthaltenen Informationen des Bestätigungs- und Schlüsselanbieterdiensts zu exportieren.

   Mit diesem Befehl werden die Dienstinformationen beispielsweise in die Datei `clsettings.json` exportiert. Wenn Sie diese Aufgaben nacheinander ausführen, haben Sie die `Get-TrustAuthorityCluster`-Information zuvor einer Variable zugewiesen (z. B. `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

   ```
   Export-TrustAuthorityServicesInfo -TrustAuthorityCluster $vTA -FilePath
   C:\vta\clsettings.json
   ```

   Die Datei wird erstellt.

Ergebnisse

Eine Datei mit Informationen zum Trust Authority-Cluster wird erstellt.

Beispiel: Exportieren der Informationen des Trust Authority-Clusters

In diesem Beispiel wird die Verwendung der PowerCLI zum Exportieren der Dienstinformationen des Trust Authority-Clusters erläutert. In der folgenden Tabelle werden die verwendeten Beispielkomponenten und -werte angezeigt.

Tabelle 9-9. Beispiel eines vSphere Trust Authority-Setups

Komponente	Wert
Variable `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
vCenter Server für Trust Authority-Cluster	192.168.210.22
Trust Authority-Administrator	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

PS C:\Users\Administrator.CORP> Export-TrustAuthorityServicesInfo -TrustAuthorityCluster $vTA
-FilePath C:\vta\clsettings.json
```

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----       10/16/2019   9:59 PM           8177 clsettings.json
```

Nächste Schritte

Fahren Sie mit Importieren der Informationen des Trust Authority-Clusters in die vertrauenswürdigen Hosts fort.

Importieren der Informationen des Trust Authority-Clusters in die vertrauenswürdigen Hosts

Nachdem Sie die Informationen des vSphere Trust Authority-Clusters in den vertrauenswürdigen Cluster importiert haben, starten die vertrauenswürdigen Hosts den Bestätigungsvorgang mit dem Trust Authority-Cluster.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.
- Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.
- Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.
- Erstellen des Schlüsselanbieters im Trust Authority-Cluster.
- Exportieren der Informationen des Trust Authority-Clusters.

Verfahren

1. Stellen Sie sicher, dass Sie als Trust Authority-Administrator mit dem vCenter Server des vertrauenswürdigen Clusters verbunden sind.

   Sie können beispielsweise `$global:defaultviservers` eingeben, um alle verbundenen Server anzuzeigen.

2. (Optional) Sie können gegebenenfalls die folgenden Befehle ausführen, um sicherzustellen, dass Sie mit dem vCenter Server des vertrauenswürdigen Clusters verbunden sind.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password
   'password'
   ```

   Hinweis Alternativ können Sie eine weitere PowerCLI-Sitzung starten, um eine Verbindung mit dem vCenter Server des vertrauenswürdigen Clusters herzustellen.

3 Stellen Sie sicher, dass der Status des vertrauenswürdigen Clusters auf „Deaktiviert“ gesetzt ist.

```
Get-TrustedCluster
```

Der Status wird als „Deaktiviert“ angezeigt.

4 Weisen Sie die `Get-TrustedCluster`-Informationen einer Variable zu.

Beispielsweise weist dieser Befehl Informationen für den Cluster `Trusted Cluster` der Variable `$TC` zu.

```
$TC = Get-TrustedCluster -Name 'Trusted Cluster'
```

5 Bestätigen Sie den Wert der Variable durch erneute Eingabe.

Beispiel:

```
$TC
```

Die `Get-TrustedCluster`-Informationen werden angezeigt.

6 Um die Informationen zum Trust Authority-Cluster in den vCenter Server zu exportieren, führen Sie das `Import-TrustAuthorityServicesInfo`-Cmdlet aus.

Beispiel: Mit diesem Befehl werden die Dienstinformationen aus der Datei `clsettings.json` importiert, die zuvor in Exportieren der Informationen des Trust Authority-Clusters exportiert wurde.

```
Import-TrustAuthorityServicesInfo -FilePath C:\vta\clsettings.json
```

Das System antwortet mit einer Bestätigungsaufforderung.

```
Confirmation
Importing the TrustAuthorityServicesInfo into Server 'ip_address'. Do you want to proceed?

[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

7 Drücken Sie an der Bestätigungsaufforderung die Eingabetaste. (Der Standardwert lautet **`Y`**.)

Die Dienstinformationen für die Hosts im Trust Authority-Cluster werden angezeigt.

8 Um den vertrauenswürdigen Cluster zu aktivieren, führen Sie das `Set-TrustedCluster`-Cmdlet aus.

Beispiel:

```
Set-TrustedCluster -TrustedCluster $TC -State Enabled
```

Das System antwortet mit einer Bestätigungsaufforderung.

```
Confirmation
Setting TrustedCluster 'cluster' with new TrustedState 'Enabled'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

Wenn sich der vertrauenswürdige Cluster nicht in einem fehlerfreien Zustand befindet, wird die folgende Warnmeldung vor der Bestätigungsmeldung angezeigt:

```
WARNING: The TrustedCluster 'cluster' is not healthy in its TrustedClusterAppliedStatus.
This cmdlet will automatically remediate the TrustedCluster.
```

9 Drücken Sie an der Bestätigungsaufforderung die Eingabetaste. (Der Standardwert lautet **Y**.)

Der vertrauenswürdige Cluster ist aktiviert.

Hinweis Sie können den vertrauenswürdigen Cluster auch aktivieren, indem Sie den Bestätigungsdienst und den Schlüsselanbieterdienst einzeln aktivieren. Verwenden Sie die folgenden Befehle: `Add-TrustedClusterAttestationServiceInfo` und `Add-TrustedClusterKeyProviderServiceInfo`. Beispielsweise können die folgenden Befehle die Dienste einzeln für den Cluster `Trusted Cluster` aktivieren, der über zwei Schlüsselanbieter- und zwei Nachweisdienste verfügt.

```
Add-TrustedClusterAttestationServiceInfo -TrustedCluster 'Trusted Cluster'
-AttestationServiceInfo (Get-AttestationServiceInfo | Select-Object -index 0,1)
Add-TrustedClusterKeyProviderServiceInfo  -TrustedCluster 'Trusted Cluster'
-KeyProviderServiceInfo (Get-KeyProviderServiceInfo | Select-Object -index 0,1)
```

---

10 Stellen Sie sicher, dass der Nachweis- und Schlüsselanbieterdienst im vertrauenswürdigen Cluster konfiguriert sind.

a Weisen Sie die `Get-TrustedCluster`-Informationen einer Variable zu.

Beispielsweise weist dieser Befehl Informationen für den Cluster `Trusted Cluster` der Variable `$TC` zu.

```
$TC = Get-TrustedCluster -Name 'Trusted Cluster'
```

b Stellen Sie sicher, dass der Bestätigungsdienst konfiguriert ist.

```
$tc.AttestationServiceInfo
```

Die Informationen des Bestätigungsdiensts werden angezeigt.

c Stellen Sie sicher, dass der Schlüsselanbieterserver konfiguriert ist.

```
$tc.KeyProviderServiceInfo
```

Die Informationen des Schlüsselanbieterdiensts werden angezeigt.

Ergebnisse

Die vertrauenswürdigen ESXi-Hosts im vertrauenswürdigen Cluster starten den Bestätigungsvorgang mit dem Trust Authority-Cluster.

Beispiel: Importieren der Informationen des Trust Authority-Clusters in die vertrauenswürdigen Hosts

Dieses Beispiel zeigt, wie die Dienstinformationen des Trust Authority-Clusters in den vertrauenswürdigen Cluster importiert werden. In der folgenden Tabelle werden die verwendeten Beispielkomponenten und -werte angezeigt.

Tabelle 9-10. Beispiel eines vSphere Trust Authority-Setups

Komponente	Wert
vCenter Server des vertrauenswürdigen Clusters	192.168.110.22
Trust Authority-Administrator	trustedadmin@vsphere.local
Name des vertrauenswürdigen Clusters	Vertrauenswürdiger Cluster
ESXi-Hosts im Trust Authority-Cluster	192.168.210.51 und 192.168.210.52
Variable `$TC`	`Get-TrustedCluster -Name 'Trusted Cluster'`

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.22                 443   VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Get-TrustedCluster

Name                   State             Id
----                   -----             --
Trusted Cluster        Disabled          TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> $TC = Get-TrustedCluster -Name 'Trusted Cluster'
PS C:\Users\Administrator.CORP> $TC

Name                   State             Id
----                   -----             --
Trusted Cluster        Disabled          TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> Import-TrustAuthorityServicesInfo -FilePath
C:\vta\clsettings.json

Confirmation
Importing the TrustAuthorityServicesInfo into Server '192.168.110.22'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

ServiceAddress                 ServicePort          ServiceGroup
```

```
--------------                  -----------          ------------
192.168.210.51                  443                  host-13:86f7ab6c-ad6f-4606-...
192.168.210.52                  443                  host-16:86f7ab6c-ad6f-4606-...
192.168.210.51                  443                  host-13:86f7ab6c-ad6f-4606-...
192.168.210.52                  443                  host-16:86f7ab6c-ad6f-4606-...

PS C:\Users\Administrator.CORP> Set-TrustedCluster -TrustedCluster $TC -State Enabled

Confirmation
Setting TrustedCluster 'Trusted Cluster' with new TrustedState 'Enabled'. Do you want to
proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):

Name                  State             Id
----                  -----             --
Trusted Cluster       Enabled           TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> $TC = Get-TrustedCluster -Name 'Trusted Cluster'
PS C:\Users\Administrator.CORP> $tc.AttestationServiceInfo

ServiceAddress                  ServicePort          ServiceGroup
--------------                  -----------          ------------
192.168.210.51                  443                  host-13:dc825986-73d2-463c-...
192.168.210.52                  443                  host-16:dc825986-73d2-463c-...

PS C:\Users\Administrator.CORP> $tc.KeyProviderServiceInfo

ServiceAddress                  ServicePort          ServiceGroup
--------------                  -----------          ------------
192.168.210.51                  443                  host-13:dc825986-73d2-463c-...
192.168.210.52                  443                  host-16:dc825986-73d2-463c-...
```

Nächste Schritte

Fahren Sie mit Konfigurieren des vertrauenswürdigen Schlüsselanbieters für vertrauenswürdige Hosts mithilfe des vSphere Client oder Konfigurieren des vertrauenswürdigen Schlüsselanbieters für vertrauenswürdige Hosts mithilfe der Befehlszeile fort.

Konfigurieren des vertrauenswürdigen Schlüsselanbieters für vertrauenswürdige Hosts mithilfe des vSphere Client

Sie können den vertrauenswürdigen Schlüsselanbieter mithilfe des vSphere Client konfigurieren.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.
- Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.
- Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.
- Erstellen des Schlüsselanbieters im Trust Authority-Cluster.

- Exportieren der Informationen des Trust Authority-Clusters.
- Importieren der Informationen des Trust Authority-Clusters in die vertrauenswürdigen Hosts.

Verfahren

1. Stellen Sie eine Verbindung zum vCenter Server des vertrauenswürdigen Clusters mithilfe des vSphere Client her.
2. Melden Sie sich als vCenter Server-Administrator oder als Administrator an, der über die Berechtigung **Kryptografievorgänge.Schlüsselserver verwalten** verfügt.
3. Wählen Sie den vCenter Server und dann **Konfigurieren** aus.
4. Wählen Sie **Schlüsselanbieter** unter **Sicherheit** aus.
5. Wählen Sie **Vertrauenswürdige Schlüsselanbieter hinzufügen** aus.

   Die verfügbaren vertrauenswürdigen Schlüsselanbieter werden mit dem Status „Verbunden“ angezeigt.
6. Wählen Sie einen vertrauenswürdigen Schlüsselanbieter aus und klicken Sie auf **Schlüsselanbieter hinzufügen**.

   Der vertrauenswürdige Schlüsselanbieter wird als „Vertrauenswürdig“ und „Verbunden“ angezeigt. Wenn dies der erste vertrauenswürdige Schlüsselanbieter ist, den Sie hinzufügen, wird er als Standard gekennzeichnet.

   Hinweis Es dauert eine gewisse Zeit, bis alle Hosts den Schlüsselanbieter abrufen können und der vCenter Server den zugehörigen Cache aktualisieren kann. Aufgrund der Art und Weise der Informationsweiterleitung müssen Sie unter Umständen einige Minuten warten, bis Sie den Schlüsselanbieter für wichtige Vorgänge auf bestimmten Hosts verwenden können.

Ergebnisse

ESXi Vertrauenswürdige Hosts können nun Kryptografievorgänge durchführen, wie z. B. das Erstellen verschlüsselter virtueller Maschinen.

Nächste Schritte

Das Verschlüsseln einer virtuellen Maschine mit einem vertrauenswürdigen Schlüsselanbieter entspricht der Benutzererfahrung bei der VM-Verschlüsselung, die erstmals in vSphere 6.5 bereitgestellt wurde. Weitere Informationen finden Sie unter Kapitel 10 Verwenden von Verschlüsselung in Ihrer vSphere-Umgebung.

Konfigurieren des vertrauenswürdigen Schlüsselanbieters für vertrauenswürdige Hosts mithilfe der Befehlszeile

Sie können vertrauenswürdige Schlüsselanbieter über die Befehlszeile konfigurieren. Sie können den vertrauenswürdigen Standardschlüsselanbieter für den vCenter Server oder auf Cluster- oder Ordnerebene in der vCenter-Objekthierarchie konfigurieren.

Voraussetzungen

- Aktivieren des Trust Authority-Administrators.
- Aktivieren des Trust Authority-Status.
- Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.
- Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.
- Erstellen des Schlüsselanbieters im Trust Authority-Cluster.
- Exportieren der Informationen des Trust Authority-Clusters.
- Importieren der Informationen des Trust Authority-Clusters in die vertrauenswürdigen Hosts.

Auf dem vertrauenswürdigen Cluster müssen Sie über eine Rolle verfügen, die das **Verschlüsselungsvorgänge.KMS verwalten**-Recht enthält.

Verfahren

1. Stellen Sie sicher, dass Sie als Administrator mit dem vCenter Server des vertrauenswürdigen Clusters verbunden sind.

   Sie können beispielsweise `$global:defaultviservers` eingeben, um alle verbundenen Server anzuzeigen.

2. (Optional) Sie können gegebenenfalls die folgenden Befehle ausführen, um sicherzustellen, dass Sie mit dem vCenter Server des vertrauenswürdigen Clusters verbunden sind.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustedCluster_VC_ip_address -User admin_user -Password 'password'
   ```

3. Rufen Sie den vertrauenswürdigen Schlüsselanbieter ab.

   ```
   Get-KeyProvider
   ```

   Sie können die Option `-Name` *keyprovider* verwenden, um einen einzelnen vertrauenswürdigen Schlüsselanbieter anzugeben.

4. Weisen Sie die Informationen über den vertrauenswürdigen `Get-KeyProvider`-Schlüsselanbieter einer Variable zu.

   Beispiel: Dieser Befehl weist die Informationen der Variable `$workload_kp` zu.

   ```
   $workload_kp = Get-KeyProvider
   ```

   Wenn Sie über mehrere vertrauenswürdige Schlüsselanbieter verfügen, können Sie `Select-Object` verwenden, um einen davon auszuwählen.

   ```
   $workload_kp = Get-KeyProvider | Select-Object -Index 0
   ```

5 Registrieren Sie den vertrauenswürdigen Schlüsselanbieter.

```
Register-KeyProvider -KeyProvider $workload_kp
```

Um weitere vertrauenswürdige Schlüsselanbieter zu registrieren, wiederholen Sie die Schritte 4 und 5.

Hinweis Es dauert eine gewisse Zeit, bis alle Hosts den Schlüsselanbieter abrufen können und der vCenter Server den zugehörigen Cache aktualisieren kann. Aufgrund der Art und Weise der Informationsweiterleitung müssen Sie unter Umständen einige Minuten warten, bis Sie den Schlüsselanbieter für wichtige Vorgänge auf bestimmten Hosts verwenden können.

6 Legen Sie den zu verwendenden vertrauenswürdigen Standardschlüsselanbieter fest.

a Führen Sie folgenden Befehl aus, um den Standardschlüsselanbieter auf der vCenter Server-Ebene festzulegen.

```
Set-KeyProvider -KeyProvider $workload_kp -DefaultForSystem
```

b Führen Sie folgenden Befehl aus, um den Schlüsselanbieter auf Clusterebene festzulegen.

Dieser Befehl legt beispielsweise den Schlüsselanbieter für den `Trusted Cluster`-Cluster fest.

```
Add-EntityDefaultKeyProvider -KeyProvider $workload_kp -Entity 'Trusted Cluster'
```

c Führen Sie folgenden Befehl aus, um den Schlüsselanbieter auf Ordnerebene festzulegen.

Dieser Befehl beispielsweise legt den Schlüsselanbieter für den Ordner `TC Folder` fest, der auf dem `workLoad`-Datencenter erstellt wurde.

```
Add-EntityDefaultKeyProvider -KeyProvider $workload_kp -Entity 'TC Folder'
```

Nächste Schritte

Das Verschlüsseln einer virtuellen Maschine mit einem vertrauenswürdigen Schlüsselanbieter entspricht der Benutzererfahrung bei der VM-Verschlüsselung, die erstmals in vSphere 6.5 bereitgestellt wurde. Weitere Informationen finden Sie unter Kapitel 10 Verwenden von Verschlüsselung in Ihrer vSphere-Umgebung.

Verwalten vSphere Trust Authority in Ihrer vSphere-Umgebung

Nach dem Konfigurieren von vSphere Trust Authority können Sie zusätzliche Vorgänge durchführen, wie z. B. Starten und Anhalten der Dienste, Hinzufügen von Hosts zu Clustern und Anzeigen des Status des Trust Authority-Clusters.

Sie können Aufgaben mithilfe des vSphere Client, der API und der PowerCLI-Cmdlets ausführen. Weitere Informationen finden Sie im *Programmierhandbuch zum vSphere Web Services SDK*, in der *VMware PowerCLI*-Dokumentation und in der *Referenz zu VMware PowerCLI-Cmdlets*.

Starten, Stoppen und Neustarten von vSphere Trust Authority-Diensten

Sie können vSphere Trust Authority-Dienste mithilfe des vSphere Client starten, beenden und neu starten.

Die Dienste, aus denen sich vSphere Trust Authority zusammensetzt, sind der Bestätigungsdienst (attestd) und der Schlüsselanbieterdienst (kmxd).

Verfahren

1. Stellen Sie eine Verbindung zum vCenter Server des vSphere Trust Authority-Clusters her, indem Sie den vSphere Client verwenden.
2. Melden Sie sich als Administrator an.
3. Navigieren Sie zu einem ESXi-Host im Trust Authority-Cluster.
4. Klicken Sie auf **Konfigurieren** und dann unter **System** auf **Dienste**.
5. Suchen Sie nach dem attestd- und dem kmxd-Dienst.
6. Wählen Sie je nach Bedarf die Option **Neustarten**, **Starten** oder **Beenden** aus.

Anzeigen der Trust Authority-Hosts

Sie können die für einen vertrauenswürdigen Cluster konfigurierten vSphere Trust Authority-Hosts mithilfe des vSphere Client anzeigen.

Verfahren

1. Stellen Sie eine Verbindung zum vCenter Server des vertrauenswürdigen Clusters mithilfe des vSphere Client her.
2. Melden Sie sich als Administrator an.
3. Wählen Sie die vCenter Server-Instanz aus.
4. Klicken Sie auf die Registerkarte **Konfigurieren** und wählen Sie **Trust Authority** unter **Sicherheit** aus.

   Die für den vertrauenswürdigen Cluster konfigurierten ESXi-Hosts im Trust Authority-Cluster werden angezeigt.

Anzeigen des Status des vSphere Trust Authority-Clusters

Sie können den Status des vSphere Trust Authority-Clusters mithilfe des vSphere Client anzeigen. Der Status lautet entweder „Aktiviert“ oder „Deaktiviert“.

Wenn der Status des Trust Authority-Clusters „Aktiviert“ ist, können die vertrauenswürdigen Hosts im vertrauenswürdigen Cluster mit dem Bestätigungs- und dem Schlüsselanbieterdienst kommunizieren.

Verfahren

1. Stellen Sie eine Verbindung zum vSphere Client des Trust Authority-Clusters her, indem Sie den vCenter Server verwenden.
2. Melden Sie sich als Administrator an.
3. Wählen Sie den Trust Authority-Cluster in der Objekthierarchie aus.
4. Klicken Sie auf die Registerkarte **Konfigurieren** und wählen Sie **Trust Authority-Cluster** unter **Trust Authority** aus.

   Der Status wird als „Aktiviert“ oder „Deaktiviert“ angezeigt.

Neustarten des Diensts für vertrauenswürdige Hosts

Sie können den Dienst, der auf Ihren vertrauenswürdigen Hosts ausgeführt wird, neu starten.

Der kmxa-Dienst wird auf den vertrauenswürdigen ESXi-Hosts ausgeführt.

Voraussetzungen

Zugriff auf die ESXi Shell muss aktiviert sein. Weitere Informationen hierzu finden Sie unter Aktivieren des Zugriffs auf die ESXi Shell.

Verfahren

1. Verwenden Sie SSH oder eine andere Remotekonsolenverbindung, um eine Sitzung auf dem vertrauenswürdigen ESXi-Host zu starten.
2. Melden Sie sich als „root“ an.
3. Führen Sie den folgenden Befehl aus.

   ```
   /etc/init.d/kmxa restart
   ```

Hinzufügen und Entfernen von vSphere Trust Authority-Hosts

Sie fügen ESXi-Hosts einem vSphere Trust Authority-Cluster hinzu und entfernen sie mithilfe von Skripts, die seitens VMware bereitgestellt werden.

In vSphere 7.0 fügen Sie ESXi-Hosts einem vorhandenen vSphere Trust Authority-Cluster oder einem vertrauenswürdigen Cluster hinzu und entfernen sie mithilfe von Skripts, die seitens VMware bereitgestellt werden. Ab vSphere 7.0 Update 1 verwenden Sie die Standardisierungsfunktion, um ESXi-Hosts einem vertrauenswürdigen Cluster hinzuzufügen. Siehe Hinzufügen eines Hosts zu einem vertrauenswürdigen Cluster mit dem vSphere Client und

Hinzufügen eines Hosts zu einem vertrauenswürdigen Cluster mit der CLI. In vSphere 7.0 Update 1 müssen Sie weiterhin Skripts verwenden, um ESXi-Hosts einem vorhandenen Trust Authority-Cluster hinzuzufügen. Weitere Informationen finden Sie in den VMware-Knowledgebase-Artikeln unter https://kb.vmware.com/s/article/77234 und https://kb.vmware.com/s/article/77146.

Hinzufügen eines Hosts zu einem vertrauenswürdigen Cluster mit dem vSphere Client

Sie können ESXi-Hosts mithilfe des vSphere Client einem vorhandenen vertrauenswürdigen Cluster hinzufügen.

Nachdem Sie zunächst einen vertrauenswürdigen Cluster konfiguriert haben, möchten Sie unter Umständen weitere ESXi-Hosts hinzufügen. Wenn Sie den Host jedoch einem vertrauenswürdigen Cluster hinzufügen, müssen Sie in einem zusätzlichen Schritt eine Standardisierung durchführen. Stellen Sie beim Standardisieren des vertrauenswürdigen Clusters sicher, dass der gewünschte Konfigurationszustand mit der angewendeten Konfiguration übereinstimmt.

In der ersten in vSphere 7.0 veröffentlichten Version von vSphere Trust Authority können Sie Skripts zum Hinzufügen eines Hosts zu einem vertrauenswürdigen Cluster ausführen. Ab vSphere 7.0 Update 1 verwenden Sie die Standardisierungsfunktion, um einem vertrauenswürdigen Cluster einen Host hinzuzufügen. In vSphere 7.0 Update 1 müssen Sie weiterhin Skripts verwenden, um einen Host zu einem vorhandenen Trust Authority-Cluster hinzuzufügen. Weitere Informationen hierzu finden Sie unter Hinzufügen und Entfernen von vSphere Trust Authority-Hosts.

Voraussetzungen

Auf dem vCenter Server für den vertrauenswürdigen Cluster muss vSphere 7.0 Update 1 oder höher ausgeführt werden.

Wenn Sie einen ESXi-Host mit einer anderen ESXi-Version oder einem anderen TPM-Hardwaretyp als dem anfänglich für den vertrauenswürdigen Cluster konfigurierten Typ hinzufügen, sind weitere Schritte notwendig. Sie müssen diese Informationen in den vSphere Trust Authority-Cluster importieren oder daraus exportieren. Siehe Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server und Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.

Notwendige Berechtigungen: Weitere Informationen finden Sie in den Aufgaben zum Hinzufügen von Hosts unter Erforderliche Berechtigungen für allgemeine Aufgaben

Verfahren

1. Stellen Sie eine Verbindung zum vCenter Server des vertrauenswürdigen Clusters mithilfe des vSphere Client her.
2. Melden Sie sich als Trust Authority-Administrator an.
3. Navigieren Sie zu einem vertrauenswürdigen Cluster.
4. Wählen Sie auf der Registerkarte **Konfigurieren** die Option **Konfiguration > Schnellstart** aus.

5 Klicken Sie auf der Karte **Hosts hinzufügen** auf **Hinzufügen**.

6 Führen Sie die angezeigten Anweisungen aus.

7 Klicken Sie auf der Registerkarte **Trust Authority** auf **Standardisieren**.

8 Um sicherzustellen, dass der vertrauenswürdige Cluster fehlerfrei ist, klicken Sie auf **Integrität überprüfen**.

Hinzufügen eines Hosts zu einem vertrauenswürdigen Cluster mit der CLI

Sie können ESXi-Hosts mithilfe der Befehlszeile einem vorhandenen vertrauenswürdigen Cluster hinzufügen.

Nachdem Sie zunächst einen vertrauenswürdigen Cluster konfiguriert haben, möchten Sie unter Umständen weitere ESXi-Hosts hinzufügen. Wenn Sie den Host jedoch einem vertrauenswürdigen Cluster hinzufügen, müssen Sie in einem zusätzlichen Schritt eine Standardisierung durchführen. Stellen Sie beim Standardisieren des vertrauenswürdigen Clusters sicher, dass der gewünschte Konfigurationszustand mit der angewendeten Konfiguration übereinstimmt.

In der ersten in vSphere 7.0 veröffentlichten Version von vSphere Trust Authority können Sie Skripts zum Hinzufügen eines Hosts zu einem vertrauenswürdigen Cluster ausführen. Ab vSphere 7.0 Update 1 verwenden Sie die Standardisierungsfunktion, um einen vertrauenswürdigen Host hinzuzufügen. In vSphere 7.0 Update 1 müssen Sie weiterhin Skripts verwenden, um einen Host zu einem vorhandenen Trust Authority-Cluster hinzuzufügen. Weitere Informationen hierzu finden Sie unter Hinzufügen und Entfernen von vSphere Trust Authority-Hosts.

Voraussetzungen

- Auf dem vCenter Server für den vertrauenswürdigen Cluster muss vSphere 7.0 Update 1 oder höher ausgeführt werden.
- PowerCLI 12.1.0 oder höher ist notwendig.
- Notwendige Berechtigungen: Weitere Informationen finden Sie in den Aufgaben zum Hinzufügen von Hosts unter Erforderliche Berechtigungen für allgemeine Aufgaben

Verfahren

1 Führen Sie alle üblichen Schritte aus, um den ESXi-Host zum vertrauenswürdigen Cluster hinzuzufügen.

2 In einer PowerCLI-Sitzung führen Sie das Cmdlet `Connect-VIServer` aus, um als Trust Authority-Administrator eine Verbindung mit dem vCenter Server des vertrauenswürdigen Clusters herzustellen.

```
Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password
'password'
```

3 Führen Sie zum Überprüfen des Status des vertrauenswürdigen Clusters das PowerCLI-cmdlet `Get-TrustedClusterAppliedStatus` aus.

```
Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'
```

4 Wenn der vertrauenswürdige Cluster fehlerhaft ist, sollten Sie das Cmdlet `Set-TrustedCluster` mit dem Parameter `-Remediate` ausführen.

```
Set-TrustedCluster -TrustedCluster 'TrustedCluster' -Remediate
```

5 Um sicherzustellen, dass der vertrauenswürdige Cluster fehlerfrei ist, führen Sie das Cmdlet `Get-TrustedClusterAppliedStatus` erneut aus.

```
Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'
```

Stilllegen vertrauenswürdiger Hosts in einem vertrauenswürdigen Cluster

Sie können vertrauenswürdige Hosts aus einem vertrauenswürdigen Cluster entfernen oder stilllegen. Sie können je nach Szenario einen oder alle vertrauenswürdigen Hosts in einem vertrauenswürdigen Cluster stilllegen.

Wenn Sie einen vertrauenswürdigen Host stilllegen, legt die Standardisierungsfunktion den gewünschten Status des vertrauenswürdigen Hosts auf den des nicht vertrauenswürdigen Clusters fest, auf den der Host verschoben wird. Der stillgelegte vertrauenswürdige Host wird zu einem regulären Host. Der vertrauenswürdige Cluster (aus dem der vertrauenswürdige Host verschoben wurde) verfügt weiterhin über die gewünschte Statuskonfiguration und fungiert auch weiterhin als vertrauenswürdiger Cluster.

Wenn Sie alle vertrauenswürdigen Hosts aus einem vertrauenswürdigen Cluster entfernen, legen Sie den vertrauenswürdigen Cluster still. Sie entfernen sowohl die gewünschte Statuskonfiguration als auch die angewendete Konfiguration aus den vertrauenswürdigen Hosts und dem vertrauenswürdigen Cluster und verschieben dann alle vertrauenswürdigen Hosts in einen nicht vertrauenswürdigen Cluster.

Sie können stillgelegte vertrauenswürdige Hosts in Ihrer Umgebung wiederverwenden. Beispielsweise können Sie die Hosts in einer nicht vertrauenswürdigen Infrastrukturkapazität oder als vSphere Trust Authority-Hosts wiederverwenden. Sie können die stillgelegten Hosts im selben vCenter Server oder einem anderen vCenter Server verwenden.

Weitere Informationen zur Konfiguration und Integrität des vertrauenswürdigen Clusters finden Sie unter Übersicht über die Clusterintegrität und Standardisierung.

Voraussetzungen

- Auf dem vCenter Server für den vertrauenswürdigen Cluster muss vSphere 7.0 Update 1 oder höher ausgeführt werden.
- Bei Verwendung von PowerCLI wird Version 12.1.0 oder höher benötigt.

Verfahren

1 Stellen Sie eine Verbindung zum vCenter Server des vertrauenswürdigen Clusters mithilfe des vSphere Client her.

2 Melden Sie sich als Trust Authority-Administrator an.

3 Navigieren Sie zu einem vertrauenswürdigen Cluster.

4 Legen Sie fest, wie die vertrauenswürdigen Hosts im vertrauenswürdigen Cluster stillgelegt werden sollen.

Aufgabe	Schritte
Beibehalten des gewünschten Konfigurationsstatus des vertrauenswürdigen Clusters und der verbleibenden vertrauenswürdigen Hosts	a Versetzen Sie die Hosts in den Wartungsmodus und verschieben Sie sie in einen neuen, leeren Cluster (d. h., der Cluster enthält keine Hosts). b Beenden Sie den Wartungsmodus auf den Hosts. c Klicken Sie für den neuen, leeren Cluster (nicht den vertrauenswürdigen Cluster) auf der Registerkarte **Trust Authority** auf **Standardisieren**. Bei der Standardisierung wird die vertrauenswürdige Konfiguration aus den verschobenen Hosts entfernt. Der vertrauenswürdige Cluster behält seine gewünschte Statuskonfiguration bei.

Entfernen des gewünschten und des angewendeten Konfigurationsstatus aller vertrauenswürdigen Hosts	a In einer PowerCLI-Sitzung führen Sie das Cmdlet `Connect-VIServer` aus, um als Trust Authority-Administrator eine Verbindung mit dem vCenter Server des vertrauenswürdigen Clusters herzustellen.
	`Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'`
	b Führen Sie das Cmdlet `Set-TrustedCluster` aus. Beispiel:
	`Set-TrustedCluster -TrustedCluster 'TrustedCluster' -State Disabled`
	Die Konfiguration der vertrauenswürdigen Infrastruktur wird aus allen vertrauenswürdigen Hosts entfernt. Außerdem wird die gewünschte Statuskonfiguration des vertrauenswürdigen Clusters entfernt.
	c Versetzen Sie alle Hosts in den Wartungsmodus und verschieben Sie sie in einen anderen Cluster.
	d Beenden Sie den Wartungsmodus auf den Hosts.

5 Um sicherzustellen, dass es sich um einen fehlerfreien vertrauenswürdigen Cluster handelt, klicken Sie auf **Integrität prüfen** auf der Registerkarte **Trust Authority** für den vertrauenswürdigen Cluster.

Nächste Schritte

Wenn Sie die spezifischen Versionen von ESXi oder die TPM-Hardware aus den stillgelegten ESXi-Hosts nicht mehr bestätigen möchten, aktualisieren Sie die Konfiguration des Trust Authority-Clusters, um optimale Sicherheit zu gewährleisten. Informationen finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/77146.

Sichern der vSphere Trust Authority-Konfiguration

Verwenden Sie die Dateien, die Sie beim Konfigurieren von vSphere Trust Authority als Trust Authority-Sicherung exportiert haben. Sie können diese Dateien zum Wiederherstellen einer Trust Authority-Bereitstellung verwenden. Behandeln Sie die Konfigurationsdateien vertraulich und sorgen Sie für eine sichere Übertragung.

Die meisten vSphere Trust Authority-Konfigurations- und -Statusinformationen werden auf den ESXi-Hosts in der ConfigStore-Datenbank gespeichert. Die vCenter Server-Verwaltungsschnittstelle, die Sie zum Sichern einer vCenter Server-Instanz verwenden, führt keine Sicherung der Konfigurationsinformationen für vSphere Trust Authority durch. Wenn Sie die Konfigurationsdateien, die Sie beim Einrichten Ihrer vSphere Trust Authority-Umgebung exportiert haben, sicher speichern, verfügen Sie über die notwendigen Informationen zum Wiederherstellen einer vSphere Trust Authority-Konfiguration. Weitere Informationen für den Fall, dass Sie diese Informationen erzeugen müssen, finden Sie unter Erfassen von Informationen zu ESXi-Hosts und dem vertrauenswürdigen vCenter Server.

Ändern des primären Schlüssels eines Schlüsselanbieters

Sie können den primären Schlüssel eines Schlüsselanbieters ändern, wenn Sie z. B. den verwendeten primären Schlüssel im Turnus wechseln möchten.

Weitere Informationen zu Schlüssellebenszyklen finden Sie unter Virtuelle Maschine – Empfohlene Vorgehensweisen für die Verschlüsselung.

Voraussetzungen

Erstellen und aktivieren Sie einen Schlüssel auf dem Schlüsselserver (KMS), der als neuer primärer Schlüssel für den vertrauenswürdigen Schlüsselanbieter verwendet wird. Dieser Schlüssel umhüllt andere Schlüssel und Geheimnisse, die von diesem vertrauenswürdigen Schlüsselanbieter verwendet werden. Weitere Informationen zum Erstellen von Schlüsseln finden Sie in der Dokumentation Ihres KMS-Anbieters.

Verfahren

1 Führen Sie den Befehl `Set-TrustAuthorityKeyProvider` aus.

   Beispiel:

```
Set-TrustAuthorityKeyProvider -MasterKeyId Key-ID
```

2 Überprüfen Sie den Status des Schlüsselanbieters.

a Weisen Sie `Get-TrustAuthorityCluster`-Informationen einer Variable zu.

Beispiel:

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

b Weisen Sie die `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA`-Informationen einer Variable zu.

Beispiel:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

c Überprüfen Sie den Status des Schlüsselanbieters, indem Sie `$kp.Status` ausführen.

Beispiel:

```
$kp.Status

KeyProviderId Health HealthDetails ServerStatus
------------- ------ ------------- ------------
domain-c8-kp4     Ok {}            {IP_address}
```

Ein Systemzustand von „OK“ weist darauf hin, dass der Schlüsselanbieter ordnungsgemäß ausgeführt wird.

Ergebnisse

Der neue primäre Schlüssel wird für alle neuen Verschlüsselungsvorgänge verwendet. Daten, die mit dem alten primären Schlüssel verschlüsselt wurden, werden nach wie vor mit dem alten Schlüssel entschlüsselt.

Übersicht über Nachweisberichte für vertrauenswürdige Hosts

In vSphere Trust Authority überprüft vCenter Server den Nachweisstatus eines vertrauenswürdigen Hosts und meldet diesen. Sie können den vSphere Client verwenden, um den Nachweisstatus von vertrauenswürdigen Hosts anzuzeigen.

vSphere Trust Authority verwendet Remotebestätigungen für vertrauenswürdige Hosts, um die Echtheit der gestarteten Software zu bestätigen. Mithilfe von Nachweisen wird sichergestellt, dass auf den vertrauenswürdigen Hosts echte VMware-Software oder von VMware signierte Partnersoftware verwendet wird. Der vCenter Server des vertrauenswürdigen Clusters kommuniziert mit dem vertrauenswürdigen Host, um einen internen Nachweisbericht zu erhalten. Der Nachweisbericht gibt an, ob der vertrauenswürdige Host über den auf dem Trust Authority-Cluster ausgeführten Nachweisdienst bestätigt wurde oder nicht. Wenn der vertrauenswürdige Host nicht bestätigt wurde, enthält der Nachweisbericht auch eine Fehlermeldung. Der vSphere Client zeigt die folgenden Nachweisstatus für vertrauenswürdige Hosts an.

Bestanden

Der vertrauenswürdige Host wurde mit einem vSphere Trust Authority-Nachweisdienst bestätigt, und der interne Nachweisbericht steht vCenter Server zur Verfügung.

Fehlgeschlagen

Der vertrauenswürdige Host konnte mit keinem vSphere Trust Authority-Nachweisdienst bestätigt werden. Der interne vCenter Server-Nachweisbericht enthält den Fehler, der vom Nachweisdienst gemeldet wurde, bei dem die Bestätigung des vertrauenswürdigen Hosts versucht wurde.

Der vSphere Client zeigt auch an, ob ein Host von vSphere Trust Authority oder von vCenter Server bestätigt wurde.

Wenn ein vertrauenswürdiger Host nicht bestätigt ist, sind virtuelle Maschinen, einschließlich verschlüsselter virtueller Maschinen, die auf dem vertrauenswürdigen Host ausgeführt werden, weiterhin zugänglich. Virtuelle Maschinen können auf einem nicht bestätigten vertrauenswürdigen Host nicht eingeschaltet werden. Sie können jedoch weiterhin unverschlüsselte virtuelle Maschinen hinzufügen. Wenn ein vertrauenswürdiger Host nicht bestätigt ist, ergreifen Sie die Schritte, um das Nachweisproblem zu beheben. Weitere Informationen zu Nachweiskonzepten finden Sie unter vSphere Trust Authority – Prozessabläufe.

Wenn Sie mehrere Trust Authority-Hosts konfiguriert haben, sind potenziell mehrere Nachweisberichte von jedem Host verfügbar. Wenn Status gemeldet werden, zeigt der vSphere Client den Status des ersten gefundenen „Bestätigt“-Berichts. Wenn keine „Bestätigt“-Berichte vorliegen, zeigt der vSphere Client den Fehler des ersten „Nicht bestätigt“-Bericht, den er findet.

Selbst wenn Sie mehrere vertrauenswürdige Trust Authority-Hosts konfiguriert haben, zeigt der vSphere Client den Status und potenziell eine Fehlermeldung aus nur einem Nachweisbericht an.

Anzeigen des Nachweisstatus des vertrauenswürdigen Clusters

Sie können den Nachweisstatus eines vertrauenswürdigen Hosts mithilfe des vSphere Client anzeigen.

Voraussetzungen

- Sowohl die vertrauenswürdigen Hosts als auch die vSphere Trust Authority-Hosts müssen ESXi Version 7.0 Update 1 oder höher ausführen.
- Die vCenter Server-Hosts für die entsprechenden Cluster müssen vSphere 7.0 Update 1 oder höher ausführen.

Verfahren

1. Stellen Sie eine Verbindung zum vCenter Server des vertrauenswürdigen Clusters mithilfe des vSphere Client her.
2. Melden Sie sich als Administrator an.

   Sie können sich als Trust Authority-Administrator oder als vSphere-Administrator anmelden.
3. Navigieren Sie zu einem Datencenter und klicken Sie auf die Registerkarte **Überwachen**.

4 Klicken Sie auf **Sicherheit**.

5 Überprüfen Sie den Status des vertrauenswürdigen Hosts in der Spalte „Integritätsnachweis“ und lesen Sie die begleitende Nachricht in der Spalte „Nachricht“.

Nächste Schritte

Wenn Fehler auftreten, finden Sie weitere Informationen unter Beheben von Problemen beim Nachweis des vertrauenswürdigen Hosts.

Beheben von Problemen beim Nachweis des vertrauenswürdigen Hosts

Die vSphere Trust Authority-Nachweisberichte bieten einen Ansatzpunkt für die Fehlerbehebung bei der Behebung von Nachweisfehlern für vertrauenswürdige Hosts.

Verfahren

1 Anzeigen des Nachweisstatus des vertrauenswürdigen Clusters.

2 Verwenden Sie die folgende Tabelle, um Fehler zu ermitteln und zu beheben.

Error	Ursache und Lösung
Die Nachweisdienste sind nicht konfiguriert.	Es wurden keine Nachweisdienste konfiguriert. Konfigurieren Sie den vertrauenswürdigen Host für die Verwendung von Nachweisdiensten, indem Sie die Standardisierungsaktion verwenden. Weitere Informationen hierzu finden Sie unter Standardisieren eines vertrauenswürdigen Clusters.
Kein TPM2-Gerät verfügbar.	Installieren und konfigurieren Sie den vertrauenswürdigen Host für die Verwendung eines Trusted Platform Module (TPM). Informationen finden Sie in der Dokumentation des Anbieters.
Öffentlicher TPM2 Endorsement Key oder Zertifikat konnte nicht abgerufen werden.	Stellen Sie sicher, dass das TPM unterstützt wird und dass es über einen gültigen Endorsement Key verfügt. Möglicherweise müssen Sie sich an den VMware Support wenden.
Der Nachweisbericht ist nicht verfügbar.	Es ist möglich, dass der vertrauenswürdige Host den Nachweis noch nicht abgeschlossen hat. Warten Sie einige Minuten, und überprüfen Sie den Nachweisstatus erneut.
Die Nachweisdienstversion ist nicht mit der Anforderung kompatibel.	Aktualisieren Sie den Host der Trust Authority, auf dem der Nachweisdienst ausgeführt wird, auf vSphere 7.0 Update 1 oder höher.
Der Nachweis ist fehlgeschlagen, da der sichere Start nicht aktiviert ist.	Überprüfen Sie, ob der vertrauenswürdige Host für die Verwendung von Secure Boot konfiguriert ist. Weitere Informationen hierzu finden Sie unter UEFI Secure Boot für ESXi-Hosts.
Die Remotesoftwareversion konnte durch den Nachweis nicht ermittelt werden.	Importieren Sie die Basisimage-Informationen des vertrauenswürdigen Hosts in den Nachweisdienst. Weitere Informationen hierzu finden Sie unter Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.

Error	Ursache und Lösung
Der Nachweis ist fehlgeschlagen, da ein TPM-Zertifikat erforderlich ist.	Stellen Sie sicher, dass das TPM unterstützt wird. Führen Sie alternativ das folgende PowerCLI-Cmdlet zur Änderung von com.vmware.esx.attestation.tpm2.settings aus, um `requireCertificateValidation` auf `false` festzulegen. `Set-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster TrustedCluster -RequireCertificateValidation:$false -RequireEndorsementKey:$true`
Der Nachweis ist aufgrund eines unbekannten TPM fehlgeschlagen.	Importieren Sie den TPM Endorsement Key in die Nachweisdienste. Weitere Informationen hierzu finden Sie unter Importieren der Informationen des vertrauenswürdigen Hosts in den Trust Authority-Cluster.
Fehler: vapi.send.failed.	Der kmxa-Dienst wird möglicherweise auf dem vertrauenswürdigen Host nicht ausgeführt oder der kmxa-Dienst kann den Nachweisdienst nicht kontaktieren. Stellen Sie sicher, dass der kmxa-Dienst gestartet wurde. Stellen Sie außerdem sicher, dass der Nachweisdienst ausgeführt wird. Weitere Informationen hierzu finden Sie unter Neustarten des Diensts für vertrauenswürdige Hosts.

Prüfen und Standardisieren der Integrität eines vertrauenswürdigen Clusters

Sie können die Integrität eines vertrauenswürdigen Clusters überprüfen und validieren. Wenn Probleme mit der Integrität eines vertrauenswürdigen Clusters auftreten, können Sie die Konfiguration eines vertrauenswürdigen Clusters standardisieren.

Übersicht über die Clusterintegrität und Standardisierung

Wenn die Konfiguration eines vertrauenswürdigen Clusters nicht fehlerfrei ist, müssen Sie die Konfigurationsinkonsistenzen beheben. Hierzu standardisieren Sie den vertrauenswürdigen Cluster. Wenn Sie einen vertrauenswürdigen Cluster standardisieren, stellen Sie sicher, dass alle vertrauenswürdigen Hosts im vertrauenswürdigen Cluster dieselbe vertrauenswürdige Konfiguration aufweisen.

Ein vertrauenswürdiger Cluster besteht aus einem vCenter Server-Cluster mit vertrauenswürdigen ESXi-Hosts, die remote vom Trust Authority-Cluster bestätigt wurden. Wenn Sie vSphere Trust Authority erstmals konfigurieren, müssen Sie die Informationen zu Trust Authority Services aus dem Trust Authority-Cluster in den vertrauenswürdigen Cluster importieren. Der vertrauenswürdige Cluster verwendet diese Konfiguration von Komponenten für die Kontaktaufnahme mit dem Schlüsselanbieterdienst und dem auf dem Trust Authority-Cluster ausgeführten Nachweisdienst. Weitere Informationen zum Konfigurieren von vertrauenswürdigen Clustern finden Sie unter Importieren der Informationen des Trust Authority-Clusters in die vertrauenswürdigen Hosts. Nachdem Sie einen vertrauenswürdigen Cluster konfiguriert haben, können Sie seine Integrität überprüfen und ihn standardisieren.

Übersicht über die Integrität eines vertrauenswürdigen Clusters

Die Überprüfung der Integrität eines vertrauenswürdigen Clusters hängt von den folgenden Umständen ab.

Gewünschte Zustandskonfiguration

Die gewünschte Zustandskonfiguration basiert auf den Informationen der Trust Authority Services, die Sie in den vertrauenswürdigen Cluster importieren. Die gewünschte Zustandskonfiguration ist die „Wahrheitsquelle“ des vertrauenswürdigen Clusters. Betrachten Sie die gewünschte Zustandskonfiguration als die Konfiguration, die bei der ersten Einrichtung des vertrauenswürdigen Clusters erstellt wurde.

Angewendete Konfiguration

Bei der angewendeten Konfiguration handelt es sich um die Registrierung der spezifischen Nachweisdienste und Schlüsselanbieterdienste, für die Sie den vertrauenswürdigen Cluster konfiguriert haben. Die angewendete Konfiguration ist das, was der vertrauenswürdige Cluster momentan ausführt. Betrachten Sie die angewendete Konfiguration als „Laufzeitkonfiguration“. Die gewünschte Zustandskonfiguration sollte mit der angewendeten Konfiguration übereinstimmen. Wenn die angewendete Konfiguration jedoch nicht mit der gewünschten Zustandskonfiguration übereinstimmt, wird der vertrauenswürdige Cluster als „nicht fehlerfrei“ eingestuft. Ein vertrauenswürdiger Cluster, der nicht fehlerfrei ist, kann eine verminderte Leistung aufweisen oder gar nicht funktionieren.

Diese Integritätsprüfung ist kein Indikator für den allgemeinen Systemzustand für einen vertrauenswürdigen Cluster oder die vSphere Trust Authority-Infrastruktur. Die Integritätsprüfung vergleicht nur die gewünschte Zustandskonfiguration des vertrauenswürdigen Clusters mit der angewendeten Konfiguration.

Übersicht über die Standardisierung vertrauenswürdiger Cluster

Die Standardisierung ist der Prozess, bei dem vSphere Trust Authority eine inkonsistente Konfiguration eines vertrauenswürdigen Clusters behebt. Die Konfiguration eines vertrauenswürdigen Clusters kann im Laufe der Zeit oder aufgrund anderer Betriebsfehler inkonsistent werden.

Verwenden Sie die Standardisierung wie folgt:

- Überprüfen Sie die Integrität des vertrauenswürdigen Clusters.
- Wenn der vertrauenswürdige Cluster nicht fehlerfrei ist, standardisieren Sie ihn.

Sie können entweder den vSphere Client oder die CLI verwenden, um die Integrität des vertrauenswürdigen Clusters zu prüfen. Siehe Überprüfen der Integrität des vertrauenswürdigen Clusters. Sie können den vSphere Client oder die CLI auch verwenden, um einen vertrauenswürdigen Cluster zu standardisieren. Weitere Informationen hierzu finden Sie unter Standardisieren eines vertrauenswürdigen Clusters.

Hinweis Die Standardisierung eignet sich auch zum Hinzufügen eines Hosts zu einem vorhandenen vertrauenswürdigen Cluster. Siehe Hinzufügen eines Hosts zu einem vertrauenswürdigen Cluster mit dem vSphere Client und Hinzufügen eines Hosts zu einem vertrauenswürdigen Cluster mit der CLI.

Überprüfen der Integrität des vertrauenswürdigen Clusters

Sie können den Integritätsstatus eines vertrauenswürdigen Clusters überprüfen, indem Sie entweder den vSphere Client oder die Befehlszeile verwenden.

Weitere Informationen finden Sie unter Übersicht über die Clusterintegrität und Standardisierung.

Voraussetzungen

- Auf dem vCenter Server für den vertrauenswürdigen Cluster muss vSphere 7.0 Update 1 oder höher ausgeführt werden.
- Bei Verwendung von PowerCLI wird Version 12.1.0 oder höher benötigt.

Verfahren

1 Überprüfen Sie die Integrität des vertrauenswürdigen Clusters.

Tool	Schritte
vSphere Client	a Stellen Sie eine Verbindung zum vCenter Server des vertrauenswürdigen Clusters mithilfe des vSphere Client her. b Melden Sie sich als Trust Authority-Administrator an. c Navigieren Sie zu einem vertrauenswürdigen Cluster, wählen Sie **Konfigurieren** und anschließend **Trust Authority** aus. d Klicken Sie auf **Integrität überprüfen**.

Befehlszeilenschnittstelle	a In einer PowerCLI-Sitzung führen Sie das Cmdlet `Connect-VIServer` aus, um als Trust Authority-Administrator eine Verbindung mit dem vCenter Server des vertrauenswürdigen Clusters herzustellen.
	`Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'`
	b Führen Sie das Cmdlet `Get-TrustedClusterAppliedStatus` aus. Beispiel:
	`Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'`

2 Wenn Fehler auftreten, finden Sie weitere Informationen unter Standardisieren eines vertrauenswürdigen Clusters.

Standardisieren eines vertrauenswürdigen Clusters

Sie können die Konfiguration eines vertrauenswürdigen Clusters mithilfe des vSphere Client oder der Befehlszeile standardisieren.

Voraussetzungen

Auf dem vCenter Server für den vertrauenswürdigen Cluster muss vSphere 7.0 Update 1 oder höher ausgeführt werden.

Verfahren

1 Stellen Sie eine Verbindung mit dem vCenter Server des vertrauenswürdigen Clusters her.

Tool	Schritte
vSphere Client	a Stellen Sie eine Verbindung zum vCenter Server des vertrauenswürdigen Clusters mithilfe des vSphere Client her. b Melden Sie sich als Trust Authority-Administrator an.
Befehlszeilenschnittstelle	In einer PowerCLI-Sitzung führen Sie das Cmdlet `Connect-VIServer` aus, um als Trust Authority-Administrator eine Verbindung mit dem vCenter Server des vertrauenswürdigen Clusters herzustellen. `Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'`

2 Standardisieren Sie den vertrauenswürdigen Cluster und überprüfen Sie dann die Integrität des vertrauenswürdigen Clusters erneut.

Tool	Schritte
vSphere Client	a Navigieren Sie zu einem vertrauenswürdigen Cluster. b Wählen Sie **Konfigurieren** und wählen Sie dann **Trust Authority**. c Klicken Sie auf **Standardisieren**. d Klicken Sie auf **Integrität überprüfen**.

Befehlszeilenschnittstelle	a Führen Sie das `Set-TrustedCluster`-Cmdlet mit dem Parameter `-Remediate` aus, wie z. B.:
	`Set-TrustedCluster -TrustedCluster 'TrustedCluster' -Remediate`
	b Führen Sie das Cmdlet `Get-TrustedClusterAppliedStatus` aus. Beispiel:
	`Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'`

Verwenden von Verschlüsselung in Ihrer vSphere-Umgebung

10

Die Verwendung von Verschlüsselung in Ihrer vSphere-Umgebung muss vorbereitet werden. Dabei spielt es keine Rolle, ob Sie einen Standardschlüsselanbieter, einen vertrauenswürdigen Schlüsselanbieter oder einen vSphere Native Key Provider verwenden.

Wenn Sie Ihre Umgebung eingerichtet haben, können Sie mithilfe des vSphere Client verschlüsselte virtuelle Maschinen und virtuelle Festplatten erstellen und vorhandene virtuelle Maschinen und Festplatten verschlüsseln.

Unter Verwendung der API und der `crypto-util`-Befehlszeile können Sie zusätzliche Aufgaben ausführen. Die API-Dokumentation finden Sie im *Programmierhandbuch zum vSphere Web Services SDK*. Informationen zu diesem Tool finden Sie der `crypto-util`-Befehlszeilenhilfe.

Erstellen einer Speicherrichtlinie für die Verschlüsselung.

Bevor Sie verschlüsselte virtuelle Maschinen erstellen können, müssen Sie eine Speicherrichtlinie für die Verschlüsselung erstellen. Die Speicherrichtlinie wird nur einmal erstellt und immer dann zugewiesen, wenn eine virtuelle Maschine oder eine virtuelle Festplatte verschlüsselt wird.

Wenn Sie VM-Verschlüsselung mit anderen I/O-Filtern oder den Assistenten **VM-Speicherrichtlinie erstellen** im vSphere Client verwenden möchten, finden Sie weitere Informationen in der Dokumentation *vSphere-Speicher*.

Voraussetzungen

- Richten Sie die Verbindung zu einem Schlüsselanbieter ein.

  Obwohl eine Speicherrichtlinie für die VM-Verschlüsselung auch ohne Verbindung zum Schlüsselanbieter erstellt werden kann, können Sie Verschlüsselungsaufgaben erst durchführen, nachdem die vertrauenswürdige Verbindung mit dem Schlüsselanbieter eingerichtet wurde.

- Erforderliche Rechte: **Verschlüsselungsvorgänge.Verschlüsselungsrichtlinien verwalten**.

Verfahren

1. Melden Sie sich beim vCenter Server mit dem vSphere Client an.
2. Wählen Sie **Home** aus, klicken Sie auf **Richtlinien und Profile** und klicken Sie dann auf **VM-Speicherrichtlinien**.

3 Klicken Sie auf **Erstellen**.

4 Wählen Sie den vCenter Server aus, geben Sie einen Richtliniennamen sowie optional eine Beschreibung ein und klicken Sie dann auf **Weiter**.

5 Aktivieren Sie auf der Seite **Richtlinienstruktur** die Option **Hostbasierte Rollen aktivieren** und klicken Sie dann auf **Weiter**.

6 Wählen Sie auf der Seite **Hostbasierte Dienste** die Option **Speicherrichtlinienkomponente verwenden** aus, wählen Sie im Dropdown-Menü **Standardeigenschaften der Verschlüsselung** aus und klicken Sie dann auf **Weiter**.

7 Behalten Sie auf der Seite **Speicherkompatibilität** die Option **Kompatibel** bei, wählen Sie einen Datenspeicher und klicken Sie dann auf **Weiter**.

8 Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

Ergebnisse

Die VM-Verschlüsselungsspeicherrichtlinie wird zur Liste hinzugefügt und steht für die Verschlüsselung einer virtuellen Maschine bereit.

Explizites Aktivieren des Hostverschlüsselungsmodus

Der Hostverschlüsselungsmodus muss aktiviert sein, wenn Sie Verschlüsselungsaufgaben wie das Erstellen einer verschlüsselten virtuellen Maschine auf einem ESXi-Host durchführen möchten. In den meisten Fällen wird der Hostverschlüsselungsmodus automatisch aktiviert, wenn Sie eine Verschlüsselungsaufgabe durchführen.

In bestimmten Fällen muss der Verschlüsselungsmodus explizit eingeschaltet werden. Weitere Informationen hierzu finden Sie unter Voraussetzungen und erforderliche Berechtigungen für die Verschlüsselung.

Voraussetzungen

Erforderliche Berechtigung: **Kryptografische Vorgänge.Host registrieren**

Verfahren

1 Melden Sie sich beim vCenter Server mit dem vSphere Client an.

2 Navigieren Sie zum ESXi-Host und klicken Sie auf **Konfigurieren**.

3 Klicken Sie unter „System“ auf **Sicherheitsprofil**.

4 Klicken Sie im Fenster „Hostverschlüsselungsmodus“ auf **Bearbeiten**.

5 Wählen Sie **Aktiviert** aus und klicken Sie auf **OK**.

Deaktivieren des Hostverschlüsselungsmodus mithilfe der API

Der Hostverschlüsselungsmodus wird beim Durchführen einer Verschlüsselungsaufgabe automatisch aktiviert, falls der Benutzer über ausreichende Rechte zum Aktivieren des Verschlüsselungsmodus verfügt. Nachdem der Hostverschlüsselungsmodus aktiviert wurde, werden alle Core-Dumps verschlüsselt, um die Freigabe von vertraulichen Informationen an Supportmitarbeiter zu vermeiden. Falls Sie die Verschlüsselung virtueller Maschinen bei einem ESXi-Host nicht mehr verwenden, können Sie den Verschlüsselungsmodus deaktivieren.

Nach der Aktivierung des Verschlüsselungsmodus für einen ESXi-Host müssen Sie ihn deaktivieren. Beispielsweise müssen Sie möglicherweise den Verschlüsselungsmodus deaktivieren, um ein ESXi-Support-Paket zu generieren (mithilfe des Befehls `vm-support`). Die Umschaltoption „Hostverschlüsselungsmodus deaktivieren“ (**Host > Konfigurieren > Sicherheitsprofil > Hostverschlüsselungsmodus bearbeiten**) funktioniert nicht, wenn Schlüsselmaterial auf dem Host vorhanden ist.

Sie können die API verwenden, um den Hostverschlüsselungsmodus zu deaktivieren, indem Sie die API-Methode „`CryptoManagerHostDisable`“ aufrufen.

Die für einen ESXi-Host definierten Verschlüsselungsmodi bzw. -zustände lauten:

- pendingIncapable: Der Host ist für die Verschlüsselung deaktiviert, das heißt, der Host kann keine vSphere VM-Verschlüsselungsvorgänge durchführen.
- incapable: Der Host ist für den Empfang vertraulicher Materialien nicht sicher.
- prepared: Der Host ist für den Empfang vertraulicher Materialien vorbereitet, verfügt aber noch nicht über einen festgelegten Hostschlüssel.
- safe: Der Host ist verschlüsselungssicher (aktiviert) und verfügt über einen Hostschlüsselsatz, das heißt, vSphere Virtual Machine Encryption-Vorgänge sind möglich.

Nachdem Sie „`CryptoManagerHostDisable`“ auf einem Host aufgerufen haben, ändert sich der Verschlüsselungsstatus des Hosts wie folgt:

- Wenn der ursprüngliche Host-Verschlüsselungsstatus nicht in der Lage (incapable) oder vorbereitet (prepared) ist, wird der Host-Verschlüsselungsstatus in „incapable“ geändert.
- Wenn der ursprüngliche Host-Verschlüsselungsstatus sicher (safe) ist, wird der Host-Verschlüsselungsstatus in „pendingIncapable“ geändert.
- Wenn der Host-Verschlüsselungsstatus „pendingIncapable“ lautet, ist der Host-Verschlüsselungsstatus weiterhin „pendingIncapable“.

Diese Aufgabe zeigt, wie Sie mithilfe des vCenter Server-MOB (Managed Object Browser) den Hostverschlüsselungsmodus deaktivieren. Weitere Informationen zur Verwendung der API finden Sie in der Dokumentation *vSphere Web Services API* unter https://developer.vmware.com/apis/968/vsphere.

Verfahren

1. Melden Sie sich beim vCenter Server als Administrator an.
2. Heben Sie die Registrierung aller verschlüsselten virtuellen Maschinen auf dem ESXi-Host auf, dessen Verschlüsselungsmodus Sie deaktivieren möchten.
3. Greifen Sie auf den MOB auf dem vCenter Server zu.

   ```
   https://vcenter_server/mob
   ```

4. Rufen Sie die Methode „`CryptoManagerHostDisable`“ auf einem Host auf.
   a. Klicken Sie unter „content name“ auf **content**.
   b. Klicken Sie unter „rootFolder“ auf **group-D1 (Datacenters)**.
   c. Klicken Sie unter „childEntity“ auf das entsprechende Datencenter.
   d. Klicken Sie unter „hostFolder“ auf den entsprechenden Host.
   e. Klicken Sie unter „childEntity“ auf den entsprechenden Cluster.
   f. Klicken Sie unter „host“ auf den entsprechenden Host.
   g. Klicken Sie unter „configManager“ auf **configManager**.
   h. Klicken Sie unter „cryptoManager“ auf **CryptoManagerHost-***Zahl*.
   i. Klicken Sie auf **CryptoManagerHostDisable**.

      Der Host-Verschlüsselungsstatus wird je nach ursprünglichem Verschlüsselungsstatus in „pendingIncapable“ oder „incapable“ geändert.
5. Wiederholen Sie Schritt 4 für andere Hosts, auf denen Sie den Verschlüsselungsmodus deaktivieren möchten.
6. Starten Sie die Hosts neu.

Ergebnisse

Sobald der Hostverschlüsselungsmodus deaktiviert ist, können Sie keine Verschlüsselungsvorgänge wie das Hinzufügen verschlüsselter virtueller Maschinen durchführen, es sei denn, Sie aktivieren den Hostverschlüsselungsmodus erneut.

Hinweis Nachdem Sie einen ESXi-Host neu gestartet haben, auf dem Sie den Verschlüsselungsmodus deaktiviert haben, ist der Hostverschlüsselungsstatus weiterhin „pendingIncapable“, wenn der Hostverschlüsselungsstatus ursprünglich „pendingIncapable“ lautete. Um den Hostverschlüsselungsmodus erneut zu aktivieren, greifen Sie erneut auf den vCenter Server-MOB zu und rufen Sie die API-Methode `ConfigureCryptoKey` auf. Verwenden Sie beim erneuten Aktivieren des Hostverschlüsselungsmodus die ursprüngliche Hostschlüssel-ID, wenn der Hostverschlüsselungsstatus „pendingIncapable“ lautet.

Erstellen einer verschlüsselten virtuellen Maschine

Nachdem Sie den KMS eingerichtet haben, können Sie verschlüsselte virtuelle Maschinen erstellen.

In dieser Aufgabe wird beschrieben, wie Sie eine verschlüsselte virtuelle Maschine mithilfe des vSphere Client erstellen. Der vSphere Client filtert nach Speicherrichtlinien für die VM-Verschlüsselung und vereinfacht somit die Erstellung verschlüsselter virtueller Maschinen.

Hinweis Das Erstellen einer verschlüsselten virtuellen Maschine geht schneller und beansprucht weniger Speicherressourcen als das Verschlüsseln einer vorhandenen virtuellen Maschine. Falls möglich, verschlüsseln Sie virtuelle Maschinen während des Erstellungsvorgangs.

Voraussetzungen

- Richten Sie eine vertrauenswürdige Verbindung mit dem KMS ein und wählen Sie einen Standard-KMS aus.
- Erstellen Sie eine Speicherrichtlinie für die Verschlüsselung oder verwenden Sie das im Lieferumfang enthaltene Beispiel für eine VM-Verschlüsselungsrichtlinie.
- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.
- Stellen Sie sicher, dass Sie über die erforderlichen Rechte verfügen:
  - **Verschlüsselungsvorgänge.Neue verschlüsseln**
  - Wenn der Hostverschlüsselungsmodus nicht auf „Aktiviert“ festgelegt ist, benötigen Sie außerdem **Verschlüsselungsvorgänge.Host registrieren**.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Wählen Sie in der Bestandsliste ein Objekt aus, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, beispielsweise einen ESXi-Host oder einen Cluster.
3. Klicken Sie mit der rechten Maustaste auf das Objekt und wählen Sie **Neue virtuelle Maschine** aus.
4. Folgen Sie den Anweisungen, um eine verschlüsselte virtuelle Maschine zu erstellen.

Option	Aktion
Erstellungstyp auswählen	Erstellen Sie eine neue virtuelle Maschine.
Namen und Ordner auswählen	Geben Sie einen eindeutigen Namen und einen Zielspeicherort für die virtuelle Maschine an.
Computing-Ressource auswählen	Geben Sie ein Objekt an, für das Sie über Berechtigungen zum Erstellen von verschlüsselten virtuellen Maschinen verfügen. Weitere Informationen hierzu finden Sie unter Voraussetzungen und erforderliche Berechtigungen für die Verschlüsselung.

Option	Aktion
Speicher auswählen	Aktivieren Sie das Kontrollkästchen **Diese virtuelle Maschine verschlüsseln**. VM-Speicherrichtlinien mit Verschlüsselung werden angezeigt. Wählen Sie eine VM-Speicherrichtlinie (das mitgelieferte Beispiel lautet „VM-Verschlüsselungsrichtlinie“) und einen kompatiblen Datenspeicher aus.
Kompatibilität auswählen	Wählen Sie die Kompatibilität aus. Sie können eine verschlüsselte virtuelle Maschine nur zu Hosts migrieren, die mit ESXi 6.5 oder höher kompatibel sind.
Gastbetriebssystem auswählen	Wählen Sie ein Gastbetriebssystem aus, das Sie später auf der virtuellen Maschine installieren möchten.
Hardware anpassen	Passen Sie die Hardware an, indem Sie z. B. die Festplattengröße oder die CPU ändern. (Optional) Wählen Sie die Registerkarte **VM-Optionen** aus und erweitern Sie **Verschlüsselung**. Wählen Sie die Festplatten aus, die nicht verschlüsselt werden sollen. Wenn Sie die Auswahl einer Festplatte aufheben, werden nur VM-Home und etwaige andere ausgewählte Festplatten verschlüsselt. Jede neue Festplatte, die Sie hinzufügen, wird verschlüsselt. Sie können die Speicherrichtlinie für einzelne Festplatten später ändern.
Bereit zum Abschließen	Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

Klonen einer verschlüsselten virtuellen Maschine

Wenn Sie eine verschlüsselte virtuelle Maschine klonen, wird der Klon mit den gleichen Schlüsseln verschlüsselt. Um Schlüssel für den Klon zu ändern, führen Sie mithilfe der API eine Neuverschlüsselung des Klons durch. Siehe *Programmierhandbuch zum vSphere Web Services SDK*.

Während des Klonens können Sie die folgenden Vorgänge ausführen.

- Erstellen Sie eine verschlüsselte virtuelle Maschine anhand einer nicht verschlüsselten oder Vorlagen-VM.
- Erstellen Sie eine entschlüsselte virtuelle Maschine anhand einer verschlüsselten oder Vorlagen-VM.
- Verschlüsseln Sie die virtuelle Zielmaschine erneut mit Schlüsseln, die sich von denen der virtuellen Quellmaschine unterscheiden.

Sie können eine Instant Clone-VM anhand einer verschlüsselten virtuellen Maschine unter der Voraussetzung erstellen, dass der Instant Clone denselben Schlüssel wie die virtuelle Quellmaschine verwendet. Sie können Schlüssel weder auf der Quell- noch auf der Instant Clone-VM erneut verschlüsseln. Weitere Informationen hierzu finden Sie unter *Programmierhandbuch zum vSphere Web Services SDK*.

Voraussetzungen

- Richten Sie eine vertrauenswürdige Verbindung mit dem KMS ein und wählen Sie einen Standard-KMS aus.

- Erstellen Sie eine Speicherrichtlinie für die Verschlüsselung oder verwenden Sie das im Lieferumfang enthaltene Beispiel für eine VM-Verschlüsselungsrichtlinie.
- Erforderliche Rechte:
  - **Verschlüsselungsvorgänge.Klonen**
  - **Verschlüsselungsvorgänge.Verschlüsseln**
  - **Verschlüsselungsvorgänge.Entschlüsseln**
  - **Verschlüsselungsvorgänge.Erneut verschlüsseln**
  - Wenn der Hostverschlüsselungsmodus nicht auf „Aktiviert“ festgelegt ist, benötigen Sie außerdem **Verschlüsselungsvorgänge.Host registrieren**-Berechtigungen.

Verfahren

1 Navigieren Sie zur virtuellen Maschine in der Bestandsliste des vSphere Client.

2 Um einen Klon einer verschlüsselten Maschine zu erstellen, klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, wählen Sie **Klonen > In virtueller Maschine klonen** und folgen Sie den Anweisungen.

Option	Aktion
Namen und Ordner auswählen	Geben Sie einen Namen und einen Zielspeicherort für den Klon an.
Computing-Ressource auswählen	Geben Sie ein Objekt an, für das Sie über Berechtigungen zum Erstellen von verschlüsselten virtuellen Maschinen verfügen. Weitere Informationen hierzu finden Sie unter Voraussetzungen und erforderliche Berechtigungen für die Verschlüsselung.
Speicher auswählen	Nehmen Sie eine Auswahl im Menü **Format für die virtuelle Festplatte auswählen** vor und wählen Sie einen Datenspeicher aus. Sie können die Speicherrichtlinie im Rahmen des Klonvorgangs ändern. Wenn Sie beispielsweise statt einer Verschlüsselungsrichtlinie eine Nicht-Verschlüsselungsrichtlinie verwenden, werden die Festplatten entschlüsselt.
Klonoptionen auswählen	Wählen Sie Klonoptionen wie in der Dokumentation zu *vSphere-Administratorhandbuch für virtuelle Maschinen* beschrieben aus.
Bereit zum Abschließen	Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

3 (Optional) Ändern Sie die Schlüssel für die geklonte virtuelle Maschine.

Die geklonte virtuelle Maschine wird standardmäßig mit denselben Schlüsseln erstellt wie die übergeordnete virtuelle Maschine. Als Best Practice wird empfohlen, die Schlüssel der geklonten virtuellen Maschine zu ändern, um sicherzustellen, dass nicht mehrere virtuelle Maschinen dieselben Schlüssel aufweisen.

a Entscheiden Sie sich für eine flache oder tiefe Neuverschlüsselung.

Wenn Sie einen anderen Daten-Verschlüsselungsschlüssel (Data Encryption Key, DEK) und einen anderen Schlüssel-Verschlüsselungsschlüssel (Key Encryption Key, KEK) verwenden möchten, führen Sie eine tiefe Neuverschlüsselung der geklonten virtuellen Maschine durch. Wenn Sie einen anderen KEK verwenden möchten, führen Sie eine flache Neuverschlüsselung der geklonten virtuellen Maschine durch. Bei einer tiefen Neuverschlüsselung müssen Sie die virtuelle Maschine ausschalten. Sie können eine flache Neuverschlüsselung bei eingeschalteter virtueller Maschine durchführen, sofern auf der virtuellen Maschine Snapshots vorhanden sind. Die flache Neuverschlüsselung einer verschlüsselten virtuellen Maschine mit Snapshots ist nur in einem einzelnen Snapshot-Zweig (Festplattenkette) zulässig. Mehrere Snapshot-Zweige werden nicht unterstützt. Wenn die flache Neuverschlüsselung fehlschlägt, bevor alle Verknüpfungen in der Kette mit dem neuen KEK aktualisiert werden, können Sie weiterhin auf die verschlüsselte virtuelle Maschine zugreifen, vorausgesetzt, Sie verfügen über die alten und neuen KEKs.

b Verschlüsseln Sie den Klon erneut über die API. Siehe *Programmierhandbuch zum vSphere Web Services SDK*.

Verschlüsseln einer bestehenden virtuellen Maschine oder virtuellen Festplatte

Sie können eine bestehende virtuelle Maschine oder virtuelle Festplatte verschlüsseln, in dem sie ihre Speicherrichtlinie ändern. Sie können virtuelle Festplatten nur für verschlüsselte virtuelle Maschinen verschlüsseln.

In dieser Aufgabe wird beschrieben, wie Sie eine bestehende virtuelle Maschine oder virtuelle Festplatte mit vSphere Client verschlüsseln.

 (Verschlüsseln virtueller Maschinen mit dem vSphere Client)

Voraussetzungen

- Richten Sie eine vertrauenswürdige Verbindung mit dem KMS ein und wählen Sie einen Standard-KMS aus.
- Erstellen Sie eine Speicherrichtlinie für die Verschlüsselung oder verwenden Sie das im Lieferumfang enthaltene Beispiel für eine VM-Verschlüsselungsrichtlinie.
- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.

- Stellen Sie sicher, dass Sie über die erforderlichen Rechte verfügen:
  - **Verschlüsselungsvorgänge.Neue verschlüsseln**
  - Wenn der Hostverschlüsselungsmodus nicht auf „Aktiviert“ festgelegt ist, benötigen Sie außerdem **Verschlüsselungsvorgänge.Host registrieren**.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Klicken Sie mit der rechten Maustaste auf die zu ändernde virtuelle Maschine und wählen Sie **VM-Richtlinien > VM-Speicherrichtlinien bearbeiten**.

   Sie können die Speicherrichtlinie für die Dateien der virtuellen Maschine, dargestellt von VM-Home, und die Speicherrichtlinie für virtuelle Festplatten festlegen.
3. Wählen Sie die Speicherrichtlinie aus.
   - Um die virtuelle Maschine und deren Festplatten zu verschlüsseln, wählen Sie eine Speicherrichtlinie für die Verschlüsselung aus und klicken Sie auf **OK**.
   - Um die virtuelle Maschine, jedoch nicht deren virtuelle Festplatten zu verschlüsseln, aktivieren Sie **Pro Datenträger konfigurieren**, wählen Sie die Speicherrichtlinie für die Verschlüsselung für VM-Home und andere Speicherrichtlinien für die virtuellen Festplatten aus und klicken Sie auf **OK**.

   Die virtuelle Festplatte einer nicht verschlüsselten virtuellen Maschine kann nicht verschlüsselt werden.
4. Auf Wunsch können Sie die virtuelle Maschine – oder die virtuelle Maschine und die Festplatten – über das Menü **Einstellungen bearbeiten** im vSphere Client verschlüsseln.
   a. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
   b. Wählen Sie die Registerkarte **VM-Optionen** aus und öffnen Sie **Verschlüsselung**. Wählen Sie eine Verschlüsselungsrichtlinie aus. Wenn Sie alle Festplatten deaktivieren, wird nur VM-Home verschlüsselt.
   c. Klicken Sie auf **OK**.

Entschlüsseln einer verschlüsselten virtuellen Maschine oder virtuellen Festplatte

Sie können eine virtuelle Maschine, deren Festplatten oder beides entschlüsseln, indem Sie die Speicherrichtlinie ändern.

In dieser Aufgabe wird beschrieben, wie Sie eine verschlüsselte virtuelle Maschine mit vSphere Client entschlüsseln.

Für alle verschlüsselten virtuellen Maschinen ist verschlüsseltes vMotion erforderlich. Während der Entschlüsselung der virtuellen Maschine werden die Einstellungen für verschlüsseltes vMotion beibehalten. Damit kein verschlüsseltes vMotion mehr verwendet wird, müssen Sie diese Einstellung explizit ändern.

In dieser Aufgabe wird erläutert, wie Sie anhand von Speicherrichtlinien entschlüsseln. Für virtuelle Festplatten können Sie für die Entschlüsselung auch das Menü **Einstellungen bearbeiten** verwenden.

Voraussetzungen

- Die virtuelle Maschine muss verschlüsselt sein.
- Die virtuelle Maschine muss ausgeschaltet sein oder sich im Wartungsmodus befinden.
- Erforderliche Berechtigungen: **Verschlüsselungsvorgänge.Entschlüsseln**

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Klicken Sie mit der rechten Maustaste auf die zu ändernde virtuelle Maschine und wählen Sie **VM-Richtlinien > VM-Speicherrichtlinien bearbeiten**.

   Sie können die Speicherrichtlinie für die Dateien der virtuellen Maschine, dargestellt von VM-Home, und die Speicherrichtlinie für virtuelle Festplatten festlegen.
3. Wählen Sie eine Speicherrichtlinie aus.
   - Um die virtuelle Maschine und deren Festplatten zu entschlüsseln, deaktivieren Sie **Pro Datenträger konfigurieren**, wählen Sie im Dropdown-Menü eine Speicherrichtlinie aus und klicken Sie auf **OK**.
   - Um die virtuelle Festplatte, jedoch nicht die virtuelle Maschine zu entschlüsseln, aktivieren Sie **Pro Datenträger konfigurieren**, wählen Sie die Speicherrichtlinie für die Verschlüsselung für VM-Home und andere Speicherrichtlinien für die virtuellen Festplatten aus und klicken Sie auf **OK**.

   Es ist nicht möglich, die virtuelle Maschine zu entschlüsseln und die Festplatte verschlüsselt zu lassen.
4. Auf Wunsch können Sie die virtuelle Maschine und die Festplatten mit vSphere Client über das Menü **Einstellungen bearbeiten** entschlüsseln.
   a. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
   b. Wählen Sie die Registerkarte **VM-Optionen** aus und erweitern Sie **Verschlüsselung**.
   c. Um die virtuelle Maschine und deren Festplatten zu entschlüsseln, wählen Sie im Dropdown-Menü **VM verschlüsseln** die Option **Keine** aus.

d Um eine virtuelle Festplatte, jedoch nicht die virtuelle Maschine zu entschlüsseln, heben Sie die Auswahl der Festplatte auf.

e Klicken Sie auf **OK**.

5 (Optional) Sie können die Einstellung für verschlüsseltes vMotion ändern.

a Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie auf **Einstellungen bearbeiten**.

b Klicken Sie auf **VM-Optionen** und öffnen Sie **Verschlüsselung**.

c Legen Sie den Wert für **Verschlüsseltes vMotion** fest.

Ändern der Verschlüsselungsrichtlinie für virtuelle Festplatten

Beim Erstellen einer verschlüsselten virtuellen Maschine über den vSphere Client können Sie festlegen, welche virtuellen Festplatten, die Sie während der Erstellung der virtuellen Maschine hinzufügen, verschlüsselt werden. Sie können verschlüsselte virtuelle Festplatten mithilfe der Option **VM-Speicherrichtlinie bearbeiten** entschlüsseln.

Hinweis Eine verschlüsselte virtuelle Maschine kann nicht verschlüsselte virtuelle Festplatten enthalten. Eine nicht verschlüsselte virtuelle Maschine kann jedoch keine verschlüsselten virtuellen Festplatten enthalten.

Weitere Informationen hierzu finden Sie unter Verschlüsseln von virtuellen Festplatten.

In dieser Aufgabe wird beschrieben, wie Sie die Verschlüsselungsrichtlinie anhand von Speicherrichtlinien ändern. Sie können auch das Menü **Einstellungen bearbeiten** verwenden, um diese Änderung vorzunehmen.

Voraussetzungen

- Sie benötigen die Berechtigung **Verschlüsselungsvorgänge.Verschlüsselungsrichtlinien verwalten**.
- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.

Verfahren

1 Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.

2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **VM-Richtlinien > VM-Speicherrichtlinien bearbeiten** aus.

3 Ändern Sie die Speicherrichtlinie.

- Um die Speicherrichtlinie für die virtuelle Maschine und deren Festplatten zu ändern, wählen Sie eine Speicherrichtlinie für die Verschlüsselung aus und klicken Sie auf **OK**.

- Um die virtuelle Maschine, jedoch nicht deren virtuelle Festplatten zu verschlüsseln, aktivieren Sie **Pro Datenträger konfigurieren**, wählen Sie die Speicherrichtlinie für die Verschlüsselung für VM-Home und andere Speicherrichtlinien für die virtuellen Festplatten aus und klicken Sie auf **OK**.

Die virtuelle Festplatte einer nicht verschlüsselten virtuellen Maschine kann nicht verschlüsselt werden.

4 Auf Wunsch können Sie die Speicherrichtlinie im Menü **Einstellungen bearbeiten** ändern.

a Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.

b Wählen Sie die Registerkarte **Virtuelle Hardware** aus, erweitern Sie eine Festplatte und wählen Sie im Dropdown-Menü eine Verschlüsselungsrichtlinie aus.

c Klicken Sie auf **OK**.

Beheben von Problemen in Bezug auf fehlende Schlüssel

Wenn der ESXi-Host den Schlüssel (KEK) für eine verschlüsselte virtuelle Maschine oder eine verschlüsselte virtuelle Festplatte nicht vom vCenter Server abrufen kann, wird die verschlüsselte VM gesperrt. Nachdem Sie die Schlüssel auf dem KMS verfügbar gemacht haben, können Sie eine gesperrte verschlüsselte virtuelle Maschine entsperren.

Unter bestimmten Umständen kann bei Verwendung eines Standardschlüsselanbieters der ESXi-Host den Schlüsselverschlüsselungsschlüssel (Key Encryption Key, KEK) für eine verschlüsselte virtuelle Maschine oder eine verschlüsselte virtuelle Festplatte nicht vom vCenter Server abrufen. In diesem Fall können Sie dennoch die Registrierung der virtuellen Maschine aufheben oder diese neu laden. Sie können jedoch keine anderen VM-Vorgänge durchführen, wie z. B. Einschalten der virtuellen Maschine. Nachdem Sie die nötigen Schritte ausgeführt haben, um die erforderlichen Schlüssel auf dem KMS verfügbar zu machen, können Sie eine gesperrte verschlüsselte virtuelle Maschine mithilfe des vSphere Client entsperren.

Wenn der Schlüssel der virtuellen Maschine nicht verfügbar ist, werden Sie durch einen vCenter Server-Alarm benachrichtigt, und der Status der virtuellen Maschine wird als ungültig angezeigt. Die virtuelle Maschine kann nicht eingeschaltet werden. Wenn der Schlüssel der virtuellen Maschine verfügbar ist, aber kein Schlüssel für eine verschlüsselte Festplatte verfügbar ist, wird der Status für die virtuelle Maschine nicht als ungültig angezeigt. Die virtuelle Maschine kann jedoch nicht eingeschaltet werden, und es kommt zu folgendem Fehler:

```
The disk [/path/to/the/disk.vmdk] is encrypted and a required key was not found.
```

Hinweis In folgendem Verfahren werden die Situationen geschildert, die zur Sperrung einer virtuellen Maschine führen können, sowie neben den zugehörigen Alarmen und Ereignisprotokollen die Vorgehensweisen im jeweiligen Fall.

Verfahren

1 Falls die Verbindung zwischen dem vCenter Server-System und dem KMS das Problem ist, generiert der vCenter Server einen VM-Alarm. Außerdem wird eine Fehlermeldung im Ereignisprotokoll angezeigt.

   Stellen Sie die Verbindung zum KMS wieder her. Wenn der KMS und die Schlüssel zur Verfügung stehen, entsperren Sie die gesperrten virtuellen Maschinen. Weitere Informationen hierzu finden Sie unter Entsperren von gesperrten virtuellen Maschinen. Sie können den Host auch neu starten und die virtuelle Maschine erneut registrieren, um sie nach der Wiederherstellung der Verbindung zu entsperren.

   Bei einer Unterbrechung der Verbindung zum KMS wird die virtuelle Maschine nicht automatisch gesperrt. Die virtuelle Maschine wechselt nur dann in einen gesperrten Zustand, wenn die folgenden Bedingungen erfüllt sind:

   - Der Schlüssel ist nicht auf dem ESXi-Host verfügbar.
   - vCenter Server kann keine Schlüssel vom KMS abrufen.

   Der ESXi-Host muss nach jedem Neustart in der Lage sein, den vCenter Server zu erreichen. vCenter Server fordert den Schlüssel mit der entsprechenden ID vom KMS an und stellt ihn auf ESXi zur Verfügung.

   Hinweis In vSphere 7.0 Update 2 und höher können Sie Verschlüsselungsschlüssel auch bei mehreren ESXi-Neustarts beibehalten. Weitere Informationen finden Sie unter Schlüsselpersistenz – Übersicht.

   Wenn die virtuelle Maschine nach dem Wiederherstellen der Verbindung zum Schlüsselanbieter weiterhin gesperrt ist, erhalten Sie weitere Informationen unter Entsperren von gesperrten virtuellen Maschinen.

2 Wenn die Verbindung wiederhergestellt wurde, registrieren Sie die virtuelle Maschine. Falls ein Fehler auftritt oder der Vorgang erfolgreich verläuft, die virtuelle Maschine jedoch gesperrt ist, stellen Sie sicher, dass Sie über das Recht **Cryptographic operations.RegisterVM** für das vCenter Server-System verfügen.

   Diese Berechtigung ist für das Einschalten einer verschlüsselten virtuellen Maschine nicht erforderlich, wenn der Schlüssel verfügbar ist. Diese Berechtigung ist für die Registrierung der virtuellen Maschine erforderlich, wenn der Schlüssel abgerufen werden muss.

3 Wenn der Schlüssel auf dem KMS nicht mehr verfügbar ist, generiert der vCenter Server einen VM-Alarm. Außerdem wird eine Fehlermeldung im Ereignisprotokoll angezeigt.

   Bitten Sie den KMS-Administrator, den Schlüssel wiederherzustellen. Sie können auf einen inaktiven Schlüssel stoßen, wenn Sie eine virtuelle Maschine einschalten, die aus der Bestandsliste entfernt und seit einiger Zeit nicht registriert wurde. Es passiert auch, wenn Sie den ESXi-Host neu starten, wenn der KMS nicht verfügbar ist.

   a Rufen Sie die Schlüssel-ID mithilfe des Managed Object Browsers (MOB) oder der vSphere API ab.

     Rufen Sie die `keyId` von der Datei `VirtualMachine.config.keyId.keyId` ab.

   b Bitten Sie den KMS-Administrator, den Schlüssel zu reaktivieren, der dieser Schlüssel-ID entspricht.

   c Nach der Wiederherstellung des Schlüssels erhalten Sie weitere Informationen unter Entsperren von gesperrten virtuellen Maschinen.

   Wenn der Schlüssel auf dem KMS wiederhergestellt werden kann, ruft vCenter Server ihn ab und leitet ihn an den ESXi-Host weiter, wenn er das nächste Mal benötigt wird.

4 Wenn auf den KMS zugegriffen werden kann und der ESXi-Host eingeschaltet ist, das vCenter Server-System jedoch nicht zur Verfügung steht, führen Sie die folgenden Schritte durch, um die virtuellen Maschinen zu entsperren.

   a Stellen Sie das vCenter Server-System wieder her oder richten Sie ein anderes vCenter Server-System ein. Legen Sie anschließend ein Vertrauensverhältnis mit dem KMS fest.

     Sie müssen den gleichen Schlüsselanbieternamen verwenden, die IP-Adresse des KMS kann sich aber unterscheiden.

   b Registrieren Sie alle gesperrten virtuellen Maschinen neu.

     Die neue vCenter Server-Instanz ruft die Schlüssel vom KMS ab, und die virtuellen Maschinen werden entsperrt.

5 Wenn die Schlüssel nur auf dem ESXi-Host fehlen, generiert der vCenter Server einen VM-Alarm, und im Ereignisprotokoll wird die folgende Meldung angezeigt:

   `Die virtuelle Maschine ist gesperrt, weil Schlüssel auf dem Host fehlen.`

   Das vCenter Server-System kann die fehlenden Schlüssel aus dem Schlüsselanbieter abrufen. Ein manuelle Wiederherstellung der Schlüssel ist nicht erforderlich. Weitere Informationen hierzu finden Sie unter Entsperren von gesperrten virtuellen Maschinen.

Entsperren von gesperrten virtuellen Maschinen

Sie werden in einem vCenter Server-Alarm informiert, wenn sich eine verschlüsselte virtuelle Maschine im gesperrten Modus befindet. Sie können eine gesperrte verschlüsselte VM mithilfe des vSphere Client (HTML5-basierter Client) entsperren, nachdem Sie die notwendigen Schritte zur Bereitstellung der erforderlichen Schlüssel auf dem KMS durchgeführt haben.

Voraussetzungen

- Vergewissern Sie sich, dass Sie über die erforderlichen Berechtigungen verfügen: **Kryptografievorgänge.RegisterVM**
- Andere Berechtigungen sind unter Umständen für optionale Aufgaben erforderlich, wie z. B. das Aktivieren von Hostverschlüsselung.
- Ermitteln Sie vor dem Entsperren einer gesperrten virtuellen Maschine die Fehlerursache und versuchen Sie, das Problem manuell zu beheben. Weitere Informationen hierzu finden Sie unter Beheben von Problemen in Bezug auf fehlende Schlüssel.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Navigieren Sie zur Registerkarte **Übersicht** der virtuellen Maschine.

   Wenn eine virtuelle Maschine gesperrt ist, wird der Alarm „Virtuelle Maschine gesperrt“ angezeigt.
3. Sie können den Alarm bestätigen oder auf „Grün“ zurücksetzen, die virtuelle Maschine zu diesem Zeitpunkt jedoch nicht entsperren.

   Wenn Sie auf **Bestätigen** oder **Auf Grün zurücksetzen** klicken, wird der Alarm ausgeblendet. Die virtuelle Maschine bleibt jedoch solange gesperrt, bis Sie sie entsperren.
4. Navigieren Sie zur Registerkarte **Überwachen** der virtuellen Maschine und klicken Sie auf **Ereignisse**, um weitere Informationen zum Grund der Sperrung der virtuellen Maschine zu erhalten.
5. Führen Sie die vorgeschlagene Fehlerbehebung durch, bevor Sie die virtuelle Maschine entsperren.
6. Navigieren Sie zur Registerkarte **Übersicht** der virtuellen Maschine und klicken Sie auf die Option **VM entsperren**, die sich unterhalb der VM-Konsole befindet.

   Eine Meldung mit der Warnung, dass Verschlüsselungsschlüsseldaten an den Host übermittelt werden, wird angezeigt.
7. Klicken Sie auf **Ja**.

Beheben von Problemen im Zusammenhang mit dem Verschlüsselungsmodus des ESXi-Hosts

Unter bestimmten Umständen kann der Verschlüsselungsmodus des ESXi-Hosts deaktiviert werden.

Für einen ESXi-Host muss der Hostverschlüsselungsmodus aktiviert sein, wenn er verschlüsselte virtuelle Maschinen enthält. Wenn der Host erkennt, dass der zugehörige Hostschlüssel fehlt, oder wenn der Schlüsselanbieter nicht verfügbar ist, kann der Host den Verschlüsselungsmodus unter Umständen nicht aktivieren. vCenter Server erzeugt einen Alarm, wenn der Hostverschlüsselungsmodus nicht aktiviert werden kann.

Verfahren

1. Wenn das Problem in der Verbindung zwischen dem vCenter Server-System und dem Schlüsselanbieter besteht, wird ein Alarm erzeugt und eine Fehlermeldung im Ereignisprotokoll angezeigt.

   Sie müssen die Verbindung mit dem Schlüsselanbieter wiederherstellen, der die betreffenden Verschlüsselungsschlüssel enthält.
2. Wenn Schlüssel fehlen, wird ein Alarm erzeugt und eine Fehlermeldung im Ereignisprotokoll angezeigt.

   Sie müssen sicherstellen, dass die Schlüssel im Schlüsselanbieter vorhanden sind. Informationen zum Wiederherstellen aus einer Sicherung finden Sie in der Dokumentation Ihres Schlüsselverwaltungsanbieters.

Nächste Schritte

Wenn der Verschlüsselungsmodus des Hosts nach der Wiederherstellung der Verbindung mit dem Schlüsselanbieter oder der manuellen Wiederherstellung der Schlüssel für den Schlüsselanbieter weiterhin deaktiviert ist, aktivieren Sie den Verschlüsselungsmodus des Hosts erneut. Weitere Informationen hierzu finden Sie unter Erneutes Aktiveren des Verschlüsselungsmodus eines ESXi-Hosts.

Erneutes Aktiveren des Verschlüsselungsmodus eines ESXi-Hosts

Ab vSphere 6.7 werden Sie in einem vCenter Server-Alarm darüber informiert, wenn der Verschlüsselungsmodus eines ESXi-Hosts deaktiviert wurde. Falls der Hostverschlüsselungsmodus deaktiviert wurde, können Sie ihn erneut aktivieren.

Voraussetzungen

- Vergewissern Sie sich, dass Sie über die erforderlichen Berechtigungen verfügen: **Kryptografievorgänge.Host registrieren**
- Ermitteln Sie vor dem erneuten Aktivieren des Verschlüsselungsmodus die Fehlerursache und versuchen Sie, das Problem manuell zu beheben.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.

2 Navigieren Sie im ESXi-Host zur Registerkarte **Übersicht**.

   Wenn der Verschlüsselungsmodus deaktiviert ist, wird ein Alarm mit dem Hinweis angezeigt, dass der Verschlüsselungsmodus für den Host aktiviert werden muss.

3 Sie können den Alarm bestätigen oder auf „Grün“ zurücksetzen, den Hostverschlüsselungsmodus zu diesem Zeitpunkt jedoch nicht erneut aktivieren.

   Wenn Sie entweder auf **Bestätigen** oder **Auf Grün zurücksetzen** klicken, wird der Alarm ausgeblendet. Der Verschlüsselungsmodus des Hosts bleibt jedoch solange deaktiviert, bis Sie ihn erneut aktivieren.

4 Navigieren Sie zur Registerkarte **Überwachen** des ESXi-Hosts und klicken Sie auf **Ereignisse**, um weitere Informationen über die Gründe für die Deaktivierung des Verschlüsselungsmodus zu erhalten.

   Führen Sie die vorgeschlagene Fehlerbehebung durch, bevor Sie den Verschlüsselungsmodus erneut aktivieren.

5 Klicken Sie auf der Registerkarte **Übersicht** auf **Hostverschlüsselungsmodus aktivieren**, um die Hostverschlüsselung erneut zu aktivieren.

   Eine Meldung mit der Warnung, dass Verschlüsselungsschlüsseldaten an den Host übermittelt werden, wird angezeigt.

6 Klicken Sie auf **Ja**.

Festlegen des Schwellenwerts für den Ablauf des Schlüsselmanagementserver-Zertifikats

Standardmäßig benachrichtigt Sie vCenter Server 30 Tage vor dem Ablaufen Ihrer Schlüsselmanagementserver-Zertifikate (Key Management Server, KMS). Sie können diesen Standardwert ändern.

KMS-Zertifikate haben ein Ablaufdatum. Wenn der Schwellenwert für das Ablaufdatum erreicht ist, werden Sie mittels eines Alarms benachrichtigt.

vCenter Server und Schlüsselanbieter tauschen zwei Arten von Zertifikaten aus: Server und Client. Im VMware Endpoint Certificate Store (VECS) auf dem vCenter Server-System werden die Serverzertifikate und ein Clientzertifikat pro Schlüsselanbieter gespeichert. Da es zwei Zertifikattypen gibt, gibt es zwei Alarme für die beiden Zertifikattypen (einen für Client- und einen für Serverzertifikate).

Verfahren

1 Melden Sie sich bei einem vCenter Server-System mit dem vSphere Client an.

2 Wählen Sie in der Objekthierarchie das vCenter Server-System aus.

3 Klicken Sie auf **Konfigurieren**.

4 Klicken Sie unter **Einstellungen** auf **Erweiterte Einstellungen** und dann auf **Einstellungen bearbeiten**.

5 Klicken Sie auf das Symbol **Filter** und geben Sie `vpxd.kmscert.threshold` ein oder führen Sie einen Bildlauf zum Konfigurationsparameter durch.

6 Geben Sie den Wert in Tagen ein und klicken Sie auf **Speichern**.

vSphere VM-Verschlüsselung und Core-Dumps

Wenn in Ihrer Umgebung vSphere VM-Verschlüsselung verwendet wird und auf dem ESXi-Host ein Fehler auftritt, wird der dadurch entstandene Core-Dump verschlüsselt, um Kundendaten zu schützen. Auch die Core-Dumps im vm-support-Paket sind verschlüsselt.

Hinweis Core-Dumps können vertrauliche Informationen enthalten. Befolgen Sie beim Umgang mit Core-Dumps die Datensicherheits- und Datenschutzrichtlinien Ihrer Organisation.

Core-Dumps auf ESXi-Hosts

Wenn ein ESXi-Host, eine Benutzer-World oder eine virtuelle Maschine fehlschlägt, wird ein Core-Dump erstellt und der Host neu gestartet. Wenn für den ESXi-Host der Verschlüsselungsmodus aktiviert ist, wird der Core-Dump mit einem Schlüssel verschlüsselt, der sich im ESXi-Schlüssel-Cache befindet. Dieser Schlüssel stammt aus dem KMS. Weitere Hintergrundinformationen finden Sie unter Wie vSphere Virtual Machine Encryption Ihre Umgebung schützt.

Wenn ein ESXi-Host aus kryptografischer Sicht „sicher“ ist und ein Core-Dump erzeugt wird, löst dies ein Ereignis aus. Das Ereignis gibt an, dass ein Core-Dump zusammen mit folgenden Informationen durchgeführt wurde: Name der World, Zeitpunkt des Auftretens, keyID des zum Verschlüsseln des Core-Dumps verwendeten Schlüssel sowie der Dateiname des Core-Dumps. Sie können das Ereignis im Ereignis-Viewer unter **Aufgaben und Ereignisse** für den vCenter Server anzeigen.

In der folgenden Tabelle werden die für jeden Core-Dump-Typ verwendeten Verschlüsselungsschlüssel nach vSphere-Version angezeigt.

Tabelle 10-1. Core-Dump-Verschlüsselungsschlüssel

Core-Dump-Typ	Verschlüsselungsschlüssel (ESXi 6.5)	Verschlüsselungsschlüssel (ESXi 6.7 und höher)
ESXi-Kernel	Hostschlüssel	Hostschlüssel
Benutzer-World (hostd)	Hostschlüssel	Hostschlüssel
Verschlüsselte virtuelle Maschine (VM)	Hostschlüssel	VM-Schlüssel

Die Vorgehensweise nach dem Neustart eines ESXi-Hosts hängt von mehreren Faktoren ab.

- In den meisten Fällen ruft vCenter Server den Schlüssel für den Host vom KMS ab und versucht, nach dem Neustart den Schlüssel an den ESXi-Host zu übermitteln. Wenn der Vorgang erfolgreich war, können Sie das vm-support-Paket generieren und den Core-Dump entschlüsseln bzw. neu verschlüsseln. Weitere Informationen hierzu finden Sie unter Entschlüsseln oder erneutes Verschlüsseln eines verschlüsselten Core-Dump.
- Wenn vCenter Server keine Verbindung zum ESXi-Host herstellen kann, können Sie den Schlüssel möglicherweise vom KMS abrufen. Weitere Informationen hierzu finden Sie unter Beheben von Problemen in Bezug auf fehlende Schlüssel.
- Wenn der Host einen benutzerdefinierten Schlüssel verwendet hat und es sich bei diesem Schlüssel nicht um den Schlüssel handelt, den vCenter Server an den Host übermittelt, können Sie den Core-Dump nicht verändern. Vermeiden Sie die Verwendung von benutzerdefinierten Schlüsseln.

Core-Dumps und vm-support-Pakete

Wenn Sie sich an den technischen Support von VMware wenden, um einen schwerwiegenden Fehler zu melden, werden Sie in der Regel von dem Support-Mitarbeiter gebeten, ein vm-support-Paket zu generieren. Das Paket enthält Protokolldateien und weitere Informationen, einschließlich Core-Dumps. Wenn die Support-Mitarbeiter mithilfe der Protokolldateien und weiteren Informationen die Probleme nicht beheben können, werden Sie möglicherweise gebeten, die Core-Dumps zu entschlüsseln und relevante Informationen zur Verfügung zu stellen. Befolgen Sie zum Schutz vertraulicher Informationen wie z. B. Schlüssel die Sicherheits- und Datenschutzrichtlinie Ihres Unternehmens. Weitere Informationen hierzu finden Sie unter Erfassen eines vm-support-Pakets für einen ESXi-Host, auf dem Verschlüsselung verwendet wird.

Core-Dumps auf vCenter Server-Systemen

Ein Core-Dump auf einem vCenter Server-System ist nicht verschlüsselt. vCenter Server enthält bereits potenziell vertrauliche Informationen. Stellen Sie mindestens sicher, dass vCenter Server geschützt ist. Weitere Informationen hierzu finden Sie unter Kapitel 4 Sichern von vCenter Server-Systemen. Alternativ können Sie Core-Dumps für das vCenter Server-System deaktivieren. Weitere Informationen in den Protokolldateien können zum Ermitteln der Ursache des Problems dienlich sein.

Erfassen eines vm-support-Pakets für einen ESXi-Host, auf dem Verschlüsselung verwendet wird

Wenn der Hostverschlüsselungsmodus für den ESXi-Host aktiviert ist, werden alle Core-Dumps im `vm-support`-Paket verschlüsselt. Sie können das Paket vom vSphere Client erfassen und ein Kennwort angeben, falls Sie davon ausgehen, dass der Core-Dump zu einem späteren Zeitpunkt entschlüsselt werden muss.

Das `vm-support`-Paket enthält u. a. Protokolldateien und Core-Dump-Dateien.

Voraussetzungen

Informieren Sie den Supportmitarbeiter darüber, dass der Hostverschlüsselungsmodus für den ESXi-Host aktiviert ist. Der Supportmitarbeiter bittet Sie möglicherweise darum, Core-Dumps zu entschlüsseln und relevante Informationen zu extrahieren.

Hinweis Core-Dumps können vertrauliche Informationen enthalten. Beachten Sie die Sicherheits- und Datenschutzrichtlinie Ihres Unternehmens, um den Schutz vertraulicher Daten wie Hostschlüssel zu gewährleisten.

Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server-System an.
2. Klicken Sie auf **Hosts und Cluster** und klicken Sie dann mit der rechten Maustaste auf den ESXi-Host.
3. Wählen Sie **Systemprotokolle exportieren** aus.
4. Wählen Sie im Dialogfeld **Kennwort für verschlüsselte Core-Dumps** aus, geben Sie ein Kennwort an und bestätigen Sie es.
5. Behalten Sie die Standardeinstellungen für die anderen Optionen bei oder nehmen Sie Änderungen vor, wenn dies vom technischen Support von VMware gefordert wird, und klicken Sie dann auf **Protokolle exportieren**.
6. Geben Sie einen Speicherort für die Datei an.
7. Falls der Supportmitarbeiter Sie dazu aufgefordert hat, den Core-Dump im `vm-support`-Paket zu entschlüsseln, melden Sie sich bei einem ESXi-Host an und führen Sie die folgenden Schritte aus.
   a. Melden Sie sich beim ESXi-Host an und stellen Sie eine Verbindung zu dem Verzeichnis her, in dem sich das `vm-support`-Paket befindet.

      Der Dateiname richtet sich nach folgendem Muster: esx.date_and_time.tgz.

   b. Stellen Sie sicher, dass das Verzeichnis ausreichend Speicherplatz für das Paket, das dekomprimierte Paket und das erneut komprimierte Paket enthält, oder verschieben Sie das Paket.

   c. Extrahieren Sie das Paket in das lokale Verzeichnis.

      ```
      vm-support -x *.tgz .
      ```

      Die daraus resultierende Dateihierarchie enthält möglicherweise Core-Dump-Dateien für den ESXi-Host (üblicherweise im Verzeichnis `/var/core`) und mehrere Core-Dump-Dateien für virtuelle Maschinen.

d Entschlüsseln Sie jede verschlüsselte Core-Dump-Datei separat.

```
crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file
--password encryptedZdump decryptedZdump
```

vm-support-incident-key-file ist die Schlüsseldatei des Vorfalls. Sie befindet sich auf der obersten Ebene im Verzeichnis.

encryptedZdump ist der Name der verschlüsselten Core-Dump-Datei.

decryptedZdump ist der von dem Befehl generierte Name der Datei. Legen Sie einen Namen fest, der *encryptedZdump* ähnelt.

e Geben Sie das Kennwort an, das Sie beim Erstellen des `vm-support`-Pakets angegeben haben.

f Entfernen Sie die verschlüsselten Core-Dumps und komprimieren Sie das Paket erneut.

```
vm-support --reconstruct
```

8 Entfernen Sie alle Dateien, die vertrauliche Informationen enthalten.

Entschlüsseln oder erneutes Verschlüsseln eines verschlüsselten Core-Dump

Ein verschlüsselter Core-Dump auf einem ESXi-Host kann mithilfe der CLI `crypto-util` entschlüsselt oder erneut verschlüsselt werden.

Sie können die Core-Dumps im vm-support-Paket selbst entschlüsseln und untersuchen. Core-Dumps können vertrauliche Informationen enthalten. Beachten Sie die Sicherheits- und Datenschutzrichtlinie Ihres Unternehmens, um den Schutz vertraulicher Daten wie Schlüssel zu gewährleisten.

Nähere Informationen zum erneuten Verschlüsseln eines Core-Dump und weiteren Funktionen von `crypto-util` finden Sie in der Befehlszeilenhilfe.

Hinweis `crypto-util` ist für fortgeschrittene Benutzer vorgesehen.

Voraussetzungen

Der zum Verschlüsseln des Core-Dumps verwendete Schlüssel muss auf dem ESXi-Host verfügbar sein, der den Core-Dump generiert hat.

Verfahren

1 Melden Sie sich direkt beim ESXi-Host an, auf dem der Core-Dump generiert wurde.

Falls sich der ESXi-Host im Sperrmodus befindet, oder wenn der SSH-Zugriff deaktiviert ist, müssen Sie möglicherweise zuerst den Zugriff aktivieren.

2 Ermitteln Sie, ob der Core-Dump verschlüsselt ist.

Option	Beschreibung
Core-Dump überwachen	`crypto-util envelope describe vmmcores.ve`
zdump-Datei	`crypto-util envelope describe --offset 4096 zdumpFile`

3 Entschlüsseln Sie den Core-Dump, je nach Typ.

Option	Beschreibung
Core-Dump überwachen	`crypto-util envelope extract vmmcores.ve vmmcores`
zdump-Datei	`crypto-util envelope extract --offset 4096 zdumpEncrypted zdumpUnencrypted`

Aktivieren und Deaktivieren von Schlüsselpersistenz auf einem ESXi-Host

Sie müssen Schlüsselpersistenz auf einem ESXi-Host aktivieren. Schlüsselpersistenz ist standardmäßig nicht aktiviert.

Konzeptionelle Informationen zur Schlüsselpersistenz finden Sie unter Schlüsselpersistenz – Übersicht.

Voraussetzungen

Anforderungen zum Aktivieren von Schlüsselpersistenz:

- ESXi 7.0 Update 2 oder höher
- Mit TPM 2.0 installierter ESXi-Host
- Zugriff auf den ESXCLI-Befehlssatz. Sie können ESXCLI-Befehle remote oder in der ESXi Shell ausführen.

Hinweis Schlüsselpersistenz ist nicht erforderlich, wenn vSphere Native Key Provider verwendet wird. vSphere Native Key Provider ist sofort einsatzbereit und kann ohne Zugriff auf einen Schlüsselserver ausgeführt werden.

Für zusätzliche Sicherheit kann das TPM auch eine Versiegelungsrichtlinie verwenden, um Manipulationen beim Start des ESXi-Hosts zu verhindern. Weitere Informationen hierzu finden Sie unter Übersicht über TPM-Versiegelungsrichtlinien.

Verfahren

1. Verwenden Sie SSH oder eine andere Remotekonsolenverbindung, um eine Sitzung auf dem ESXi-Host zu starten.
2. Melden Sie sich als „root“ an.
3. Aktivieren oder deaktivieren Sie Schlüsselpersistenz.
   a. So aktivieren Sie Schlüsselpersistenz:

   ```
   esxcli system security keypersistence enable
   ```

   b. So deaktivieren Sie Schlüsselpersistenz:

   ```
   esxcli system security keypersistence disable --remove-all-stored-keys
   ```

Erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine mithilfe des vSphere Client

Sie können den vSphere Client verwenden, um eine flache erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine durchzuführen. Aus geschäftlichen oder Konformitätsgründen können Sie eine erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine durchführen.

Eine flache erneute Schlüsselerstellung oder erneute Schlüsselerstellung (auch als flache Neuverschlüsselung bezeichnet) ermöglicht die Verwendung eines neuen (und unterschiedlichen) Schlüsselverschlüsselungsschlüssels (Key Encryption Key, KEK) auf einer verschlüsselten virtuellen Maschine. Sie können einen Vorgang zur erneuten Schlüsselerstellung durchführen, während die virtuelle Maschine eingeschaltet ist. Sie können auch eine erneute Schlüsselerstellung durchführen, wenn auf der virtuellen Maschine Snapshots vorhanden sind. Die erneute Schlüsselerstellung einer verschlüsselten virtuellen Maschine mit Snapshots ist nur in einem einzelnen Snapshot-Zweig (Festplattenkette) zulässig. Mehrere Snapshot-Zweige werden nicht unterstützt. Wenn die erneute Schlüsselerstellung fehlschlägt, bevor alle Verknüpfungen in der Kette mit dem neuen KEK aktualisiert werden, können Sie weiterhin auf die verschlüsselte virtuelle Maschine zugreifen, vorausgesetzt, Sie verfügen über die alten und neuen KEKs.

Voraussetzungen

Notwendige Berechtigung: **Kryptografievorgänge.Schlüsselserver verwalten**

Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server-System an.
2. Durchsuchen Sie die Bestandsliste und wählen Sie die verschlüsselte virtuelle Maschine aus.
3. Klicken Sie mit der rechten Maustaste auf die verschlüsselte virtuelle Maschine und wählen Sie **VM-Richtlinien** aus.
4. Wählen Sie **Erneut verschlüsseln** aus.

5 Klicken Sie auf **Ja**.

Die verschlüsselte virtuelle Maschine wird mit dem neuen KEK neu verschlüsselt.

Hinweis Wenn die erneute Schlüsselerstellung fehlschlägt, veröffentlicht das Ereignissubsystem das folgende Ereignis:

```
com.vmware.vc.vm.crypto.RekeyFail
```

Sichern von virtuellen Maschinen mit Virtual Trusted Platform Module

11

Mithilfe der vTPM-Funktion (Virtual Trusted Platform Module) können Sie einer virtuellen Maschine einen virtuellen TPM 2.0-Kryptoprozessor hinzufügen.

Ein vTPM ist eine softwarebasierte Darstellung eines physischen Trusted Platform Module 2.0-Chips. Ein vTPM verhält sich wie jedes andere virtuelle Gerät. Sie können ein vTPM genauso wie virtuelle CPUs, Arbeitsspeicher, Festplatten- oder Netzwerk-Controller zu einer virtuellen Maschine hinzufügen. Ein vTPM benötigt keinen Trusted Platform Module-Hardware-Chip.

Dieses Kapitel enthält die folgenden Themen:

Virtual Trusted Platform Module – Übersicht

Ein vTPM (Virtual Trusted Platform Module) ist eine softwarebasierte Darstellung eines physischen Trusted Platform Module 2.0-Chips. Ein vTPM verhält sich wie jedes andere virtuelle Gerät.

Was ist ein vTPM?

vTPMs bieten hardwarebasierte sicherheitsbezogene Funktionen wie zufallsbasierte Zahlengenerierung, Nachweise, Schlüsselgenerierung und vieles mehr. Wenn vTPM zu einer virtuellen Maschine hinzugefügt wird, kann damit das Gastbetriebssystem Schlüssel, die privat sind, aktivieren. Diese Schlüssel werden nicht für das Gastbetriebssystem selbst verfügbar gemacht. Aus diesem Grund sind die Angriffspunkte von virtuellen Maschinen reduziert. In der Regel wirkt sich eine Gefährdung des Gastbetriebssystems auch auf dessen Geheimnisse aus. Die

Aktivierung eines vTPM verringert dieses Risiko jedoch deutlich. Diese Schlüssel können nur durch das Gastbetriebssystem für die Verschlüsselung oder Signierung verwendet werden. Mit einem angehängten vTPM kann ein Client die Identität der virtuellen Maschine remote bestätigen und die ausgeführte Software überprüfen.

Sie können ein vTPM zu einer neuen oder einer vorhandenen virtuellen Maschine hinzufügen. Ein vTPM benötigt VM-Verschlüsselung, um wichtige TPM-Daten zu schützen. Wenn Sie ein vTPM konfigurieren, werden die Dateien der virtuellen Maschine verschlüsselt, die Festplatten hingegen nicht. Sie haben die Möglichkeit, Verschlüsselung für die virtuelle Maschine und die zugehörigen Festplatten explizit hinzuzufügen.

Wenn Sie eine mit einem vTPM aktivierte virtuelle Maschine sichern, muss die Sicherung alle Daten der virtuellen Maschine umfassen, einschließlich der Datei `*.nvram`. Wenn die Datei `*.nvram` nicht in der Sicherung enthalten ist, können Sie eine virtuelle Maschine nicht mit einem vTPM wiederherstellen. Da die VM-Home-Dateien einer vTPM-fähigen virtuellen Maschine verschlüsselt sind, stellen Sie darüber hinaus sicher, dass die Verschlüsselungsschlüssel zum Zeitpunkt der Wiederherstellung verfügbar sind.

Ein vTPM benötigt keinen physischen TPM 2.0-Chip (Trusted Platform Module) auf dem ESXi-Host. Wenn Sie jedoch einen Hostnachweis durchführen möchten, benötigen Sie eine externe Entität, z. B. einen physischen TPM 2.0-Chip. Weitere Informationen hierzu finden Sie unter Sichern von ESXi-Hosts mit Trusted Platform Module.

Hinweis Einer mit einem vTPM aktivierten virtuellen Maschine ist standardmäßig keine Speicherrichtlinie zugeordnet. Nur die VM-Dateien (VM-Home) sind verschlüsselt. Sie haben die Möglichkeit, Verschlüsselung für die virtuelle Maschine und die zugehörigen Festplatten explizit hinzuzufügen. Die VM-Dateien wären dann jedoch bereits verschlüsselt.

vSphere-Anforderungen für vTPMs

Zur Verwendung eines vTPM muss die vSphere-Umgebung folgende Voraussetzungen erfüllen:

- Anforderungen an virtuelle Maschinen:
  - EFI-Firmware
  - Hardwareversion 14 und höher
- Anforderungen an Komponenten:
  - vCenter Server 6.7 und höher für virtuelle Windows-Maschinen verwenden vCenter Server 7.0 Update 2 und höher für virtuelle Linux-Maschinen.
  - VM-Verschlüsselung (zum Verschlüsseln der Home-Dateien der virtuellen Maschine).
  - Für vCenter Server konfigurierter Schlüsselanbieter. Weitere Informationen hierzu finden Sie unter Vergleich von vSphere-Schlüsselanbietern.
- Unterstützung folgender Gastbetriebssysteme:
  - Linux

- Windows Server 2008 und höher
- Windows 7 und höher

Unterschiede zwischen einem Hardware-TPM und einem virtuellen TPM

Sie verwenden ein Hardware-TPM (Trusted Platform Module), um sichere Speicherung von Anmeldeinformationen und Schlüsseln bereitzustellen. Ein vTPM führt dieselben Funktionen wie ein TPM durch, stellt aber kryptografische Koprozessorfunktionen in der Software bereit. Ein vTPM verwendet die `.nvram`-Datei, die mithilfe von VM-Verschlüsselung verschlüsselt wird, als sicheren Speicher.

Ein Hardware-TPM enthält einen vorab geladenen Schlüssel mit der Bezeichnung „Endorsement Key“ (EK). Der EK besitzt einen privaten und öffentlichen Schlüssel. Der EK stellt dem TPM eine eindeutige Identität bereit. Für ein vTPM wird dieser Schlüssel entweder von der VMware Certificate Authority (VMCA) oder einer Drittanbieterzertifizierungsstelle (CA, Certificate Authority) bereitgestellt. Sobald das vTPM einen Schlüssel verwendet, wird der Schlüssel in der Regel nicht geändert, da ansonsten vertrauliche im vTPM gespeicherte Informationen ungültig werden. Das vTPM wendet sich zu keiner Zeit an die Drittanbieter-Zertifizierungsstelle.

Erstellen einer virtuellen Maschine mit einem Virtual Trusted Platform Module

Beim Erstellen einer virtuellen Maschine können Sie ein Virtual Trusted Platform Module (vTPM) hinzufügen, um verbesserte Sicherheitseinstellungen für das Gastbetriebssystem zur Verfügung zu stellen. Vor dem Hinzufügen eines vTPM müssen Sie einen Schlüsselanbieter erstellen.

Das virtuelle TPM von VMware ist mit TPM 2.0 kompatibel und erstellt einen virtuellen Chip mit aktiviertem TPM zur Verwendung durch die virtuelle Maschine und das von ihr gehostete Gastbetriebssystem.

Voraussetzungen

- Stellen Sie sicher, dass Ihre vSphere-Umgebung mit einem Schlüsselanbieter konfiguriert ist. Weitere Informationen hierzu finden Sie unter:
  - Konfigurieren von vSphere Trust Authority
  - Kapitel 7 Konfigurieren und Verwalten eines Standardschlüsselanbieters
  - Kapitel 8 Konfigurieren und Verwalten eines vSphere Native Key Providers
- Als Gastbetriebssystem können Sie Windows Server 2008 und höher, Windows 7 und höher oder Linux verwenden.
- Auf den in Ihrer Umgebung ausgeführten ESXi-Hosts muss ESXi 6.7 oder höher (Windows-Gastbetriebssystem) oder 7.0 Update 2 (Linux-Gastbetriebssystem) installiert sein.
- Die virtuelle Maschine muss EFI-Firmware nutzen.

- Stellen Sie sicher, dass Sie über die erforderlichen Rechte verfügen:
  - **Verschlüsselungsvorgänge.Klonen**
  - **Verschlüsselungsvorgänge.Verschlüsseln**
  - **Verschlüsselungsvorgänge.Neue verschlüsseln**
  - **Verschlüsselungsvorgänge.Migrieren**
  - **Verschlüsselungsvorgänge.VM registrieren**

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Wählen Sie in der Bestandsliste ein Objekt aus, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, beispielsweise einen ESXi-Host oder einen Cluster.
3. Klicken Sie mit der rechten Maustaste auf das Objekt, wählen Sie **Neue virtuelle Maschine** aus und befolgen Sie die Anweisungen zum Erstellen einer virtuellen Maschine.

Option	Aktion
Erstellungstyp auswählen	Erstellen Sie eine neue virtuelle Maschine.
Namen und Ordner auswählen	Legen Sie einen Namen und einen Zielspeicherort fest.
Computing-Ressource auswählen	Geben Sie ein Objekt an, für das Sie über Berechtigungen zum Erstellen einer virtuellen Maschine verfügen. Weitere Informationen hierzu finden Sie unter Voraussetzungen und erforderliche Berechtigungen für die Verschlüsselung.
Speicher auswählen	Wählen Sie einen kompatiblen Datenspeicher aus.
Kompatibilität auswählen	Sie müssen **ESXi 6.7 und höher** für ein Windows-Gastbetriebssystem oder **ESXi 7.0 U2** und höher für ein Linux-Gastbetriebssystem auswählen.
Gastbetriebssystem auswählen	Wählen Sie Windows oder Linux als Gastbetriebssystem aus.
Hardware anpassen	Klicken Sie auf **Neues Gerät hinzufügen** und wählen Sie **Trusted Platform Module** aus. Passen Sie die Hardware weiter an, indem Sie beispielsweise die Festplattengröße oder die CPU ändern.
Bereit zum Abschließen	Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

Ergebnisse

Die vTPM-fähige virtuelle Maschine wird wie angegeben in Ihrem Bestand angezeigt.

Aktivieren des virtuellen Trusted Platform Module für eine vorhandene virtuelle Maschine

Sie können ein virtuelles Trusted Platform Module (vTPM) einer vorhandenen virtuellen Maschine hinzufügen, um verbesserte Sicherheitseinstellungen für das Gastbetriebssystem zur Verfügung zu stellen. Vor dem Hinzufügen eines vTPM müssen Sie einen Schlüsselanbieter erstellen.

VMware Virtual TPM ist mit TPM 2.0 kompatibel und erstellt einen virtuellen Chip mit aktiviertem TPM zur Verwendung durch die virtuelle Maschine und das von ihr gehostete Gastbetriebssystem.

Voraussetzungen

- Stellen Sie sicher, dass Ihre vSphere-Umgebung für einen Schlüsselanbieter konfiguriert ist. Weitere Informationen hierzu finden Sie unter:
  - Konfigurieren von vSphere Trust Authority
  - Kapitel 7 Konfigurieren und Verwalten eines Standardschlüsselanbieters
  - Kapitel 8 Konfigurieren und Verwalten eines vSphere Native Key Providers
- Als Gastbetriebssystem können Sie Windows Server 2008 und höher, Windows 7 und höher oder Linux verwenden.
- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.
- Auf den in Ihrer Umgebung ausgeführten ESXi-Hosts muss ESXi 6.7 oder höher (Windows-Gastbetriebssystem) oder 7.0 Update 2 (Linux-Gastbetriebssystem) installiert sein.
- Die virtuelle Maschine muss EFI-Firmware nutzen.
- Stellen Sie sicher, dass Sie über die erforderlichen Rechte verfügen:
  - **Verschlüsselungsvorgänge.Klonen**
  - **Verschlüsselungsvorgänge.Verschlüsseln**
  - **Verschlüsselungsvorgänge.Neue verschlüsseln**
  - **Verschlüsselungsvorgänge.Migrieren**
  - **Verschlüsselungsvorgänge.VM registrieren**

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Klicken Sie mit der rechten Maustaste auf die zu ändernde virtuelle Maschine in der Bestandsliste und wählen Sie **Einstellungen bearbeiten** aus.
3. Klicken Sie im Dialogfeld **Einstellungen bearbeiten** auf **Neues Gerät hinzufügen** und wählen Sie **Trusted Platform Module** aus.
4. Klicken Sie auf **OK**.

   Auf der Registerkarte **Übersicht** der virtuellen Maschine wird nun das virtuelle Trusted Platform Module im Bereich **VM-Hardware** aufgeführt.

Entfernen eines virtuellen Trusted Platform Module von einer virtuellen Maschine

Sie können die virtuelle Trusted Platform Module-Sicherheit (vTPM) von einer virtuellen Maschine entfernen.

Das Entfernen eines vTPM-Geräts führt dazu, dass alle verschlüsselten Informationen auf der virtuellen Maschine nicht mehr wiederherstellbar sind. Bevor Sie vTPM von einer virtuellen Maschine entfernen, müssen Sie alle Anwendungen im Gastbetriebssystem deaktivieren, die das vTPM-Gerät (wie z. B. BitLocker) verwenden. Wenn Sie dies nicht tun, kann die virtuelle Maschine unter Umständen nicht gestartet werden. Darüber hinaus können Sie ein vTPM-Gerät auch nicht aus einer virtuellen Maschine entfernen, die Snapshots enthält.

Voraussetzungen

- Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.
- Stellen Sie sicher, dass Sie über die erforderliche Berechtigung verfügen: **Verschlüsselungsvorgänge.Entschlüsseln**

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Klicken Sie mit der rechten Maustaste auf die zu ändernde virtuelle Maschine in der Bestandsliste und wählen Sie **Einstellungen bearbeiten** aus.
3. Suchen Sie im Dialogfeld **Einstellungen bearbeiten** auf der Registerkarte **Virtuelle Hardware** den Eintrag für Trusted Platform Module.
4. Bewegen Sie den Mauszeiger über das Gerät und klicken Sie auf das Symbol **Entfernen**.

   Dieses Symbol wird nur für die virtuelle Hardware angezeigt, die Sie sicher entfernen können.
5. Klicken Sie auf **Löschen**, um zu bestätigen, dass Sie das Gerät entfernen möchten.

   Das vTPM-Gerät ist zum Entfernen markiert.
6. Klicken Sie auf **OK**.

   Vergewissern Sie sich, dass der Eintrag für das virtuelle Trusted Platform Module nicht mehr auf der Registerkarte **Übersicht** der virtuellen Maschine im Bereich **VM-Hardware** angezeigt wird.

Angeben vTPM-fähiger virtueller Maschinen

Sie können feststellen, welche Ihrer virtuellen Maschinen für die Verwendung eines Virtual Trusted Platform Module (vTPM) aktiviert sind.

Sie können eine Liste aller virtuellen Maschinen in Ihrer Bestandsliste generieren, in der der Name, das Betriebssystem und der vTPM-Status der virtuellen Maschinen angezeigt werden. Sie können diese Liste zur Verwendung in Konformitätsprüfungen auch in eine CSV-Datei exportieren.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Wählen Sie eine vCenter Server-Instanz, einen Host oder einen Cluster aus.
3. Klicken Sie auf der Registerkarte **VMs** auf **Virtuelle Maschinen**.

4 Um alle virtuellen Maschinen anzuzeigen, auf denen ein TPM aktiviert ist, klicken Sie in der unteren linken Ecke auf das **Spaltenauswahl**-Symbol mit den drei Balken und wählen Sie **TPM** aus.

   In der TPM-Spalte wird für virtuelle Maschinen, auf denen TPM aktiviert ist, „Vorhanden“ angezeigt. Virtuelle Maschinen ohne TPM werden als „Nicht vorhanden“ aufgeführt.

5 Sie können den Inhalt einer Bestandslistenansicht in eine CSV-Datei exportieren.

   a Klicken Sie rechts unten in einer Listenansicht auf **Exportieren**.

      Das Dialogfeld „Listeninhalt exportieren“ wird angezeigt; hier werden die Optionen angezeigt, die in die CSV-Datei aufgenommen werden können.

   b Legen Sie fest, ob alle Zeilen oder die aktuelle Auswahl an Zeilen in der CSV-Datei aufgeführt werden sollen.

   c Wählen Sie aus den verfügbaren Optionen die Spalten aus, die in der CSV-Liste aufgeführt werden sollen.

   d Klicken Sie auf **Exportieren**.

      Die CSV-Datei wird generiert und ist zum Download verfügbar.

Anzeigen von Zertifikaten des Virtual Trusted Platform Module-Geräts

Im Lieferumfang von vTPM-Geräten (Virtual Trusted Platform Module) sind vorkonfigurierte Standardzertifikate enthalten, die von Ihnen überprüft werden können.

Voraussetzungen

In Ihrer Umgebung muss eine virtuelle Maschine mit aktiviertem vTPM vorhanden sein.

Verfahren

1 Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.

2 Wählen Sie in der Bestandsliste ein Objekt aus, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, beispielsweise einen ESXi-Host oder einen Cluster.

3 Klicken Sie auf **VMs** und dann auf **Virtuelle Maschinen**.

4 Wählen Sie die vTPM-fähige VM aus, deren Zertifikatsinformationen angezeigt werden sollen.

   Klicken Sie bei Bedarf in der unteren linken Ecke auf das **Spaltenauswahl**-Symbol mit den drei Balken und wählen Sie **TPM** aus, um virtuelle Maschinen mit einem TPM mit Status „Vorhanden“ anzuzeigen.

5 Klicken Sie auf die Registerkarte **Konfigurieren**.

6 Wählen Sie unter **TPM** die Option **Zertifikate** aus.

7 Wählen Sie das Zertifikat aus und zeigen Sie dessen Informationen an.

8 (Optional) Klicken Sie zum Exportieren der Zertifikatsinformationen auf **Exportieren**.

Das Zertifikat wird auf der Festplatte gespeichert.

Nächste Schritte

Sie können das Standardzertifikat durch ein von einer Drittanbieter-Zertifizierungsstelle (CA) ausgestelltes Zertifikat ersetzen. Weitere Informationen hierzu finden Sie unter Exportieren und Ersetzen von Virtual Trusted Platform Module-Gerätezertifikaten.

Exportieren und Ersetzen von Virtual Trusted Platform Module-Gerätezertifikaten

Sie können das im Lieferumfang eines vTPM-Geräts (Virtual Trusted Platform Module) enthaltene Standardzertifikat ersetzen.

Voraussetzungen

In Ihrer Umgebung muss eine virtuelle Maschine mit aktiviertem vTPM vorhanden sein.

Verfahren

1 Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.

2 Wählen Sie in der Bestandsliste ein Objekt aus, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, beispielsweise einen ESXi-Host oder einen Cluster.

3 Wählen Sie in der Bestandsliste die virtuelle Maschine mit aktiviertem vTPM aus, deren Zertifikatsinformationen Sie ersetzen möchten.

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

5 Wählen Sie unter **TPM** die Option **Signieranforderungen** aus.

6 Wählen Sie ein Zertifikat aus.

7 Um die Zertifikatsinformationen zu exportieren, klicken Sie auf **Exportieren**.

Das Zertifikat wird auf der Festplatte gespeichert.

8 Rufen Sie für die von Ihnen exportierte Zertifikatsignieranforderung (Certificate Signing Request, CSR) ein von einer Drittanbieter-Zertifizierungsstelle (Certificate Authority, CA) ausgestelltes Zertifikat ab.

Sie können eine beliebige Zertifizierungsstelle verwenden, die in Ihrer IT-Umgebung möglicherweise verfügbar ist.

9 Wenn Ihnen das neue Zertifikat zur Verfügung steht, ersetzen Sie das vorhandene Zertifikat.

a Klicken Sie mit der rechten Maustaste in der Bestandsliste auf die virtuelle Maschine, deren Zertifikat Sie ersetzen möchten, und wählen Sie **Einstellungen bearbeiten** aus.

b Erweitern Sie im Dialogfeld **Einstellungen bearbeiten** die Option **Sicherheitsgeräte** und erweitern Sie dann **Trusted Platform Module**.

Das Zertifikat wird angezeigt.

c Klicken Sie für das Zertifikat, das Sie ersetzen möchten, auf **Ersetzen**.

Das Dialogfeld **Datei-Upload** wird angezeigt.

d Suchen Sie das neue Zertifikat auf Ihrer lokalen Maschine und laden Sie es hoch.

Das neue Zertifikat ersetzt das Standardzertifikat, das im Lieferumfang Ihres vTPM-Geräts enthalten war.

e Der Zertifikatsname wird auf der Registerkarte **Übersicht** der virtuellen Maschine unter der Liste **Virtuelles Trusted Platform Module** aktualisiert.

Sichern von Windows-Gastbetriebssystemen mit virtualisierungsbasierter Sicherheit

12

Ab vSphere 6.7 können Sie Microsoft VBS (Virtualization-Based Security, Virtualisierungsbasierte Sicherheit) auf unterstützten Windows-Gastbetriebssystemen aktivieren.

Microsoft VBS, eine Funktion von Windows 10 und Windows Server 2016, verwendet Hardware- und Softwarevirtualisierung zur Verbesserung der Systemsicherheit, indem ein isoliertes auf einen Hypervisor beschränktes spezialisiertes Subsystem erstellt wird.

Mit VBS können Sie die folgenden Windows-Sicherheitsfunktionen verwenden, um das System zusätzlich zu sichern und wichtige System- und Benutzergeheimnisse vor Missbrauch zu schützen:

- Credential Guard: Zielt darauf ab, wichtige System- und Benutzergeheimnisse zu isolieren und vor Missbrauch zu schützen.
- Device Guard: Stellt eine Gruppe von Funktionen bereit, mit denen die Ausführung von Malware auf einem Windows-System vermieden werden kann.
- Konfigurierbare Codeintegrität: Stellt sicher, dass nur vertrauenswürdiger Code nach dem Bootloader-Programm ausgeführt wird.

Weitere Informationen finden Sie im Thema zu virtualisierungsbasierter Sicherheit in der Microsoft-Dokumentation.

Nachdem Sie VBS für eine virtuelle Maschine über vCenter Server aktiviert haben, aktivieren Sie VBS innerhalb des Windows-Gastbetriebssystems.

Dieses Kapitel enthält die folgenden Themen:

Virtualisierungsbasierte Sicherheit – Empfohlene Vorgehensweisen

Befolgen Sie die empfohlenen Vorgehensweisen für virtualisierungsbasierte Sicherheit (VBS), um Sicherheit und Handhabbarkeit Ihrer Windows-Gastbetriebssystemumgebung zu maximieren.

Vermeiden Sie Probleme, indem Sie diese empfohlenen Vorgehensweisen befolgen.

VBS-Hardware

Verwenden Sie folgende Hardware für VBS:

- Intel
  - Haswell-CPU oder höher. Verwenden Sie für eine optimale Leistung die Skylake-EP-CPU oder höher.
  - Die Ivy-Bridge-CPU ist akzeptabel.
  - Die Sandy-Bridge-CPU kann die Leistung beeinträchtigen.
- AMD
  - CPUs der Zen 2-Serie (Rome) oder höher.
  - Ältere CPUs können die Leistung beeinträchtigen.

Die Risikominderungen für die Schwachstelle „Machine Check Exception on Page Size Change Intel CPU“ können sich negativ auf die Leistung des Gastbetriebssystems auswirken, wenn VBS verwendet wird. Weitere Informationen finden Sie im VMware Knowledge Base-Artikel unter https://kb.vmware.com/kb/76050.

Kompatibilität des Windows-Gastbetriebssystems

Auf Intel wird VBS für virtuelle Maschinen unter Windows 10, Windows Server 2016 und höher unterstützt. Für die Windows Server 2016-Versionen 1607 und 1703 sind jedoch Patches erforderlich. In der Microsoft-Dokumentation finden Sie Informationen zur Hardwarekompatibilität der ESXi-Hosts. Die Verwendung von Intel-CPUs für VBS erfordert vSphere 6.7 oder höher und Hardwareversion 14.

Auf AMD wird VBS auf virtuellen Maschinen mit Windows 10, Version 1809 und Windows 2019 und höher unterstützt. Die Verwendung von AMD-CPUs für VBS erfordert vSphere 7.0 Update 2 oder höher und Hardwareversion 19.

Anfänglich war für Windows 10 erforderlich, dass Sie Hyper-V für VBS aktivieren. Die Aktivierung von Hyper-V ist für Windows 10 nicht mehr erforderlich. Dasselbe gilt für Windows Server 2016 und höher. Weitere Informationen finden Sie in der aktuellen Microsoft-Dokumentation und in den *VMware vSphere-Versionshinweisen* .

Nicht unterstützte VMware-Funktionen auf VBS

Die folgenden Funktionen werden bei aktivierter VBS auf einer virtuellen Maschine nicht unterstützt:

- Fault Tolerance
- PCI-Passthrough
- CPU oder Arbeitsspeicher im laufenden Betrieb hinzufügen

Installations- und Upgrade-Einschränkungen mit VBS

Vor der Konfiguration von VBS müssen Sie sich mit den folgenden Einschränkungen hinsichtlich Installation und Aktualisierung vertraut machen:

- Neue virtuelle Maschinen, die in niedrigeren virtuellen Hardwareversionen als Version 14 für Windows 10 und Windows Server 2016 und höher konfiguriert werden, werden standardmäßig mit dem Legacy-BIOS erstellt. Sie müssen das Gastbetriebssystem neu installieren, nachdem Sie den Firmware-Typ der virtuellen Maschine von Legacy-BIOS in UEFI geändert haben.
- Wenn Sie Ihre virtuellen Maschinen von vorherigen vSphere-Versionen zu vSphere 6.7 oder höher migrieren und VBS auf den virtuellen Maschinen aktivieren möchten, verwenden Sie UEFI, um eine Neuinstallation des Betriebssystems zu vermeiden.

Aktivieren der virtualisierungsbasierten Sicherheit auf einer virtuellen Maschine

Sie können die virtualisierungsbasierte Sicherheit (VBS) von Microsoft für unterstützte Windows-Gastbetriebssysteme während der Erstellung einer virtuellen Maschine aktivieren.

Die Aktivierung von VBS ist ein Prozess, bei dem VBS zuerst in der virtuellen Maschine und anschließend im Windows-Gastbetriebssystem aktiviert wird.

Voraussetzungen

Weitere Informationen zu geeigneten CPUs finden Sie unter Virtualisierungsbasierte Sicherheit – Empfohlene Vorgehensweisen.

Die Verwendung von Intel-CPUs für VBS erfordert vSphere 6.7 oder höher. Erstellen Sie eine virtuelle Maschine, für die Hardwareversion 14 oder höher und eines der folgenden unterstützten Gastbetriebssysteme verwendet wird:

- Windows 10 (64 Bit) oder höhere Versionen
- Windows Server 2016 (64 Bit) oder höhere Versionen

Die Verwendung von AMD-CPUs für VBS erfordert vSphere 7.0 Update 2 oder höher. Erstellen Sie eine virtuelle Maschine, für die Hardwareversion 19 oder höher und eines der folgenden unterstützten Gastbetriebssysteme verwendet wird:

- Windows 10 (64 Bit), Version 1809 oder höhere Versionen

- Windows Server 2019 (64 Bit) oder höhere Versionen

Stellen Sie sicher, dass Sie die neuesten Patches für Windows 10, Version 1809, und Windows Server 2019 installieren, bevor Sie VBS aktivieren.

Verfahren

1. Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.
2. Wählen Sie in der Bestandsliste ein Objekt aus, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, beispielsweise einen ESXi-Host oder einen Cluster.
3. Klicken Sie mit der rechten Maustaste auf das Objekt, wählen Sie **Neue virtuelle Maschine** aus und befolgen Sie die Anweisungen zum Erstellen einer virtuellen Maschine.

Option	Aktion
Erstellungstyp auswählen	Erstellen Sie eine virtuelle Maschine.
Namen und Ordner auswählen	Legen Sie einen Namen und einen Zielspeicherort fest.
Computing-Ressource auswählen	Geben Sie ein Objekt an, für das Sie über Rechte zum Erstellen von virtuellen Maschinen verfügen.
Speicher auswählen	Wählen Sie in der VM-Speicherrichtlinie die entsprechende Speicherrichtlinie aus. Wählen Sie einen kompatiblen Datenspeicher aus.
Kompatibilität auswählen	Intel-CPU: Stellen Sie sicher, dass **ESXi 6.7 und höher** ausgewählt ist. AMD-CPU: Stellen Sie sicher, dass **ESXi 7.0 U2 und höher** ausgewählt ist.
Gastbetriebssystem auswählen	Wählen Sie für das Windows Gastbetriebssystem die Option aus, die der Betriebssystemversion am besten entspricht. Aktivieren Sie das Kontrollkästchen **Virtualisierungsbasierte Sicherheit für Windows aktivieren**.
Hardware anpassen	Passen Sie die Hardware an, indem Sie z. B. die Festplattengröße oder die CPU ändern.
Bereit zum Abschließen	Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

Ergebnisse

Sobald die virtuelle Maschine erstellt ist, vergewissern Sie sich, dass auf der Registerkarte **Übersicht** in der Beschreibung des Gastbetriebssystems „VBS wahr“ angezeigt wird.

Nächste Schritte

Weitere Informationen hierzu finden Sie unter Aktivieren der virtualisierungsbasierten Sicherheit im Gastbetriebssystem.

Aktivieren der virtualisierungsbasierten Sicherheit auf einer vorhandenen virtuellen Maschine

Sie können die virtualisierungsbasierte Sicherheit (VBS) von Microsoft auf vorhandenen virtuellen Maschinen für unterstützte Windows-Gastbetriebssysteme aktivieren.

Die Aktivierung von VBS ist ein Prozess, bei dem VBS zuerst in der virtuellen Maschine und anschließend im Gastbetriebssystem aktiviert wird.

Hinweis Neue virtuelle Maschinen, die in niedrigeren Hardwareversionen als Version 14 für Windows 10, Windows Server 2016 und Windows Server 2019 konfiguriert werden, werden standardmäßig mit dem Legacy-BIOS erstellt. Wenn Sie den Firmwaretyp der virtuellen Maschine von Legacy-BIOS in UEFI ändern, müssen Sie das Gastbetriebssystem neu installieren.

Voraussetzungen

Weitere Informationen zu geeigneten CPUs finden Sie unter Virtualisierungsbasierte Sicherheit – Empfohlene Vorgehensweisen.

Die Verwendung von Intel-CPUs für VBS erfordert vSphere 6.7 oder höher. Die virtuelle Maschine muss mit der Hardwareversion 14 oder höher und einem der folgenden unterstützten Gastbetriebssysteme erstellt worden sein:

- Windows 10 (64 Bit) oder höhere Versionen
- Windows Server 2016 (64 Bit) oder höhere Versionen

Die Verwendung von AMD-CPUs für VBS erfordert vSphere 7.0 Update 2 oder höher. Die virtuelle Maschine muss mit der Hardwareversion 19 oder höher und einem der folgenden unterstützten Gastbetriebssysteme erstellt worden sein:

- Windows 10 (64 Bit), Version 1809 oder höhere Versionen
- Windows Server 2019 (64 Bit) oder höhere Versionen

Stellen Sie sicher, dass Sie die neuesten Patches für Windows 10, Version 1809, und Windows Server 2019 installieren, bevor Sie VBS aktivieren.

Verfahren

1. Navigieren Sie im vSphere Client zur virtuellen Maschine.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
3. Klicken Sie auf die Registerkarte **VM-Optionen**.
4. Aktivieren Sie das Kontrollkästchen **Aktivieren** für die virtualisierungsbasierte Sicherheit.
5. Klicken Sie auf **OK**.

Ergebnisse

Vergewissern Sie sich, dass auf der Registerkarte **Übersicht** der virtuellen Maschine in der Beschreibung des Gastbetriebssystems „VBS wahr“ angezeigt wird.

Nächste Schritte

Weitere Informationen hierzu finden Sie unter Aktivieren der virtualisierungsbasierten Sicherheit im Gastbetriebssystem.

Aktivieren der virtualisierungsbasierten Sicherheit im Gastbetriebssystem

Sie können die virtualisierungsbasierte Sicherheit (VBS) von Microsoft für unterstützte Windows-Gastbetriebssysteme aktivieren.

Sie aktivieren VBS innerhalb des Windows-Gastbetriebssystems. Windows konfiguriert und erzwingt VBS über ein Gruppenrichtlinienobjekt (GPO). Mit dem Gruppenrichtlinienobjekt können Sie die verschiedenen von VBS bereitgestellten Dienste aus- und einschalten, beispielsweise sicherer Start, Device Guard und Credential Guard. Bei bestimmten Windows-Versionen müssen Sie einen zusätzlichen Schritt zur Aktivierung der Hyper-V-Plattform durchführen.

In der Microsoft-Dokumentation finden Sie Details zum Bereitstellen von Device Guard, um die virtualisierungsbasierte Sicherheit zu aktivieren.

Voraussetzungen

- Stellen Sie sicher, dass die virtualisierungsbasierte Sicherheit für die virtuelle Maschine aktiviert ist.

Verfahren

1. Bearbeiten Sie unter Microsoft Windows die Gruppenrichtlinie, um VBS zu aktivieren, und wählen Sie andere VBS-bezogene Sicherheitsoptionen aus.
2. (Optional) Bei Microsoft Windows-Versionen vor Redstone 4 aktivieren Sie die Hyper-V-Plattform in der Systemsteuerung unter „Windows-Funktionen“.
3. Starten Sie das Gastbetriebssystem neu.

Deaktivieren der virtualisierungsbasierten Sicherheit

Falls Sie die virtualisierungsbasierte Sicherheit (VBS) bei einer virtuellen Maschine nicht mehr verwenden, können Sie sie deaktivieren. Bei der Deaktivierung von VBS für die virtuelle Maschine bleiben die VBS-Optionen von Windows unverändert, sie rufen dann aber möglicherweise Leistungsprobleme hervor. Deaktivieren Sie VBS-Optionen in Windows, bevor Sie VBS auf der virtuellen Maschine deaktivieren.

Voraussetzungen

Stellen Sie sicher, dass die virtuelle Maschine ausgeschaltet ist.

Verfahren

1. Navigieren Sie im vSphere Client zu der virtuellen Maschine mit aktivierter VBS.

   Hilfe bei der Suche nach virtuellen Maschinen mit aktivierter VBS finden Sie unter Identifizieren von VBS-fähigen virtuellen Maschinen.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.

3 Klicken Sie auf **VM-Optionen**.

4 Deaktivieren Sie das Kontrollkästchen **Aktivieren** für die virtualisierungsbasierte Sicherheit.

   Sie werden in einer Meldung daran erinnert, VBS im Gastbetriebssystem zu deaktivieren.

5 Klicken Sie auf **OK**.

6 Stellen Sie sicher, dass auf der Registerkarte **Übersicht** der virtuellen Maschine in der Beschreibung des Gastbetriebssystems nicht mehr „VBS wahr“ angezeigt wird.

Identifizieren von VBS-fähigen virtuellen Maschinen

Sie können ermitteln, auf welcher Ihrer virtuellen Maschinen VBS zu Berichterstellungs- und Übereinstimmungszwecken aktiviert ist.

Verfahren

1 Stellen Sie mit dem vSphere Client eine Verbindung zu vCenter Server her.

2 Wählen Sie eine vCenter Server-Instanz, ein Datencenter oder einen Host in der Bestandsliste aus.

3 Klicken Sie auf der Registerkarte **VMs** auf **Virtuelle Maschinen**.

4 Klicken Sie in der unteren linken Ecke auf die **Spaltenauswahl**-Symbol mit den den drei Balken und aktivieren Sie das Kontrollkästchen **VBS**, um die Spalte **VBS** anzuzeigen.

5 Durchsuchen Sie die Spalte **VBS** nach „Vorhanden“.

Sichern der vSphere-Netzwerke 13

Das Sichern der vSphere-Netzwerke ist ein wesentlicher Bestandteil für den Schutz Ihrer Umgebung. Die verschiedenen vSphere-Komponenten werden auf unterschiedliche Weise gesichert. Ausführliche Informationen zu Netzwerken in der vSphere-Umgebung finden Sie in der Dokumentation *vSphere-Netzwerk*.

Dieses Kapitel enthält die folgenden Themen:

Einführung in die Netzwerksicherheit in vSphere

Die Netzwerksicherheit in der vSphere-Umgebung weist viele gemeinsame Merkmale mit der Absicherung einer physischen Netzwerkumgebung auf, aber auch einige Merkmale, die nur virtuelle Maschinen betreffen.

Firewalls

Fügen Sie Firewallschutz für das virtuelle Netzwerk durch Installation und Konfiguration von hostbasierten Firewalls auf bestimmten oder allen VMs hinzu.

Aus Effizienzgründen können Sie private Ethernet-Netzwerke virtueller Maschinen oder Virtuelle Netzwerke einrichten. In virtuellen Netzwerken installieren Sie eine hostbasierte Firewall auf einer VM am Eingang des virtuellen Netzwerks. Diese Firewall dient als Schutzpufferzone zwischen dem physischen Netzwerkadapter und den übrigen VMs im virtuellen Netzwerk.

Hostbasierte Firewalls können die Leistung beeinträchtigen. Stimmen Sie Ihre Sicherheitsbedürfnisse mit den Leistungszielen ab, bevor Sie hostbasierte Firewalls auf VMs an anderen Positionen im virtuellen Netzwerk installieren.

Weitere Informationen hierzu finden Sie unter Absichern des Netzwerks mit Firewalls.

Segmentierung

Behalten Sie verschiedene Zonen aus virtuellen Maschinen innerhalb eines Hosts auf verschiedenen Netzwerksegmenten bei. Wenn Sie jede virtuelle Maschinenzone in deren eigenem Netzwerksegment isolieren, minimieren Sie das Risiko eines Datenverlusts zwischen zwei Zonen. Segmentierung verhindert verschiedene Bedrohungen, einschließlich ARP-Manipulation (Address Resolution Protocol). Bei der ARP-Manipulation verändert ein Angreifer die ARP-Tabelle dahingehend, dass MAC- und IP-Adressen neu zugeordnet werden, und erhält somit Zugriff auf Netzwerkverkehr von und zu einem Host. Angreifer verwenden diese ARP-Manipulation für Man-in-the-Middle-Angriffe (MITM), für Denial of Service-Angriffe (DoS), zur Übernahme des Zielsystems und zur anderweitigen Beeinträchtigung des virtuellen Netzwerks.

Durch eine umsichtige Planung der Segmentierung wird das Risiko von Paketübertragungen zwischen VM-Zonen gesenkt. Durch die Segmentierung werden Spionageangriffe verhindert, die das Senden von Netzwerkverkehr an das Opfer erforderlich machen. So kann ein Angreifer auch keinen unsicheren Dienst in einer virtuellen Maschinenzone aktivieren, um auf andere virtuelle Maschinenzonen im Host zuzugreifen. Die Segmentierung können Sie mithilfe einer der beiden folgenden Methoden implementieren.

- Verwenden Sie getrennte physische Netzwerkadapter für Zonen virtueller Maschinen, damit die Zonen auch tatsächlich voneinander getrennt sind. Die Beibehaltung getrennter physischer Netzwerkadapter für die virtuellen Maschinenzonen stellt unter Umständen die sicherste Methode nach dem Anlegen des ersten Segments dar. Dieser Ansatz ist weniger anfällig für Konfigurationsfehler.
- Richten Sie virtuelle LANs (VLANs) zur Absicherung des Netzwerks ein. VLANs bieten fast alle Sicherheitsvorteile, die der Installation physisch getrennter Netzwerke innewohnen, ohne dass zusätzliche Hardware angeschafft werden muss. Bei Verwendung von VLANs fallen keine Kosten für Bereitstellung und Verwaltung zusätzlicher Geräte, Verkabelung usw. an. Weitere Informationen hierzu finden Sie unter Absichern virtueller Maschinen durch VLANs.

Verhindern des nicht autorisierten Zugriffs

Anforderungen an die Sicherung von VMs entsprechen häufig den Anforderungen an die Sicherung physischer Maschinen.

- Wenn ein VM-Netzwerk an ein physisches Netzwerk angeschlossen ist, kann es ebenso Sicherheitslücken aufweisen wie ein Netzwerk, das aus physischen Maschinen besteht.

- Selbst wenn Sie eine VM nicht an das physische Netzwerk anschließen, kann die VM von anderen VMs angegriffen werden.

VMs sind voneinander isoliert. Eine VM kann weder Lese- noch Schreibvorgänge im Speicher einer anderen VM ausführen noch auf deren Daten zugreifen, ihre Anwendungen verwenden usw. Dennoch kann jede VM oder VM-Gruppe innerhalb des Netzwerks weiterhin Ziel eines unerlaubten Zugriffs durch andere VMs sein. Schützen Sie Ihre VMs vor unerlaubtem Zugriff.

Weitere Informationen zum Schutz virtueller Maschinen finden Sie im NIST-Dokument mit dem Titel „Sichere virtuelle Netzwerkkonfiguration zum Schutz virtueller Maschinen (VM)“ unter:

https://csrc.nist.gov/publications/detail/sp/800-125b/final

Absichern des Netzwerks mit Firewalls

Sicherheitsadministratoren verwenden Firewalls, um das Netzwerk oder ausgewählte Komponenten innerhalb des Netzwerks vor unerlaubten Zugriffen zu schützen.

Firewalls kontrollieren den Zugriff auf die Geräte in ihrem Umfeld, indem sie alle Ports außer denen abriegeln, die der Administrator explizit oder implizit als zulässig definiert. Die Ports, die Administratoren öffnen, erlauben Datenverkehr zwischen Geräten auf beiden Seiten der Firewall.

Wichtig Mit der ESXi-Firewall in ESXi 5.5 und höher kann der vMotion-Datenverkehr nicht pro Netzwerk gefiltert werden. Daher müssen Sie Regeln für Ihre externe Firewall installieren, um sicherzustellen, dass keine eingehenden Verbindungen mit dem vMotion-Socket hergestellt werden können.

In der Umgebung mit virtuellen Maschinen können Sie das Layout für die Firewalls zwischen den Komponenten planen.

- Firewalls zwischen physischen Maschinen, z. B. vCenter Server-Systemen und ESXi-Hosts.
- Firewalls zwischen zwei virtuellen Maschinen – beispielsweise zwischen einer virtuellen Maschine, die als externer Webserver dient, und einer virtuellen Maschine, die an das interne Firmennetzwerk angeschlossen ist.
- Firewalls zwischen einem physischen Computer und einer virtuellen Maschine, wenn Sie beispielsweise eine Firewall zwischen einen physischen Netzwerkadapter und eine virtuelle Maschine schalten.

Die Nutzungsweise von Firewalls in einer ESXi-Konfiguration hängt davon ab, wie Sie das Netzwerk nutzen möchten und wie sicher die einzelnen Komponenten sein müssen. Wenn Sie zum Beispiel ein virtuelles Netzwerk erstellen, in dem jede virtuelle Maschine eine andere Benchmark-Testsuite für die gleiche Abteilung ausführt, ist das Risiko ungewollten Zugriffs von einer virtuellen Maschine auf eine andere minimal. Eine Konfiguration, bei der Firewalls zwischen den virtuellen Maschinen vorhanden sind, ist daher nicht erforderlich. Um jedoch eine Störung der Testläufe durch einen externen Host zu verhindern, kann eine Firewall am Eingangspunkt zum virtuellen Netzwerk konfiguriert werden, um alle virtuellen Maschinen zu schützen.

Eine Liste aller unterstützten Ports und Protokolle in VMware, einschließlich vSphere und vSAN, finden Sie im Tool VMware Ports and Protocols™ unter https://ports.vmware.com/. Sie können Ports nach VMware-Produkt durchsuchen, eine benutzerdefinierte Portliste erstellen und Portlisten drucken oder speichern.

Firewalls in Konfigurationen mit vCenter Server

Wenn Sie über vCenter Server auf ESXi-Hosts zugreifen, schützen Sie vCenter Server normalerweise durch eine Firewall.

Firewalls müssen an den Zugangspunkten vorhanden sind. Eine Firewall kann zwischen den Clients und vCenter Server vorhanden sein, oder vCenter Server und die Clients können sich beide hinter einer Firewall befinden.

Eine Liste aller unterstützten Ports und Protokolle in VMware, einschließlich vSphere und vSAN, finden Sie im Tool VMware Ports and Protocols™ unter https://ports.vmware.com/. Sie können Ports nach VMware-Produkt durchsuchen, eine benutzerdefinierte Portliste erstellen und Portlisten drucken oder speichern.

Mit vCenter Server konfigurierte Netzwerke können über den vSphere Client, über andere UI-Clients oder Clients, die die vSphere API verwenden, Daten erhalten. Während des normalen Betriebs wartet vCenter Server an bestimmten Ports auf Daten von verwalteten Hosts und Clients. vCenter Server geht auch davon aus, dass die verwalteten Hosts an bestimmten Ports auf Daten von vCenter Server warten. Wenn sich zwischen diesen Elementen eine Firewall befindet, muss sichergestellt werden, dass Firewall-Ports für den Datenverkehr geöffnet wurden.

Firewalls können je nach Netzwerkauslastung und der für Clients erforderlichen Sicherheitsstufe auch an anderen Zugriffspunkten im Netzwerk hinzugefügt werden. Bestimmen Sie die Installationspunkte für Ihre Firewalls anhand der Sicherheitsrisiken für Ihre Netzwerkkonfiguration. Die folgenden Firewall-Installationspunkte werden häufig verwendet.

- Zwischen dem vSphere Client oder einem Netzwerkverwaltungs-Client eines Drittanbieters und vCenter Server.
- Wenn die Benutzer über einen Webbrowser auf virtuelle Maschinen zugreifen, zwischen dem Webbrowser und dem ESXi-Host.
- Wenn die Benutzer über den vSphere Client auf virtuelle Maschinen zugreifen, zwischen dem vSphere Client und dem ESXi-Host. Diese Verbindung ist ein Zusatz zu der Verbindung zwischen dem vSphere Client und vCenter Server und benötigt einen anderen Port.
- Zwischen vCenter Server und den ESXi-Hosts.
- Zwischen den ESXi-Hosts in Ihrem Netzwerk. Zwar ist der Datenverkehr zwischen Hosts normalerweise vertrauenswürdig, aber Sie können bei befürchteten Sicherheitsrisiken zwischen den einzelnen Computern dennoch Firewalls zwischen den Hosts installieren.

  Wenn Sie Firewalls zwischen ESXi-Hosts hinzufügen und die Migration virtueller Maschinen zwischen diesen Hosts planen, öffnen Sie Ports in einer beliebigen Firewall, die den Quellhost von den Zielhosts trennt.

- Zwischen ESXi-Hosts und Netzwerkspeicher, z. B. NFS- oder iSCSI-Speicher. Diese Ports sind nicht VMware-spezifisch. Konfigurieren Sie sie anhand der Spezifikationen für das jeweilige Netzwerk.

Herstellen einer Verbindung mit einem vCenter Server über eine Firewall

Öffnen Sie TCP-Port 443 in der Firewall, um vCenter Server den Empfang von Daten zu ermöglichen.

vCenter Server verwendet standardmäßig TCP-Port 443, um die Datenübertragung von seinen Clients zu überwachen. Wenn eine Firewall zwischen vCenter Server und den Clients vorhanden ist, müssen Sie eine Verbindung konfigurieren, über die vCenter Server Daten von den Clients empfangen kann. Die Firewall-Konfiguration hängt von den an Ihrer Site verwendeten Komponenten ab. Weitere Informationen erhalten Sie von Ihrem lokalen Firewall-Systemadministrator.

Verbinden von ESXi-Hosts über Firewalls

Wenn Sie eine Firewall zwischen Ihren ESXi-Hosts und vCenter Server eingerichtet haben, stellen Sie sicher, dass die verwalteten Hosts Daten empfangen können.

Öffnen Sie zum Konfigurieren einer Verbindung für den Empfang von Daten Ports für den Datenverkehr von Diensten, wie z. B. vSphere High Availability, vMotion und vSphere Fault Tolerance. In ESXi-Firewall-Konfiguration finden Sie eine Erläuterung zu Konfigurationsdateien, vSphere Client-Zugriff und Firewall-Befehlen. Eine Liste der Ports finden Sie im VMware-Tool „Ports und Protokolle“™ unter https://ports.vmware.com.

Firewalls für Konfigurationen ohne vCenter Server

Wenn vCenter Servernicht in Ihrer Umgebung vorhanden ist, können die Clients keine direkte Verbindung zum ESXi-Netzwerk herstellen.

Sie können auf verschiedene Arten eine Verbindung mit einem eigenständigen ESXi-Host herstellen.

- VMware Host Client
- ESXCLI-Schnittstelle
- vSphere Web Services SDK oder vSphere Automation SDKs
- Drittanbieterclients

Die Firewall-Anforderungen für eigenständige Hosts sind mit den Anforderungen vergleichbar, wenn ein vCenter Server vorhanden ist.

- Verwenden Sie eine Firewall, um die ESXi-Ebene oder je nach Konfiguration Ihre Clients und die ESXi-Ebene zu schützen. Diese Firewall bietet einen Grundschutz für das Netzwerk.

- Die Lizenzierung gehört in dieser Konfiguration zu dem ESXi-Paket, das Sie auf allen Hosts installieren. Da die Lizenzierung in ESXi integriert ist, wird ein separater License Server mit einer Firewall nicht benötigt.

Firewallports können mit ESXCLI oder dem VMware Host Client konfiguriert werden. Weitere Informationen hierzu finden Sie unter *Verwaltung eines einzelnen Hosts von vSphere – VMware Host Client*.

Herstellen einer Verbindung mit der VM-Konsole über eine Firewall

Bestimmte Ports müssen für die Kommunikation zwischen Administrator bzw. Benutzer und der VM-Konsole geöffnet sein. Welche Ports geöffnet sein müssen, hängt vom Typ der VM-Konsole ab sowie davon, ob Sie die Verbindung über vCenter Server mit dem vSphere Client oder direkt mit dem ESXi-Host vom VMware Host Client aus herstellen.

Weitere Informationen zu Ports, Zweck und Klassifizierung (eingehend, ausgehend oder bidirektional) finden Sie im Tool VMware Ports and Protocols™ unter https://ports.vmware.com.

Herstellen der Verbindung zu einer browserbasierten VM-Konsole über den vSphere Client

Beim Herstellen einer Verbindung mit dem vSphere Client stellen Sie stets eine Verbindung zum vCenter Server-System her, das den ESXi-Host verwaltet, und greifen von hier aus auf die VM-Konsole zu.

Falls Sie den vSphere Client verwenden und eine Verbindung zu einer browserbasierten VM-Konsole herstellen, muss der folgende Zugriff möglich sein:

- Die Firewall muss vSphere Client den Zugriff auf vCenter Server auf Port 443 erlauben.
- Die Firewall muss vCenter Server den Zugriff auf den ESXi-Host auf Port 902 erlauben.

Herstellen der Verbindung zu einer VMware Remote Console über den vSphere Client

Falls Sie vSphere Client verwenden und eine Verbindung zu einer VMware Remote Console (VMRC) herstellen, muss der folgende Zugriff möglich sein:

- Die Firewall muss dem vSphere Client Zugriff auf vCenter Server auf Port 443 gewähren.
- Die Firewall muss dem VMRC Zugriff auf vCenter Server auf Port 443 und auf den ESXi-Host auf Port 902 für VMRC-Versionen vor 11.0 und Port 443 für VMRC Version 11.0 und höher gewähren. Weitere Informationen zu den Portanforderungen von VMRC Version 11.0 und ESXi finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/76672.

Herstellen einer Direktverbindung zu ESXi-Hosts mit dem VMware Host Client

Sie können die VM-Konsole des VMware Host Client verwenden, wenn Sie eine direkte Verbindung zu einem ESXi-Host herstellen.

Hinweis Verwenden Sie den VMware Host Client nicht, um eine Direktverbindung mit Hosts herzustellen, die von einem vCenter Server-System verwaltet werden. Wenn Sie im VMware Host Client an Hosts dieses Typs Änderungen vornehmen, wird Ihre Umgebung instabil.

Die Firewall muss Zugriff auf den ESXi-Host auf Port 443 und 902 gewähren.

Der VMware Host Client verwendet Port 902 für Verbindungen der MKS-Aktivitäten des Gastbetriebssystems auf virtuellen Maschinen. Die Benutzer interagieren über diesen Port mit dem Gastbetriebssystem und den Anwendungen der virtuellen Maschine. Für diese Aufgabe unterstützt VMware nur diesen Port.

Sichern des physischen Switches

Sichern Sie den physischen Switch auf jedem ESXi-Host, um zu verhindern, dass Angreifer Zugriff auf den Host und seine virtuellen Maschinen erhalten.

Um besten Host-Schutz zu gewährleisten, stellen Sie sicher, dass die physischen Switch-Ports mit deaktiviertem Spanning-Tree konfiguriert sind, und dass die Nichtverhandlungsoption für Trunk-Links zwischen externen physischen Switches und virtuellen Switches im VST-Modus (Virtual Switch Tagging) konfiguriert ist.

Verfahren

1. Melden Sie sich beim physischen Switch an, und stellen Sie sicher, dass das Spanning-Tree-Protokoll deaktiviert ist oder dass PortFast für alle physischen Switch-Ports konfiguriert ist, die mit ESXi-Hosts verbunden sind.
2. Für virtuelle Maschinen, die Überbrückungen oder Routing ausführen, prüfen Sie regelmäßig, dass der erste physische Switch-Port (upstream) mit BPDU Guard konfiguriert ist, dass PortFast deaktiviert ist und dass das Spanning-Tree-Protokoll aktiviert ist.

   Um in vSphere 5.1 oder höher zu verhindern, dass der physische Switch möglichen DoS-Angriffen (Denial of Service) ausgesetzt ist, können Sie den Gast-BPDU-Filter für ESXi-Hosts aktivieren.
3. Melden Sie sich beim physischen Switch an, und stellen Sie sicher, dass Dynamic Trunking Protocol (DTP) nicht für die physischen Switch-Ports aktiviert ist, die mit den ESXi-Hosts verbunden sind.
4. Prüfen Sie physische Switch-Ports routinemäßig, um sicherzustellen, dass sie ordnungsgemäß als Trunk-Ports konfiguriert sind, wenn sie mit VLAN-Trunking-Ports für virtuellen Switch verbunden sind.

Sichern von Standard-Switch-Ports durch Sicherheitsrichtlinien

Die VMkernel-Portgruppe bzw. die VM-Portgruppe auf einem Standard-Switch verfügt über eine konfigurierbare Sicherheitsrichtlinie. Die Sicherheitsrichtlinie bestimmt, wie streng der Schutz gegen Imitations- oder Abfangangriffe auf virtuelle Maschinen sein soll.

Ähnlich wie bei physischen Netzwerkadaptern können VM-Netzwerkadapter die Identität einer anderen virtuellen Maschine annehmen. Die Annahme einer fremden Identität stellt ein Sicherheitsrisiko dar.

- Ein Netzwerkadapter einer virtuellen Maschine kann Datenblöcke übertragen, die von einer anderen virtuellen Maschine zu stammen scheinen, damit er Datenblöcke aus dem Netzwerk empfangen kann, die für die jeweilige virtuelle Maschine bestimmt sind.
- Ein virtueller Netzwerkadapter kann so konfiguriert werden, dass er Datenblöcke empfängt, die für andere Maschinen bestimmt sind.

Wenn Sie eine VMkernel- oder eine VM-Portgruppe zu einem Standard-Switch hinzufügen, konfiguriert ESXi eine Sicherheitsrichtlinie für die Ports in der Gruppe. Mit dieser Sicherheitsrichtlinie können Sie sicherstellen, dass der Host verhindert, dass die Gastbetriebssysteme der virtuellen Maschinen andere Computer im Netzwerk imitieren können. Das Gastbetriebssystem, das die Annahme einer anderen Identität durchführen könnte, erkennt nicht, dass die die Annahme einer fremden Identität verhindert wurde.

Die Sicherheitsrichtlinie bestimmt, wie streng der Schutz gegen Imitations- oder Abfangangriffe auf virtuelle Maschinen sein soll. Weitere Informationen über die ordnungsgemäße Verwendung der Einstellungen im Sicherheitsprofil finden Sie im Abschnitt „Sicherheitsrichtlinie“ des Handbuchs *vSphere-Netzwerk*. In diesem Abschnitt wird Folgendes erläutert:

- Wie VM-Netzwerkadapter Übertragungen steuern.
- Wie auf dieser Ebene Angriffe durchgeführt werden

Sichern von vSphere Standard-Switches

Datenverkehr auf dem Standard-Switch kann vor Ebene 2-Angriffen gesichert werden, indem Sie einige der MAC-Adressmodi der VM-Netzwerkadapter beschränken.

Jeder VM-Netzwerkadapter weist eine ursprüngliche MAC-Adresse und eine geltende MAC-Adresse auf.

Ursprüngliche MAC-Adresse

Die ursprüngliche MAC-Adresse wird beim Erstellen des Adapters zugewiesen. Obwohl die ursprüngliche MAC-Adresse von außerhalb des Gastbetriebssystems neu konfiguriert werden kann, kann sie nicht vom Gastbetriebssystem selbst geändert werden.

Geltende MAC-Adresse

Jeder Adapter verfügt über eine geltende MAC-Adresse, die eingehenden Netzwerkdatenverkehr mit einer Ziel-MAC-Adresse, die nicht der geltenden MAC-Adresse entspricht, herausfiltert. Das Gastbetriebssystem ist für die Einstellung der geltenden MAC-Adresse verantwortlich. In der Regel stimmen die geltende MAC-Adresse und die ursprünglich zugewiesene MAC-Adresse überein.

Bei der Erstellung eines VM-Netzwerkadapters stimmen die geltende und die ursprünglich zugewiesene MAC-Adresse überein. Das Gastbetriebssystem kann die geltende MAC-Adresse jedoch jederzeit auf einen anderen Wert setzen. Wenn ein Betriebssystem die geltende MAC-Adresse ändert, empfängt der Netzwerkadapter Netzwerkdatenverkehr, der für die neue MAC-Adresse bestimmt ist.

Beim Versand von Datenpaketen über einen Netzwerkadapter schreibt das Gastbetriebssystem in der Regel die geltende MAC-Adresse des eigenen Netzwerkadapters in das Feld mit der Quell-MAC-Adresse der Ethernet-Frames. Die MAC-Adresse des Empfänger-Netzwerkadapters wird in das Feld mit der Ziel-MAC-Adresse geschrieben. Der empfangende Adapter akzeptiert Datenpakete nur dann, wenn die Ziel-MAC-Adresse im Paket mit seiner eigenen geltenden MAC-Adresse übereinstimmt.

Ein Betriebssystem kann Frames mit einer imitierten Quell-MAC-Adresse senden. Daher kann ein Betriebssystem die Identität eines vom Empfängernetzwerk autorisierten Netzwerkadapters annehmen und böswillige Angriffe auf die Geräte in einem Netzwerk durchführen.

Schützen Sie virtuellen Datenverkehr vor Imitierungs- und Abfangangriffen auf Layer 2, indem Sie eine Sicherheitsrichtlinie für Portgruppen oder Ports konfigurieren.

Die Sicherheitsrichtlinie für verteilte Portgruppen und Ports umfasst die folgenden Optionen:

- MAC-Adressänderungen (siehe MAC-Adressänderungen)
- Promiscuous-Modus (siehe Betrieb im Promiscuous-Modus)
- Gefälschte Übertragungen (siehe Gefälschte Übertragungen)

Sie können die Standardeinstellungen durch Auswählen des mit dem Host verknüpften virtuellen Switches über den vSphere Client anzeigen und ändern. Weitere Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

MAC-Adressänderungen

Die Sicherheitsrichtlinie eines virtuellen Switches beinhaltet die Option **MAC-Adressänderungen**. Mit dieser Option können virtuelle Maschinen Frames mit einer MAC-Adresse empfangen, die nicht mit der in der VMX konfigurierten Adresse identisch ist.

Wenn die Option **MAC-Adressänderungen** auf **Akzeptieren** festgelegt ist, akzeptiert ESXi Anforderungen, die geltende MAC-Adresse einer virtuellen Maschine in eine andere als die ursprünglich zugewiesene Adresse zu ändern.

Wenn die Option **MAC-Adressänderungen** auf **Ablehnen** festgelegt ist, lehnt ESXi Anforderungen ab, die geltende MAC-Adresse einer virtuellen Maschine in eine andere als die ursprünglich zugewiesene Adresse zu ändern. Diese Einstellung schützt den Host vor MAC-Imitationen. Der Port, der von dem Adapter der virtuellen Maschine zum Senden der Anforderung verwendet wird, ist deaktiviert, und der Adapter der virtuellen Maschine erhält keine weiteren Frames mehr, bis die geltende MAC-Adresse mit der ursprünglichen MAC-Adresse übereinstimmt. Das Gastbetriebssystem erkennt nicht, dass die Anforderung zum Ändern der MAC-Adresse nicht angenommen wurde.

Hinweis Der iSCSI-Initiator basiert darauf, dass er MAC-Adressänderungen von bestimmten Speichertypen erhalten kann. Wenn Sie ESXi-iSCSI mit iSCSI-Speicher verwenden, legen Sie die Option **MAC-Adressänderungen** auf **Akzeptieren** fest.

In bestimmten Situationen ist es tatsächlich notwendig, dass mehrere Adapter in einem Netzwerk die gleiche MAC-Adresse haben, zum Beispiel wenn Sie den Microsoft-Netzwerk-Lastausgleich im Unicast-Modus verwenden. Bei Verwendung des Microsoft-NetzwerkLastausgleichs im Standard-Multicast-Modus haben die Adapter nicht die gleiche MAC-Adresse.

Hinweis Ab vSphere 7.0 wurden die Standardwerte für **Gefälschte Übertragungen** und **MAC-Adressänderungen** in „Ablehnen“ anstelle von „Akzeptieren“ geändert. Wenden Sie sich an Ihren Speicheranbieter, um dies zu überprüfen.

Gefälschte Übertragungen

Die Option **Gefälschte Übertragungen** beeinflusst den Datenverkehr, der von einer virtuellen Maschine versendet wird.

Wenn die Option **Gefälschte Übertragungen** auf **Akzeptieren** festgelegt ist, vergleicht ESXi die Quell- und die geltende MAC-Adresse nicht.

Zum Schutz gegen MAC-Imitation können Sie die Option **Gefälschte Übertragungen** auf **Ablehnen** einstellen. In diesem Fall vergleicht der Host die Quell-MAC-Adresse, die vom Gastbetriebssystem übertragen wird, mit der geltenden MAC-Adresse für den Adapter der virtuellen Maschine, um festzustellen, ob sie übereinstimmen. Wenn die Adressen nicht übereinstimmen, verwirft der ESXi-Host das Paket.

Das Gastbetriebssystem erkennt nicht, dass der Adapter der virtuellen Maschine die Pakete mit der imitierten MAC-Adresse nicht senden kann. Der ESXi-Host fängt alle Pakete mit imitierten Adressen vor der Übermittlung ab. Das Gastbetriebssystem geht ggf. davon aus, dass die Pakete verworfen wurden.

Hinweis Ab vSphere 7.0 wurden die Standardwerte für **Gefälschte Übertragungen** und **MAC-Adressänderungen** in „Ablehnen“ anstelle von „Akzeptieren“ geändert.

Betrieb im Promiscuous-Modus

Der Promiscuous-Modus deaktiviert jegliche Empfangsfilterung, die der Adapter der virtuellen Maschine ausführt, sodass das Gastbetriebssystem den gesamten Datenverkehr aus dem

Netzwerk empfängt. Standardmäßig kann der Adapter der virtuellen Maschine nicht im Promiscuous-Modus betrieben werden.

Der Promiscuous-Modus kann zwar für die Nachverfolgung von Netzwerkaktivitäten nützlich sein, aber er ist ein unsicherer Betriebsmodus, da jeder Adapter im Promiscuous-Modus Zugriff auf alle Pakete hat, selbst wenn manche Pakete nur für einen spezifischen Netzwerkadapter bestimmt sind. Das bedeutet, dass ein Administrator oder Root-Benutzer in einer virtuellen Maschine rein theoretisch den Datenverkehr, der für andere Gast- oder Hostbetriebssysteme bestimmt ist, einsehen kann.

Weitere Informationen zum Konfigurieren des VM-Adapters für den Promiscuous-Modus finden Sie im Thema zur Konfiguration der Sicherheitsrichtlinie für einen vSphere Standard Switch oder eine standardmäßige Portgruppe in der Dokumentation zu *vSphere-Netzwerk*.

Hinweis Unter bestimmten Umständen ist es notwendig, für einen Standard-Switch oder einen verteilten virtuellen Switch den Promiscuous-Modus zu konfigurieren, zum Beispiel wenn Sie eine Software zur Netzwerkeinbruchserkennung oder einen Paket-Sniffer verwenden.

Schutz von Standard-Switches und VLANs

Die Standard-Switches von VMware schützen vor bestimmten Bedrohungen der VLAN-Sicherheit. Durch den Aufbau der Standard-Switches schützen sie VLANs gegen viele Arten von Angriffen, die meist auf VLAN-Hopping basieren.

Dieser Schutz garantiert jedoch nicht, dass Ihre virtuellen Maschinen gegen andere Arten von Angriffen immun sind. So schützen Standard-Switches zum Beispiel nicht das physische Netzwerk vor diesen Angriffen, sie schützen nur das virtuelle Netzwerk.

Standard-Switches und VLANs können gegen folgende Arten von Angriffen schützen:

MAC-Flooding

Diese Angriffe überschwemmen den Switch mit Datenpaketen, die MAC-Adressen enthalten, die als von verschiedenen Quellen stammend gekennzeichnet wurden. Viele Switches verwenden eine assoziative Speichertabelle, um die Quelladresse für jedes Datenpaket zu speichern. Wenn die Tabelle voll ist, schaltet der Switch ggf. in einen vollständig geöffneten Status um, in dem alle eingehenden Pakete auf allen Ports übertragen werden, sodass der Angreifer den gesamten Datenverkehr des Switches verfolgen kann. In diesem Fall kann es auch zu Paketlecks in andere VLANs kommen.

Zwar speichern die Standard-Switches von VMware eine MAC-Adressentabelle, aber sie erhalten die MAC-Adressen nicht von erkennbarem Datenverkehr und sind daher gegen diese Art von Angriffen immun.

Angriffe durch 802.1q- und ISL-Kennzeichnung

Bei diesem Angriff werden die Datenblöcke durch den Switch an ein anderes VLAN weitergeleitet, indem der Switch durch einen Trick dazu gebracht wird, als Verbindungsleitung zu fungieren und den Datenverkehr an andere VLANs weiterzuleiten.

Die Standard-Switches von VMware führen das dynamische Trunking, das für diese Art des Angriffs notwendig ist, nicht aus, und sind daher immun.

Doppelt gekapselte Angriffe

Bei dieser Art von Angriffen erstellt der Angreifer ein doppelt gekapseltes Paket, in dem sich der VLAN-Bezeichner im inneren Tag vom VLAN-Bezeichner im äußeren Tag unterscheidet. Um Rückwärtskompatibilität zu gewährleisten, entfernen native VLANs standardmäßig das äußere Tag von übertragenen Paketen. Wenn ein nativer VLAN-Switch das äußere Tag entfernt, bleibt nur das innere Tag übrig, welches das Paket zu einem anderen VLAN weiterleitet, als im jetzt fehlenden äußeren Tag angegeben war.

Die Standard-Switches von VMware verwerfen alle doppelt eingekapselten Datenblöcke, die eine virtuelle Maschine auf einem für ein bestimmtes VLAN konfigurierten Port senden möchte. Daher sind sie immun gegen diese Art von Angriffen.

Multicast-Brute-Force-Angriffe

Bei diesen Angriffen wird eine große Anzahl von Multicast-Datenblöcken fast zeitgleich an ein bekanntes VLAN gesendet, um den Switch zu überlasten, damit er versehentlich einige Datenblöcke in andere VLANs überträgt.

Die Standard-Switches von VMware erlauben es Datenblöcken nicht, ihren richtigen Übertragungsbereich (VLAN) zu verlassen und sind daher gegen diese Art von Angriffen immun.

Spanning-Tree-Angriffe

Diese Angriffe zielen auf das Spanning-Tree-Protokoll (STP), das zur Steuerung der Überbrückung verschiedener Teile des LANs verwendet wird. Der Angreifer sendet Pakete der Bridge Protocol Data Unit (BPDU) in dem Versuch, die Netzwerktopologie zu ändern und sich selbst als Root-Bridge einzusetzen. Als Root-Bridge kann der Angreifer dann die Inhalte übertragener Datenblöcke mitschneiden.

Die Standard-Switches von VMware unterstützen STP nicht und sind daher gegen diese Art von Angriffen immun.

Zufallsdatenblock-Angriffe

Bei diesen Angriffen wird eine große Anzahl Pakete gesendet, bei denen die Quell- und Zieladressen gleich sind, diese jedoch Felder unterschiedlicher Länge, Art und mit verschiedenem Inhalt enthalten. Ziel des Angriffes ist es zu erzwingen, dass Pakete versehentlich in ein anderes VLAN fehlgeleitet werden.

Die Standard-Switches von VMware sind gegen diese Art von Angriffen immun.

Da mit der Zeit immer neue Sicherheitsgefahren auftreten, kann diese Liste möglicher Angriffe nicht vollständig sein. Rufen Sie regelmäßig die VMware-Sicherheitsressourcen im Internet ab, um mehr über Sicherheit, neue Sicherheitswarnungen und die Sicherheitstaktiken von VMware zu erfahren.

Sichern von vSphere Distributed Switches und verteilten Portgruppen

Die Administratoren haben mehrere Optionen zum Sichern von vSphere Distributed Switches in ihrer vSphere-Umgebung.

Für VLANs in einem vSphere Distributed Switch gelten dieselben Regeln wie in einem Standard-Switch. Weitere Informationen finden Sie unter Schutz von Standard-Switches und VLANs.

Verfahren

1 Deaktivieren Sie für verteilte Portgruppen mit statischer Bindung die Funktion zum automatischen Erweitern.

   Die automatische Erweiterung ist in vSphere 5.1 und höher standardmäßig aktiviert.

   Um die automatische Erweiterung zu deaktivieren, konfigurieren Sie die Eigenschaft `autoExpand` unter der verteilten Portgruppe mit dem vSphere Web Services SDK oder über eine Befehlszeilenschnittstelle. Siehe die Dokumentation zu *vSphere Web Services SDK*.

2 Stellen Sie sicher, dass alle privaten VLAN IDs aller vSphere Distributed Switches vollständig dokumentiert sind.

3 Bei Verwendung von VLAN-Tagging in einer dvPortgroup müssen die VLAN-IDs mit denen der externen VLAN-fähigen Upstream-Switches übereinstimmen. Wenn die VLAN-IDs nicht ordnungsgemäß aufgezeichnet werden, kann die versehentliche Wiederverwendung von IDs zu unbeabsichtigtem Datenverkehr führen. Ebenso kann bei fehlenden oder falschen VLAN-IDs der Datenverkehr zwischen physischen und virtuellen Maschinen blockiert werden.

4 Stellen Sie sicher, dass in einer virtuellen Portgruppe, die einem vSphere Distributed Switch zugeordnet ist, keine nicht verwendeten Ports vorhanden sind.

5 Kennzeichnen Sie alle vSphere Distributed Switches.

   Für mit einem ESXi-Host verknüpfte vSphere Distributed Switches ist ein Textfeld für den Namen des Switches erforderlich. Diese Bezeichnung dient als funktionaler Deskriptor für den Switch, genauso wie der mit einem physischen Switch verknüpfte Hostname. Die Bezeichnung am vSphere Distributed Switch zeigt die Funktion oder das IP-Subnetz des Switches an. Sie können zum Beispiel den Switch als intern bezeichnen, um anzugeben, dass er nur für interne Netzwerke auf dem privaten virtuellen Switch einer virtuellen Maschine dient. Über physikalische Netzwerkadapter erfolgt kein Datenverkehr.

6 Deaktivieren Sie die Netzwerk-Systemstatusprüfung für Ihre vSphere Distributed Switches, wenn Sie sie nicht regelmäßig verwenden.

   Die Netzwerk-Systemstatusprüfung ist standardmäßig deaktiviert. Nach der Aktivierung enthalten die Systemstatusprüfungspakete Informationen zum Host, Switch und Port, die ein Angreifer möglicherweise verwenden kann. Verwenden Sie die Netzwerk-Systemstatusprüfung nur zur Fehlerbehebung und deaktivieren Sie sie nach Abschluss der Fehlerbehebung.

7 Schützen Sie virtuellen Datenverkehr vor Imitierungs- und Abfangangriffen auf Layer 2, indem Sie eine Sicherheitsrichtlinie für Portgruppen oder Ports konfigurieren.

Die Sicherheitsrichtlinie für verteilte Portgruppen und Ports umfasst die folgenden Optionen:

- MAC-Adressänderungen (siehe MAC-Adressänderungen)
- Promiscuous-Modus (siehe Betrieb im Promiscuous-Modus)
- Gefälschte Übertragungen (siehe Gefälschte Übertragungen)

Durch Auswahl von **Verteilte Portgruppen verwalten** im Kontextmenü des Distributed Switch und Klicken auf **Sicherheit** im Assistenten können Sie die aktuellen Einstellungen einsehen und ändern. Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

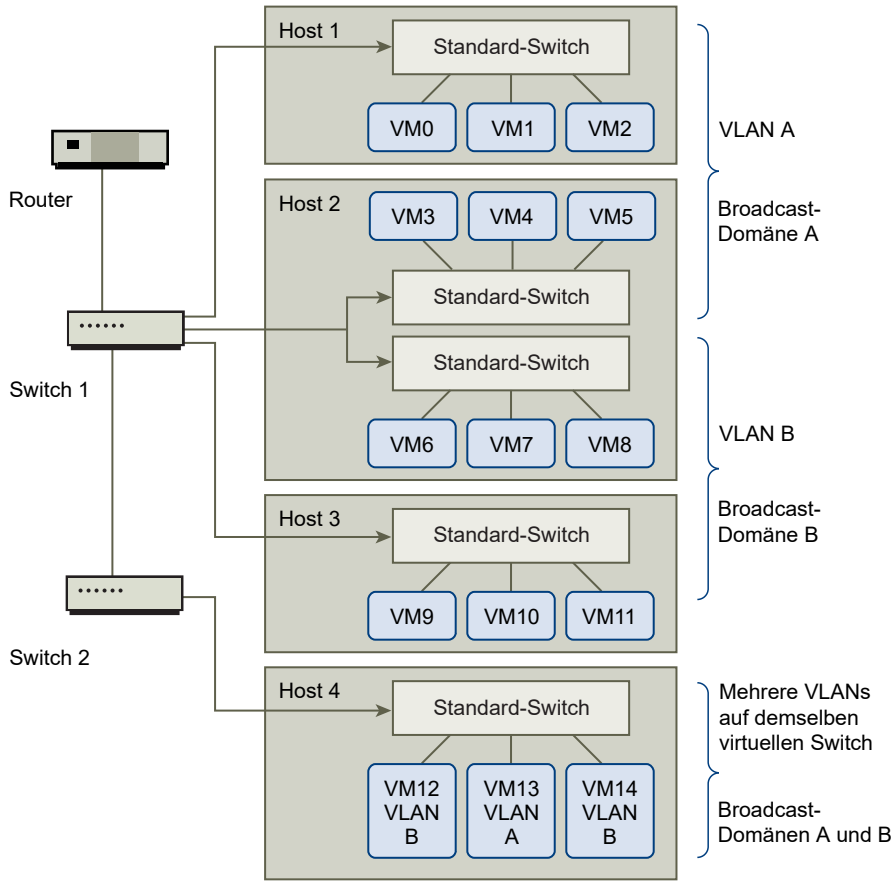
Absichern virtueller Maschinen durch VLANs

Das Netzwerk gehört zu den gefährdetsten Teilen eines jeden Systems. Ihre VM-Netzwerk muss genauso wie ihr physisches Netzwerk geschützt werden. Durch die Verwendung von VLANs kann die Sicherheit des Netzwerks in Ihrer Umgebung verbessert werden.

VLANs sind eine Netzwerkarchitektur nach dem IEEE-Standard und verfügen über spezifische Kennzeichnungsmethoden, durch die Datenpakete nur an die Ports weitergeleitet werden, die zum VLAN gehören. Wenn das VLAN ordnungsgemäß konfiguriert ist, ist es ein zuverlässiges Mittel zum Schutz einer Gruppe virtueller Maschinen vor zufälligem und böswilligem Eindringen.

Mit VLANs können Sie ein physisches Netzwerk so in Segmente aufteilen, dass zwei Computer oder virtuelle Maschinen im Netzwerk nur dann Pakete untereinander austauschen können, wenn sie zum gleichen VLAN gehören. So gehören zum Beispiel Buchhaltungsunterlagen und -transaktionen zu den wichtigsten vertraulichen internen Informationen eines Unternehmens. Wenn in einem Unternehmen die virtuellen Maschinen der Verkaufs-, Logistik- und Buchhaltungsmitarbeiter an das gleiche physische Netzwerk angeschlossen sind, können Sie die virtuellen Maschinen für die Buchhaltungsabteilung schützen, indem Sie VLANs einrichten.

Abbildung 13-1. Beispielplan eines VLAN



Bei dieser Konfiguration verwenden alle Mitarbeiter der Buchhaltungsabteilung virtuelle Maschinen im VLAN A, die Mitarbeiter der Vertriebsabteilung verwenden die virtuellen Maschinen im VLAN B.

Der Router leitet die Datenpakete mit Buchhaltungsdaten an die Switches weiter. Diese Pakete sind so gekennzeichnet, dass sie nur an VLAN A weitergeleitet werden dürfen. Daher sind die Daten auf die Broadcast-Domäne A beschränkt und können nur an die Broadcast-Domäne B weitergeleitet werden, wenn der Router entsprechend konfiguriert wurde.

Bei dieser VLAN-Konfiguration wird verhindert, dass Mitarbeiter des Vertriebs Datenpakete abfangen können, die für die Buchhaltungsabteilung bestimmt sind. Die Buchhaltungsabteilung kann zudem auch keine Datenpakete empfangen, die für den Vertrieb bestimmt sind. Virtuelle Maschinen, die an einen gemeinsamen virtuellen Switch angebunden sind, können sich dennoch in unterschiedlichen VLANs befinden.

Sicherheitsempfehlungen für VLANs

Wie Sie die VLANs einrichten, um Teile eines Netzwerks abzusichern, hängt von Faktoren wie dem Gastbetriebssystem und der Konfiguration der Netzwerkgeräte ab.

ESXi ist mit einer vollständigen VLAN-Implementierung nach IEEE 802.1q ausgestattet. Zwar kann VMware keine spezifischen Empfehlungen aussprechen, wie die VLANs eingerichtet werden sollten, es sollten jedoch bestimmte Faktoren berücksichtigt werden, wenn ein VLAN ein Bestandteil Ihrer Sicherheitsrichtlinien ist.

Sichern von VLANs

Administratoren haben mehrere Möglichkeiten, um die VLANs in ihrer vSphere-Umgebung zu sichern.

Verfahren

1. Stellen Sie sicher, dass für Portgruppen keine VLAN-Werte konfiguriert sind, die für physische Upstream-Switches reserviert sind.

   Legen Sie für VLAN-IDs keine Werte fest, die für den physischen Switch reserviert sind.

2. Stellen Sie sicher, dass für Portgruppen nicht VLAN 4095 konfiguriert ist, außer Sie verwenden Virtual Guest Tagging (VGT).

   In vSphere gibt es drei Arten von VLAN-Tagging:

   - External Switch Tagging (EST)
   - Virtual Switch Tagging (VST): Der virtuelle Switch kennzeichnet mit der konfigurierten VLAN-ID den eingehenden Datenverkehr für die angefügten virtuellen Maschinen und entfernt das VLAN-Tag im ausgehenden Datenverkehr. Zum Einrichten des VST-Modus weisen Sie eine VLAN-ID zwischen 1 und 4094 zu.
   - Virtual Guest Tagging (VGT): VLANs werden von virtuellen Maschinen abgewickelt. Zum Aktivieren des VGT-Modus legen Sie 4095 als VLAN-ID fest. Auf einem Distributed Switch können Sie mithilfe der Option **VLAN-Trunking** auch Datenverkehr der virtuellen Maschine basierend auf dem VLAN zulassen.

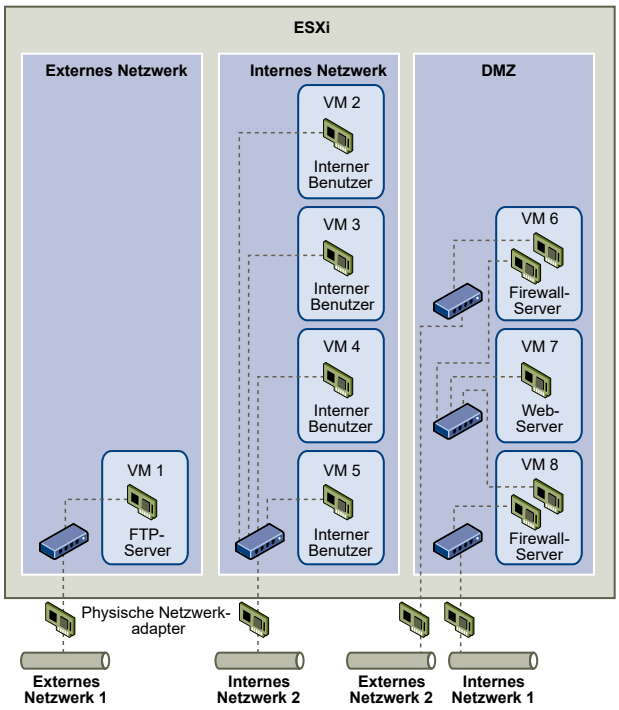
   Auf einem Standard-Switch können Sie den VLAN-Netzwerkmodus auf Switch- oder Portgruppenebene konfigurieren, und auf einem Distributed Switch auf der Ebene der verteilten Portgruppe oder des Ports.

3. Stellen Sie sicher, dass alle VLANs auf jedem virtuellen Switch vollständig dokumentiert sind und dass jeder virtuelle Switch alle erforderlichen VLANs und nur die erforderlichen VLANs aufweist.

Erstellen mehrerer Netzwerke auf einem einzelnen ESXi-Host

Das ESXi-System wurde so entworfen, dass Sie bestimmte Gruppen virtueller Maschinen an das interne Netzwerk, andere an das externe Netzwerk und wiederum andere an beide Netzwerke anbinden können - alle auf demselben Host. Diese Fähigkeit basiert auf der grundlegenden Isolierung virtueller Maschinen im Zusammenspiel mit der überlegt geplanten Nutzung von Funktionen zur virtuellen Vernetzung.

Abbildung 13-2. Konfigurierte externe Netzwerke, interne Netzwerke und DMZ auf einem ESXi-Host



In der Abbildung hat der Systemadministrator einen Host in drei verschiedene VM-Zonen unterteilt: FTP-Server, interne virtuelle Maschinen und DMZ. Jede Zone erfüllt eine bestimmte Funktion.

FTP-Server

Die virtuelle Maschine 1 wurde mit FTP-Software konfiguriert und dient als Speicherbereich für Daten von und an externe Ressourcen, z. B. für von einem Dienstleister lokalisierte Formulare und Begleitmaterialien.

Diese virtuelle Maschine ist nur mit dem externen Netzwerk verbunden. Sie verfügt über einen eigenen virtuellen Switch und physischen Netzwerkadapter, die sie mit dem externen Netzwerk 1 verbinden. Dieses Netzwerk ist auf Server beschränkt, die vom Unternehmen zum Empfang von Daten aus externen Quellen verwendet werden. Das Unternehmen verwendet beispielsweise das externe Netzwerk 1, um FTP-Daten von Dienstleistern zu empfangen und den Dienstleistern FTP-Zugriff auf Daten zu gewähren, die auf extern verfügbaren Servern gespeichert sind. Zusätzlich zur Verarbeitung der Daten für die virtuelle Maschine 1 verarbeitet das externe Netzwerk 1 auch Daten für FTP-Server auf anderen ESXi-Hosts am Standort.

Da sich die virtuelle Maschine 1 keinen virtuellen Switch oder physischen Netzwerkadapter mit anderen virtuellen Maschinen auf dem Host teilt, können die anderen virtuellen Maschinen auf dem Host keine Datenpakete in das Netzwerk der virtuellen Maschine 1 übertragen oder daraus empfangen. Dadurch werden Spionageangriffe verhindert, da dem Opfer dafür Netzwerkdaten gesendet werden müssen. Außerdem kann der Angreifer dadurch die

natürliche Anfälligkeit von FTP nicht zum Zugriff auf andere virtuelle Maschinen auf dem Host nutzen.

Interne virtuelle Maschinen

Die virtuellen Maschinen 2 bis 5 sind der internen Verwendung vorbehalten. Diese virtuellen Maschinen verarbeiten und speichern vertrauliche firmeninterne Daten wie medizinische Unterlagen, juristische Dokumente und Betrugsermittlungen. Daher müssen Systemadministratoren für diese virtuellen Maschinen den höchsten Schutz gewährleisten.

Diese virtuellen Maschinen sind über ihren eigenen virtuellen Switch und physischen Netzwerkadapter an das Interne Netzwerk 2 angeschlossen. Das interne Netzwerk 2 ist der internen Nutzung durch Mitarbeiter wie Reklamationssachbearbeiter, firmeninterne Anwälte und andere Sachbearbeiter vorbehalten.

Die virtuellen Maschinen 2 bis 5 können über den virtuellen Switch untereinander und über den physischen Netzwerkadapter mit internen Maschinen an anderen Stellen des internen Netzwerks 2 kommunizieren. Sie können nicht mit Computern oder virtuellen Maschinen kommunizieren, die Zugang zu den externen Netzwerken haben. Wie beim FTP-Server können diese virtuellen Maschinen keine Datenpakete an Netzwerke anderer virtueller Maschinen senden oder sie von diesen empfangen. Ebenso können die anderen virtuellen Maschinen keine Datenpakete an die virtuellen Maschinen 2 bis 5 senden oder von diesen empfangen.

DMZ

Die virtuellen Maschinen 6 bis 8 wurden als DMZ konfiguriert, die von der Marketingabteilung dazu verwendet wird, die externe Website des Unternehmens bereitzustellen.

Diese VM-Gruppe ist dem externen Netzwerk 2 und dem internen Netzwerk 1 zugeordnet. Das Unternehmen nutzt das externe Netzwerk 2 zur Unterstützung der Webserver, die von der Marketing- und der Finanzabteilung zur Bereitstellung der Unternehmenswebsite und anderer webbasierter Anwendungen für externe Benutzer verwendet werden. Das interne Netzwerk 1 ist der Verbindungskanal, den die Marketingabteilung zur Veröffentlichung ihrer Inhalte auf der Unternehmenswebsite, zur Bereitstellung von Downloads und Diensten wie Benutzerforen verwendet.

Da diese Netzwerke vom externen Netzwerk 1 und vom internen Netzwerk 2 getrennt sind und die virtuellen Maschinen keine gemeinsamen Kontaktpunkte (Switches oder Adapter) aufweisen, besteht kein Angriffsrisiko für den FTP-Server oder die Gruppe interner virtueller Maschinen (weder als Ausgangspunkt noch als Ziel).

Wenn die Isolierung der virtuellen Maschinen genau beachtet wird, die virtuellen Switches ordnungsgemäß konfiguriert werden und die Netzwerktrennung eingehalten wird, können alle drei Zonen der virtuellen Maschinen auf dem gleichen ESXi-Host untergebracht werden, ohne dass Datenverluste oder Ressourcenmissbräuche befürchtet werden müssen.

Das Unternehmen erzwingt die Isolierung der virtuellen Maschinengruppen durch die Verwendung mehrerer interner und externer Netzwerke und die Sicherstellung, dass die virtuellen Switches und physischen Netzwerkadapter jeder Gruppe von denen anderer Gruppen getrennt sind.

Da keiner der virtuellen Switches sich über mehrere Zonen erstreckt, wird das Risiko des Durchsickerns von Daten von einer Zone in eine andere ausgeschaltet. Ein virtueller Switch kann aufbaubedingt keine Datenpakete direkt an einen anderen virtuellen Switch weitergeben. Datenpakete können nur unter folgenden Umständen von einem virtuellen Switch zu einem anderen gelangen:

- Wenn die virtuellen Switches an das gleiche physische LAN angeschlossen sind
- Wenn die virtuellen Switches an eine gemeinsame virtuelle Maschine angeschlossen sind, die unter Umständen zum Übertragen von Datenpaketen verwendet werden kann

In der Beispielkonfiguration wird keine dieser Bedingungen erfüllt. Wenn die Systemadministratoren sicherstellen möchten, dass es keine gemeinsamen virtuellen Switch-Pfade gibt, können sie mögliche gemeinsame Kontaktpunkte suchen, indem sie den Netzwerk-Switch-Plan im vSphere Client überprüfen.

Zum Schutz der Ressourcen der virtuellen Maschinen kann der Systemadministrator eine Reservierung und Einschränkung der Ressourcen für jede virtuelle Maschine vornehmen, um das Risiko von DoS- und DDoS-Angriffen einzudämmen. Der Systemadministrator kann den ESXi-Host und die virtuellen Maschinen außerdem durch die Installation von Softwarefirewalls im Front-End und Back-End der DMZ, durch Positionierung des ESXi-Hosts hinter einer physischen Firewall und der an das Netzwerk angeschlossenen Speicherressourcen an jeweils einen eigenen virtuellen Switch schützen.

Internet Protocol Security (IPsec)

Internet Protocol Security (IPsec) sichert die von einem Host ausgehende und bei diesem eingehende IP-Kommunikation. ESXi-Hosts unterstützen IPsec mit IPv6.

Wenn Sie IPsec auf einem Host einrichten, aktivieren Sie die Authentifizierung und Verschlüsselung ein- und ausgehender Pakete. Wann und wie der IP-Datenverkehr verschlüsselt wird, hängt davon ab, wie Sie die Sicherheitsverbindungen und -richtlinien des Systems einrichten.

Eine Sicherheitsverbindung bestimmt, wie das System den Datenverkehr verschlüsselt. Beim Erstellen einer Sicherheitsverbindung geben Sie Quelle und Ziel, Verschlüsselungsparameter und einen Namen für die Sicherheitsverbindung an.

Eine Sicherheitsrichtlinie legt fest, wann das System Datenverkehr verschlüsseln soll. Die Sicherheitsrichtlinie enthält Informationen zu Quelle und Ziel, Protokoll und Richtung des zu verschlüsselnden Datenverkehrs, dem Modus (Transport oder Tunnel) und der zu verwendenden Sicherheitsverbindung.

Auflisten der verfügbaren Sicherheitsverbindungen

ESXi kann eine Liste aller Sicherheitsverbindungen zur Verfügung stellen, die zur Verwendung durch Sicherheitsrichtlinien verfügbar sind. Die Liste enthält sowohl die vom Benutzer erstellten Sicherheitsverbindungen als auch die Sicherheitsverbindungen, die der VMkernel mithilfe von Internet Key Exchange installiert hat.

Sie können mithilfe des Befehls `esxcli` eine Liste der verfügbaren Sicherheitsverbindungen abrufen.

Verfahren

- Geben Sie an der Eingabeaufforderung den Befehl **`esxcli network ip ipsec sa list`** ein.

Ergebnisse

ESXi zeigt eine Liste aller verfügbaren Sicherheitsverbindungen an.

Hinzufügen einer IPsec-Sicherheitsverbindung

Fügen Sie eine Sicherheitsverbindung hinzu, um Verschlüsselungsparameter für den zugeordneten IP-Datenverkehr festzulegen.

Sie können eine Sicherheitsverbindung mithilfe des Befehls `esxcli` hinzufügen.

Verfahren

- Geben Sie an der Eingabeaufforderung den Befehl **`esxcli network ip ipsec sa add`** zusammen mit einer oder mehreren der nachfolgenden Optionen ein.

Option	Beschreibung
`--sa-source=` ***Quelladresse***	Erforderlich. Geben Sie die Quelladresse an.
`--sa-destination=` ***Zieladresse***	Erforderlich. Geben Sie die Zieladresse an.
`--sa-mode=` ***Modus***	Erforderlich. Geben Sie als Modus entweder `transport` oder `tunnel` an.
`--sa-spi=` ***Sicherheitsparameter-Index***	Erforderlich. Geben Sie den Sicherheitsparameter-Index an. Der Sicherheitsparameter-Index identifiziert die Sicherheitsverbindung dem Host gegenüber. Er muss eine Hexadezimalzahl mit dem Präfix 0x sein. Jede von Ihnen erstellte Sicherheitsverbindung muss eine eindeutige Kombination aus Protokoll und Sicherheitsparameter-Index besitzen.
`--encryption-algorithm=` ***Verschlüsselungsalgorithmus***	Erforderlich. Verwenden Sie einen der folgenden Parameter, um den Verschlüsselungsalgorithmus anzugeben. ■ `3des-cbc` ■ `aes128-cbc` ■ `null` (bietet keine Verschlüsselung)
`--encryption-key=` ***Verschlüsselungsschlüssel***	Erforderlich, wenn Sie einen Verschlüsselungsalgorithmus angeben. Geben Sie den Verschlüsselungsschlüssel an. Sie können Schlüssel als ASCII-Text oder als Hexadezimalzahl mit dem Präfix 0x eingeben.
`--integrity-algorithm=` ***Authentifizierungsalgorithmus***	Erforderlich. Geben Sie den Authentifizierungsalgorithmus an: `hmac-sha1` oder `hmac-sha2-256`.

Option	Beschreibung
--integrity-key= ***Authentifizierungsschlüssel***	Erforderlich. Geben Sie den Authentifizierungsschlüssel an. Sie können Schlüssel als ASCII-Text oder als Hexadezimalzahl mit dem Präfix 0x eingeben.
--sa-name= ***Name***	Erforderlich. Geben Sie einen Namen für die Sicherheitsverbindung an.

Beispiel: Befehl für eine neue Sicherheitsverbindung

Im folgenden Beispiel wurden Zeilenumbrüche hinzugefügt, um die Lesbarkeit zu verbessern.

```
esxcli network ip ipsec sa add
--sa-source 3ffe:501:ffff:0::a
--sa-destination 3ffe:501:ffff:0001:0000:0000:0000:0001
--sa-mode transport
--sa-spi 0x1000
--encryption-algorithm 3des-cbc
--encryption-key 0x697076367265616479 6c6f676f336465736362636f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x69707636726561647 96c6f67736861316f757432
--sa-name sa1
```

Entfernen einer IPsec-Sicherheitsverbindung

Sie können eine Sicherheitsverbindung mithilfe des ESXCLI-Befehls entfernen.

Voraussetzungen

Stellen Sie sicher, dass die gewünschte Sicherheitsverbindung zurzeit nicht verwendet wird. Wenn Sie versuchen, eine Sicherheitsverbindung zu entfernen, die gerade verwendet wird, schlägt der Entfernungsvorgang fehl.

Verfahren

- Geben Sie an der Eingabeaufforderung den Befehl **esxcli network ip ipsec sa remove --sa-name** ***security_association_name*** ein.

Auflisten der verfügbaren IPsec-Sicherheitsrichtlinien

Die verfügbaren Sicherheitsrichtlinien können Sie mit dem Befehl ESXCLI auflisten.

Verfahren

- Geben Sie an der Eingabeaufforderung den Befehl **esxcli network ip ipsec sp list** ein.

Ergebnisse

Der Host zeigt eine Liste aller verfügbaren Sicherheitsrichtlinien an.

Erstellen einer IPsec-Sicherheitsrichtlinie

Erstellen Sie eine Sicherheitsrichtlinie, um festzulegen, wann die in einer Sicherheitsverbindung angegebenen Authentifizierungs- und Verschlüsselungsparameter verwendet werden sollen. Sie können eine Sicherheitsrichtlinie mithilfe des ESXCLI-Befehls hinzufügen.

Voraussetzungen

Fügen Sie vor dem Erstellen einer Sicherheitsrichtlinie eine Sicherheitsverbindung mit den entsprechenden Authentifizierungs- und Verschlüsselungsparametern hinzu, wie unter Hinzufügen einer IPsec-Sicherheitsverbindung beschrieben.

Verfahren

- Geben Sie an der Eingabeaufforderung den Befehl **`esxcli network ip ipsec sp add`** zusammen mit einer oder mehreren der nachfolgenden Optionen ein.

Option	Beschreibung
`--sp-source=` ***Quelladresse***	Erforderlich. Geben Sie Quell-IP-Adresse und die Präfixlänge an.
`--sp-destination=` ***Zieladresse***	Erforderlich. Geben Sie Zieladresse und die Präfixlänge an.
`--source-port=` ***Port***	Erforderlich. Geben Sie den Quellport an. Der Quellport muss eine Zahl zwischen 0 und 65535 sein.
`--destination-port=` ***Port***	Erforderlich. Geben Sie den Zielport an. Der Quellport muss eine Zahl zwischen 0 und 65535 sein.
`--upper-layer-protocol=` ***Protokoll***	Verwenden Sie einen der folgenden Parameter, um das Protokoll für höhere Schichten anzugeben. ■ `tcp` ■ `udp` ■ `icmp6` ■ `any`
`--flow-direction=` ***Richtung***	Wählen Sie als Richtung, in der Sie den Datenverkehr überwachen möchten, entweder `in` oder `out` aus.
`--action=` ***Aktion***	Geben Sie mithilfe eines der folgenden Parameters die Aktion an, die ausgeführt werden soll, wenn auf Datenverkehr mit den angegebenen Parametern gestoßen wird. ■ `none`: Keine Aktion ausführen. ■ `discard`: Keinen ein- oder ausgehenden Datenverkehr zulassen. ■ `ipsec`: Die in der Sicherheitsverbindung angegebenen Authentifizierungs- und Verschlüsselungsinformationen verwenden, um zu ermitteln, ob die Daten aus einer vertrauenswürdigen Quelle stammen.
`--sp-mode=` ***Modus***	Geben Sie als Modus entweder `tunnel` oder `transport` an.
`--sa-name=`*Name der Sicherheitsverbindung*	Erforderlich. Geben Sie den Namen der Sicherheitsverbindung an, die die Sicherheitsrichtlinie verwenden soll.
`--sp-name=`*Name*	Erforderlich. Geben Sie einen Namen für die Sicherheitsrichtlinie an.

Beispiel: Befehl für eine neue Sicherheitsrichtlinie

Im folgenden Beispiel wurden Zeilenumbrüche hinzugefügt, um die Lesbarkeit zu verbessern.

```
esxcli network ip ipsec add
--sp-source=2001:db8:1::/64
--sp-destination=2002:db8:1::/64
--source-port=23
--destination-port=25
--upper-layer-protocol=tcp
--flow-direction=out
--action=ipsec
--sp-mode=transport
--sa-name=sa1
--sp-name=sp1
```

Entfernen einer IPsec-Sicherheitsrichtlinie

Sie können eine Sicherheitsrichtlinie mithilfe des ESXCLI-Befehls vom ESXi-Host entfernen.

Voraussetzungen

Stellen Sie sicher, dass die gewünschte Sicherheitsrichtlinie zurzeit nicht verwendet wird. Wenn Sie versuchen, eine Sicherheitsrichtlinie zu entfernen, die gerade verwendet wird, schlägt der Entfernungsvorgang fehl.

Verfahren

- Geben Sie an der Eingabeaufforderung den Befehl **`esxcli network ip ipsec sp remove --sa-name`** ***`Name der Sicherheitsrichtlinie`*** ein.

  Um alle Sicherheitsrichtlinien zu entfernen, geben Sie den Befehl **`esxcli network ip ipsec sp remove --remove-all`** ein.

Sicherstellen einer korrekten SNMP-Konfiguration

Wenn SNMP nicht ordnungsgemäß konfiguriert ist, können Überwachungsinformationen an einen bösartigen Host gesendet werden. Der bösartige Host kann dann mithilfe dieser Informationen einen Angriff planen.

ESXi enthält einen SNMP-Agenten, der Benachrichtigungen (Traps und Informs) senden und `GET`-, `GETBULK`- und `GETNEXT`-Anforderungen empfangen kann. SNMP ist standardmäßig nicht aktiviert. SNMP muss auf jedem ESXi-Host konfiguriert werden. Für die Konfiguration können Sie ESXCLI, PowerCLI oder das vSphere Web Services SDK verwenden.

Detaillierte Informationen zum Konfigurieren von SNMP, einschließlich SNMP v3, finden Sie in der Dokumentation *vSphere-Überwachung und -Leistung*. SNMP v3 bietet eine höhere Sicherheit als SNMP v1 und SNMP v2c, einschließlich der Schlüsselauthentifizierung und -verschlüsselung. Unter *ESXCLI – Referenz* finden Sie weitere Informationen zu den `esxcli system snmp`-Befehlsoptionen.

Verfahren

1 Führen Sie den folgenden Befehl aus, um festzustellen, ob SNMP verwendet wird.

```
esxcli system snmp get
```

2 Führen Sie folgenden Befehl aus, um SNMP zu aktivieren.

```
esxcli system snmp set --enable true
```

3 Führen Sie folgenden Befehl aus, um SNMP zu deaktivieren.

```
esxcli system snmp set --enable false
```

vSphere Networking, empfohlene Vorgehensweisen für die Sicherheit

Die Einhaltung der Best Practices für die Netzwerksicherheit dient der Integritätswahrung Ihrer vSphere-Bereitstellung.

Allgemeine Netzwerksicherheitsempfehlungen

Das Befolgen allgemeiner Netzwerksicherheitsempfehlungen ist der erste Schritt zum Absichern Ihrer Netzwerkumgebung. Anschließend können Sie sich spezielle Bereiche vornehmen, wie Absichern des Netzwerks mit Firewalls oder Verwendung von IPsec.

- Das Spanning-Tree-Protokoll (STP) erkennt und verhindert die Bildung von Schleifen in der Netzwerktopologie. Virtuelle VMware-Switches verhindern Schleifen anderweitig, bieten aber keine direkte Unterstützung für STP. Wenn sich die Netzwerktopologie ändert, dauert es zwischen 30 und 50 Sekunden, bis das Netzwerk die Topologie erneut erlernt. Während dieser Zeit darf kein Datenverkehr übertragen werden. Zur Vermeidung dieser Probleme haben Netzwerkanbieter Funktionen zum Aktivieren von Switch-Ports erstellt, die die Weiterleitung des Datenverkehrs fortsetzen. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/kb/1003804. In der Dokumentation des Netzwerkanbieters finden Sie Informationen zu geeigneten Konfigurationen für das Netzwerk und die Netzwerkhardware.
- Stellen Sie sicher, dass Netflow-Daten für einen verteilten virtuellen Switch nur an autorisierte Collector-IP-Adressen gesendet werden. Netflow-Exporte werden nicht verschlüsselt und können Informationen über das virtuelle Netzwerk enthalten. Diese vertraulichen Informationen können unter Umständen während der Übertragung von Angreifern angezeigt und erfasst werden. Wenn ein Netflow-Export erforderlich ist, prüfen Sie, ob alle Netflow-Ziel-IP-Adressen korrekt sind.
- Stellen Sie mithilfe der rollenbasierten Zugriffssteuerung sicher, dass nur autorisierte Administratoren Zugriff auf virtuelle Netzwerkkomponenten haben. Geben Sie beispielsweise Administratoren virtueller Maschinen nur Zugriff auf Portgruppen, in denen sich ihre virtuellen Maschinen befinden. Geben Sie Netzwerkadministratoren Berechtigungen für alle virtuellen

Netzwerkkomponenten, aber keinen Zugriff auf virtuelle Maschinen. Durch Beschränkung des Zugriffs verringert sich das Risiko einer Fehlkonfiguration, sei es zufällig oder absichtlich, und wichtige Sicherheitskonzepte der Trennung der Verantwortlichkeiten und der geringsten Berechtigung werden in Kraft gesetzt.

- Stellen Sie sicher, dass für Portgruppen nicht der Wert des nativen VLAN konfiguriert ist. Physische Switches werden häufig mit einem nativen VLAN konfiguriert, bei dem es sich standardmäßig um VLAN 1 handelt. ESXi verfügt nicht über ein natives VLAN. Frames, für die das VLAN in der Portgruppe angegeben ist, weisen ein Tag auf, aber Frames, für die kein VLAN in der Portgruppe angegeben ist, werden nicht gekennzeichnet. Dies kann zu Problemen führen, da mit „1“ gekennzeichnete virtuelle Maschinen am Ende zum nativen VLAN des physischen Switches gehören.

  Beispielsweise werden Frames in VLAN 1 von einem physischen Cisco-Switch nicht gekennzeichnet, da VLAN1 das native VLAN auf diesem physischen Switch ist. Frames vom ESXi-Host, die als VLAN 1 festgelegt sind, werden jedoch mit einer „1“ gekennzeichnet. Das führt dazu, dass für das native VLAN bestimmter Datenverkehr vom ESXi-Host nicht korrekt weitergeleitet wird, da er mit einer „1“ gekennzeichnet ist, statt keine Kennzeichnung aufzuweisen. Datenverkehr vom physischen Switch, der vom nativen VLAN stammt, ist nicht sichtbar, da er nicht gekennzeichnet ist. Wenn die ESXi-Portgruppe für den virtuellen Switch die native VLAN-ID verwendet, ist Datenverkehr von virtuellen Maschinen auf diesem Port nicht für das native VLAN auf dem Switch sichtbar, da der Switch nicht gekennzeichneten Datenverkehr erwartet.
- Stellen Sie sicher, dass für Portgruppen keine VLAN-Werte konfiguriert sind, die für physische Upstream-Switches reserviert sind. Physische Switches reservieren bestimmte VLAN-IDs zu internen Zwecken und erlauben mit diesen Werten konfigurierten Datenverkehr in vielen Fällen nicht. Beispielsweise reservieren Cisco Catalyst-Switches in der Regel die VLANs 1001 bis 1024 und 4094. Die Verwendung eines reservierten VLAN kann einen Denial-of-Service-Fehler im Netzwerk verursachen.
- Stellen Sie sicher, dass für Portgruppen nicht VLAN 4095 konfiguriert ist, außer für Virtual Guest Tagging (VGT). Durch Festlegen von VLAN 4095 für eine Portgruppe wird der VGT-Modus aktiviert. In diesem Modus übermittelt der virtuelle Switch alle Netzwerk-Frames an die virtuelle Maschine, ohne die VLAN-Tags zu ändern, und überlässt deren Verarbeitung der virtuellen Maschine.
- Beschränken Sie Außerkraftsetzungen für die Konfiguration auf Portebene auf einem verteilten virtuellen Switch. Außerkraftsetzungen für die Konfiguration auf Portebene sind standardmäßig deaktiviert. Bei aktivierten Außerkraftsetzungen können Sie andere Sicherheitseinstellungen für eine virtuelle Maschine verwenden als die Einstellungen auf Portgruppenebene. Für bestimmte virtuelle Maschinen sind andere Konfigurationen erforderlich. Dies muss jedoch unbedingt überwacht werden. Wenn Außerkraftsetzungen nicht überwacht werden, kann jeder, der sich Zugriff auf eine virtuelle Maschine mit einer weniger sicheren Konfiguration für den virtuellen Switch verschafft, diese Sicherheitslücke auszunutzen versuchen.

- Stellen Sie sicher, dass gespiegelter Verkehr auf einem Port des verteilten virtuellen Switches nur an autorisierte Collector-Ports oder VLANs gesendet wird. Ein vSphere Distributed Switch kann Datenverkehr zwischen Ports spiegeln, damit Paketerfassungsgeräte bestimmte Verkehrsflussdaten erfassen können. Bei der Portspiegelung wird eine Kopie des gesamten angegebenen Datenverkehrs in unverschlüsseltem Format gesendet. Dieser gespiegelte Datenverkehr enthält die kompletten Daten in den erfassten Paketen und kann, wenn er an das falsche Ziel weitergeleitet wird, ein Datenleck verursachen. Wenn Portspiegelung erforderlich ist, sollten Sie sicherstellen, dass alle Ziel-VLAN-, Port- und Uplink-IDs der Portspiegelung richtig sind.

Bezeichnungen von Netzwerkkomponenten

Das Identifizieren der unterschiedlichen Komponenten Ihrer Netzwerkarchitektur ist wichtig. Dadurch wird sichergestellt, dass es bei der Vergrößerung Ihres Netzwerks nicht zu Fehlern kommt.

Befolgen Sie diese Best Practices:

- Stellen Sie sicher, dass Portgruppen mit einer eindeutigen Netzwerkbezeichnung konfiguriert werden. Diese Bezeichnungen dienen als funktionale Deskriptoren für die Portgruppen und helfen Ihnen dabei, die Funktion jeder Portgruppe zu identifizieren, wenn das Netzwerk komplexer wird.
- Stellen Sie sicher, dass jeder vSphere Distributed Switch über eine eindeutige Netzwerkbezeichnung verfügt, die die Funktion oder das IP-Subnetz des Switches angibt. Diese Bezeichnung dient als funktionaler Deskriptor für den Switch, genauso wie physische Switches einen Hostnamen erfordern. Sie können den Switch beispielsweise als intern bezeichnen, um darauf hinzuweisen, dass er für interne Netzwerke dient. Sie können die Bezeichnung für einen virtuellen Standard-Switch nicht ändern.

Dokumentieren und Überprüfen der vSphere-VLAN-Umgebung

Überprüfen Sie Ihre VLAN-Umgebung regelmäßig, um Probleme zu vermeiden. Dokumentieren Sie Ihre vSphere-VLAN-Umgebung umfassend und stellen Sie sicher, dass VLAN-IDs nur einmal verwendet werden. Ihre Dokumentation kann bei der Fehlerbehebung helfen und spielt bei der Erweiterung Ihrer Umgebung eine wichtige Rolle.

Verfahren

1 Vollständige Dokumentation aller vSphere- und VLAN-IDs

   Bei Verwendung von VLAN-Tagging auf virtuellen Switches müssen die IDs mit denen der externen VLAN-fähigen Upstream-Switches übereinstimmen. Wenn die VLAN-IDs nicht vollständig nachverfolgbar sind, kann es zu Wiederverwendung von IDs kommen und damit zu Datenverkehr zwischen den falschen physischen und virtuellen Maschinen. Ebenso kann bei fehlenden oder falschen VLAN-IDs der Datenverkehr zwischen physischen und virtuellen Maschinen an unerwünschten Stellen blockiert werden.

2 Sorgen Sie für eine vollständige Dokumentation der VLAN-IDs von allen verteilten virtuellen Portgruppen (dvPortgroup-Instanzen).

   Bei Verwendung von VLAN-Tagging in einer dvPortgroup müssen die IDs mit denen der externen VLAN-fähigen Upstream-Switches übereinstimmen. Wenn die VLAN-IDs nicht vollständig nachverfolgbar sind, kann es zu Wiederverwendung von IDs kommen und damit zu Datenverkehr zwischen den falschen physischen und virtuellen Maschinen. Ebenso kann bei fehlenden oder falschen VLAN-IDs der Datenverkehr zwischen physischen und virtuellen Maschinen an unerwünschten Stellen blockiert werden.

3 Sorgen Sie für eine vollständige Dokumentation der VLAN-IDs von allen verteilten virtuellen Switches.

   Private VLANs (PVLANs) für verteilte virtuelle Switches erfordern primäre und sekundäre VLAN-IDs. Diese IDs müssen mit denen der externen PVLAN-fähigen Upstream-Switches übereinstimmen. Wenn die VLAN-IDs nicht vollständig nachverfolgbar sind, kann es zu Wiederverwendung von IDs kommen und damit zu Datenverkehr zwischen den falschen physischen und virtuellen Maschinen. Ebenso kann bei fehlenden oder falschen PVLAN-IDs der Datenverkehr zwischen physischen und virtuellen Maschinen an unerwünschten Stellen blockiert werden.

4 Stellen Sie sicher, dass VLAN-Trunk-Links nur mit physischen Switch-Ports verbunden sind, die als Trunk-Links agieren.

   Beim Verbinden eines virtuellen Switches mit einem VLAN-Trunk-Port müssen Sie sowohl den virtuellen Switch als auch den physischen Switch am Uplink-Port ordnungsgemäß konfigurieren. Wenn der physische Switch nicht ordnungsgemäß konfiguriert ist, werden Frames mit dem VLAN 802.1q-Header an einen Switch weitergeleitet, der diese Frames nicht erwartet.

Einführung von Netzwerkisolierungspraktiken

Mit Netzwerkisolierungspraktiken können Sie die Netzwerksicherheit in der vSphere-Umgebung erhöhen.

Isolieren des Verwaltungsnetzwerks

Das vSphere-Verwaltungsnetzwerk bietet Zugriff auf die vSphere-Verwaltungsschnittstelle der einzelnen Komponenten. Die Dienste, die auf der Verwaltungsschnittstelle ausgeführt werden, bieten Angreifern die Chance, sich privilegierten Zugriff auf die Systeme zu verschaffen. Die Wahrscheinlichkeit ist hoch, dass Remoteangriffe mit der Verschaffung von Zugriff auf dieses Netzwerk beginnen. Wenn ein Angreifer sich Zugriff auf das Verwaltungsnetzwerk verschafft, hat er eine gute Ausgangsposition für ein weiteres Eindringen.

Kontrollieren Sie den Zugriff auf das Verwaltungsnetzwerk streng, indem Sie es mit der Sicherheitsebene der sichersten VM, die auf einem ESXi-Host oder -Cluster ausgeführt wird, schützen. Unabhängig davon, wie stark das Verwaltungsnetzwerk eingeschränkt ist, benötigen Administratoren Zugriff auf dieses Netzwerk, um die ESXi-Hosts und das vCenter Server-System zu konfigurieren.

Platzieren Sie die vSphere-Verwaltungsportgruppe in einem dedizierten VLAN auf einem üblichen Standard-Switch. Der Produktionsdatenverkehr (VM) kann den Standard-Switch freigeben, wenn das VLAN der vSphere-Verwaltungsportgruppe nicht von Produktions-VMs verwendet wird.

Überprüfen Sie, ob das Netzwerksegment nicht geroutet ist, mit Ausnahme von Netzwerken, in denen andere verwaltungsrelevante Elemente gefunden wurden. Das Routing eines Netzwerksegments kann für vSphere Replication sinnvoll sein. Stellen Sie insbesondere sicher, dass der Datenverkehr der Produktions-VM nicht zu diesem Netzwerk geroutet werden kann.

Kontrollieren Sie den Zugriff auf Verwaltungsfunktionen mithilfe eines der folgenden Ansätze streng.

- Konfigurieren Sie für den Zugriff auf das Verwaltungsnetzwerk in besonders vertraulichen Umgebungen ein kontrolliertes Gateway oder eine andere Kontrollmethode. Legen Sie beispielsweise fest, dass Administratoren eine Verbindung zum Verwaltungsnetzwerk über ein VPN herstellen müssen. Gestatten Sie den Zugriff auf das Verwaltungsnetzwerk nur vertrauenswürdigen Administratoren.
- Konfigurieren Sie Bastionhosts, die Verwaltungsclients ausführen.

Isolieren von Speicherdatenverkehr

Stellen Sie sicher, dass der IP-basierte Speicherdatenverkehr isoliert ist. IP-basierter Speicher umfasst iSCSI und NFS. VMs können virtuelle Switches und VLANs mit den IP-basierten Speicherkonfigurationen gemeinsam nutzen. Bei diesem Konfigurationstyp kann der IP-basierte Speicherdatenverkehr unautorisierten VM-Benutzern ausgesetzt sein.

IP-basierter Speicher ist häufig nicht verschlüsselt. Jeder Benutzer mit Zugriff auf dieses Netzwerk kann IP-basierten Speicherdatenverkehr anzeigen. Um zu verhindern, dass unautorisierte Benutzer den IP-basierten Speicherdatenverkehr anzeigen, trennen Sie den IP-basierten Speicher-Netzwerkdatenverkehr logisch vom Produktionsdatenverkehr. Konfigurieren Sie die IP-basierten Speicheradapter auf getrennten VLANs oder Netzwerksegmenten im VMkernel-Verwaltungsnetzwerk, um zu verhindern, dass unautorisierte Benutzer den Datenverkehr einsehen.

Isolieren von vMotion-Datenverkehr

vMotion-Migrationsinformationen werden als einfacher Text übermittelt. Jeder Benutzer mit Zugriff auf das Netzwerk, über das diese Informationen fließen, kann sie anzeigen. Potenzielle Angreifer können vMotion-Datenverkehr abfangen, um an die Speicherinhalte einer VM zu gelangen. Sie können auch einen MiTM-Angriff durchführen, bei dem die Inhalte während der Migration geändert werden.

Trennen Sie den vMotion-Datenverkehr vom Produktionsdatenverkehr in einem isolierten Netzwerk. Richten Sie das Netzwerk so ein, dass es nicht routing-fähig ist. Stellen Sie also sicher, dass kein Layer 3-Router dieses und andere Netzwerke umfasst, um Fremdzugriff auf das Netzwerk zu verhindern.

Verwenden Sie ein dediziertes VLAN auf einem üblichen Standard-Switch für die vMotion-Portgruppe. Der Produktionsdatenverkehr (VM) kann den gleichen Standard-Switch nutzen, wenn das VLAN der vMotion-Portgruppe VLAN nicht von Produktions-VMs verwendet wird.

Isolieren von vSAN-Datenverkehr

Isolieren Sie bei der Konfiguration Ihres vSAN-Netzwerks den vSAN-Datenverkehr in einem eigenen Schicht-2-Netzwerksegment. Sie können diesen Vorgang mithilfe von dedizierten Switches oder Ports oder mithilfe eines VLAN durchführen.

Bedarfsgerechtes Verwenden von virtuellen Switches mit der vSphere Network Appliance-API

Konfigurieren Sie den Host nicht zum Senden von Netzwerkinformationen an eine virtuelle Maschine, es sei denn, Sie verwenden Produkte, die die vSphere Network Appliance API (DvFilter) nutzen. Wenn die vSphere Network Appliance API aktiviert ist, kann ein Angreifer versuchen, eine virtuelle Maschine mit dem Filter zu verbinden. Diese Verbindung kann Zugriff auf das Netzwerk anderer virtueller Maschinen auf dem Host bereitstellen.

Wenn Sie ein Produkt verwenden, das diese API nutzt, überprüfen Sie, ob der Host ordnungsgemäß konfiguriert ist. Informationen finden Sie in den Abschnitten zu DvFilter *Entwickeln und Bereitstellen von vSphere-Lösungen, vServices und ESX-Agenten*. Wenn Ihr Host zum Verwenden der API eingerichtet ist, stellen Sie sicher, dass der Wert des Parameters `Net.DVFilterBindIpAddress` dem Produkt entspricht, das die API verwendet.

Verfahren

1. Navigieren Sie zum Host im Navigator von vSphere Client.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter „System“ auf **Erweiterte Systemeinstellungen**.
4. Führen Sie einen Bildlauf nach unten zu `Net.DVFilterBindIpAddress` aus und überprüfen Sie, ob der Parameter einen leeren Wert aufweist.

   Die Reihenfolge der Parameter ist nicht streng alphabetisch. Geben Sie **`DVFilter`** in das Textfeld „Filter“ ein, um alle zugehörigen Parameter anzuzeigen.
5. Überprüfen Sie die Einstellung.
   - Wenn Sie die DvFilter-Einstellungen nicht verwenden, stellen Sie sicher, dass der Wert leer ist.
   - Wenn Sie die DvFilter-Einstellungen nicht verwenden, stellen Sie sicher, dass der Parameterwert richtig ist. Der Wert muss mit dem Wert übereinstimmen, den das Produkt, das den DvFilter verwendet, verwendet.

Empfohlene Vorgehensweisen für mehrere vSphere-Komponenten

14

Einige empfohlene Vorgehensweisen für die Sicherheit, wie das Einrichten von PTP oder NTP in Ihrer Umgebung, wirken sich auf mehr als eine vSphere-Komponente aus. Berücksichtigen Sie diese Empfehlungen beim Konfigurieren Ihrer Umgebung.

Weitere Informationen hierzu finden Sie unter Kapitel 3 Sichern der ESXi-Hosts und Kapitel 5 Sichern von virtuellen Maschinen.

Dieses Kapitel enthält die folgenden Themen:

- Synchronisieren der Systemuhren im vSphere-Netzwerk
- Speichersicherheit, empfohlene Vorgehensweisen
- Überprüfen, ob das Senden von Hostleistungsdaten an Gastbetriebssysteme deaktiviert ist
- Einstellen von Zeitüberschreitungen für ESXi Shell und vSphere Client

Synchronisieren der Systemuhren im vSphere-Netzwerk

Stellen Sie sicher, dass auf allen Komponenten im vSphere-Netzwerk die Systemuhren synchronisiert sind. Wenn die Systemuhren auf den physischen Maschinen in Ihrem vSphere-Netzwerk nicht synchronisiert sind, werden SSL-Zertifikate und SAML-Token, die zeitabhängig sind, bei der Kommunikation zwischen Netzwerkmaschinen möglicherweise nicht als gültig erkannt.

Nicht synchronisierte Systemuhren können Authentifizierungsprobleme verursachen, was zu einer fehlgeschlagenen Installation führen bzw. verhindern kann, dass der `vmware-vpxd`-Dienst der vCenter Server gestartet wird.

Zeitinkonsistenzen in vSphere können zu einem Fehlschlagen von Firstboot auf verschiedenen Diensten führen, je nachdem, wo in der Umgebung die Zeit nicht korrekt ist und wann sie synchronisiert wird. Probleme treten am häufigsten auf, wenn der ESXi-Zielhost für den Ziel-vCenter Server nicht mit NTP oder PTP synchronisiert ist. Ebenso können Probleme auftreten, wenn die Ziel-vCenter Server zu einem ESXi-Host migriert wird, der aufgrund des vollautomatisierten DRS auf eine andere Zeit festgelegt ist.

Um Probleme mit der Zeitsynchronisierung zu verhindern, stellen Sie sicher, dass die folgenden Angaben korrekt sind, bevor Sie eine vCenter Server installieren, migrieren oder aktualisieren.

- Der ESXi-Zielhost, auf dem der Ziel-vCenter Server bereitgestellt werden soll, ist mit NTP oder PTP synchronisiert.
- Der ESXi-Host, auf dem der Quell-vCenter Server ausgeführt wird, ist mit NTP oder PTP synchronisiert.
- Wenn die vCenter Server Appliance mit einem externen Platform Services Controller verbunden ist, stellen Sie beim Aktualisieren oder Migrieren von vSphere 6.5 oder 6.7 auf vSphere 7.0 sicher, dass der ESXi-Host, der den externen Platform Services Controller ausführt, mit NTP oder PTP synchronisiert ist.
- Stellen Sie beim Upgraden oder Migrieren von vSphere 6.5 oder 6.7 auf vSphere 7.0 sicher, dass der Quell-vCenter Server oder die vCenter Server Appliance und der externe Platform Services Controller die richtige Uhrzeit aufweisen.
- Wenn Sie eine vCenter Server 6.5- oder 6.7-Instanz mit einem externen Platform Services Controller auf vSphere 7.0 upgraden, erfolgt beim Upgrade eine Konvertierung in eine vCenter Server-Instanz mit einem eingebetteten Platform Services Controller.

Stellen Sie sicher, dass alle Windows-Hostmaschinen, auf denen vCenter Server ausgeführt wird, mit dem NTP (Network Time Server)-Server synchronisiert sind. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/1318.

Um ESXi-Systemuhren mit einem NTP- oder PTP-Server zu synchronisieren, können Sie den VMware Host Client verwenden. Informationen zum Bearbeiten der Uhrzeitkonfiguration eines ESXi-Hosts finden Sie in der Dokumentation *Verwaltung eines einzelnen Hosts von vSphere – VMware Host Client*.

Informationen zum Ändern der Einstellungen der Uhrzeitsynchronisierung für vCenter Server finden Sie unter „Konfigurieren der Systemzeitzone und Zeitsynchronisierungseinstellungen“ in *vCenter Server-Konfiguration*.

Eine Anleitung zum Bearbeiten der Uhrzeitkonfiguration für einen Host mithilfe des vSphere Client finden Sie im Kapitel „Bearbeiten der Uhrzeitkonfiguration für einen Host“ unter *vCenter Server und Hostverwaltung*.

- Synchronisieren der ESXi-Systemuhren mit einem NTP-Server

  Stellen Sie vor der Installation von vCenter Server sicher, dass auf allen Maschinen im vSphere-Netzwerk die Systemuhren synchronisiert sind.
- Konfigurieren der Einstellungen für die Uhrzeitsynchronisierung in vCenter Server

  Sie können die Einstellungen für die Uhrzeitsynchronisierung in vCenter Server nach der Bereitstellung ändern.

Synchronisieren der ESXi-Systemuhren mit einem NTP-Server

Stellen Sie vor der Installation von vCenter Server sicher, dass auf allen Maschinen im vSphere-Netzwerk die Systemuhren synchronisiert sind.

Diese Aufgabe erläutert, wie Sie NTP über den VMware Host Client einrichten.

Verfahren

1 Starten Sie den VMware Host Client und stellen Sie eine Verbindung mit dem ESXi-Host her.

2 Klicken Sie auf **Verwalten**.

3 Klicken Sie unter **System** auf **Datum und Uhrzeit** und anschließend auf **Einstellungen bearbeiten**.

4 Wählen Sie **NTP (Network Time Protocol) verwenden (NTP-Client aktivieren)** aus.

5 Geben Sie im Textfeld „NTP-Server“ die IP-Adresse oder den vollqualifizierten Domänennamen mindestens eines NTP-Servers ein, der synchronisiert werden soll.

6 Wählen Sie im Dropdown-Menü **Startrichtlinie für NTP-Dienst** die Option **Mit dem Host starten und beenden** aus.

7 Klicken Sie auf **Speichern**.

   Der Host wird mit dem NTP-Server synchronisiert.

Konfigurieren der Einstellungen für die Uhrzeitsynchronisierung in vCenter Server

Sie können die Einstellungen für die Uhrzeitsynchronisierung in vCenter Server nach der Bereitstellung ändern.

Wenn Sie vCenter Server bereitstellen, können Sie für die Uhrzeitsynchronisierung entweder einen NTP-Server oder VMware Tools auswählen. Wenn sich die Uhrzeiteinstellungen in Ihrem vSphere-Netzwerk ändern, können Sie vCenter Server bearbeiten und die Uhrzeitsynchronisierungseinstellungen anhand der Befehle in der Appliance-Shell konfigurieren.

Wenn Sie die regelmäßige Uhrzeitsynchronisierung aktivieren, legt VMware Tools die Uhrzeit des Gastbetriebssystems auf die Uhrzeit des Hostcomputers fest.

Nach der Uhrzeitsynchronisierung prüft VMware Tools minütlich, ob die Uhrzeit auf dem Gastbetriebssystem mit der Uhrzeit auf dem Host übereinstimmt. Ist dies nicht der Fall, wird die Uhrzeit auf dem Gastbetriebssystem wieder mit der Uhrzeit auf dem Host synchronisiert.

Native Uhrzeitsynchronisierungssoftware wie Network Time Protocol (NTP) ist normalerweise genauer als die regelmäßige Uhrzeitsynchronisierung von VMware Tools und daher vorzuziehen. Sie können nur eine Form der regelmäßigen Uhrzeitsynchronisierung in vCenter Server verwenden. Wenn Sie sich für die native Uhrzeitsynchronisierungssoftware entscheiden, wird die regelmäßigen Uhrzeitsynchronisierung durch VMware Tools für vCenter Server deaktiviert und umgekehrt.

Verwenden der Uhrzeitsynchronisierung von VMware Tools

Sie können vCenter Server für die Verwendung der Uhrzeitsynchronisierung von VMware Tools einrichten.

Verfahren

1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Administrator- oder Superadministratorrolle an.

   Der Standardbenutzer mit der Superadministratorrolle ist „root“.

2 Führen Sie den Befehl aus, um auf VMware Tools basierte Uhrzeitsynchronisierung zu aktivieren.

```
timesync.set --mode host
```

3 (Optional) Führen Sie den Befehl aus, um zu überprüfen, ob Sie die Uhrzeitsynchronisierung von VMware Tools erfolgreich angewendet haben.

```
timesync.get
```

   Der Befehl gibt zurück, dass sich die Uhrzeitsynchronisierung im Host-Modus befindet.

Ergebnisse

Die Uhrzeit der Appliance wird mit der Uhrzeit des ESXi-Hosts synchronisiert.

Hinzufügen oder Ersetzen von NTP-Servern in der vCenter Server-Konfiguration

Wenn Sie die vCenter Server für die Verwendung der NTP-basierten Uhrzeitsynchronisierung einrichten möchten, müssen Sie zuerst die NTP-Server zur vCenter Server-Konfiguration hinzufügen.

Verfahren

1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Administrator- oder Superadministratorrolle an.

   Der Standardbenutzer mit der Superadministratorrolle ist „root“.

2 Fügen Sie der vCenter Server-Konfiguration NTP-Server hinzu, indem Sie den folgenden `ntp.set`-Befehl ausführen.

```
ntp.set --servers IP-addresses-or-host-names
```

   In diesem Befehl ist *IP-addresses-or-host-names* eine kommagetrennte Liste der IP-Adressen oder Hostnamen der NTP-Server.

   Dieser Befehl entfernt die aktuellen NTP-Server (sofern vorhanden) und fügt der Konfiguration die neuen NTP-Server hinzu. Wenn die Uhrzeitsynchronisierung auf einem NTP-Server basiert, wird der NTP-Daemon neu gestartet, um die neuen NTP-Server erneut zu laden. Andernfalls ersetzt dieser Befehl die aktuellen NTP-Server in der NTP-Konfiguration durch die neuen NTP-Server, die Sie angeben.

3 (Optional) Führen Sie den folgenden Befehl aus, um zu überprüfen, ob Sie die neuen NTP-Konfigurationseinstellungen erfolgreich angewendet haben.

```
ntp.get
```

Der Befehl gibt eine durch Leerzeichen getrennte Liste der Server zurück, die für die NTP-Synchronisierung konfiguriert sind. Bei aktivierter NTP-Synchronisierung gibt der Befehl zurück, dass die NTP-Konfiguration den Status „Erreichbar“ aufweist. Falls die NTP-Synchronisierung deaktiviert ist, gibt der Befehl zurück, dass die NTP-Konfiguration den Status „Nicht erreichbar“ aufweist.

4 (Optional) Führen Sie den folgenden Befehl aus, um zu überprüfen, ob der NTP-Server erreichbar ist.

```
ntp.test --servers IP-addresses-or-host-names
```

Der Befehl gibt den Status der NTP-Server zurück.

Nächste Schritte

Bei deaktivierter NTP-Synchronisierung können Sie die Zeitsynchronisierungseinstellungen auf dem vCenter Server auf Basis eines NTP-Servers konfigurieren. Weitere Informationen hierzu finden Sie unter Synchronisieren der Uhrzeit in vCenter Server mit einem NTP-Server.

Synchronisieren der Uhrzeit in vCenter Server mit einem NTP-Server

Sie können die Uhrzeitsynchronisierungseinstellungen in vCenter Server so konfigurieren, dass sie auf einem NTP-Server basieren.

Voraussetzungen

Richten Sie in der vCenter Server-Konfiguration mindestens einen NTP-Server (Network Time Protocol) ein. Weitere Informationen hierzu finden Sie unter Hinzufügen oder Ersetzen von NTP-Servern in der vCenter Server-Konfiguration.

Verfahren

1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Administrator- oder Superadministratorrolle an.

Der Standardbenutzer mit der Superadministratorrolle ist „root“.

2 Führen Sie den Befehl aus, um NTP-basierte Uhrzeitsynchronisierung zu aktivieren.

```
timesync.set --mode NTP
```

3 (Optional) Führen Sie den Befehl aus, um zu überprüfen, ob Sie die NTP-Synchronisierung erfolgreich angewendet haben.

```
timesync.get
```

Der Befehl gibt zurück, dass sich die Uhrzeitsynchronisierung im NTP-Modus befindet.

Speichersicherheit, empfohlene Vorgehensweisen

Befolgen Sie die von Ihrem Speicheranbieter empfohlenen Vorgehensweisen für die Speichersicherheit. Sie können auch CHAP und beiderseitiges CHAP nutzen, um iSCSI-Speicher zu sichern, SAN-Ressourcen zu maskieren und in Zonen einzuteilen und die Kerberos-Anmeldedaten für NFS 4.1 zu konfigurieren.

Weitere Informationen finden Sie in der Dokumentation zu *Verwalten von VMware vSAN*.

Absichern von iSCSI-Speicher

Der Speicher, den Sie für einen Host konfigurieren, kann ein oder mehrere SANs (Speichernetzwerke) umfassen, die iSCSI verwenden. Wenn Sie iSCSI auf einem Host konfigurieren, können Sie Maßnahmen ergreifen, um Sicherheitsrisiken zu minimieren.

iSCSI ermöglicht den Zugriff auf SCSI-Geräte und den Austausch von Datensätzen durch die Nutzung von TCP/IP über einen Netzwerkport und nicht über einen direkten Anschluss an einem SCSI-Gerät. Eine iSCSI-Transaktion fasst Blöcke von rohen SCSI-Daten in iSCSI-Datensätzen zusammen und überträgt die Daten an das anfordernde Gerät bzw. den Benutzer.

iSCSI SANs unterstützen die effiziente Nutzung der bestehenden Ethernet-Infrastruktur, um Hosts den Zugriff auf Speicherressourcen zu gewähren, die sie dynamisch freigeben können. iSCSI SANs sind eine kostengünstige Speicherlösung für Umgebungen, die auf einen gemeinsamen Speicherpool angewiesen sind, um viele Benutzer zu bedienen. Wie in allen vernetzten Systemen sind auch iSCSI-SANs anfällig für Sicherheitsverletzungen.

Hinweis Die Anforderungen und Vorgehensweisen für die Absicherung von iSCSI-SANs ähneln denen für Hardware-iSCSI-Adapter, die Hosts zugewiesen sind, sowie für iSCSI, die direkt über den Host konfiguriert werden.

Schützen von iSCSI-Geräten

Um iSCSI-Geräte zu schützen, stellen Sie sicher, dass sich der ESXi-Host bzw. der Initiator beim iSCSI-Gerät bzw. dem Ziel authentifizieren kann, wenn der Host versucht, auf Daten auf der Ziel-LUN zuzugreifen.

Die Authentifizierung stellt sicher, dass der Initiator das Recht hat, auf ein Ziel zuzugreifen. Sie gewähren dieses Recht, wenn Sie auf dem iSCSI-Gerät die Authentifizierung konfigurieren.

ESXi unterstützt für iSCSI weder Secure Remote Protocol (SRP) noch Authentifizierungsverfahren mit öffentlichen Schlüsseln. Sie können Kerberos nur mit NFS 4.1 verwenden.

ESXi unterstützt sowohl CHAP-Authentifizierung als auch beiderseitige CHAP-Authentifizierung. In der Dokumentation *vSphere-Speicher* wird erläutert, wie Sie die beste Authentifizierungsmethode für Ihr iSCSI-Gerät auswählen und CHAP einrichten.

Stellen Sie die Eindeutigkeit Ihrer CHAP-Geheimnisse sicher. Legen Sie ein anderes gegenseitiges Authentifizierungskennwort für jeden Host fest. Wenn möglich, legen Sie für jeden Client jeweils ein Kennwort fest, das sich vom Kennwort des ESXi-Hosts unterscheidet. Eindeutige Kennwörter stellen sicher, dass bei Manipulation eines bestimmten Hosts ein Angreifer nicht einen beliebigen anderen Host erstellen und sich beim Speichergerät authentifizieren kann. Mit einem einzelnen gemeinsamen geheimen Schlüssel kann sich ein Angreifer durch die Manipulation eines Hosts möglicherweise beim Speichergerät authentifizieren.

Schützen eines iSCSI-SAN

Bei der Planung der iSCSI-Konfiguration sollten Sie Maßnahmen zur Verbesserung der allgemeinen Sicherheit des iSCSI-SAN ergreifen. Die iSCSI-Konfiguration ist nur so sicher wie das IP-Netzwerk. Wenn Sie also hohe Sicherheitsstandards bei der Netzwerkeinrichtung befolgen, schützen Sie auch den iSCSI-Speicher.

Nachfolgend sind einige spezifische Vorschläge zum Umsetzen hoher Sicherheitsstandards aufgeführt.

Schützen übertragener Daten

Eines der Hauptrisiken bei iSCSI-SANs ist, dass der Angreifer übertragene Speicherdaten mitschneiden kann.

Ergreifen Sie zusätzliche Maßnahmen, um zu verhindern, dass Angreifer iSCSI-Daten sehen können. Weder der Hardware-iSCSI-Adapter noch der ESXi-iSCSI-Initiator verschlüsseln Daten, die zu und von den Zielen übertragen werden. Dies macht die Daten anfälliger für Sniffing-Angriffe.

Wenn die virtuellen Maschinen die gleichen Standard-Switches und VLANs wie die iSCSI-Struktur verwenden, ist der iSCSI-Datenverkehr potenziell dem Missbrauch durch Angreifer der virtuellen Maschinen ausgesetzt. Um sicherzustellen, dass Angreifer die iSCSI-Übertragungen nicht überwachen können, achten Sie darauf, dass keine Ihrer virtuellen Maschinen das iSCSI-Speichernetzwerk sehen kann.

Wenn Sie einen Hardware-iSCSI-Adapter verwenden, erreichen Sie dies, indem Sie sicherstellen, dass der iSCSI-Adapter und der physische Netzwerkadapter von ESXi nicht versehentlich außerhalb des Hosts durch eine gemeinsame Verwendung des Switches oder in anderer Form verbunden sind. Wenn Sie iSCSI direkt über den ESXi-Host konfigurieren, können Sie dies erreichen, indem Sie den iSCSI-Speicher über einen anderen Standard-Switch konfigurieren als denjenigen, der durch Ihre virtuellen Maschinen verwendet wird.

Zusätzlich zum Schutz durch einen eigenen Standard-Switch können Sie das iSCSI-SAN durch die Konfiguration eines eigenen VLAN für das iSCSI-SAN schützen, um Leistung und Sicherheit zu verbessern. Wenn die iSCSI-Konfiguration sich in einem eigenen VLAN befindet, wird sichergestellt, dass keine Geräte außer dem iSCSI-Adapter Einblick in Übertragungen im iSCSI-SAN haben. Auch eine Netzwerküberlastung durch andere Quellen kann den iSCSI-Datenverkehr nicht beeinträchtigen.

Sichern der iSCSI-Ports

Wenn Sie die iSCSI-Geräte ausführen, öffnet ESXi keine Ports, die Netzwerkverbindungen überwachen. Durch diese Maßnahme wird die Chance, dass ein Angreifer über ungenutzte Ports in ESXi eindringen und Kontrolle über ihn erlangen kann, reduziert. Daher stellt der Betrieb von iSCSI kein zusätzliches Sicherheitsrisiko für das ESXi-Ende der Verbindung dar.

Beachten Sie, dass auf jedem iSCSI-Zielgerät mindestens ein freigegebener TCP-Port für iSCSI-Verbindungen vorhanden sein muss. Wenn es Sicherheitsprobleme in der Software des iSCSI-Geräts gibt, können die Daten unabhängig von ESXi in Gefahr sein. Installieren Sie alle Sicherheitspatches des Speicherherstellers und beschränken Sie die Anzahl der an das iSCSI-Netzwerk angeschlossenen Geräte, um dieses Risiko zu verringern.

Maskieren von SAN-Ressourcen und Einteilen derselben in Zonen

Sie können Zoneneinteilung und LUN-Maskierung verwenden, um SAN-Aktivitäten zu trennen und den Zugriff auf Speichergeräte zu beschränken.

Sie können den Zugriff auf Speicher in Ihrer vSphere-Umgebung schützen, indem Sie Zoneneinteilung und LUN-Maskierung für Ihre SAN-Ressourcen verwenden. Sie können zum Beispiel Zonen, die zum Testen definiert sind, unabhängig innerhalb des SAN verwalten, damit sie nicht mit der Aktivität in den Produktionszonen in Konflikt geraten. Ebenso können Sie verschiedene Zonen für verschiedene Abteilungen einrichten.

Berücksichtigen Sie beim Einrichten von Zonen etwaige Hostgruppen, die auf dem SAN-Gerät eingerichtet sind.

Zoneneinteilungs- und Maskierungsfunktionen für die einzelnen SAN-Switches und Festplatten-Arrays sowie die Tools für die LUN-Maskierung sind anbieterspezifisch.

Weitere Informationen finden Sie in der Dokumentation Ihres SAN-Anbieters und in der Dokumentation zu *vSphere-Speicher*.

Verwenden von Kerberos für NFS 4.1

Mit NFS-Version 4.1 unterstützt ESXi den Kerberos-Authentifizierungsmechanismus.

Beim RPCSEC_GSS-Kerberos-Mechanismus handelt es sich um einen Authentifizierungsdienst. Mit diesem Dienst kann ein auf ESXi installierter NFS 4.1-Client vor dem Mounten einer NFS-Freigabe seine Identität bei einem NFS-Server nachweisen. Die Kerberos-Sicherheit verwendet Verschlüsselung beim Einsatz in einer ungesicherten Netzwerkverbindung.

Die ESXi-Implementierung von Kerberos für NFS 4.1 weist die beiden Sicherheitsmodelle krb5 und krb5i auf, die ein unterschiedliches Sicherheitsniveau bieten.

- Kerberos nur für Authentifizierung (krb5) unterstützt die Identitätsprüfung.
- Kerberos für Authentifizierung und Datenintegrität (krb5i) bietet neben der Identitätsprüfung auch Datenintegritätsdienste. Mit diesen Diensten kann NFS-Datenverkehr vor Manipulation geschützt werden, indem Datenpakete auf potenzielle Modifikationen überprüft werden.

Kerberos unterstützt Verschlüsselungsalgorithmen, die nicht autorisierte Benutzer daran hindern, auf NFS-Datenverkehr zuzugreifen. Der NFS 4.1-Client in ESXi versucht, mithilfe des Algorithmus AES256-CTS-HMAC-SHA1-96 oder AES128-CTS-HMAC-SHA1-96 auf eine Freigabe auf dem NAS-Server zuzugreifen. Stellen Sie vor der Verwendung Ihrer NFS 4.1-Datenspeicher sicher, dass AES256-CTS-HMAC-SHA1-96 oder AES128-CTS-HMAC-SHA1-96 auf dem NAS-Server aktiviert ist.

In der folgenden Tabelle werden die von ESXi unterstützten Kerberos-Sicherheitsstufen verglichen.

Tabelle 14-1. Kerberos-Sicherheitstypen

		ESXi 6.0	ESXi 6.5 und höher
Kerberos nur für Authentifizierung (krb5)	Integritätsprüfsumme für RPC-Header	Ja mit DES	Ja mit AES
	Integritätsprüfsumme für RPC-Daten	Nein	Nein
Kerberos für Authentifizierung und Datenintegrität (krb5i)	Integritätsprüfsumme für RPC-Header	Kein krb5i	Ja mit AES
	Integritätsprüfsumme für RPC-Daten		Ja mit AES

Wenn Sie die Kerberos-Authentifizierung verwenden, ist Folgendes zu beachten:

- ESXi verwendet Kerberos zusammen mit der Active Directory-Domäne.
- Als vSphere-Administrator geben Sie Active Directory-Anmeldedaten an, um einem NFS-Benutzer Zugriff auf NFS 4.1-Kerberos-Datenspeicher zu erteilen. Ein einzelner Anmeldedatensatz wird zum Zugriff auf alle Kerberos-Datenspeicher, die auf diesem Host gemountet sind, verwendet.
- Wenn mehrere ESXi-Hosts den NFS 4.1-Datenspeicher gemeinsam nutzen, müssen Sie dieselben Active Directory-Anmeldedaten für alle Hosts verwenden, die auf den gemeinsam genutzten Datenspeicher zugreifen. Um den Zuweisungsvorgang zu automatisieren, legen Sie den Benutzer in Hostprofilen fest und wenden das Profil auf alle ESXi-Hosts an.
- Es ist nicht möglich, zwei Sicherheitsmechanismen (AUTH_SYS und Kerberos) für denselben NFS 4.1-Datenspeicher zu verwenden, der von mehreren Hosts gemeinsam genutzt wird.

Eine schrittweise Anleitung finden Sie in der Dokumentation *vSphere-Speicher*.

Überprüfen, ob das Senden von Hostleistungsdaten an Gastbetriebssysteme deaktiviert ist

vSphere umfasst Leistungsindikatoren für virtuelle Maschinen auf Windows-Betriebssystemen, bei denen VMware Tools installiert ist. Leistungsindikatoren ermöglichen den Besitzern virtueller Maschinen eine exakte Leistungsanalyse innerhalb des Gastbetriebssystems. Standardmäßig legt vSphere gegenüber der virtuellen Gastmaschine keine Hostinformationen offen.

Standardmäßig ist die Funktion zum Senden von Hostleistungsdaten an eine virtuelle Maschine deaktiviert. Durch diese Standardeinstellung wird verhindert, dass eine virtuelle Maschine detaillierte Informationen über den physischen Host erhält. Tritt ein Sicherheitsverstoß im Zusammenhang mit der virtuellen Maschine auf, werden durch die Einstellung dem Angreifer keine Hostdaten zur Verfügung gestellt.

Hinweis Die grundlegende Vorgehensweise wird im Folgenden beschrieben. Verwenden Sie die ESXCLI- oder VMware PowerCLI-Befehle, um diese Aufgabe auf allen Hosts gleichzeitig auszuführen.

Verfahren

1. Navigieren Sie auf dem ESXi-System, das die virtuelle Maschine hostet, zur VMX-Datei.

   Die Konfigurationsdateien der virtuellen Maschinen befinden sich im Verzeichnis `/vmfs/volumes/`*`Datenspeicher`*, wobei es sich bei *Datenspeicher* um den Namen des Speichergeräts handelt, auf dem die Dateien der virtuellen Maschine gespeichert sind.
2. Stellen Sie sicher, dass in der VMX-Datei der folgende Parameter gesetzt ist.

   ```
   tools.guestlib.enableHostInfo=FALSE
   ```
3. Speichern und schließen Sie die Datei.

Ergebnisse

Von der virtuellen Gastmaschine aus können keine Leistungsinformationen abgerufen werden.

Einstellen von Zeitüberschreitungen für ESXi Shell und vSphere Client

Um zu verhindern, dass Angreifer eine Sitzung im Leerlauf verwenden können, legen Sie Zeitüberschreitungen für die ESXi Shell und vSphere Client fest.

Zeitüberschreitung für ESXi Shell

Für ESXi Shell können Sie die folgenden Zeitüberschreitungen über den vSphere Client oder über die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) festlegen.

Verfügbarkeits-Zeitüberschreitung

Der Zeitüberschreitungswert für die Verfügbarkeit gibt die Zeitspanne an, während der Sie sich nach der Aktivierung der ESXi Shell anmelden müssen. Nach Ablauf dieser Zeitspanne wird der Dienst deaktiviert und die Benutzer können sich nicht mehr anmelden.

Leerlauf-Zeitüberschreitung

Der Zeitüberschreitungswert für die Leerlaufzeit gibt die Zeitspanne an, die verstreichen darf, bis Sie bei interaktiven Sitzungen, die sich im Leerlauf befinden, abgemeldet werden. Änderungen an den Zeitüberschreitungswerten für die Leerlaufzeit werden erst wirksam, wenn sich ein Benutzer das nächste Mal bei der ESXi Shell anmeldet. Änderungen wirken sich nicht auf vorhandene Sitzungen aus.

Zeitüberschreitung für vSphere Client

vSphere Client-Sitzungen werden standardmäßig nach 120 Minuten beendet. So ändern Sie die Standardeinstellungen:

1 Navigieren Sie im vSphere Client zur vCenter Server-Instanz.

2 Wählen Sie die Registerkarte **Konfigurieren** und unter **Einstellungen** die Option **Allgemein** aus.

3 Klicken Sie auf **Bearbeiten**.

4 Wählen Sie **Zeitüberschreitungseinstellungen**.

5 Geben Sie die gewünschten Einstellungen ein und klicken Sie auf **Speichern**.

Verwalten der Konfiguration des TLS-Protokolls mit dem TLS-Konfigurationsprogramm

15

In vSphere ist standardmäßig nur TLS aktiviert. TLS 1.0 und TLS 1.1 sind standardmäßig deaktiviert. In vSphere ist TLS 1.0 und TLS 1.1 immer deaktiviert. Dabei spielt es keine Rolle, ob Sie eine Neuinstallation, ein Upgrade oder eine Migration durchführen. Sie können ältere Versionen des Protokolls vorübergehend mit dem TLS Configurator-Dienstprogramm auf vSphere-Systemen aktivieren. Sie können dann die älteren, weniger sicheren Versionen deaktivieren, sobald für alle Verbindungen TLS 1.2 verwendet wird.

Analysieren Sie vor einer Neukonfiguration Ihre Umgebung. Je nach den Anforderungen an Ihre Umgebung und Ihren Softwareversionen müssen Sie unter Umständen zusätzlich zu TLS 1.2 TLS 1.0 und TLS 1.1 erneut aktivieren, um die Interoperabilität zu erhalten. Für VMware-Produkte finden Sie im VMware-Knowledgebase-Artikel unter https://kb.vmware.com/s/article/2145796 eine Liste der VMware-Produkte, die TLS 1.2 unterstützen. Fragen zur Integration von Drittanbieterprodukten werden in der Dokumentation Ihres Anbieters beantwortet. Das TLS-Konfigurationsprogramm funktioniert mit vSphere 7.0 und früheren Versionen, einschließlich 6.7, 6.5 und 6.0.

Dieses Kapitel enthält die folgenden Themen:

Ports, die die Deaktivierung von TLS-Versionen unterstützen

Wenn Sie das TLS-Konfigurationsprogramm in der vSphere-Umgebung ausführen, können Sie TLS für Ports deaktivieren, die TLS auf vCenter Server- und ESXi-Hosts verwenden. Sie können TLS 1.0 oder sowohl TLS 1.0 als auch TLS 1.1 deaktivieren.

Ab vSphere 7.0 führt vCenter Server zwei Reverse-Proxy-Dienste aus:

- VMware-Reverse-Proxy-Dienst, `rhttpproxy`
- Envoy

Bei Envoy handelt es sich um einen Edge- und Dienst-Proxy, der als Open Source bereitgestellt wird. Envoy belegt Port 443 und alle eingehenden vCenter Server-Anfragen werden über Envoy weitergeleitet. In vSphere 7.0 dient `rhttpproxy` als Konfigurationsverwaltungsserver für Envoy. Folglich wird die TLS-Konfiguration auf `rhttpproxy` angewendet, wodurch die Konfiguration an Envoy gesendet wird.

vCenter Server und ESXi verwenden Ports, die für TLS-Protokolle aktiviert oder deaktiviert werden können. Die `scan`-Option des Dienstprogramms zur TLS-Konfiguration zeigt an, welche Versionen von TLS für jeden Dienst aktiviert sind. Weitere Informationen finden Sie unter Suchen nach aktivierten TLS-Protokollen in vCenter Server.

Eine Liste aller unterstützten Ports und Protokolle in VMware, einschließlich vSphere und vSAN, finden Sie im Tool VMware Ports and Protocols™ unter https://ports.vmware.com/. Sie können Ports nach VMware-Produkt durchsuchen, eine benutzerdefinierte Portliste erstellen und Portlisten drucken oder speichern.

Hinweise und Vorsichtsmaßnahmen

- vSphere 6.7 ist die letzte Version von vCenter Server für Windows. In der *vSphere-Sicherheit*-Dokumentation für Version 6.7 des Produkts finden Sie Informationen zum Neukonfigurieren von TLS für Update Manager-Ports auf vCenter Server für Windows.
- Sie können TLS 1.2 verwenden, um die Verbindung zwischen vCenter Server und einem externen Microsoft SQL Server zu verschlüsseln. Eine reine TLS 1.2-Verbindung zu einer externen Oracle-Datenbank kann nicht verwendet werden. Informationen finden Sie in dem VMware-Knowledgebase-Artikel unter https://kb.vmware.com/kb/2149745.
- Deaktivieren Sie TLS 1.0 für vSphere 6.7 und frühere Versionen nicht für eine vCenter Server- oder Platform Services Controller-Instanz, die unter Windows Server 2008 ausgeführt wird. Windows 2008 unterstützt nur TLS 1.0. Weitere Informationen hierzu finden Sie im Microsoft TechNet-Artikel *TLS/SSL-Einstellungen* im *Leitfaden zu Serverrollen und Technologien*.
- Bei einer Änderung der TLS-Protokolle müssen Sie den ESXi-Host neu starten, um die Änderungen zu übernehmen. Sie müssen den Host auch dann neu starten, wenn Sie die Änderungen über die Clusterkonfiguration anwenden, indem Sie Hostprofile verwenden. Sie können den Host sofort neu starten oder den Neustart auf einen besser geeigneten Zeitpunkt verschieben.

Aktivieren oder Deaktivieren von TLS-Versionen in vSphere

Die Deaktivierung von TLS-Versionen besteht aus mehreren Phasen. Durch Deaktivieren der TLS-Versionen in der richtigen Reihenfolge wird sichergestellt, dass Ihre Umgebung während des Vorgangs weiterhin betriebsbereit ist.

vSphere Lifecycle Manager ist immer im Lieferumfang des vCenter Server-Systems enthalten, und das Skript aktualisiert den entsprechenden Port.

1 Führen Sie das TLS-Konfigurationsprogramm auf vCenter Server aus.

2 Führen Sie das TLS-Konfigurationsprogramm auf jedem ESXi-Host aus, der vom vCenter Server verwaltet wird. Sie können diese Aufgabe für einzelne Hosts oder für alle Hosts in einem Cluster ausführen.

Voraussetzungen

Sie können TLS in Ihrer Umgebung auf zwei Arten verwenden.

- TLS 1.0 deaktivieren und TLS 1.1 und TLS 1.2 aktivieren.
- TLS 1.0 und TLS 1.1 deaktivieren und TLS 1.2 aktivieren.

Führen Sie eine optionale manuelle Sicherung durch

Das TLS-Konfigurationsdienstprogramm führt bei jeder Änderung von vCenter Server durch das Skript eine Sicherung aus. Wenn Sie eine Sicherung für ein bestimmtes Verzeichnis benötigen, können Sie eine manuelle Sicherung durchführen.

Das Sichern der ESXi-Konfiguration wird nicht unterstützt.

Für vCenter Server lautet das Standardverzeichnis folgendermaßen: `/tmp/`*`yearmonthday`*`T`*`time`*.

Verfahren

1 Wechseln Sie zum Verzeichnis `/usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator`.

2 Zum Erstellen einer Sicherung in einem bestimmten Verzeichnis führen Sie folgenden Befehl aus.

```
Verzeichnispfad/VcTlsReconfigurator> ./reconfigureVc backup -d Sicherungsverzeichnispfad
```

3 Stellen Sie sicher, dass die Sicherung erfolgreich war.

Eine erfolgreiche Sicherung ist dem folgenden Beispiel ähnlich. Die Reihenfolge der angezeigten Dienste ist möglicherweise bei jeder Ausführung des Befehls `reconfigureVc backup` unterschiedlich. Dies liegt an der Art und Weise, auf die der Befehl ausgeführt wird.

```
vCenter Transport Layer Security reconfigurator, version=7.0.0, build=15518531
For more information refer to the following article: https://kb.vmware.com/kb/2147469
Log file: "/var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log".
================= Backing up vCenter Server TLS configuration ==================
Using backup directory: /tmp/20200206T183550
Backing up: vmware-rbd-watchdog
Backing up: vmware-vpxd
Backing up: vmcam
Backing up: vmware-stsd
Backing up: vmdird
```

```
Backing up: vmware-sps
Backing up: vmware-rhttpproxy
Backing up: vami-lighttp
Backing up: vmware-updatemgr
Backing up: rsyslog
```

4 (Optional) Wenn Sie später eine Wiederherstellung durchgeführt haben, können Sie den folgenden Befehl ausführen.

```
reconfigureVc restore -d optional_custom_backup_directory_path
```

Aktivieren oder Deaktivieren von TLS-Versionen auf vCenter Server-Systemen

Mit dem TLS-Konfigurationsprogramm können Sie TLS-Versionen auf vCenter Server-Systemen aktivieren oder deaktivieren. Sie können im Rahmen dieses Prozesses TLS 1.0 deaktivieren und TLS 1.1 und TLS 1.2 aktivieren. Oder Sie können TLS 1.0 und TLS 1.1 deaktivieren und nur TLS 1.2 aktivieren.

Voraussetzungen

Stellen Sie sicher, dass die von vCenter Server verwalteten Hosts und Dienste mithilfe einer TLS-Version, die aktiviert bleibt, kommunizieren können. Für Produkte, die nur mithilfe von TLS 1.0 kommunizieren, wird die Verbindung getrennt.

Verfahren

1 Melden Sie sich beim vCenter Server-System mit dem Benutzernamen und dem Kennwort für „administrator@vsphere.local“ oder als anderes Mitglied der Administratorengruppe von vCenter Single Sign-On an, das Skripts ausführen darf.

2 Navigieren Sie zu dem Verzeichnis, in dem sich das Skript befindet.

```
cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
```

3 Führen Sie den Befehl je nach gewünschter TLS-Version aus.

- Um TLS 1.0 zu deaktivieren und sowohl TLS 1.1 also auch TLS 1.2 zu aktivieren, führen Sie den folgenden Befehl aus.

  ```
  directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2
  ```

- Um TLS 1.0 und TLS 1.1 zu deaktivieren und nur TLS 1.2 zu aktivieren, führen Sie den folgenden Befehl aus.

  ```
  directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2
  ```

4 Wenn in Ihrer Umgebung andere vCenter Server-Systeme vorhanden sind, wiederholen Sie den Vorgang auf jedem vCenter Server-System.

5 Wiederholen Sie die Konfiguration auf jedem ESXi-Host.

Aktivieren oder Deaktivieren von TLS-Versionen auf ESXi-Hosts

Mit dem TLS-Konfigurationsprogramm können Sie TLS-Versionen auf einem ESXi-Host aktivieren oder deaktivieren. Sie können im Rahmen dieses Prozesses TLS 1.0 deaktivieren und TLS 1.1 und TLS 1.2 aktivieren. Oder Sie können TLS 1.0 und TLS 1.1 deaktivieren und nur TLS 1.2 aktivieren.

Für ESXi-Hosts verwenden Sie ein anderes Dienstprogramm als für die anderen Komponenten Ihrer vSphere-Umgebung. Das Dienstprogramm ist versionsspezifisch und kann für eine vorherige Version nicht verwendet werden.

Sie können ein Skript zum Konfigurieren von mehreren Hosts schreiben.

Voraussetzungen

Stellen Sie sicher, dass alle Produkte oder Dienste im Zusammenhang mit dem ESXi-Host mithilfe von TLS 1.1 oder TLS 1.2 kommunizieren können. Für Produkte, die nur mithilfe von TLS 1.0 kommunizieren, wird die Verbindung getrennt.

Die Bash-Shell muss in der vCenter Server Appliance aktiviert werden.

Verfahren

1 Melden Sie sich über SSH mit dem Benutzernamen und dem Kennwort des vCenter Single Sign-On-Benutzers, der Skripts ausführen darf, bei vCenter Server Appliance an.

2 Um die Bash-Shell zu aktivieren, geben Sie in der Befehlszeile **`shell`** ein.

3 Navigieren Sie zu dem Verzeichnis, in dem sich das Skript befindet.

```
cd /usr/lib/vmware-TlsReconfigurator/EsxTlsReconfigurator
```

4 Führen Sie für einen ESXi-Host, der Teil eines Clusters ist, einen der folgenden Befehle aus.

- Um TLS 1.0 zu deaktivieren und sowohl TLS 1.1 also auch TLS 1.2 auf allen Hosts in einem Cluster zu aktivieren, führen Sie den folgenden Befehl aus.

  ```
  ./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.1
  TLSv1.2
  ```

- Um TLS 1.0 und TLS 1.1 zu deaktivieren und nur TLS 1.2 auf allen Hosts in einem Cluster zu aktivieren, führen Sie den folgenden Befehl aus.

  ```
  ./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2
  ```

5 Führen Sie für einen einzelnen Host, der nicht Teil eines Clusters ist, einen der folgenden Befehle aus.

- Um TLS 1.0 zu deaktivieren und sowohl TLS 1.1 also auch TLS 1.2 für einen einzelnen Host zu aktivieren, führen Sie den folgenden Befehl aus.

```
./reconfigureEsx vCenterHost -h ESXi_Host_Name -u Administrative_User -p TLSv1.1
TLSv1.2
```

- Um TLS 1.0 und TLS 1.1 zu deaktivieren und nur TLS 1.2 für einen einzelnen Host zu aktivieren, führen Sie den folgenden Befehl aus.

```
./reconfigureEsx vCenterHost -h ESXi_Host_Name -u Administrative_User -p TLSv1.2
```

Hinweis Um einen eigenständigen ESXi-Host neu zu konfigurieren, melden Sie sich bei einem vCenter Server-System an und führen Sie den Befehl `reconfigureEsx` mit den Optionen `ESXiHost -h` *HOST* `-u` *ESXi_ USER* aus. Für die Option *HOST* können Sie die IP-Adresse oder den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) eines einzelnen ESXi-Hosts oder eine Liste von Host-IP-Adressen oder FQDNs angeben. Wenn Sie sich beispielsweise bei einem vCenter Server anmelden und den folgenden Befehl ausführen, werden sowohl TLS 1.1 als auch TLS 1.2 auf zwei ESXi-Hosts aktiviert:

```
./reconfigureEsx ESXiHost -h 198.51.100.2 198.51.100.3 -u root -p TLSv1.1 TLSv1.2
```

Alternativ können Sie sich zum Neukonfigurieren eines eigenständigen ESXi-Hosts beim Host anmelden und die erweiterte Einstellung `UserVars.ESXiVPsDisabledProtocols` ändern. Weitere Informationen finden Sie im Thema „Konfigurieren erweiterter TLS/SSL-Schlüsseloptionen“ in der Dokumentation zu *Verwaltung eines einzelnen Hosts von vSphere – VMware Host Client*.

6 Starten Sie den ESXi-Host neu, um die TLS-Protokolländerungen abzuschließen.

Suchen nach aktivierten TLS-Protokollen in vCenter Server

Nachdem Sie TLS-Versionen auf vCenter Server aktivieren oder deaktivieren, können Sie das TLS-Konfigurationsprogramm verwenden, um Ihre Änderungen anzuzeigen.

Die `scan`-Option des Dienstprogramms zur TLS-Konfiguration zeigt an, welche Versionen von TLS für jeden Dienst aktiviert sind.

Verfahren

1 Melden Sie sich beim vCenter Server-System an.

   a Stellen Sie mithilfe von SSH eine Verbindung mit der Appliance her und melden Sie sich als Benutzer mit Berechtigungen zum Ausführen von Skripts an.

   b Wenn die Bash-Shell derzeit nicht aktiviert ist, führen Sie die folgenden Befehle aus.

```
shell.set --enabled true
shell
```

2 Wechseln Sie zum Verzeichnis `VcTlsReconfigurator`.

```
cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
```

3 Um anzuzeigen, für welche Dienste TLS aktiviert ist, und die verwendeten Ports anzuzeigen, führen Sie den folgenden Befehl aus.

```
reconfigureVc scan
```

Zurücksetzen von TLS-Konfigurationsänderungen

Mit dem TLS-Konfigurationsprogramm können Sie Konfigurationsänderungen zurücksetzen. Wenn Sie die Änderungen zurücksetzen, werden Protokolle aktiviert, die Sie mit dem TLS-Konfigurationsprogramm deaktiviert haben.

Voraussetzungen

Verwenden Sie vor dem Zurücksetzen von Änderungen die vCenter Server-Verwaltungsschnittstelle, um eine Sicherung des vCenter Server durchzuführen.

Verfahren

1 Stellen Sie eine Verbindung zum vCenter Server her, auf dem Sie als Benutzer mit der Berechtigung zum Ausführen von Skripts Änderungen rückgängig machen möchten.

2 Wenn die Bash-Shell derzeit nicht aktiviert ist, führen Sie die folgenden Befehle aus.

```
shell.set --enabled true
shell
```

3 Wechseln Sie zum Verzeichnis `VcTlsReconfigurator`.

```
cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
```

4 Prüfen Sie die vorherige Sicherung.

```
grep "backup directory" /var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log
```

Die Ausgabe ähnelt derjenigen im folgenden Beispiel.

```
2016-11-17T17:29:20.950Z INFO Using backup directory: /tmp/20161117T172920
2016-11-17T17:32:59.019Z INFO Using backup directory: /tmp/20161117T173259
```

5 Führen Sie den folgenden Befehl aus, um eine Wiederherstellung vorzunehmen.

```
reconfigureVc restore -d Directory_path_from_previous_step
```

Die Ausgabe ähnelt derjenigen im folgenden Beispiel.

```
2016-11-17T17:29:20.950Z INFO Using backup directory: /tmp/20161117T172920
2016-11-17T17:32:59.019Z INFO Using backup directory: /tmp/20161117T173259
```

6 Wiederholen Sie diesen Vorgang für alle anderen vCenter Server-Instanzen.

Definierte Rechte

16

In den folgenden Tabellen werden die Standardrechte aufgelistet, die mit einem Benutzer kombiniert und einem Objekt zugeordnet werden können, wenn sie für eine Rolle ausgewählt werden.

Stellen Sie beim Festlegen der Berechtigungen sicher, dass alle Objekttypen mit geeigneten Rechten für jede spezielle Aktion eingerichtet sind. Für einige Vorgänge sind neben dem Zugriff auf das bearbeitete Objekt auch Zugriffsberechtigungen für den Root-Ordner oder den übergeordneten Ordner erforderlich. Für einige Vorgänge sind Zugriffs- oder Ausführungsberechtigungen in einem übergeordneten Ordner und einem bezogenen Objekt erforderlich.

Mit vCenter Server-Erweiterungen werden möglicherweise zusätzliche Rechte definiert, die hier nicht aufgeführt werden. Weitere Informationen zu diesen Rechten finden Sie in der Dokumentation der Erweiterung.

Dieses Kapitel enthält die folgenden Themen:

- Rechte für Erweiterungen
- Rechte für Bereitstellungsfunktion externer Statistiken
- Rechte für Ordner
- Globale Rechte
- Rechte für Bereitstellungsfunktion für Aktualisierungen des Systemzustands
- Host-CIM-Rechte
- Rechte für die Hostkonfiguration
- Hostbestandsliste
- Rechte für lokale Hostoperationen
- vSphere Replication-Rechte von Hosts
- Hostprofil-Berechtigungen
- vSphere mit Tanzu-Berechtigungen
- Netzwerkberechtigungen
- Leistungsrechte
- Rechte für Berechtigungen
- Profilgesteuerte Speicherrechte
- Rechte für Ressourcen
- Rechte für geplante Aufgaben
- Sitzungsrechte
- Speicheransichtsberechtigungen
- Rechte für Aufgaben
- Transfer Service-Rechte
- Rechte für VcTrusts/VcIdentity
- Rechte für „Administrator der vertrauenswürdigen Infrastruktur“
- vApp-Rechte
- Rechte für VcIdentityProviders
- Rechte für die Konfiguration von VMware vSphere Lifecycle Manager
- Rechte für ESXi-Integritätsperspektiven für VMware vSphere Lifecycle Manager
- Allgemeine Rechte für VMware vSphere Lifecycle Manager
- Rechte für die Hardwarekompatibilität von VMware vSphere Lifecycle Manager
- Rechte für VMware vSphere Lifecycle Manager-Images
- Rechte für die Standardisierung von VMware vSphere Lifecycle Manager-Images

- Rechte für VMware vSphere Lifecycle Manager-Einstellungen
- Rechte für die Verwaltung von VMware vSphere Lifecycle Manager-Baselines
- Rechte zum Verwalten von Patches und Upgrades für VMware vSphere Lifecycle Manager
- Rechte zum Hochladen von Dateien für VMware vSphere Lifecycle Manager
- Berechtigungen für das Konfigurieren virtueller Maschinen
- Rechte für Vorgänge als Gast auf virtuellen Maschinen
- Rechte für die Interaktion virtueller Maschinen
- Rechte für die Bestandsliste der virtuellen Maschine
- Rechte für das Bereitstellen virtueller Maschinen
- Rechte für die Dienstkonfiguration der virtuellen Maschine
- Rechte für die Snapshot-Verwaltung von virtuellen Maschinen
- vSphere Replication-Rechte der VM
- vServices-Rechte
- vSphere-Tag-Berechtigungen
- vSphere Client-Rechte

Alarmrechte

Alarmrechte steuern die Fähigkeit, Alarme für Bestandslistenobjekte zu erstellen, zu ändern und darauf zu reagieren.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-1. Alarmrechte

Rechtename	Beschreibung	Erforderlich bei
Alarme.Alarm bestätigen	Ermöglicht die Unterdrückung aller Alarmaktionen für alle ausgelösten Alarme.	Objekt, für das ein Alarm definiert ist
Alarme.Alarm erstellen	Ermöglicht das Erstellen eines neuen Alarms. Beim Erstellen von Alarmen mit einer benutzerdefinierten Aktion wird das Recht zum Ausführen der Aktion überprüft, wenn der Benutzer den Alarm erstellt.	Objekt, für das ein Alarm definiert ist

Tabelle 16-1. Alarmrechte (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Alarme.Alarmaktion deaktivieren	Ermöglicht das Verhindern, dass eine Alarmaktion ausgeführt wird, nachdem ein Alarm ausgelöst wurde. Dies deaktiviert nicht den Alarm.	Objekt, für das ein Alarm definiert ist
Alarme.Deaktivieren oder Aktivieren des Alarms für Element	Ermöglicht das Aktivieren oder Deaktivieren eines bestimmten Alarms für einen bestimmten Zieltyp.	Objekt, für das der Alarm ausgelöst werden kann
Alarme.Alarm ändern	Ermöglicht die Änderung der Eigenschaften eines Alarms.	Objekt, für das ein Alarm definiert ist
Alarme.Alarm entfernen	Ermöglicht das Löschen eines Alarms.	Objekt, für das ein Alarm definiert ist
Alarme.Alarmstatus festlegen	Ermöglicht das Ändern des Status des konfigurierten Ereignisalarms. Der Status kann den Wert **Normal**, **Warnung** oder **Alarm** annehmen.	Objekt, für das ein Alarm definiert ist

Rechte für Auto Deploy und Image-Profile

Auto Deploy-Rechte bestimmen, wer welche Aufgaben für Auto Deploy-Regeln ausführen kann und wer einen Host zuordnen kann. Auto Deploy-Rechte ermöglichen auch die Kontrolle darüber, wer ein Image-Profil erstellen oder bearbeiten kann.

In der folgenden Tabelle werden Rechte beschrieben, die bestimmen, wer Auto Deploy-Regeln und -Regelsätze verwalten kann und wer Image-Profile erstellen und bearbeiten kann. Siehe *Installation und Einrichtung von vCenter Server*.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-2. Auto Deploy-Rechte

Rechtename	Beschreibung	Erforderlich bei
Auto Deploy.-Host.Maschine verknüpfen	Ermöglicht Benutzern das Zuordnen eines Hosts zu einem Computer.	vCenter Server
Auto Deploy.Image-Profil.Erstellen	Ermöglicht das Erstellen von Image-Profilen.	vCenter Server
Auto Deploy.Image-Profil.Bearbeiten	Ermöglicht das Bearbeiten von Image-Profilen.	vCenter Server
Auto Deploy.Regel.Erstellen	Ermöglicht das Erstellen von Auto Deploy-Regeln.	vCenter Server
Auto Deploy.Regel.Löschen	Ermöglicht das Löschen von Auto Deploy-Regeln.	vCenter Server

Tabelle 16-2. Auto Deploy-Rechte (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Auto Deploy.Rule.Edit	Ermöglicht das Bearbeiten von Auto Deploy-Regeln.	vCenter Server
Auto Deploy.Regelsatz.Aktivieren	Ermöglicht das Aktivieren von Auto Deploy-Regelsätzen.	vCenter Server
Auto Deploy.Regelsatz.Bearbeiten	Ermöglicht das Bearbeiten von Auto Deploy-Regelsätzen.	vCenter Server

Zertifikatsrechte

Zertifikatsrechte bestimmen, welche Benutzer ESXi-Zertifikate verwalten können.

Dieses Recht bestimmt, wer die Zertifikatsverwaltung für ESXi-Hosts durchführen kann. Im Abschnitt zu den erforderlichen Rechten für Zertifikatverwaltungsvorgänge der Dokumentation *vSphere-Authentifizierung* finden Sie Informationen zur vCenter Server-Zertifikatsverwaltung.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-3. Rechte für Hostzertifikate

Rechtename	Beschreibung	Erforderlich bei
Zertifikate.Zertifikate verwalten	Ermöglicht die Zertifikatsverwaltung für ESXi-Hosts.	vCenter Server

Berechtigungen der Zertifizierungsstelle

Mit Berechtigungen der Zertifizierungsstelle werden Aspekte der VMCA-Zertifikate (VMware Certificate Authority) gesteuert.

Tabelle 16-4. Berechtigungen der Zertifizierungsstelle

Rechtename	Beschreibung	Erforderlich bei
Zertifizierungsstelle.Erstellen/Löschen (Administratorrechte).	Ermöglicht Vollzugriff auf Administratorebene für die Verwaltung von vCenter Server-Zertifikaten.	vCenter Server
Zertifizierungsstelle.Erstellen/Löschen (unter Administratorrechten).	Ermöglicht die Anzeige des VMCA-Rootzertifikats auf der Seite „Zertifikatsverwaltung“ im vSphere Client.	vCenter Server

Berechtigungen der Zertifikatsverwaltung

Über die Berechtigungen der Zertifikatsverwaltung werden die Benutzer bestimmt, die vCenter Server-Zertifikate verwalten können.

Tabelle 16-5. Berechtigungen der Zertifikatsverwaltung

Rechtename	Beschreibung	Erforderlich bei
Zertifikatverwaltung.Erstellen/Löschen (Administratorrechte).	Ermöglicht Vollzugriff auf Administratorebene auf verschiedene interne APIs und Funktionen für zertifikatsbezogene vCenter Server-Vorgänge.	vCenter Server
Zertifikatverwaltung.Erstellen/Löschen (unter Administratorrechten).	Ermöglicht verringerten administrativen Zugriff auf verschiedene interne APIs und Funktionen. Mit dieser Berechtigung werden zertifikatsbezogene Vorgänge so eingeschränkt, dass der Benutzer Nicht-Administratorrechte nicht eskalieren kann. Zu den zulässigen Vorgängen gehören: ■ Erzeugen von Zertifikatsignieranforderungen ■ Erstellen und Abrufen vertrauenswürdiger Stammzertifikatsketten ■ Löschen vertrauenswürdiger Stammzertifikatsketten, die von einem Benutzer mit der Berechtigung **Zertifikatverwaltung.Erstellen/Löschen (unter Administratorrechten).** erstellt wurden ■ Abrufen von Maschinen-SSL-Zertifikaten ■ Abrufen der Signaturzertifikatsketten zum Validieren von Token, die von vCenter Server ausgegeben wurden	vCenter Server

CNS-Rechte

Mit CNS-Rechten (Cloud Native Store) werden die Benutzer gesteuert, die auf die CNS-Benutzeroberfläche zugreifen können.

Tabelle 16-6. CNS-Rechte

Rechtename	Beschreibung	Erforderlich bei
CNS.Durchsuchbar	Ermöglicht dem Speicheradministrator die Anzeige der CNS-Benutzeroberfläche (Cloud Native Storage).	Root-vCenter Server

Rechte für Inhaltsbibliotheken

Inhaltsbibliotheken bieten einfache und effiziente Verwaltung für Vorlagen virtueller Maschinen und vApps. Mit Rechten für Inhaltsbibliotheken wird gesteuert, wer verschiedene Aspekte von Inhaltsbibliotheken anzeigen oder verwalten darf.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Hinweis Die Vererbung von Berechtigungen für Inhaltsbibliotheken geschieht im Kontext einer einzelnen vCenter Server-Instanz. Inhaltsbibliotheken sind jedoch aus Sicht der Bestandsliste keine direkt untergeordneten Elemente eines vCenter Server-Systems. Das direkt übergeordnete Element für Inhaltsbibliotheken ist das globale Rootobjekt. Wenn Sie also eine Berechtigung auf vCenter Server-Ebene festlegen und an die untergeordneten Objekte weitergeben, gilt die Berechtigung für Datencenter, Ordner, Cluster, Hosts, virtuelle Maschinen usw. Diese Berechtigung gilt jedoch nicht für die Inhaltsbibliotheken, die in dieser vCenter Server-Instanz angezeigt werden und die Sie verwenden. Um eine Berechtigung für eine Inhaltsbibliothek in zuzuweisen, muss ein Administrator dem Benutzer die Berechtigung als globale Berechtigung erteilen. Globale Berechtigungen unterstützen das lösungsübergreifende Zuweisen von Berechtigungen von einem globalen Stammobjekt aus.

Tabelle 16-7. Rechte für Inhaltsbibliotheken

Rechtename	Beschreibung	Erforderlich bei
Inhaltsbibliothek.Bibliothekselement hinzufügen	Ermöglicht das Hinzufügen von Elementen in einer Bibliothek.	Bibliothek
Inhaltsbibliothek.Stammzertifikat zum Vertrauensspeicher hinzufügen	Ermöglicht das Hinzufügen von Stammzertifikaten zum Speicher für vertrauenswürdige Stammzertifikate.	vCenter Server
Inhaltsbibliothek.Vorlage einchecken	Ermöglicht das Einchecken von Vorlagen.	Bibliothek
Inhaltsbibliothek.Vorlage auschecken	Ermöglicht das Auschecken von Vorlagen.	Bibliothek
Inhaltsbibliothek.Abonnement für veröffentlichte Bibliothek erstellen	Ermöglicht das Erstellen eines Bibliotheksabonnements.	Bibliothek
Inhaltsbibliothek.Lokale Bibliothek erstellen	Ermöglicht die Erstellung lokaler Bibliotheken auf dem festgelegten vCenter Server-System.	vCenter Server
Inhaltsbibliothek.Harbor-Registrierung erstellen oder löschen	Ermöglicht das Erstellen oder Löschen des VMware Tanzu Harbor-Registrierungsdiensts.	vCenter Server für die Erstellung. Registrierung für Löschen.
Inhaltsbibliothek.Abonnierte Bibliothek erstellen	Ermöglicht die Erstellung abonnierter Bibliotheken.	vCenter Server
Inhaltsbibliothek.Harbor-Registrierungsprojekt erstellen, löschen oder bereinigen	Ermöglicht das Erstellen, Löschen oder Bereinigen von VMware Tanzu Harbor-Registrierungsprojekten.	Registrierung

Tabelle 16-7. Rechte für Inhaltsbibliotheken (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Inhaltsbibliothek.Bibliothekselement löschen	Ermöglicht das Löschen von Bibliothekselementen.	Bibliothek. Legen Sie diese Berechtigung zum Weitergeben an alle Bibliothekselemente fest.
Inhaltsbibliothek.Lokale Bibliothek löschen	Ermöglicht das Löschen einer lokalen Bibliothek.	Bibliothek
Inhaltsbibliothek.Stammzertifikat aus Vertrauensspeicher löschen	Ermöglicht das Löschen von Stammzertifikaten aus dem Speicher für vertrauenswürdige Stammzertifikate.	vCenter Server
Inhaltsbibliothek.Abonnierte Bibliothek löschen	Ermöglicht das Löschen einer abonnierten Bibliothek.	Bibliothek
Inhaltsbibliothek.Abonnement einer veröffentlichten Bibliothek löschen	Ermöglicht das Löschen eines Abonnements in einer Bibliothek.	Bibliothek
Inhaltsbibliothek.Dateien herunterladen	Ermöglicht das Herunterladen von Dateien aus der Inhaltsbibliothek.	Bibliothek
Inhaltsbibliothek.Bibliothekselement entfernen	Ermöglicht das Entfernen von Elementen. Der Inhalt einer abonnierten Bibliothek kann zwischengespeichert oder nicht zwischengespeichert werden. Wenn der Inhalt zwischengespeichert wird, können Sie ein Bibliothekselement durch Entfernen freigeben, wenn Sie über dieses Recht verfügen.	Bibliothek. Legen Sie diese Berechtigung zum Weitergeben an alle Bibliothekselemente fest.
Inhaltsbibliothek.Abonnierte Bibliothek entfernen	Ermöglicht das Entfernen einer abonnierten Bibliothek. Der Inhalt einer abonnierten Bibliothek kann zwischengespeichert oder nicht zwischengespeichert werden. Wenn der Inhalt zwischengespeichert wird, können Sie eine Bibliothek durch Entfernen freigeben, wenn Sie über dieses Recht verfügen.	Bibliothek
Inhaltsbibliothek.Speicher importieren	Ermöglicht einem Benutzer den Import eines Bibliothekselements, wenn die Quelldatei-URL mit `ds://` oder `file://` beginnt. Dieses Recht ist für den Administrator der Inhaltsbibliothek standardmäßig deaktiviert. Da ein Import aus einer Speicher-URL den Import von Inhalten impliziert, aktivieren Sie dieses Recht nur im Bedarfsfall und wenn keine Sicherheitsbedenken für den Benutzer bestehen, der den Import ausführt.	Bibliothek
Inhaltsbibliothek.Harbor-Registrierungsressourcen auf der angegebenen Computing-Ressource verwalten	Ermöglicht die Verwaltung von VMware Tanzu Harbor-Registrierungsressourcen.	Computing-Cluster

Tabelle 16-7. Rechte für Inhaltsbibliotheken (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Inhaltsbibliothek.Abonnementinformationen prüfen	Mit diesem Recht können Lösungsbenutzer und APIs die Abonnementinformationen einer Remote-Bibliothek einschließlich URL, SSL-Zertifikat und Kennwort untersuchen. Die resultierende Struktur beschreibt, ob die Abonnementkonfiguration erfolgreich ist oder ob Probleme wie beispielsweise SSL-Fehler vorliegen.	Bibliothek
Inhaltsbibliothek.Bibliothekselement für seine Abonnenten veröffentlichen	Ermöglicht die Veröffentlichung von Bibliothekselementen an Abonnenten.	Bibliothek. Legen Sie diese Berechtigung zum Weitergeben an alle Bibliothekselemente fest.
Inhaltsbibliothek.Bibliothek für ihre Abonnenten veröffentlichen	Ermöglicht die Veröffentlichung von Bibliotheken an Abonnenten.	Bibliothek
Inhaltsbibliothek.Speicherinfos lesen	Ermöglicht das Lesen des Inhaltsbibliotheksspeichers.	Bibliothek
Inhaltsbibliothek.Bibliothekselement synchronisieren	Ermöglicht die Synchronisation von Bibliothekselementen.	Bibliothek. Legen Sie diese Berechtigung zum Weitergeben an alle Bibliothekselemente fest.
Inhaltsbibliothek.Abonnierte Bibliothek synchronisieren	Ermöglicht die Synchronisation von abonnierten Bibliotheken.	Bibliothek
Inhaltsbibliothek.Typenintrospektion	Ermöglicht einem Lösungsbenutzer oder einer API, den Typ der Unterstützungs-Plug-Ins für den Content Library Service zu untersuchen.	Bibliothek
Inhaltsbibliothek.Konfigurationseinstellungen aktualisieren	Ermöglicht die Aktualisierung der Konfigurationseinstellungen. Diesem Recht sind keine Benutzerschnittstellenelemente auf dem vSphere Client zugeordnet.	Bibliothek
Inhaltsbibliothek.Dateien aktualisieren	Ermöglicht Ihnen das Hochladen von Inhalt in die Inhaltsbibliothek. Ermöglicht Ihnen außerdem, Dateien aus einem Bibliothekselement zu entfernen.	Bibliothek
Inhaltsbibliothek.Bibliothek aktualisieren	Ermöglicht Updates für die Inhaltsbibliothek.	Bibliothek
Inhaltsbibliothek.Bibliothekselement aktualisieren	Ermöglicht Updates für Bibliothekselemente.	Bibliothek. Legen Sie diese Berechtigung zum Weitergeben an alle Bibliothekselemente fest.
Inhaltsbibliothek.Lokale Bibliothek aktualisieren	Ermöglicht Updates lokaler Bibliotheken.	Bibliothek

Tabelle 16-7. Rechte für Inhaltsbibliotheken (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Inhaltsbibliothek.Abonnierte Bibliothek aktualisieren	Ermöglicht die Aktualisierung der Eigenschaften einer abonnierten Bibliothek.	Bibliothek
Inhaltsbibliothek.Abonnement einer veröffentlichten Bibliothek aktualisieren	Ermöglicht Aktualisierungen der Abonnementparameter. Benutzer können Parameter wie die vCenter Server-Instanzspezifikation der abonnierten Bibliothek und die Platzierung der zugehörigen VM-Vorlagenelemente aktualisieren.	Bibliothek
Inhaltsbibliothek.Konfigurationseinstellungen anzeigen	Ermöglicht das Anzeigen der Konfigurationseinstellungen. Diesem Recht sind keine Benutzerschnittstellenelemente auf dem vSphere Client zugeordnet.	Bibliothek

Rechte für Verschlüsselungsvorgänge

Mit Rechten für Verschlüsselungsvorgänge wird gesteuert, wer welchen Verschlüsselungsvorgangstyp für welchen Objekttyp durchführen kann.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-8. Rechte für Verschlüsselungsvorgänge

Rechtename	Beschreibung	Erforderlich bei
Kryptografievorgänge.Direktzugriff	Erlaubt Benutzern den Zugriff auf verschlüsselte Ressourcen. Benutzer können virtuelle Maschinen exportieren, mit NFC auf virtuelle Maschinen zugreifen und eine Konsolensitzung auf einer verschlüsselten virtuellen Maschine öffnen.	Virtuelle Maschine, Host oder Datenspeicher
Verschlüsselungsvorgänge.Festplatte hinzufügen	Erlaubt Benutzern das Hinzufügen einer Festplatte zu einer verschlüsselten virtuellen Maschine.	Virtuelle Maschine
Verschlüsselungsvorgänge.Klonen	Erlaubt Benutzern das Klonen einer verschlüsselten virtuellen Maschine.	Virtuelle Maschine
Verschlüsselungsvorgänge.Entschlüsseln	Erlaubt Benutzern das Entschlüsseln einer virtuellen Maschine oder Festplatte.	Virtuelle Maschine
Verschlüsselungsvorgänge.Verschlüsseln	Erlaubt Benutzern das Verschlüsseln einer virtuellen Maschine oder VM-Festplatte.	Virtuelle Maschine

Tabelle 16-8. Rechte für Verschlüsselungsvorgänge (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Verschlüsselungsvorgänge.Neue verschlüsseln	Erlaubt Benutzern das Verschlüsseln einer virtuellen Maschine während der Erstellung einer virtuellen Maschine bzw. einer Festplatte während der Festplattenerstellung.	Ordner der virtuellen Maschine
Verschlüsselungsvorgänge.Verschlüsselungsrichtlinien verwalten	Erlaubt Benutzern die Verwaltung von VM-Speicherrichtlinien mithilfe von Verschlüsselungs-E/A-Filtern. Standardmäßig nutzen virtuelle Maschinen, die die Speicherrichtlinie Verschlüsselung verwenden, keine anderen Speicherrichtlinien.	vCenter Server-Root-Ordner
Verschlüsselungsvorgänge.KMS verwalten	Erlaubt Benutzern die Verwaltung des Schlüsselmanagementservers (Key Management Server) für das vCenter Server-System. Zu den Verwaltungsaufgaben zählen das Hinzufügen und Entfernen von KMS-Instanzen sowie das Einrichten einer Vertrauensstellung für den KMS.	vCenter Server-System
Verschlüsselungsvorgänge.Schlüssel verwalten	Erlaubt Benutzern die Ausführung von Schlüsselverwaltungsvorgängen. Diese Vorgänge werden über den vSphere Client nicht unterstützt, können jedoch mit `crypto-util` oder der API ausgeführt werden.	vCenter Server-Root-Ordner
Verschlüsselungsvorgänge.Migrieren	Erlaubt Benutzern die Migration einer verschlüsselten virtuellen Maschine auf einen anderen ESXi-Host. Unterstützt die Migration mit bzw. ohne vMotion und Storage vMotion. Die Migration zu einer anderen vCenter Server-Instanz wird unterstützt.	Virtuelle Maschine
Verschlüsselungsvorgänge.Erneut verschlüsseln	Erlaubt Benutzern die erneute Verschlüsselung von virtuellen Maschinen oder Festplatten mit einem anderen Schlüssel. Dieses Recht ist für detaillierte und oberflächliche erneute Verschlüsselungsvorgänge erforderlich.	Virtuelle Maschine

Tabelle 16-8. Rechte für Verschlüsselungsvorgänge (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Verschlüsselungsvorgänge.VM registrieren	Erlaubt Benutzern die Registrierung einer verschlüsselten virtuellen Maschine bei einem anderen ESXi-Host.	Ordner der virtuellen Maschine
Verschlüsselungsvorgänge.Host registrieren	Erlaubt Benutzern die Aktivierung der Verschlüsselung auf einem Host. Die Verschlüsselung auf einem Host kann explizit oder bei der Erstellung der virtuellen Maschine aktiviert werden.	Hostordner für eigenständige Hosts, Cluster für Hosts im Cluster
Verschlüsselungsvorgänge.Informationen zum KMS lesen	Ermöglicht Benutzern die Auflistung von vSphere Native Key Providern auf dem vCenter Server und auf Hosts. Ermöglicht Benutzers außerdem, Informationen zum vSphere Native Key Provider abzurufen.	vCenter Server oder Host

dvPort-Gruppenrechte

Rechte für verteilte virtuelle Portgruppen steuern die Fähigkeit, verteilte virtuelle Portgruppen zu erstellen, zu löschen und zu ändern.

In der Tabelle sind die Rechte beschrieben, die zum Erstellen und Konfigurieren von verteilten virtuellen Portgruppen erforderlich sind.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-9. Rechte für verteilte virtuelle Portgruppen

Rechtename	Beschreibung	Erforderlich bei
dvPort-Gruppe.Erstellen	Ermöglicht das Erstellen einer verteilten virtuellen Portgruppe.	Virtuelle Portgruppen
dvPort-Gruppe.Löschen	Ermöglicht das Löschen einer verteilten virtuellen Portgruppe. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Virtuelle Portgruppen
dvPort-Gruppe.Ändern	Ermöglicht das Ändern der Konfiguration einer verteilten virtuellen Portgruppe.	Virtuelle Portgruppen

Tabelle 16-9. Rechte für verteilte virtuelle Portgruppen (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
dvPort-Gruppe.Richtlinienvorgang	Ermöglicht das Festlegen der Richtlinien einer verteilten virtuellen Portgruppe.	Virtuelle Portgruppen
dvPort-Gruppe.Geltungsbereichsvorgang	Ermöglicht das Festlegen des Geltungsbereichs einer verteilten virtuellen Portgruppe.	Virtuelle Portgruppen

Rechte für Distributed Switches

Rechte für Distributed Switches steuern die Fähigkeit, Aufgaben im Zusammenhang mit der Verwaltung von Distributed Switch-Instanzen durchzuführen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-10. Rechte für vSphere Distributed Switch

Rechtename	Beschreibung	Erforderlich bei
Distributed Switch.Erstellen	Ermöglicht das Erstellen eines Distributed Switch.	Datencenter, Netzwerkordner
Distributed Switch.Löschen	Ermöglicht das Entfernen eines Distributed Switch. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Distributed Switches
Distributed Switch.Hostvorgang	Ermöglicht das Ändern der Hostmitglieder eines Distributed Switch.	Distributed Switches
Distributed Switch.Ändern	Ermöglicht das Ändern der Konfiguration eines Distributed Switch.	Distributed Switches
Distributed Switch.Verschieben	Ermöglicht das Verschieben eines vSphere Distributed Switch in einen anderen Ordner.	Distributed Switches
Distributed Switch.Network I/O Control-Vorgang	Ermöglicht das Ändern der Ressourceneinstellungen für einen vSphere Distributed Switch.	Distributed Switches
Distributed switch.Richtlinienvorgang	Ermöglicht das Ändern der Richtlinie eines vSphere Distributed Switch.	Distributed Switches
Distributed Switch.Portkonfigurationsvorgang	Ermöglicht das Ändern der Konfiguration eines Ports in einem vSphere Distributed Switch.	Distributed Switches

Tabelle 16-10. Rechte für vSphere Distributed Switch (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Distributed Switch.Porteinstellungsvorgang	Ermöglicht das Ändern der Einstellung eines Ports in einem vSphere Distributed Switch.	Distributed Switches
Distributed Switch.VSPAN-Vorgang	Ermöglicht das Ändern der VSPAN-Konfiguration eines vSphere Distributed Switch.	Distributed Switches

Rechte für Datencenter

Rechte für Datencenter steuern die Fähigkeit, Datencenter in der Bestandsliste des vSphere Client zu erstellen und zu bearbeiten.

Alle Rechte für Datencenter werden nur in vCenter Server verwendet. Das Recht **Datencenter erstellen** wird in Datencenterordnern oder im Stammobjekt definiert. Alle anderen Rechte für Datencenter werden mit Datencentern, Datencenterordnern oder dem Stammobjekt kombiniert.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-11. Rechte für Datencenter

Rechtename	Beschreibung	Erforderlich bei
Datencenter.Datencenter erstellen	Ermöglicht das Erstellen eines neuen Datencenters.	Datencenterordner oder Stammobjekt
Datencenter.Datencenter verschieben	Ermöglicht das Verschieben eines Datencenters. Das Recht muss für Quelle und Ziel vorhanden sein.	Datencenter, Quelle und Ziel
Datencenter.Konfiguration des Netzwerkprotokollprofils	Ermöglicht die Konfiguration des Netzwerkprofils für ein Datencenter.	Datencenter
Datencenter.IP-Pool-Zuteilung abfragen	Ermöglicht die Konfiguration eines Pools von IP-Adressen.	Datencenter
Datencenter.Datencenter neu konfigurieren	Ermöglicht die Neukonfiguration eines Datencenters.	Datencenter
Datencenter.IP-Zuteilung freigeben	Ermöglicht die Freigabe der zugewiesenen IP-Zuteilung für ein Datencenter.	Datencenter
Datencenter.Datencenter entfernen	Ermöglicht das Entfernen eines Datencenters. Dieser Vorgang kann nur ausführt werden, wenn diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Datencenter und übergeordnetes Objekt
Datencenter.Datencenter umbenennen	Ermöglicht das Ändern des Namens eines Datencenters.	Datencenter

Berechtigungen für Datenspeicher

Rechte für Datenspeicher steuern die Fähigkeit, Datenspeicher zu durchsuchen, zu verwalten und Speicherplatz zuzuteilen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-12. Berechtigungen für Datenspeicher

Rechtename	Beschreibung	Erforderlich bei
Datenspeicher.Speicher zuteilen	Ermöglicht die Zuteilung von Speicherplatz auf einem Datenspeicher für eine virtuelle Maschine, einen Snapshot, einen Klon oder eine virtuelle Festplatte.	Datenspeicher
Datenspeicher.Datenspeicher durchsuchen	Ermöglicht die Suche nach Dateien in einem Datenspeicher.	Datenspeicher
Datenspeicher.Datenspeicher konfigurieren	Ermöglicht die Konfiguration eines Datenspeichers.	Datenspeicher
Datenspeicher.Dateivorgänge auf niedriger Ebene	Ermöglicht die Durchführung von Lese-, Schreib-, Lösch- und Umbenennungsvorgängen im Datenspeicherbrowser.	Datenspeicher
Datenspeicher.Datenspeicher verschieben	Ermöglicht das Verschieben eines Datenspeichers zwischen Ordnern. Das Recht muss für Quelle und Ziel vorhanden sein.	Datenspeicher, Quelle und Ziel
Datenspeicher.Datenspeicher entfernen	Ermöglicht das Entfernen eines Datenspeichers. Dieses Recht ist veraltet. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Datenspeicher
Datenspeicher.Datei entfernen	Ermöglicht das Löschen von Dateien im Datenspeicher. Dieses Recht ist veraltet. Weisen Sie das Recht **Dateivorgänge auf niedriger Ebene** zu.	Datenspeicher
Datenspeicher.Datenspeicher umbenennen	Ermöglicht das Umbenennen eines Datenspeichers.	Datenspeicher
Datenspeicher.Dateien der virtuellen Maschine aktualisieren	Ermöglicht das Aktualisieren der Dateipfade der VM-Dateien auf einem Datenspeicher, nachdem der Datenspeicher neu signiert wurde.	Datenspeicher
Datenspeicher.Metadaten der virtuellen Maschine aktualisieren	Ermöglicht das Aktualisieren von Metadaten der virtuellen Maschine für einen Datenspeicher.	Datenspeicher

Rechte für Datenspeichercluster

Datenspeicher-Clusterrechte steuern die Konfiguration des Datenspeicher-Clusters für Speicher-DRS.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-13. Rechte für Datenspeichercluster

Rechtename	Beschreibung	Erforderlich bei
Datenspeicher-Cluster.Datenspeicher-Cluster konfigurieren	Ermöglicht das Erstellen von und die Konfiguration von Einstellungen für Datenspeicher-Cluster für Speicher-DRS.	Datenspeicher-Cluster

ESX Agent Manager-Rechte

Die ESX Agent Manager-Rechte steuern die Vorgänge, die im Zusammenhang mit ESX Agent Manager und den virtuelle Maschinen des Agenten stehen. Beim ESX Agent Manager handelt es sich um einen Dienst, mit dem Sie Management-VMs installieren können, die mit einem Host verknüpft sind und nicht von VMware DRS oder anderen Diensten betroffen sind, mit denen virtuelle Maschinen migriert werden.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-14. ESX Agent Manager

Rechtename	Beschreibung	Erforderlich bei
ESX Agent Manager.Konfigurieren	Ermöglicht die Bereitstellung einer virtuellen Maschine eines Agenten auf einem Host oder Cluster.	virtuelle Maschinen
ESX Agent Manager.Ändern	Ermöglicht Änderungen an einer virtuellen Maschine eines Agenten, wie z. B. das Ausschalten oder Löschen der virtuellen Maschine.	virtuelle Maschinen
ESX Agent View.Anzeigen	Ermöglicht die Anzeige einer virtuellen Maschine eines Agenten.	virtuelle Maschinen

Rechte für Erweiterungen

Berechtigungen für Erweiterungen steuern die Fähigkeit, Erweiterungen zu installieren und zu verwalten.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-15. Rechte für Erweiterungen

Rechtename	Beschreibung	Erforderlich bei
Erweiterung.Erweiterung registrieren	Ermöglicht die Registrierung einer Erweiterung (Plug-In).	Root-vCenter Server
Erweiterung.Registrierung der Erweiterung aufheben	Ermöglicht die Aufhebung der Registrierung einer Erweiterung (Plug-In).	Root-vCenter Server
Erweiterung.Erweiterung aktualisieren	Ermöglicht die Aktualisierung einer Erweiterung (Plug-In).	Root-vCenter Server

Rechte für Bereitstellungsfunktion externer Statistiken

Rechte für die Bereitstellungsfunktion externer Statistiken steuern die Möglichkeit, vCenter Server über Statistiken des proaktiven Distributed Resource Scheduler (DRS) zu benachrichtigen.

Diese Rechte gelten für eine ausschließlich VMware-interne API.

Rechte für Ordner

Berechtigungen für Ordner steuern die Fähigkeit, Ordner zu erstellen und zu verwalten.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-16. Rechte für Ordner

Rechtename	Beschreibung	Erforderlich bei
Ordner.Ordner erstellen	Ermöglicht das Erstellen eines neuen Ordners.	Ordner
Ordner.Ordner löschen	Ermöglicht das Löschen eines Ordners. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Ordner
Ordner.Ordner verschieben	Ermöglicht das Verschieben eines Ordners. Das Recht muss für Quelle und Ziel vorhanden sein.	Ordner
Ordner.Ordner umbenennen	Ermöglicht das Ändern des Namens eines Ordners.	Ordner

Globale Rechte

Globale Rechte steuern globale Aufgaben im Zusammenhang mit Aufgaben, Skripts und Erweiterungen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-17. Globale Rechte

Rechtename	Beschreibung	Erforderlich bei
Global.Als vCenter Server agieren	Ermöglicht die Vorbereitung oder Initiierung eines vMotion-Sendevorgangs bzw. eines vMotion-Empfangsvorgangs.	Root-vCenter Server
Global.Aufgabe abbrechen	Ermöglicht den Abbruch einer ausgeführten oder in der Warteschlange abgelegten Aufgabe.	Bestandslistenobjekt mit Bezug zur Aufgabe
Global.Kapazitätsplanung	Ermöglicht die Aktivierung der Verwendung der Kapazitätsplanung für eine geplante Konsolidierung von physischen Maschinen in virtuelle Maschinen.	Root-vCenter Server
Global.Diagnose	Ermöglicht den Abruf einer Liste von Diagnosedateien, Protokollheader, Binärdateien oder Diagnosepaketen. Um Sicherheitsverstöße zu verhindern, beschränken Sie diese Berechtigungen für die vCenter Server-Administratorrolle.	Root-vCenter Server
Global.Methoden deaktivieren	Ermöglicht Servern für vCenter Server-Erweiterungen das Deaktivieren bestimmter Vorgänge für Objekte, die von vCenter Server verwaltet werden.	Root-vCenter Server
Global.Methoden aktivieren	Ermöglicht Servern für vCenter Server-Erweiterungen das Aktivieren bestimmter Vorgänge für Objekte, die von vCenter Server verwaltet werden.	Root-vCenter Server
Global.Global-Tag	Ermöglicht das Hinzufügen oder Entfernen von Global-Tags.	Root-Host oder vCenter Server
Global.Zustand	Ermöglicht das Anzeigen des Status der vCenter Server-Komponenten.	Root-vCenter Server
Global.Lizenzen	Ermöglicht das Anzeigen installierter Lizenzen und das Hinzufügen bzw. Entfernen von Lizenzen.	Root-Host oder vCenter Server
Global.Ereignis protokollieren	Ermöglicht das Protokollieren eines benutzerdefinierten Ereignisses für ein bestimmtes verwaltetes Element.	Beliebiges Objekt
Global.Benutzerdefinierte Attribute verwalten	Ermöglicht das Hinzufügen, Entfernen oder Umbenennen von benutzerdefinierten Felddefinitionen.	Root-vCenter Server
Global.Proxy	Ermöglicht Zugriff auf eine interne Schnittstelle für das Hinzufügen oder Entfernen von Endpunkten zu oder vom Proxy.	Root-vCenter Server
Global.Skriptaktion	Ermöglicht das Planen einer Skriptaktion zusammen mit einem Alarm.	Beliebiges Objekt

Tabelle 16-17. Globale Rechte (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Global.Dienst-Manager	Ermöglicht die Verwendung des `resxtop` Befehls in ESXCLI.	Root-Host oder vCenter Server
Global.Benutzerdefinierte Attribute festlegen	Ermöglicht das Anzeigen, Erstellen oder Entfernen benutzerdefinierter Attribute für ein verwaltetes Objekt.	Beliebiges Objekt
Global.Einstellungen	Ermöglicht das Lesen und Ändern von vCenter Server-Konfigurationseinstellungen zur Laufzeit.	Root-vCenter Server
Global.System-Tag	Ermöglicht das Hinzufügen oder Entfernen von System-Tags.	Root-vCenter Server

Rechte für Bereitstellungsfunktion für Aktualisierungen des Systemzustands

Rechte für die Bereitstellungsfunktion für Aktualisierungen des Systemzustands steuern die Möglichkeit für Hardwareanbieter, vCenter Server über Proactive HA-Ereignisse zu benachrichtigen.

Diese Rechte gelten für eine ausschließlich VMware-interne API.

Host-CIM-Rechte

Host-CIM-Rechte steuern die Verwendung von CIM für die Statusüberwachung des Hosts.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-18. Host-CIM-Rechte

Rechtename	Beschreibung	Erforderlich bei
Host.CIM.CIM-Interaktion	Ermöglicht es einem Client, ein Ticket für CIM-Dienste abzurufen.	Hosts

Rechte für die Hostkonfiguration

Rechte für die Hostkonfiguration steuern die Fähigkeit, Hosts zu konfigurieren.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-19. Rechte für die Hostkonfiguration

Rechtename	Beschreibung	Erforderlich bei
Host.Konfiguration.Erweiterte Einstellungen	Ermöglicht das Festlegen erweiterter Optionen für die Hostkonfiguration.	Hosts
Host.Konfiguration.Authentifizierungsspeicher	Ermöglicht das Konfigurieren von Active Directory-Authentifizierungsspeichern.	Hosts
Host.Konfiguration.PciPassthru-Einstellungen ändern	Ermöglicht Änderungen an den PciPassthru-Einstellungen eines Hosts.	Hosts
Host.Konfiguration.SNMP-Einstellungen ändern	Ermöglicht Änderungen an den SNMP-Einstellungen eines Hosts.	Hosts
Host.Konfiguration.Datums- und Uhrzeiteinstellungen ändern	Ermöglicht das Ändern der Datums- und Uhrzeiteinstellungen auf dem Host.	Hosts
Host.Konfiguration.Einstellungen ändern	Ermöglicht das Einstellen des Sperrmodus auf ESXi-Hosts.	Hosts
Host.Konfiguration.Verbindung	Ermöglicht Änderungen am Verbindungsstatus eines Hosts („Verbunden“ oder „Nicht verbunden“).	Hosts
Host.Konfiguration.Firmware	Ermöglicht Updates der Firmware des ESXi-Hosts.	Hosts
Host.Konfiguration.Hyper-Threading	Ermöglicht das Aktivieren und Deaktivieren von Hyper-Threading in einem Host-CPU-Scheduler.	Hosts
Host.Konfiguration.Image-Konfiguration	Ermöglicht Änderungen am Image, das einem Host zugeordnet ist.	
Host.Konfiguration.Wartung	Ermöglicht das Aktivieren bzw. Deaktivieren des Wartungsmodus für den Host sowie das Herunterfahren und Neustarten des Hosts.	Hosts
Host.Konfiguration.Arbeitsspeicherkonfiguration	Ermöglicht Änderungen an der Hostkonfiguration.	Hosts
Host.Konfiguration.Netzwerkkonfiguration	Ermöglicht das Konfigurieren von Netzwerk, Firewall und vMotion-Netzwerk.	Hosts
Host.Konfiguration.Betrieb	Ermöglicht das Konfigurieren der Energieverwaltungseinstellungen des Hosts.	Hosts
Host.Konfiguration.Patch abfragen	Ermöglicht das Abfragen installierbarer Patches und das Installieren von Patches auf dem Host.	Hosts
Host.Konfiguration.Sicherheitsprofil und Firewall	Ermöglicht das Konfigurieren von Internetdiensten wie SSH, Telnet, SNMP und Hostfirewall.	Hosts
Host.Konfiguration.Konfiguration für Speicherpartition	Ermöglicht das Verwalten der VMFS-Datenspeicher und Diagnosepartitionen. Benutzer mit diesem Recht können nach neuen Speichergeräten suchen und iSCSI verwalten.	Hosts
Host.Konfiguration.System-Management	Ermöglicht Erweiterungen eine Änderung des Dateisystems auf dem Host.	Hosts

Tabelle 16-19. Rechte für die Hostkonfiguration (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Host.Konfiguration.Systemressourcen	Ermöglicht das Aktualisieren der Konfiguration der Systemressourcenhierarchie.	Hosts
Host.Konfiguration.Autostart-Konfiguration für virtuelle Maschine	Ermöglicht Änderungen an der Reihenfolge des automatischen Startens und des automatischen Beendens von virtuellen Maschinen auf einem einzelnen Host.	Hosts

Hostbestandsliste

Rechte für die Hostbestandsliste steuern das Hinzufügen von Hosts zur Bestandsliste, das Hinzufügen von Hosts zu Clustern und das Verschieben von Hosts in der Bestandsliste.

In der Tabelle sind die Rechte beschrieben, die zum Hinzufügen und Verschieben von Hosts und Clustern in der Bestandsliste erforderlich sind.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-20. Rechte für die Hostbestandsliste

Rechtename	Beschreibung	Erforderlich bei
Host.Bestandsliste.Host zu Cluster hinzufügen	Ermöglicht das Hinzufügen eines Hosts zu einem vorhandenen Cluster.	Cluster
Host.Bestandsliste.Eigenständigen Host hinzufügen	Ermöglicht das Hinzufügen eines eigenständigen Hosts.	Hostordner
Host.Bestandsliste.Cluster erstellen	Ermöglicht das Erstellen eines neuen Clusters.	Hostordner
Host.Bestandsliste.Cluster ändern	Ermöglicht das Ändern der Eigenschaften eines Clusters.	Cluster
Host.Bestandsliste.Cluster oder eigenständigen Host verschieben	Ermöglicht das Verschieben eines Clusters oder eigenständigen Hosts zwischen Ordnern. Das Recht muss für Quelle und Ziel vorhanden sein.	Cluster
Host.Bestandsliste.Host verschieben	Ermöglicht das Verschieben einer Gruppe vorhandener Hosts in einen oder aus einem Cluster. Das Recht muss für Quelle und Ziel vorhanden sein.	Cluster
Host.Bestandsliste.Cluster entfernen	Ermöglicht das Löschen eines Clusters oder eines eigenständigen Hosts. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Cluster, Server

Tabelle 16-20. Rechte für die Hostbestandsliste (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Host.Bestandsliste.Host entfernen	Ermöglicht das Entfernen eines Hosts. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Hosts und übergeordnetes Objekt
Host.Bestandsliste.Cluster umbenennen	Ermöglicht das Umbenennen eines Clusters.	Cluster

Rechte für lokale Hostoperationen

Rechte für lokale Hostoperationen steuern Aktionen, die bei einer Direktverbindung zwischen dem VMware Host Client und einem Host durchgeführt werden.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-21. Rechte für lokale Hostoperationen

Rechtename	Beschreibung	Erforderlich bei
Host.Lokale Vorgänge.Host zu vCenter hinzufügen	Ermöglicht die Installation und das Entfernen von vCenter-Agenten (z. B. vpxa und aam) auf einem Host.	Root-Host
Host.Lokale Vorgänge.Virtuelle Maschine erstellen	Ermöglicht es, eine neue virtuelle Maschine auf einer Festplatte von Grund auf zu erstellen, ohne diese auf dem Host zu registrieren.	Root-Host
Host.Lokale Vorgänge.Virtuelle Maschine löschen	Ermöglicht das Löschen einer virtuellen Maschine auf einer Festplatte. Wird für registrierte und nicht registrierte virtuelle Maschinen unterstützt.	Root-Host
Host.Lokale Vorgänge.Benutzergruppen verwalten	Ermöglicht die Verwaltung lokaler Konten auf einem Host.	Root-Host
Host.Lokale Vorgänge.Virtuelle Maschine neu konfigurieren	Ermöglicht die erneute Konfiguration einer virtuellen Maschine.	Root-Host

vSphere Replication-Rechte von Hosts

vSphere Replication-Rechte von Hosts steuern die Verwendung der VM-Replizierung durch VMware vCenter Site Recovery Manager™ für einen Host.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-22. vSphere Replication-Rechte von Hosts

Rechtename	Beschreibung	Erforderlich bei
Host.vSphere Replication.Replizierung verwalten	Ermöglicht die Verwaltung der Replizierung virtueller Maschinen auf diesem Host.	Hosts

Hostprofil-Berechtigungen

Hostprofil-Rechte steuern Vorgänge im Zusammenhang mit dem Erstellen und Ändern von Hostprofilen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-23. Hostprofil-Berechtigungen

Rechtename	Beschreibung	Erforderlich bei
Hostprofil.Bereinigen	Ermöglicht das Löschen von Informationen zu Profilen.	Root-vCenter Server
Hostprofil.Erstellen	Ermöglicht das Erstellen eines Hostprofils.	Root-vCenter Server
Hostprofil.Löschen	Ermöglicht das Löschen eines Hostprofils.	Root-vCenter Server
Hostprofil.Bearbeiten	Ermöglicht das Bearbeiten eines Hostprofils.	Root-vCenter Server
Hostprofil.Exportieren	Ermöglicht das Exportieren eines Hostprofils.	Root-vCenter Server
Hostprofil.Anzeigen	Ermöglicht das Anzeigen eines Hostprofils.	Root-vCenter Server

vSphere mit Tanzu-Berechtigungen

Mit Berechtigungen für Namespaces wird gesteuert, wer VMware vSphere® mit VMware Tanzu™-Namespaces erstellen und verwalten kann.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-24. Berechtigungen für Namespaces

Rechtename	Beschreibung	Erforderlich bei
Namespaces.Lässt Vorgänge zur Außerbetriebnahme von Festplatten zu	Ermöglicht die Außerbetriebnahme von Datenspeichern.	Datenspeicher
Namespaces.Dateien der Arbeitslastkomponente sichern	Ermöglicht das Sichern der Inhalte des etcd-Clusters (wird nur in VMware Cloud on AWS verwendet).	Cluster
Namespaces.Clusterweite Konfiguration ändern	Ermöglicht das Ändern der clusterweiten Konfiguration sowie das Aktivieren und Deaktivieren von Cluster-Namespaces.	Cluster
Namespaces.Clusterweite Namespace-Self-Service-Konfiguration ändern	Ermöglicht das Ändern der Namespace-Self-Service-Konfiguration.	Cluster (zum Aktivieren und Deaktivieren) Vorlagen (zum Ändern der Konfiguration) vCenter Server (zum Erstellen einer Vorlage)
Namespaces.Namespace-Konfiguration ändern	Ermöglicht das Ändern der Optionen für die Namespace-Konfiguration, wie z. B. Ressourcenzuteilung und Benutzerberechtigungen.	Cluster
Namespaces.Clusterfunktionen umschalten	Ermöglicht die Änderung des Status von Clusterfunktionen (wird intern nur für VMware Cloud on AWS verwendet).	Cluster
Namespaces.Upgrade von Clustern auf neuere Versionen durchführen	Ermöglicht die Initiierung des Cluster-Upgrades.	Cluster

Netzwerkberechtigungen

Rechte für Netzwerk steuern Aufgaben im Zusammenhang mit der Netzwerkverwaltung.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-25. Netzwerkberechtigungen

Rechtename	Beschreibung	Erforderlich bei
Netzwerk.Netzwerk zuweisen	Ermöglicht das Zuweisen eines Netzwerks zu einer virtuellen Maschine.	Netzwerke, virtuelle Maschinen
Netzwerk.Konfigurieren	Ermöglicht das Konfigurieren eines Netzwerks.	Netzwerke, virtuelle Maschinen

Tabelle 16-25. Netzwerkberechtigungen (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Netzwerk.Netzwerk verschieben	Ermöglicht das Verschieben eines Netzwerks zwischen Ordnern. Das Recht muss für Quelle und Ziel vorhanden sein.	Netzwerke
Netzwerk.Entfernen	Ermöglicht das Entfernen eines Netzwerks. Dieses Recht ist veraltet. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Netzwerke

Leistungsrechte

Leistungsrechte steuern das Ändern von Einstellungen für Leistungsstatistiken.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-26. Leistungsrechte

Rechtename	Beschreibung	Erforderlich bei
Leistung.Intervalle ändern	Ermöglicht das Erstellen, Entfernen und Aktualisieren von Intervallen zum Sammeln von Leistungsdaten.	Root-vCenter Server

Rechte für Berechtigungen

Berechtigungsrechte steuern das Zuweisen von Rollen und Berechtigungen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-27. Rechte für Berechtigungen

Rechtename	Beschreibung	Erforderlich bei
Berechtigungen.Berechtigung ändern	Ermöglicht das Definieren einer oder mehrerer Berechtigungsregeln für eine Instanz oder das Aktualisieren von Regeln, wenn diese für einen bestimmten Benutzer oder eine bestimmte Gruppe der Instanz bereits vorhanden sind. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Beliebiges Objekt und übergeordnetes Objekt
Berechtigungen.Recht ändern	Ermöglicht das Ändern der Gruppe oder Beschreibung eines Rechts. Diesem Recht sind keine Benutzerschnittstellenelemente auf dem vSphere Client zugeordnet.	
Berechtigungen.Rolle ändern	Ermöglicht das Aktualisieren des Namens einer Rolle und der mit der Rolle verbundenen Rechte.	Beliebiges Objekt
Berechtigungen.Rollenberechtigungen neu zuweisen	Ermöglicht das Zuweisen aller Berechtigungen einer Rolle zu einer anderen Rolle.	Beliebiges Objekt

Profilgesteuerte Speicherrechte

Profilgesteuerte Speicherrechte steuern Vorgänge im Zusammenhang mit Speicherprofilen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-28. Profilgesteuerte Speicherrechte

Rechtename	Beschreibung	Erforderlich bei
Profilgesteuerter Speicher.Update des profilgesteuerten Speichers	Ermöglicht Änderungen an Speicherprofilen wie das Erstellen und Aktualisieren von Speicherfunktionen und Speicherprofilen für virtuelle Maschinen.	Root-vCenter Server
Profilgesteuerter Speicher.Ansicht des profilgesteuerten Speichers	Ermöglicht die Anzeige von definierten Storage Capabilities und Speicherprofilen.	Root-vCenter Server

Rechte für Ressourcen

Rechte für Ressourcen steuern die Erstellung und Verwaltung von Ressourcenpools sowie die Migration von virtuellen Maschinen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-29. Rechte für Ressourcen

Rechtename	Beschreibung	Erforderlich bei
Ressourcen.Empfehlung anwenden	Ermöglicht das Akzeptieren eines Vorschlags des Servers zum Ausführen einer Migration mit vMotion.	Cluster
Ressourcen.vApp dem Ressourcenpool zuweisen	Ermöglicht die Zuweisung einer vApp zu einem Ressourcenpool.	Ressourcenpools
Ressource.Virtuelle Maschine zu Ressourcenpool zuweisen	Ermöglicht die Zuweisung einer virtuellen Maschine zu einem Ressourcenpool.	Ressourcenpools
Ressourcen.Ressourcenpool erstellen	Ermöglicht die Erstellung von Ressourcenpools.	Ressourcenpools, Cluster
Ressourcen.Ausgeschaltete virtuelle Maschine migrieren	Ermöglicht die Migration einer ausgeschalteten virtuellen Maschine auf einen anderen Ressourcenpool oder Host.	virtuelle Maschinen
Ressourcen.Eingeschaltete virtuelle Maschine migrieren	Ermöglicht die Migration mithilfe von vMotion einer eingeschalteten virtuellen Maschine auf einen anderen Ressourcenpool oder Host.	
Ressourcen.Ressourcenpool ändern	Ermöglicht Änderungen an den Zuweisungen eines Ressourcenpools.	Ressourcenpools
Ressourcen.Ressourcenpool verschieben	Ermöglicht das Verschieben eines Ressourcenpools. Das Recht muss für Quelle und Ziel vorhanden sein.	Ressourcenpools
Ressourcen.vMotion abfragen	Ermöglicht die Abfrage der allgemeinen vMotion-Kompatibilität einer virtuellen Maschine mit einer Hostgruppe.	Root-vCenter Server
Ressourcen.Ressourcenpool entfernen	Ermöglicht das Löschen eines Ressourcenpools. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	Ressourcenpools
Ressourcen.Ressourcenpool umbenennen	Ermöglicht das Umbenennen eines Ressourcenpools.	Ressourcenpools

Rechte für geplante Aufgaben

Rechte für geplante Aufgaben steuern das Erstellen, Bearbeiten und Entfernen von geplanten Aufgaben.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-30. Rechte für geplante Aufgaben

Rechtename	Beschreibung	Erforderlich bei
Geplante Aufgabe.Aufgaben erstellen	Ermöglicht die Planung einer Aufgabe. Wird zusätzlich zu den Rechten zum Ausführen der geplanten Aktion zum Planungszeitpunkt benötigt.	Beliebiges Objekt
Geplante Aufgabe.Aufgabe ändern	Ermöglicht die Neukonfiguration der Eigenschaften der geplanten Aufgabe.	Beliebiges Objekt
Geplante Aufgabe.Aufgabe entfernen	Ermöglicht das Entfernen einer geplanten Aufgabe aus der Warteschlange.	Beliebiges Objekt
Geplante Aufgabe.Aufgabe ausführen	Ermöglicht die sofortige Ausführung der geplanten Aufgabe. Zum Erstellen und Ausführen einer geplanten Aufgabe ist außerdem die Berechtigung zum Durchführen der zugeordneten Aktion erforderlich.	Beliebiges Objekt

Sitzungsrechte

Sitzungsrechte steuern die Fähigkeit von Erweiterungen, Sitzungen auf dem vCenter Server-System zu öffnen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-31. Sitzungsrechte

Rechtename	Beschreibung	Erforderlich bei
Sitzungen.Benutzeridentität annehmen	Ermöglicht die Imitation eines anderen Benutzers. Diese Funktion wird von Erweiterungen verwendet.	Root-vCenter Server
Sitzungen.Meldung	Ermöglicht das Festlegen der globalen Anmeldenachricht.	Root-vCenter Server
Sitzungen.Sitzung überprüfen	Ermöglicht die Überprüfung der Sitzungsgültigkeit.	Root-vCenter Server
Sitzungen.Sitzungen anzeigen und beenden	Ermöglicht das Anzeigen von Sitzungen und das Erzwingen der Abmeldung der angemeldeten Benutzer.	Root-vCenter Server

Speicheransichtsberechtigungen

Speicheransichtsberechtigungen bestimmen die Rechte für Speicherüberwachungsdienst-APIs.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-32. Speicheransichtsberechtigungen

Rechtename	Beschreibung	Erforderlich bei
Speicheransichten.Dienst konfigurieren	Erlaubt berechtigten Benutzern die Verwendung aller Speicherüberwachungsdienst-APIs. Verwenden Sie **Speicheransichten.Anzeigen** für schreibgeschützte Rechte für Speicherüberwachungsdienst-APIs.	Root-vCenter Server
Speicheransichten.Anzeigen	Erlaubt berechtigten Benutzern die Verwendung schreibgeschützter Speicherüberwachungsdienst-APIs.	Root-vCenter Server

Rechte für Aufgaben

Rechte für Aufgaben steuern die Fähigkeit von Erweiterungen, Aufgaben für vCenter Server zu erstellen und zu aktualisieren.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-33. Rechte für Aufgaben

Rechtename	Beschreibung	Erforderlich bei
Aufgaben.Aufgabe erstellen	Erlaubt einer Erweiterung die Erstellung einer benutzerdefinierten Aufgabe. Diesem Recht sind keine Benutzerschnittstellenelemente auf dem vSphere Client zugeordnet.	Root-vCenter Server
Aufgaben.Aufgabe aktualisieren	Erlaubt einer Erweiterung die Aktualisierung einer benutzerdefinierten Aufgabe. Diesem Recht sind keine Benutzerschnittstellenelemente auf dem vSphere Client zugeordnet.	Root-vCenter Server

Transfer Service-Rechte

Transfer Service-Rechte werden intern von VMware verwendet. Diese Rechte sollten Sie nicht verwenden.

Rechte für VcTrusts/VcIdentity

Mit den Rechten für VcTrusts/VcIdentity wird der Zugriff auf verschiedene interne APIs und Funktionen im Zusammenhang mit der Vertrauensstellung zwischen vCenter Server-Systemen gesteuert.

Tabelle 16-34. Rechte für VcTrusts/VcIdentity

Rechtename	Beschreibung	Erforderlich bei
VcTrusts/VcIdentity.Erstellen/Aktualisieren/Löschen (Administratorrechte)	Ermöglicht den Vollzugriff auf Administratorebene auf verschiedene interne APIs und Funktionen im Zusammenhang mit der Vertrauensstellung zwischen vCenter Server-Systemen.	Nicht verfügbar
VcTrusts/VcIdentity.Erstellen/Aktualisieren/Löschen (unterhalb von Administratorrechten)	Ermöglicht verringerten Administratorzugriff auf verschiedene interne APIs und Funktionen im Zusammenhang mit der Vertrauensstellung zwischen vCenter Server-Systemen. Mit diesem Recht wird das Erstellen/Aktualisieren/Löschen von VcTrusts/VcIdentity so eingeschränkt, dass der Benutzer Nicht-Administratorrechte nicht eskalieren kann.	Nicht verfügbar

Rechte für „Administrator der vertrauenswürdigen Infrastruktur“

Die Rechte für „Administrator der vertrauenswürdigen Infrastruktur“ beziehen sich auf das Konfigurieren und Verwalten einer vSphere Trust Authority-Bereitstellung..

Diese Rechte bestimmen, wer Konfigurations- und Verwaltungsaufgaben für eine vSphere Trust Authority-Bereitstellung durchführen kann. Weitere Informationen zur Trust Authority-Rolle und zur Gruppe „TrustedAdmins“ finden Sie unter Voraussetzungen und notwendige Berechtigungen für vSphere Trust Authority.

Tabelle 16-35. Rechte für „Administrator der vertrauenswürdigen Infrastruktur“

Rechtename	Beschreibung	Erforderlich bei
Administrator der vertrauenswürdigen Infrastruktur.Vertrauensstellung des Schlüsselservers konfigurieren	Ermöglicht das Verwalten der Schlüsselanbieter des Schlüsselanbieterdiensts.	Root-vCenter Server
Administrator der vertrauenswürdigen Infrastruktur.TPM-Zertifikate des vertrauenswürdigen Autoritätshosts konfigurieren	Ermöglicht das Erstellen und Ändern der Einstellungen des Nachweisdiensts.	Root-vCenter Server

Tabelle 16-35. Rechte für „Administrator der vertrauenswürdigen Infrastruktur“ (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Administrator der vertrauenswürdigen Infrastruktur.Metadaten des vertrauenswürdigen Autoritätshosts konfigurieren	Ermöglicht das Bearbeiten der Basisimages, die durch den Nachweisdienst bestätigt werden.	Root-vCenter Server
Administrator der vertrauenswürdigen Infrastruktur.Nachweis-SSO konfigurieren	Ermöglicht das Bearbeiten der Hosts, denen die Trust Authority-Hosts vertrauen können.	Root-vCenter Server
Administrator einer vertrauenswürdigen Infrastruktur.Token-Konvertierungsrichtlinie konfigurieren	Ermöglicht die Konfiguration der Token-Konvertierungsrichtlinie.	Root-vCenter Server
Administrator der vertrauenswürdigen Infrastruktur.Hosts der vertrauenswürdigen Infrastruktur auflisten	Ermöglicht das Lesen von Informationen bezüglich der vertrauenswürdigen Hosts und der Trust Authority-Hosts.	Root-vCenter Server
Administrator der vertrauenswürdigen Infrastruktur.Informationen zu STS auflisten	Ermöglicht das Exportieren der Details des vertrauenswürdigen Hosts, sodass sie in den Trust Authority-Cluster importiert werden können.	Root-vCenter Server
Administrator der vertrauenswürdigen Infrastruktur.Hosts der vertrauenswürdigen Infrastruktur verwalten	Ermöglicht das Bearbeiten der Informationen zu den vertrauenswürdigen Hosts und den Trust Authority-Hosts.	Root-vCenter Server
Administrator der vertrauenswürdigen Infrastruktur.Vertrauensstellung des Schlüsselservers lesen	Ermöglicht das Lesen der Schlüsselanbieter des Schlüsselanbieterdiensts.	Root-vCenter Server
Administrator der vertrauenswürdigen Infrastruktur.Nachweis-SSO lesen	Ermöglicht das Lesen, welchen Hosts die Trust Authority-Hosts vertrauen können.	Root-vCenter Server

Tabelle 16-35. Rechte für „Administrator der vertrauenswürdigen Infrastruktur“ (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Administrator der vertrauenswürdigen Infrastruktur.TPM-Zertifikate des vertrauenswürdigen Autoritätshosts abrufen	Ermöglicht das Lesen der Einstellungen des Nachweisdiensts.	Root-vCenter Server
Administrator der vertrauenswürdigen Infrastruktur.Metadaten des vertrauenswürdigen Autoritätshosts abrufen	Ermöglicht das Lesen, welche Basisimages durch den Nachweisdienst bestätigt werden können.	Root-vCenter Server

vApp-Rechte

vApp-Rechte steuern Vorgänge im Zusammenhang mit dem Bereitstellen und Konfigurieren einer vApp.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-36. vApp-Rechte

Rechtename	Beschreibung	Erforderlich bei
vApp.Virtuelle Maschine hinzufügen	Ermöglicht das Hinzufügen einer virtuellen Maschine zu einer vApp.	vApps
vApp.Ressourcenpool zuweisen	Ermöglicht das Zuweisen eines Ressourcenpools zu einer vApp.	vApps
vApp.vApp zuweisen	Ermöglicht das Zuweisen einer vApp zu einer anderen vApp.	vApps
vApp.Klonen	Ermöglicht das Klonen einer vApp.	vApps
vApp.Erstellen	Ermöglicht das Erstellen einer vApp.	vApps
vApp.Löschen	Ermöglicht das Löschen einer vApp. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	vApps
vApp.Exportieren	Ermöglicht das Exportieren einer vApp aus vSphere.	vApps
vApp.Importieren	Ermöglicht das Importieren einer vApp in vSphere.	vApps

Tabelle 16-36. vApp-Rechte (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
vApp.Verschieben	Ermöglicht das Verschieben einer vApp an einen neuen Speicherort in der Bestandsliste.	vApps
vApp.Ausschalten	Ermöglicht das Ausschalten einer vApp.	vApps
vApp.Einschalten	Ermöglicht das Einschalten einer vApp.	vApps
vApp.Umbenennen	Ermöglicht das Umbenennen einer vApp.	vApps
vApp.Anhalten	Ermöglicht das Anhalten einer vApp.	vApps
vApp.Aufheben der Registrierung	Ermöglicht das Aufheben der Registrierung einer vApp. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	vApps
vApp.OVF-Umgebung anzeigen	Ermöglicht das Anzeigen der OVF-Umgebung einer eingeschalteten virtuellen Maschine innerhalb einer vApp.	vApps
vApp.vApp-Anwendungskonfiguration	Ermöglicht das Ändern der internen Struktur einer vApp (z. B. Produktinformationen und Eigenschaften).	vApps
vApp.vApp-Instanzkonfiguration	Ermöglicht das Ändern der Konfiguration einer vApp-Instanz (z. B. Richtlinien).	vApps
vApp.vApp-managedBy-Konfiguration	Ermöglicht einer Erweiterung oder Lösung, eine vApp so zu markieren, als würde sie von dieser Erweiterung oder Lösung verwaltet. Diesem Recht sind keine Benutzerschnittstellenelemente auf dem vSphere Client zugeordnet.	vApps
vApp.vApp-Ressourcenkonfiguration	Ermöglicht das Ändern einer vApp-Ressourcenkonfiguration. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	vApps

Rechte für VcIdentityProviders

Mit den Rechten für VcIdentityProviders wird der Zugriff auf die VcIdentityProviders-API gesteuert.

Tabelle 16-37. Rechte für VcIdentityProviders

Rechtename	Beschreibung	Erforderlich bei
VcIdentityProviders.Erstellen	Ermöglicht den Zugriff vom Typ „Nur erstellen“ auf die VcIdentityProviders-API (vCenter Server-Identitätsanbieter).	Nicht verfügbar
VcIdentityProviders.Verwalten	Ermöglicht den Schreibzugriff auf Administratorebene (Erstellen, Lesen, Aktualisieren, Löschen) auf die VcIdentityProviders-API (vCenter Server-Identitätsanbieter).	Nicht verfügbar
VcIdentityProviders.Lesen	Ermöglicht den Lesezugriff auf die VcIdentityProviders-API (vCenter Server-Identitätsanbieter).	Nicht verfügbar

Rechte für die Konfiguration von VMware vSphere Lifecycle Manager

Mit Rechten für die Konfiguration von VMware vSphere Lifecycle Manager wird die Fähigkeit zum Konfigurieren des vSphere Lifecycle Manager-Diensts gesteuert.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Hinweis Weisen Sie nur Administratoren oder vertrauenswürdigen Benutzern Rechte zu, die VMware vSphere Lifecycle Manager-APIs zum Akzeptieren von URLs verwenden.

Tabelle 16-38. Rechte für die Konfiguration von VMware vSphere Lifecycle Manager

Rechtename	Beschreibung	Erforderlich bei
VMware vSphere Lifecycle Manager.Konfigurieren. Dienst konfigurieren	Ermöglicht Ihnen die Konfiguration des vSphere Lifecycle Manager-Diensts und der geplanten Aufgabe zum Herunterladen von Patches.	Root-vCenter Server

Rechte für ESXi-Integritätsperspektiven für VMware vSphere Lifecycle Manager

Mit Rechten für ESXi-Integritätsperspektiven für VMware vSphere Lifecycle Manager wird die Möglichkeit gesteuert, die Integrität von ESXi-Hosts und -Clustern zu überprüfen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-39. Rechte für ESXi-Integritätsperspektiven für VMware vSphere Lifecycle Manager

Rechtename	Beschreibung	Erforderlich bei
VMware vSphere Lifecycle Manager.ESXi-Integritätsperspektiven. Lesen	Ermöglicht das Abfragen des Zustands von ESXi-Hosts und -Clustern.	Hosts Cluster
VMware vSphere Lifecycle Manager.ESXi-Integritätsperspektiven. Schreiben	Nicht verfügbar	Nicht verfügbar

Allgemeine Rechte für VMware vSphere Lifecycle Manager

Mit den allgemeinen Rechten für VMware vSphere Lifecycle Manager wird die Fähigkeit zum Lesen und Schreiben von Lifecyle Manager-Ressourcen gesteuert.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-40. Allgemeine Rechte für VMware vSphere Lifecycle Manager

Rechtename	Beschreibung	Erforderlich bei
VMware vSphere Lifecycle Manager.Lifecycle Manager: Allgemeine Rechte.Lesen	Ermöglicht das Lesen der vSphere Lifecycle Manager-Ressourcen. Diese Berechtigung ist erforderlich, um Aufgabeninformationen zu erhalten.	Root-vCenter Server
VMware vSphere Lifecycle Manager.Lifecycle Manager: Allgemeine Rechte.Schreiben	Ermöglicht das Schreiben der vSphere Lifecycle Manager-Ressourcen. Dieses Recht ist erforderlich, um eine vSphere Lifecycle Manager-Aufgabe abzubrechen.	Root-vCenter Server

Rechte für die Hardwarekompatibilität von VMware vSphere Lifecycle Manager

Mit Rechten für die Hardwarekompatibilität von VMware vSphere Lifecycle Manager wird die Fähigkeit gesteuert, potenzielle Hardwarekompatibilitätsprobleme zu erkennen und zu beheben.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-41. Rechte für die Hardwarekompatibilität von VMware vSphere Lifecycle Manager

Rechtename	Beschreibung	Erforderlich bei
VMware vSphere Lifecycle Manager.Lifecycle Manager: Berechtigungen für die Hardwarekompatibilität. Kompatibilität für den Zugriff auf Hardware	Ermöglicht den Zugriff auf die Hardwarekompatibilitätsdaten und das Beheben potenzieller Hardwarekompatibilitätsprobleme	Hosts

Rechte für VMware vSphere Lifecycle Manager-Images

Mit Rechten für VMware vSphere Lifecycle Manager-Images wird die Fähigkeit zur Verwaltung von Images gesteuert.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Hinweis Weisen Sie nur Administratoren oder vertrauenswürdigen Benutzern Rechte zu, die VMware vSphere Lifecycle Manager-APIs zum Akzeptieren von URLs verwenden.

Tabelle 16-42. Rechte für VMware vSphere Lifecycle Manager-Images

Rechtename	Beschreibung	Erforderlich bei
VMware vSphere Lifecycle Manager.Lifecycle Manager: Image-Rechte.Lesen	Ermöglicht das Lesen von vSphere Lifecycle Manager-Images. Dieses Recht ist für Folgendes erforderlich: ■ Auflisten aller Entwürfe für einen Cluster ■ Erhalten weiterer Informationen zu einem Entwurf ■ Durchführen einer Prüfung für einen Entwurf ■ Validieren eines Entwurfs ■ Abrufen des Inhalts eines Entwurfs ■ Ermitteln der Liste der effektiven Komponenten ■ Erhalten der Inhalte des Dokuments mit dem aktuellen gewünschten Zustand ■ Starten einer Prüfung in einem Cluster ■ Erhalten des Konformitätsergebnisses ■ Erhalten einer Empfehlung ■ Exportieren des aktuellen gewünschten Zustands als Depot, JSON-Datei oder ISO	Root-vCenter Server
VMware vSphere Lifecycle Manager.Lifecycle Manager: Image-Rechte.Schreiben	Ermöglicht das Verwalten von vSphere Lifecycle Manager-Images. Dieses Recht ist für Folgendes erforderlich: ■ Erstellen, Löschen oder Übergeben eines Entwurfs ■ Importieren des gewünschten Zustands ■ Generieren von Empfehlungen ■ Festlegen oder Löschen verschiedener Teile eines Entwurfs	Root-vCenter Server

Rechte für die Standardisierung von VMware vSphere Lifecycle Manager-Images

Mit Rechten für VMware vSphere Lifecycle Manager-Images wird die Fähigkeit zur Standardisierung von Images gesteuert.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-43. Rechte für die Standardisierung von VMware vSphere Lifecycle Manager-Images

Rechtename	Beschreibung	Erforderlich bei
VMware vSphere Lifecycle Manager.Lifecycle Manager: Image-Standardisierungsrechte .Lesen	Ermöglicht die Ausführung der Vorabprüfung für die Standardisierung.	Cluster
VMware vSphere Lifecycle Manager.Lifecycle Manager: Image-Standardisierungsrechte .Schreiben	Ermöglicht die Ausführung der Standardisierung.	Cluster

Rechte für VMware vSphere Lifecycle Manager-Einstellungen

Mit Rechten für VMware vSphere Lifecycle Manager-Einstellungen wird die Fähigkeit zur Verwaltung von Depots und Standardisierungsrichtlinien gesteuert.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Hinweis Weisen Sie nur Administratoren oder vertrauenswürdigen Benutzern Rechte zu, die VMware vSphere Lifecycle Manager-APIs zum Akzeptieren von URLs verwenden.

Tabelle 16-44. Rechte für VMware vSphere Lifecycle Manager-Einstellungen

Rechtename	Beschreibung	Erforderlich bei
VMware vSphere Lifecycle Manager.Lifecycle Manager: Rechte für Einstellungen.Lesen	Ermöglicht das Lesen von vSphere Lifecycle Manager-Depots und Standardisierungsrichtlinien.	Root-vCenter Server
VMware vSphere Lifecycle Manager.Lifecycle Manager: Rechte für Einstellungen.Schreiben	Ermöglicht das Schreiben von vSphere Lifecycle Manager-Depots und Standardisierungsrichtlinien.	Root-vCenter Server

Rechte für die Verwaltung von VMware vSphere Lifecycle Manager-Baselines

Mit Rechten für die Verwaltung von VMware vSphere Lifecycle Manager-Baselines wird die Fähigkeit gesteuert, Baselines und Baselinegruppen zu verwalten.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-45. Rechte für die Verwaltung von VMware vSphere Lifecycle Manager-Baselines

Rechtename	Beschreibung	Erforderlich bei
VMware vSphere Lifecycle Manager.Baseline verwalten. Baseline anhängen	Ermöglicht das Anhängen von Baselines und Baselinegruppen an Objekte in der vSphere-Bestandsliste.	Root-vCenter Server
VMware vSphere Lifecycle Manager.Baseline verwalten.Baseline verwalten	Ermöglicht das Erstellen, Bearbeiten oder Löschen von Baselines und Baselinegruppen.	Root-vCenter Server

Rechte zum Verwalten von Patches und Upgrades für VMware vSphere Lifecycle Manager

Mit den Rechten zum Verwalten von Patches und Upgrades für VMware vSphere Lifecycle Manager wird die Fähigkeit zum Anzeigen, Prüfen und Standardisieren anwendbarer Patches, Erweiterungen oder Upgrades gesteuert.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-46. Rechte zum Verwalten von Patches und Upgrades für VMware vSphere Lifecycle Manager

Rechtename	Beschreibung	Erforderlich bei
VMware vSphere Lifecycle Manager.Patches und Upgrades verwalten.Standardisieren zum Übernehmen von Patches, Erweiterungen und Upgrades	Ermöglicht die Standardisierung von virtuellen Maschinen und Hosts, um Patches, Erweiterungen oder Upgrades anzuwenden, wenn Sie Baselines verwenden. Mit diesem Recht können Sie außerdem den Konformitätsstatus anzeigen.	Root-vCenter Server
VMware vSphere Lifecycle Manager.Patches und Upgrades verwalten.Auf passende Patches, Erweiterungen und Upgrades prüfen	Ermöglicht das Prüfen von virtuellen Maschinen und Hosts, um nach anwendbaren Patches, Erweiterungen oder Upgrades zu suchen, wenn Sie Baselines verwenden.	Root-vCenter Server
VMware vSphere Lifecycle Manager.Patches und Upgrades verwalten.Patches und Erweiterungen bereitstellen	Ermöglicht das Staging von Patches oder Erweiterungen auf ESXi-Hosts, wenn Sie Baselines verwenden. Außerdem ermöglicht Ihnen dieses Recht die Anzeige des Konformitätsstatus der ESXi-Hosts.	Root-vCenter Server
VMware vSphere Lifecycle Manager.Patches und Upgrades verwalten.Konformitätsstatus anzeigen	Ermöglicht die Anzeige der Zeigen Sie Baseline-Konformitätsinformationen für ein Objekt in der vSphere-Bestandsliste.	Root-vCenter Server

Rechte zum Hochladen von Dateien für VMware vSphere Lifecycle Manager

Mit Rechten zum Hochladen von Dateien für VMware vSphere Lifecycle Manager wird die Fähigkeit gesteuert, Updates in das vSphere Lifecycle Manager-Depot zu importieren.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Hinweis Weisen Sie nur Administratoren oder vertrauenswürdigen Benutzern Rechte zu, die VMware vSphere Lifecycle Manager-APIs zum Akzeptieren von URLs verwenden.

Tabelle 16-47. Rechte zum Hochladen von Dateien für VMware vSphere Lifecycle Manager

Rechtename	Beschreibung	Erforderlich bei
VMware vSphere Lifecycle Manager.Datei hochladen.Datei hochladen	Ermöglicht das Hochladen von Upgrade-ISO und Offline-Patchpaketen.	Root-vCenter Server

Berechtigungen für das Konfigurieren virtueller Maschinen

Rechte für die Konfiguration virtueller Maschinen steuern die Fähigkeit, Optionen und Geräte für virtuelle Maschinen zu konfigurieren.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-48. Berechtigungen für das Konfigurieren virtueller Maschinen

Rechtename	Beschreibung	Erforderlich bei
Virtuelle Maschine.Konfiguration.Festplatten-Lease abrufen	Ermöglicht Festplatten-Lease-Vorgänge für eine virtuelle Maschine.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Vorhandene Festplatte hinzufügen	Ermöglicht das Hinzufügen einer vorhandenen virtuellen Festplatte zu einer virtuellen Maschine.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Neue Festplatte hinzufügen	Ermöglicht das Erstellen einer neuen virtuellen Festplatte für eine virtuelle Maschine.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Gerät hinzufügen oder entfernen	Ermöglicht das Hinzufügen oder Entfernen von Geräten (ausgenommen Festplatten).	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Erweiterte Konfiguration	Ermöglicht das Hinzufügen oder Ändern erweiterter Parameter in der Konfigurationsdatei der virtuellen Maschine.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.CPU-Anzahl ändern	Ermöglicht das Ändern der Anzahl virtueller CPUs.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Arbeitsspeicher ändern	Ermöglicht das Ändern der Größe des Arbeitsspeichers, der der virtuellen Maschine zugeteilt ist.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Einstellungen ändern	Ermöglicht das Ändern der allgemeinen Einstellungen der virtuellen Maschine.	virtuelle Maschinen

Tabelle 16-48. Berechtigungen für das Konfigurieren virtueller Maschinen (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Virtuelle Maschine.Konfiguration.Platzierung der Auslagerungsdatei ändern	Ermöglicht das Ändern der Richtlinie zur Platzierung der Auslagerungsdatei für eine virtuelle Maschine.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Ressourcen ändern	Ermöglicht das Ändern der Ressourcenkonfiguration für eine Gruppe von VM-Knoten in einem vorgegebenen Ressourcenpool.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Host-USB-Gerät konfigurieren	Ermöglicht das Verbinden eines hostbasierten USB-Geräts mit einer virtuellen Maschine.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Rohgerät konfigurieren	Ermöglicht das Hinzufügen oder Entfernen einer Raw-Festplattenzuordnung oder eines SCSI-Passthrough-Geräts. Wenn dieser Parameter gesetzt wird, werden alle weiteren Rechte zum Ändern von Raw-Geräten außer Kraft gesetzt, einschließlich des Verbindungsstatus.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.managedBy konfigurieren	Gestattet es einer Erweiterung oder Lösung, eine virtuelle Maschine als von dieser Erweiterung oder Lösung verwaltet zu markieren.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Verbindungseinstellungen anzeigen	Ermöglicht die Konfiguration von Optionen für Remotekonsolen virtueller Maschinen.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Virtuelle Festplatte erweitern	Ermöglicht das Vergrößern einer virtuellen Festplatte.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Geräteeinstellungen ändern	Ermöglicht das Ändern der Eigenschaften eines vorhandenen Geräts.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Kompatibilität der Fault Tolerance abfragen	Ermöglicht das Prüfen, ob eine virtuelle Maschine mit Fault Tolerance kompatibel ist.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Dateien ohne Besitzer abfragen	Ermöglicht das Abfragen von Dateien ohne Besitzer.	virtuelle Maschinen

Tabelle 16-48. Berechtigungen für das Konfigurieren virtueller Maschinen (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Virtuelle Maschine.Konfiguration.Von Pfad neu laden	Ermöglicht das Ändern des Pfads einer VM-Konfiguration bei gleichzeitigem Aufrechterhalten der Identität der virtuellen Maschine. Lösungen wie z. B. VMware vCenter Site Recovery Manager verwenden diesen Vorgang, um die Identität der virtuellen Maschine während eines Failovers und Failbacks aufrechtzuerhalten.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Festplatte entfernen	Ermöglicht das Entfernen eines virtuellen Festplattengeräts.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Umbenennen	Ermöglicht das Umbenennen einer virtuellen Maschine oder das Ändern zugeordneter Anmerkungen für eine virtuelle Maschine.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Gastinformationen zurücksetzen	Ermöglicht das Bearbeiten der Gastbetriebssystem-Informationen für eine virtuelle Maschine.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Anmerkung festlegen	Ermöglicht das Hinzufügen oder Bearbeiten einer Anmerkung für eine virtuelle Maschine.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Festplattenwechsel-Verfolgung umschalten	Ermöglicht das Aktivieren bzw. Deaktivieren der Änderungsverfolgung für Festplatten der virtuellen Maschine.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Verzweigtes übergeordnetes Element umschalten	Ermöglicht das Aktivieren bzw. Deaktivieren eines übergeordneten vmfork.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Kompatibilität der virtuellen Maschine aktualisieren	Ermöglicht das Upgrade der Kompatibilitätsversion der virtuellen Maschine.	virtuelle Maschinen

Rechte für Vorgänge als Gast auf virtuellen Maschinen

Rechte für Gastvorgänge auf virtuellen Maschinen steuern die Fähigkeit zur Interaktion der Daten und Anwendungen innerhalb des Gastbetriebssystems einer virtuellen Maschine mit der API.

Weitere Informationen zu diesen Vorgängen finden Sie in der Dokumentation *vSphere Web Services-API-Referenz*.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-49. Vorgänge als Gast auf virtuelle Maschinen

Rechtename	Beschreibung	Gültig für Objekt
Virtuelle Maschine.Gastbetriebssysteme.Änderung des Alias der Gastbetriebssysteme	Ermöglicht Gastvorgänge auf virtuellen Maschinen, die das Ändern des Alias für die virtuelle Maschine beinhalten.	virtuelle Maschinen
Virtuelle Maschine.Gastbetriebssysteme.Aliasspeicher im Gast abfragen	Ermöglicht Gastvorgänge auf virtuellen Maschinen, die das Abfragen des Alias für die virtuelle Maschine beinhalten.	virtuelle Maschinen
Virtuelle Maschine.Gastbetriebssysteme.Änderungen des Gastbetriebssystems	Ermöglicht Gastvorgänge auf virtuellen Maschinen, die Änderungen am Gastbetriebssystem einer virtuellen Maschine einschließen, wie z. B. das Übertragen einer Datei auf eine virtuelle Maschine. Diesem Recht sind keine Benutzerschnittstelleneleme nte auf dem vSphere Client zugeordnet.	virtuelle Maschinen
Virtuelle Maschine.Gastbetriebssysteme.Programmausführung im Gastbetriebssystem	Ermöglicht Gastvorgänge auf virtuellen Maschinen, die das Ausführen einer Anwendung auf der virtuellen Maschine einschließen. Diesem Recht sind keine Benutzerschnittstelleneleme nte auf dem vSphere Client zugeordnet.	virtuelle Maschinen
Virtuelle Maschine.Gastbetriebssysteme.Abfragen des Gastbetriebssystems	Ermöglicht Gastvorgänge auf virtuellen Maschinen, die Abfragen des Gastbetriebssystems einschließen, wie z. B. das Auflisten von Dateien im Gastbetriebssystem. Diesem Recht sind keine Benutzerschnittstelleneleme nte auf dem vSphere Client zugeordnet.	virtuelle Maschinen

Rechte für die Interaktion virtueller Maschinen

Rechte für die Interaktion virtueller Maschinen steuern die Fähigkeit, mit der Konsole einer virtuellen Maschine zu interagieren, Medien zu konfigurieren, Betriebsvorgänge auszuführen und VMware Tools zu installieren.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-50. Interaktion virtueller Maschinen

Rechtename	Beschreibung	Erforderlich bei
Virtuelle Maschine.Interaktion.Frage beantworten	Ermöglicht die Behebung von Problemen beim Statuswechsel virtueller Maschinen und bei Laufzeitfehlern.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Sicherungsvorgang der virtuellen Maschine	Ermöglicht die Ausführung von Sicherungsvorgängen bei virtuellen Maschinen.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.CD-Medien konfigurieren	Ermöglicht die Konfiguration eines virtuellen DVD- oder CD-ROM-Laufwerks.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Diskettenmedien konfigurieren	Ermöglicht die Konfiguration eines virtuellen Diskettenlaufwerks.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Konsoleninteraktion	Ermöglicht die Interaktion mit der virtuellen Maus, der virtuellen Tastatur und dem virtuellen Bildschirm der virtuellen Maschine.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Screenshot erstellen	Ermöglicht die Erstellung eines Screenshots einer virtuellen Maschine.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Alle Festplatten defragmentieren	Ermöglicht Defragmentierungsvorgänge für alle Festplatten der virtuellen Maschine.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Geräteverbindung	Ermöglicht die Änderung des Verbindungsstatus der virtuellen Geräte einer virtuellen Maschine, die getrennt werden können.	virtuelle Maschinen

Tabelle 16-50. Interaktion virtueller Maschinen (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Virtuelle Maschine.Interaktion.Drag & Drop	Ermöglich das Ziehen und Ablegen von Dateien zwischen einer virtuellen Maschine und einem Remoteclient.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Verwaltung des Gastbetriebssystems durch VIX API	Ermöglicht das Management des Betriebssystems der virtuellen Maschine über die VIX API.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.USB HID-Scancodes einfügen	Ermöglicht das Einfügen von USB HID-Scancodes.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Anhalten oder Wiederaufnehmen	Ermöglicht das Anhalten oder Fortsetzen der virtuellen Maschine.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Zurücksetzungs- oder Verkleinerungsvorgänge ausführen	Ermöglicht die Ausführung von Zurücksetzungs- oder Verkleinerungsvorgängen auf der virtuellen Maschine.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Ausschalten	Ermöglicht das Ausschalten einer eingeschalteten virtuellen Maschine. Dabei wird das Gastbetriebssystem heruntergefahren.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Einschalten	Ermöglicht das Einschalten einer ausgeschalteten virtuellen Maschine und die Wiederaufnahme des Betriebs einer angehaltenen virtuellen Maschine.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Sitzung auf virtueller Maschine aufzeichnen	Ermöglicht die Aufzeichnung einer Sitzung auf einer virtuellen Maschine.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Wiedergabesitzung auf der virtuellen Maschine	Ermöglicht die Wiedergabe einer aufgezeichneten Sitzung auf einer virtuellen Maschine.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Zurücksetzen	Ermöglicht das Zurücksetzen einer virtuellen Maschine und den Neustart des Gastbetriebssystems.	virtuelle Maschinen

Tabelle 16-50. Interaktion virtueller Maschinen (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Virtuelle Maschine.Interaktion.Fault Tolerance fortsetzen	Ermöglicht die Fortsetzung von Fault Tolerance für eine virtuelle Maschine.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Anhalten	Ermöglicht das Anhalten einer eingeschalteten virtuellen Maschine. Dabei wird das Gastsystem in den Standby-Modus versetzt.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Fault Tolerance anhalten	Ermöglicht die Unterbrechung von Fault Tolerance für eine virtuelle Maschine.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Failover testen	Ermöglicht das Testen des Fault Tolerance-Failovers, indem die sekundäre virtuelle Maschine als primäre virtuelle Maschine festgelegt wird.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Neustart sekundärer VM testen	Ermöglicht das Beenden einer sekundären virtuellen Maschine für eine virtuelle Maschine mit Fault Tolerance.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Fault Tolerance ausschalten	Ermöglicht die Deaktivierung von Fault Tolerance für eine virtuelle Maschine.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.Fault Tolerance einschalten	Ermöglicht die Aktivierung von Fault Tolerance für eine virtuelle Maschine.	virtuelle Maschinen
Virtuelle Maschine.Interaktion.VMware Tools installieren	Ermöglicht die Einrichtung bzw. die Aufhebung der Einrichtung des CD-Installationsprogramms für VMware Tools als CD-ROM für das Gastbetriebssystem.	virtuelle Maschinen

Rechte für die Bestandsliste der virtuellen Maschine

Rechte für die Bestandsliste virtueller Maschinen steuern das Hinzufügen, Verschieben und Entfernen von virtuellen Maschinen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-51. Rechte für die Bestandsliste der virtuellen Maschine

Rechtename	Beschreibung	Erforderlich bei
Virtuelle Maschine.Bestandsliste. Aus vorhandener erstellen	Ermöglicht das Erstellen einer virtuellen Maschine basierend auf einer vorhandenen virtuellen Maschine oder Vorlage (durch Klonen oder Bereitstellen über eine Vorlage).	Cluster, Hosts, Ordner für virtuelle Maschinen
Virtuelle Maschine.Bestandsliste. Neu erstellen	Ermöglicht das Erstellen einer virtuellen Maschine und die Zuteilung von Ressourcen für ihre Ausführung.	Cluster, Hosts, Ordner für virtuelle Maschinen
Virtuelle Maschine.Bestandsliste. Verschieben	Ermöglicht das Verlagern einer virtuellen Maschine in der Hierarchie. Die Berechtigung muss für Quelle und Ziel vorhanden sein.	virtuelle Maschinen
Virtuelle Maschine.Bestandsliste. Registrieren	Ermöglicht das Hinzufügen einer vorhandenen virtuellen Maschine zu einer vCenter Server- oder Host-Bestandsliste.	Cluster, Hosts, Ordner für virtuelle Maschinen
Virtuelle Maschine.Bestandsliste. Entfernen	Ermöglicht das Löschen einer virtuellen Maschine. Durch das Löschen werden die zugrunde liegenden Dateien der virtuellen Maschine von der Festplatte entfernt. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	virtuelle Maschinen
Virtuelle Maschine.Bestandsliste. Registrierung aufheben	Ermöglicht das Aufheben der Registrierung einer virtuellen Maschine in einer vCenter Server- oder Host-Bestandsliste. Dieser Vorgang kann nur ausführt werden, wenn dem Benutzer oder der Gruppe diese Berechtigung sowohl dem Objekt als auch seinem übergeordneten Objekt zugewiesen ist.	virtuelle Maschinen

Rechte für das Bereitstellen virtueller Maschinen

Rechte für das Bereitstellen virtueller Maschinen steuern Aktivitäten im Bezug auf das Bereitstellen und Anpassen von virtuelle Maschinen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-52. Rechte für das Bereitstellen virtueller Maschinen

Rechtename	Beschreibung	Erforderlich bei
Virtuelle Maschine.Bereitstellung.Festplattenzugriff zulassen	Ermöglicht das Öffnen einer Festplatte auf einer virtuellen Maschine für den zufallsbasierten Lese- und Schreibzugriff. Wird meistens für die Remoteeinrichtung von Festplatten verwendet.	virtuelle Maschinen
Virtuelle Maschine.Bereitstellung.Dateizugriff zulassen	Ermöglicht Vorgänge für Dateien, die einer virtuellen Maschine zugeordnet sind, einschließlich VMX, Festplatten, Protokollen und NVRAM.	virtuelle Maschinen
Virtuelle Maschine.Bereitstellung.Lesezugriff auf Festplatte zulassen	Ermöglicht das Öffnen einer Festplatte auf einer virtuellen Maschine für den zufallsbasierten Lesezugriff. Wird meistens für die Remoteeinrichtung von Festplatten verwendet.	virtuelle Maschinen
Virtuelle Maschine.Bereitstellung.Download virtueller Maschinen zulassen	Ermöglicht das Lesen von Dateien, die einer virtuellen Maschine zugeordnet sind, einschließlich VMX, Festplatten, Protokollen und NVRAM.	Root-Host oder vCenter Server
Virtuelle Maschine.Bereitstellung.Upload von Dateien virtueller Maschinen zulassen	Ermöglicht das Schreiben von Dateien, die einer virtuellen Maschine zugeordnet sind, einschließlich VMX, Festplatten, Protokollen und NVRAM.	Root-Host oder vCenter Server
Virtuelle Maschine.Bereitstellung.Vorlage klonen	Ermöglicht das Klonen einer Vorlage.	Vorlagen
Virtuelle Maschine.Bereitstellung.Virtuelle Maschine klonen	Ermöglicht das Klonen einer vorhandenen virtuellen Maschine und das Zuweisen von Ressourcen.	virtuelle Maschinen
Virtuelle Maschine.Bereitstellung.Vorlage aus virtueller Maschine erstellen	Ermöglicht das Erstellen einer neuen Vorlage anhand einer virtuellen Maschine.	virtuelle Maschinen
Virtuelle Maschine.Bereitstellung.Gast anpassen	Ermöglicht die benutzerdefinierte Anpassung des Gastbetriebssystems einer virtuellen Maschine ohne sie zu verschieben.	virtuelle Maschinen
Virtuelle Maschine.Bereitstellung.Vorlage bereitstellen	Ermöglicht das Bereitstellen einer virtuellen Maschine anhand einer Vorlage.	Vorlagen
Virtuelle Maschine.Bereitstellung.Als Vorlage markieren	Ermöglicht das Kennzeichnen einer vorhandenen, ausgeschalteten virtuellen Maschine als Vorlage.	virtuelle Maschinen
Virtuelle Maschine.Bereitstellung.Als virtuelle Maschine markieren	Ermöglicht das Kennzeichnen einer vorhandenen Vorlage als virtuelle Maschine.	Vorlagen

Tabelle 16-52. Rechte für das Bereitstellen virtueller Maschinen (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Virtuelle Maschine.Bereitstellung.Anpassungsspezifikation ändern	Ermöglicht das Erstellen, Ändern oder Löschen von Anpassungsspezifikationen.	Root-vCenter Server
Virtuelle Maschine.Bereitstellung.Festplatten heraufstufen	Ermöglicht das Heraufstufen von Vorgängen auf den Festplatten einer virtuellen Maschine.	virtuelle Maschinen
Virtuelle Maschine.Bereitstellung.Anpassungsspezifikationen lesen	Ermöglicht das Lesen einer Anpassungsspezifikation.	virtuelle Maschinen

Rechte für die Dienstkonfiguration der virtuellen Maschine

Rechte für die Dienstkonfiguration der virtuellen Maschine bestimmen, wer die Überwachungs- und Verwaltungsaufgaben für die Dienstkonfiguration ausführen kann.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-53. Rechte für die Dienstkonfiguration der virtuellen Maschine

Rechtename	Beschreibung
Virtuelle Maschine.Dienstkonfiguration.Benachrichtigungen zulassen	Ermöglicht das Erstellen und Nutzen von Benachrichtigungen zum Dienststatus.
Virtuelle Maschine.Dienstkonfiguration.Abrufen globaler Ereignisbenachrichtigungen zulassen	Ermöglicht die Abfrage, ob Benachrichtigungen vorhanden sind.
Virtuelle Maschine.Dienstkonfiguration.Dienstkonfiguration verwalten	Ermöglicht das Erstellen, Ändern und Löschen von VM-Diensten.
Virtuelle Maschine.Dienstkonfiguration.Dienstkonfiguration ändern	Ermöglicht das Ändern der bestehenden Dienstkonfiguration der virtuellen Maschine.
Virtuelle Maschine.Dienstkonfiguration.Dienstkonfigurationen abfragen	Ermöglicht das Abrufen einer Liste der VM-Dienste.
Virtuelle Maschine.Dienstkonfiguration.Dienstkonfiguration lesen	Ermöglicht das Abrufen der bestehenden Dienstkonfiguration der virtuellen Maschine.

Rechte für die Snapshot-Verwaltung von virtuellen Maschinen

Rechte in Bezug auf die Snapshot-Verwaltung von virtuellen Maschinen steuern die Fähigkeit, Snapshots aufzunehmen, zu löschen, umzubenennen und wiederherzustellen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-54. Rechte in Bezug auf den Status von virtuellen Maschinen

Rechtename	Beschreibung	Erforderlich bei
Virtuelle Maschine.Snapshot-Verwaltung.Snapshot erstellen	Ermöglicht das Erstellen eines neuen Snapshots vom aktuellen Status der virtuellen Maschine.	virtuelle Maschinen
Virtuelle Maschine.Snapshot-Verwaltung.Snapshot entfernen	Ermöglicht das Entfernen eines Snapshots aus dem Snapshotverlauf.	virtuelle Maschinen
Virtuelle Maschine.Snapshot-Verwaltung.Snapshot umbenennen	Ermöglicht das Umbenennen eines Snapshots durch Zuweisen eines neuen Namens und/oder einer neuen Beschreibung.	virtuelle Maschinen
Virtuelle Maschine.Snapshot-Verwaltung.Snapshot wiederherstellen	Ermöglicht das Zurücksetzen der virtuellen Maschine auf den Status, der in einem bestimmten Snapshot vorgelegen hat.	virtuelle Maschinen

vSphere Replication-Rechte der VM

vSphere Replication-Rechte der VM steuern die Verwendung der Replizierung durch VMware vCenter Site Recovery Manager™ für virtuelle Maschinen.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-55. vSphere Replication der VM

Rechtename	Beschreibung	Erforderlich bei
Virtuelle Maschine.vSphere Replication.Replizierung konfigurieren	Ermöglicht die Konfiguration der vSphere Replication der VM.	virtuelle Maschinen
Virtuelle Maschine .vSphere Replication.Replizierung verwalten	Ermöglicht das Auslösen der Online-, Offline- oder Vollsynchronisierung bei einer vSphere Replication der VM.	virtuelle Maschinen
Virtuelle Maschine .vSphere Replication.Replizierung überwachen	Ermöglicht die Überwachung einer vSphere Replication der VM.	virtuelle Maschinen

vServices-Rechte

vServices-Rechte steuern den Zugriff virtueller Maschinen und vApps auf Funktionen zum Erstellen, Konfigurieren und Aktualisieren von vService-Abhängigkeiten.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-56. vServices

Rechtename	Beschreibung	Erforderlich bei
vService.Abhängigkeit erstellen	Ermöglicht das Erstellen einer vService-Abhängigkeit für virtuelle Maschinen oder vApps.	vApps und virtuelle Maschinen
vService.Abhängigkeit löschen	Ermöglicht das Entfernen einer vService-Abhängigkeit für eine virtuelle Maschine oder vApp.	vApps und virtuelle Maschinen
vService.Abhängigkeitskonfiguration neu konfigurieren	Ermöglicht die Neukonfiguration einer Abhängigkeit, um den Anbieter oder die Bindung zu aktualisieren.	vApps und virtuelle Maschinen
vService.Abhängigkeit aktualisieren	Ermöglicht Aktualisierungen einer Abhängigkeit, um den Namen oder die Beschreibung zu konfigurieren.	vApps und virtuelle Maschinen

vSphere-Tag-Berechtigungen

Die vSphere-Tag-Berechtigungen bestimmen, ob Tags und Tag-Kategorien erstellt und gelöscht und ob Tags in vCenter Server-Bestandslistenobjekten zugewiesen und entfernt werden können.

Sie können dieses Recht auf verschiedenen Ebenen in der Hierarchie festlegen. Wenn Sie beispielsweise ein Recht auf der Ordnerebene festgelegt haben, können Sie das Recht an ein oder mehrere Objekte innerhalb des Ordners weitergeben. Die in der Required On-Spalte aufgelisteten Objekte müssen, auf direkte oder geerbte Art und Weise, über das Recht verfügen.

Tabelle 16-57. vSphere-Tag-Berechtigungen

Rechtename	Beschreibung	Erforderlich bei
vSphere Tagging.vSphere Tag zuweisen oder Zuweisung aufheben	Ermöglicht das Zuweisen oder das Aufheben der Zuweisung eines Tags für ein Objekt in der vCenter Server-Bestandliste.	Beliebiges Objekt
vSphere Tagging.Zuweisen eines vSphere Tags zu einem Objekt bzw. Aufheben der Zuweisung eines vSphere Tags zu einem Objekt	Lässt zu, dass Objekten Tags zugewiesen oder nicht zugewiesen werden. Verwenden Sie dieses Recht, um zu begrenzen, welchen Objekten Benutzer Tags zuweisen oder deren Zuweisung entfernen können.	Beliebiges Objekt
vSphere Tagging.vSphere Tag erstellen	Ermöglicht das Erstellen eines Tags.	Beliebiges Objekt
vSphere Tagging.vSphere Tag-Kategorie erstellen	Ermöglicht das Erstellen einer Tag-Kategorie.	Beliebiges Objekt
vSphere Tagging.vSphere Tag löschen	Ermöglicht das Löschen eines Tags.	Beliebiges Objekt
vSphere Tagging.vSphere Tag-Kategorie löschen	Ermöglicht das Löschen einer Tag-Kategorie.	Beliebiges Objekt
vSphere Tagging.vSphere Tag bearbeiten	Ermöglicht das Bearbeiten eines Tags.	Beliebiges Objekt
vSphere Tagging.vSphere Tag-Kategorie bearbeiten	Ermöglicht das Bearbeiten einer Tag-Kategorie.	Beliebiges Objekt
vSphere Tagging.UsedBy-Feld für Kategorie ändern	Ermöglicht das Ändern des UsedBy-Felds für eine Tag-Kategorie.	Beliebiges Objekt
vSphere Tagging.UsedBy-Feld für Tag ändern	Ermöglicht das Ändern des UsedBy-Felds für ein Tag.	Beliebiges Objekt

vSphere Client-Rechte

vSphere Client-Rechte steuern den Offlinezugriff auf den vCenter Server.

Diese Rechte gelten nur für VMware Cloud.

Grundlegende Informationen zu vSphere Hardening und Übereinstimmung

17

Organisationen erwarten, dass ihre Daten geschützt werden, indem das Risiko von Datendiebstahl, Cyberangriffen oder nicht autorisiertem Zugriff verringert wird. Häufig müssen Organisationen auch diverse Vorschriften aus Regierungs- oder privaten Standards einhalten, wie diejenigen des National Institute of Standards and Technology (NIST) und der Defense Information Systems Agency Security Technical Implementation Guides (DISA STIG). Wenn sichergestellt werden soll, dass Ihre vSphere-Umgebung diese Standards erfüllt, muss ein Verständnis breiter gefasster Kriterien gegeben sein, die Mitarbeiter, Prozesse und Technologie einschließen.

Eine Übersicht über die verschiedenen Sicherheits- und Übereinstimmungsthemen, die Sie beachten sollten, unterstützt Sie beim Planen der Übereinstimmungsstrategie. Darüber hinaus finden Sie auf der VMware-Website zusätzliche Ressourcen zur Übereinstimmung.

Dieses Kapitel enthält die folgenden Themen:

- Sicherheit vs. Übereinstimmung in der vSphere-Umgebung
- Grundlegendes zum vSphere Security Configuration Guide
- Informationen zum National Institute of Standards and Technology
- Informationen zu DISA STIGs
- Informationen zu VMware Security Development Lifecycle
- Überwachungsprotokollierung
- Grundlegendes zur Sicherheit und Übereinstimmung – nächste Schritte
- vCenter Server und FIPS

Sicherheit vs. Übereinstimmung in der vSphere-Umgebung

Die Begriffe Sicherheit und Übereinstimmung werden häufig wie Synonyme verwendet. Es handelt sich jedoch um eindeutige und unterschiedliche Konzepte.

Sicherheit, womit häufig Informationssicherheit gemeint ist, wird in der Regel als ein Satz technischer, physischer und administrativer Kontrollen definiert, die Sie implementieren, um für Vertraulichkeit, Integrität und Verfügbarkeit zu sorgen. Sie sichern beispielsweise einen Host, indem Sie eingrenzen, welche Konten sich bei ihm auf welchen Wegen (SSH, direkte Konsole usw.) anmelden können. Übereinstimmung ist im Gegensatz dazu eine Reihe von

Anforderungen, die erforderlich sind, um die minimalen Kontrollen zu erfüllen, die von verschiedenen Vorschriftenrahmen festgelegt wurden und eingeschränkte Leitlinien für jeden spezifischen Technologie-, Anbieter- oder Konfigurationstyp bereitstellen. Zum Beispiel hat die Zahlungskartenbranche (Payment Card Industry, PCI) Sicherheitsrichtlinien festgelegt, damit die Organisationen ihre Kundenkontodaten proaktiv besser schützen können.

Sicherheit verringert das Risiko von Datendiebstahl, Cyberangriffen oder nicht autorisiertem Zugriff, während die Übereinstimmung nachweist, dass eine Sicherheitskontrolle eingerichtet wurde, in der Regel innerhalb eines bestimmten Zeitrahmens. Sicherheit wird hauptsächlich in den Designentscheidungen aufgeführt und zeigt sich in den Technologiekonfigurationen. Übereinstimmung konzentriert sich auf die Zuordnung des Bezugs zwischen Sicherheitskontrollen und spezifischen Anforderungen. Eine Übereinstimmungszuordnung bietet eine zentrale Ansicht zur Auflistung vieler der erforderlichen Sicherheitskontrollen. Diese Kontrollen werden durch die jeweiligen Übereinstimmungsanforderungen der einzelnen Sicherheitskontrollen detaillierter aufgeführt, die von einer Domäne vorgegeben werden, wie NIST, PCI, FedRAMP, HIPAA usw.

Effektive Cybersicherheits- und Übereinstimmungsprogramme basieren auf drei Grundlagen: Mitarbeitern, Prozessen und Technologie. Oft wird fälschlicherweise angenommen, dass Technologie allein ausreicht, um alle Cybersicherheitsbedürfnisse zu erfüllen. Technologie spielt in der Tat eine umfassende und wichtige Rolle bei der Entwicklung und Ausführung eines Informationssicherheitsprogramms. Technologie ohne Prozesse und Verfahren, Sensibilisierung und Schulung führt allerdings zu einer Schwachstelle in Ihrer Organisation.

Beim Definieren Ihrer Sicherheits- und Übereinstimmungsstrategien müssen Sie Folgendes beachten:

- Alle Mitarbeiter benötigen allgemeine Sensibilisierung und Schulung, die IT-Mitarbeiter darüber hinaus spezifische Schulung.
- Der Prozess definiert, wie Aktivitäten, Rollen und Dokumentation in Ihrem Unternehmen verwendet werden, um Risiken zu minimieren. Prozesse sind nur wirksam, wenn die Mitarbeiter sie ordnungsgemäß befolgen.
- Anhand von Technologie können die Auswirkungen eines Cybersicherheitsrisikos für Ihre Organisation verhindert oder reduziert werden. Welche Technologie Sie verwenden, hängt von der Risikoakzeptanzstufe Ihrer Organisation ab.

VMware bietet Compliance-Kits an, die sowohl einen Audit-Leitfaden als auch einen Leitfaden zur Produktanwendbarkeit enthalten und so die Lücke zwischen den Compliance- und gesetzlichen Anforderungen und den Implementierungsleitfäden schließen. Weitere Informationen finden Sie unter https://core.vmware.com/compliance.

Glossar für Übereinstimmungsbegriffe

Übereinstimmung führt bestimmte wichtige Begriffe und Definitionen ein.

Tabelle 17-1. Übereinstimmungsbegriffe

Begriff	Definition
CJIS	Criminal Justice Information Services (Informationsdienst Strafrechtspflege). Im Kontext der Übereinstimmung stellt der CJIS eine Sicherheitsrichtlinie zusammen, die vorgibt, welche Sicherheitsvorkehrungen lokale, bundesstaatliche und nationale Strafrechts- und Vollzugsbehörden treffen müssen, um sensible Informationen wie Fingerabdrücke und Angaben zu Vorstrafen zu schützen.
DISA STIG	Defense Information Systems Agency Security Technical Implementation Guide (Verteidigungsinformationssystembehörde – technisches Sicherheitsimplementierungshandbuch). Die Defense Information Systems Agency (DISA) ist die Behörde, die für die Aufrechterhaltung des Sicherheitsstatus der IT-Infrastruktur des Verteidigungsministeriums (Department of Defense, DoD) verantwortlich ist. DISA führt diese Aufgabe durch Entwicklung und Einsatz von Security Technical Implementation Guides (STIGs) aus.
FedRAMP	Federal Risk and Authorization Management Program (Bundesprogramm für Risiko- und Autorisierungsmanagement). FedRAMP ist ein US-Regierungsprogramm, das einen standardisierten Ansatz für die Sicherheitsbeurteilung, Autorisierung und fortlaufende Überwachung von Cloudprodukten und -services bereitstellt.
HIPAA	Health Insurance Portability and Accountability Act (Gesetz zur Übertragbarkeit und Rechenschaftspflicht für Gesundheitsversicherungen). Der HIPAA wurde 1996 vom US-Kongress verabschiedet und legt Folgendes fest: ■ Er gibt Millionen von amerikanischen Arbeitnehmern und deren Familien die Möglichkeit, Gesundheitsversicherungen zu übertragen und weiter zu unterhalten, wenn sie ihre Arbeitsstelle wechseln oder verlieren. ■ Er verringert Betrug und Missbrauch im Gesundheitswesen ■ Er gibt branchenweite Standards für Informationen im Gesundheitswesen zur elektronischen Abrechnung und anderen Prozessen vor ■ Er schreibt den Schutz und die vertrauliche Handhabung geschützter Gesundheitsdaten vor Dieser letzte Punkt ist für die Dokumentation von *vSphere-Sicherheit* besonders wichtig.

Tabelle 17-1. Übereinstimmungsbegriffe (Fortsetzung)

Begriff	Definition
NCCoE	National Cybersecurity Center of Excellence (Nationales Kompetenzzentrum für Cybersicherheit). NCCoE ist eine Organisation der US-Regierung, die Lösungen für Cybersicherheitsprobleme von US-Unternehmen entwickelt und öffentlich bereitstellt. Das Zentrum stellt ein Team aus Mitarbeitern von Cybersicherheit-Technologieunternehmen, anderen Bundesbehörden und Akademikern zusammen, um die einzelnen Probleme zu bearbeiten.
NIST	National Institute of Standards and Technology (Nationales Institut für Standards und Technologie). Das NIST ist eine nichtregulatorische Bundesbehörde, die 1901 innerhalb des US-Handelsministeriums gegründet wurde. Das NIST hat die Aufgabe, die Innovation und industrielle Wettbewerbsfähigkeit der USA zu fördern, indem Messtechniken, Standards und Technologie so vorangetrieben werden, dass sie die wirtschaftliche Sicherheit erhöhen und unsere Lebensqualität verbessern.
PAG	Product Applicability Guide (Produktanwendbarkeitshandbuch). Ein Dokument, das den Organisationen allgemeine Leitlinien an die Hand gibt, wenn sie die Lösungen eines Unternehmens zur Einhaltung der Übereinstimmungsanforderungen erwägen.
PCI DSS	Payment Card Industry Data Security Standard (Datensicherheitsstandard der Zahlungskartenindustrie). Eine Reihe von Sicherheitsstandards, mit denen sichergestellt werden soll, dass alle Unternehmen, die Kreditkarteninformationen annehmen, verarbeiten, speichern oder übertragen, eine sichere Umgebung bereitstellen.
VVD/VCF-Übereinstimmungslösungen	VMware Validated Design/VMware Cloud Foundation. Die VMware Validated Designs stellen umfangreiche und umfassend getestete Entwürfe bereit, um ein softwaredefiniertes Datencenter errichten und betreiben zu können. Anhand von VVD/VCF-Übereinstimmungslösungen können Kunden die Übereinstimmungsanforderungen zahlreicher Regierungs- und Branchenbestimmungen erfüllen.

Grundlegendes zum vSphere Security Configuration Guide

VMware erstellt Handbücher für das „Hardening“, d. h., die Verstärkung der Sicherheit. Diese enthalten bindende Anleitungen zur sicheren Bereitstellung und Nutzung von VMware-Produkten. Für vSphere ist dieses Handbuch der *vSphere Security Configuration Guide* (Handbuch für die vSphere-Sicherheitskonfiguration, früher als *Handbuch für „Hardening“* bezeichnet).

Der *vSphere Security Configuration Guide* enthält Best Practices für die Sicherheit von vSphere. Der *vSphere Security Configuration Guide* ist nicht direkt regulatorischen Richtlinien oder Frameworks zugeordnet und daher kein Konformitätshandbuch. Außerdem ist der *vSphere Security Configuration Guide* nicht für die Verwendung als Sicherheitscheckliste vorgesehen. Beim Thema Sicherheit muss man immer einen Kompromiss eingehen. Bei der Umsetzung von Sicherheitskontrollen kann sich dies negativ auf Benutzerfreundlichkeit, Leistung oder andere operative Aufgaben auswirken. Berücksichtigen Sie Ihre Arbeitslasten, Nutzungsmuster, die Organisationsstruktur usw. sorgfältig, bevor Sie Sicherheitsänderungen vornehmen, unabhängig davon, ob der Hinweis von VMware oder aus anderen Branchenquellen stammt. Wenn Ihre Organisation regulatorischen Konformitätsanforderungen unterliegt, lesen Sie Sicherheit vs. Übereinstimmung in der vSphere-Umgebung oder besuchen Sie https://core.vmware.com/compliance. Diese Site enthält Compliance Kits und Produktüberwachungshandbücher, die vSphere-Administratoren und regulatorische Auditoren dabei unterstützen, die virtuelle Infrastruktur für regulatorische Frameworks zu sichern und zu bestätigen, wie z. B. NIST 800-53v4, NIST 800-171, PCI DSS, HIPAA, CJIS, ISO 27001 und mehr.

Folgende Punkte werden im *vSphere Security Configuration Guide* nicht behandelt:

- Software, die innerhalb der virtuellen Maschine ausgeführt wird, wie z. B. das Gastbetriebssystem und Anwendungen
- Datenverkehr über Netzwerke der virtuellen Maschinen
- Sicherheit der Add-on-Produkte

Der *vSphere Security Configuration Guide* ist nicht dazu gedacht, als „Übereinstimmungs“-Tool verwendet zu werden. Der *vSphere Security Configuration Guide* unterstützt Sie bei den ersten Schritten auf dem Weg zur Übereinstimmung, stellt aber für sich allein nicht sicher, dass Ihre Bereitstellung Übereinstimmung aufweist. Weitere Informationen zur Übereinstimmung finden Sie unter Sicherheit vs. Übereinstimmung in der vSphere-Umgebung.

Lesen des vSphere Security Configuration Guide

Der *vSphere Security Configuration Guide* ist ein Tabellenkalkulationsblatt, das sicherheitsbezogene Richtlinien enthält, welche Sie bei der Änderung Ihrer vSphere-Sicherheitskonfiguration unterstützen. Diese Richtlinien sind in Registerkarten basierend auf den betroffenen Komponenten gruppiert, mit einigen oder allen der folgenden Spalten.

Tabelle 17-2. Spalten des vSphere Security Configuration Guide in Tabellenkalkulationsformat

Spaltenüberschrift	Beschreibung
Leitlinien-ID	Eine eindeutige zweiteilige ID, die eine Sicherheitskonfigurations- oder Hardening-Empfehlung bezeichnet. Der erste Teil gibt die Komponente an und ist wie folgt definiert: ■ ESXi: ESXi-Hosts ■ VM: virtuelle Maschinen ■ vNetwork: virtuelle Switches
Beschreibung	Eine kurze Erklärung der jeweiligen Empfehlung.

Tabelle 17-2. Spalten des vSphere Security Configuration Guide in Tabellenkalkulationsformat (Fortsetzung)

Spaltenüberschrift	Beschreibung
Diskussion	Beschreibung der Schwachstelle, auf die sich eine bestimmte Empfehlung bezieht.
Konfigurationsparameter	Stellt die anwendbaren Konfigurationsparameter oder Dateinamen bereit, sofern vorhanden.
Gewünschter Wert	Der gewünschten Zustand oder Wert der Empfehlung. Mögliche Werte: ■ Nicht verfügbar ■ Standortspezifisch ■ Falsch ■ True ■ Aktiviert ■ Deaktiviert ■ Nicht vorhanden oder falsch
Standardwert	Der von vSphere festgelegte Standardwert.
Ist der gewünschte Wert der Standard?	Gibt an, ob die Sicherheitseinstellung der Produkt-Standardkonfiguration entspricht.
Aktion erforderlich	Der Typ der Aktion, die bei einer bestimmten Empfehlung durchzuführen ist. Zu den Aktionen zählen: ■ Update ■ Nur Überwachung ■ Ändern ■ Hinzufügen ■ Entfernen
Festlegen des Standorts in vSphere Client	Schritte für die Prüfung des Werts mithilfe von vSphere Client
Negative funktionale Auswirkung bei der Änderung von Standard?	Beschreibung möglicher negativer Auswirkungen der Anwendung der Sicherheitsempfehlung.
PowerCLI-Befehlsbeurteilung	Schritte für die Prüfung des Werts mithilfe von PowerCLI.
Beispiel für PowerCLI-Befehlsstandardisierung	Schritte zum Einrichten (Standardisieren) des Werts mithilfe von PowerCLI.
vCLI-Befehlsstandardisierung	Schritte zum Einrichten (Standardisieren) des Werts mithilfe der vCLI-Befehle.
PowerCLI-Befehlsbeurteilung	Schritte für die Prüfung des Werts mithilfe der PowerCLI-Befehle.
PowerCLI-Befehlsstandardisierung	Schritte zum Einrichten (Standardisieren) des Werts mithilfe der PowerCLI-Befehle.
Kann mithilfe des Hostprofils eingerichtet werden	Gibt an, ob die Einstellung anhand der Hostprofile erreicht werden kann (gilt nur für ESXi-Richtlinien).
Absichern	Bei TRUE ist für die Richtlinie nur eine Implementierung möglich, um Übereinstimmung aufzuweisen. Bei FALSE kann die Leitlinienimplementierung durch mehr als eine Konfigurationseinstellung erfolgen. Die tatsächliche Einstellung ist häufig standortspezifisch.

Tabelle 17-2. Spalten des vSphere Security Configuration Guide in Tabellenkalkulationsformat (Fortsetzung)

Spaltenüberschrift	Beschreibung
Standortsspezifische Einstellung	Bei TRUE hängt die Übereinstimmung der Einstellung mit der Richtlinie von Regeln oder Standards ab, die für diese vSphere-Bereitstellung spezifisch sind.
Überwachungseinstellung	Bei TRUE muss der Wert der aufgelisteten Einstellung möglicherweise geändert werden, um standortspezifische Regeln zu erfüllen.

Hinweis Diese Spalten können im Lauf der Zeit nach Bedarf geändert werden. Zu neu hinzugefügten Spalten zählen beispielsweise die Spalten „DISA STIG ID“, „Absichern“ und „Standortspezifisch“. Prüfen Sie auf https://blogs.vmware.com, ob Ankündigungen zu Updates des *vSphere-Handbuchs zur sicheren Konfiguration* vorhanden sind.

Wenden Sie die Richtlinien im *vSphere-Handbuch zur sicheren Konfiguration* nicht unüberlegt auf Ihre Umgebung an. Nehmen Sie sich die Zeit, jede Einstellung zu bewerten und eine informierte Entscheidung zu treffen, ob Sie sie anwenden möchten. Als Minimum können Sie die Anweisungen in den Beurteilungsspalten nutzen, um die Sicherheit Ihrer Bereitstellung zu überprüfen.

Das *vSphere-Handbuch zur sicheren Konfiguration* ist eine Hilfestellung für die ersten Schritte bei der Übereinstimmungsimplementierung in Ihrer Bereitstellung. Wenn Sie ihn zusammen mit den Richtlinien der Defense Information Systems Agency (DISA) und anderen Übereinstimmungsrichtlinien verwenden, können Sie mithilfe des *vSphere-Handbuchs zur sicheren Konfiguration* vSphere-Sicherheitskontrollen an den Übereinstimmungsanforderungen jeder Richtlinie ausrichten.

Informationen zum National Institute of Standards and Technology

Das National Institute of Standards and Technology (Nationales Institut für Standards und Technologie, NIST) ist eine nicht regulatorische Regierungsbehörde, die Technologien, Metriken, Standards und Richtlinien entwickelt. Die Übereinstimmung mit NIST-Standards und -Richtlinien hat in vielen Branchen heute oberste Priorität.

Das National Institute of Standards and Technology (Nationale Institut für Standards und Technologie, NIST) wurde 1901 begründet und ist nun Teil des US-Handelsministeriums. Das NIST ist eines der ältesten naturwissenschaftlichen Laboratorien der Vereinigten Staaten. Heute werden NIST-Messungen für die Unterstützung von Technologien ganz unterschiedlicher Größenordnungen eingesetzt: von nanoskaligen Geräten bis hin zu erdbebensicheren Wolkenkratzern und globalen Kommunikationsnetzen.

Der Federal Information Security Management Act (FISMA) ist ein 2002 verabschiedetes Bundesgesetz der Vereinigten Staaten, das es den Bundesbehörden zur Auflage machte, ein Programm für Informationssicherheit und -schutz zu entwickeln, zu dokumentieren und umzusetzen. Das NIST spielt eine wichtige Rolle bei der FISMA-Implementierung, indem wichtige Sicherheitsstandards und -richtlinien (z. B. FIPS 199, FIPS-200 und SP-800-Serie) entwickelt werden.

Regierung und private Organisationen verwenden NIST 800-53, um Informationssysteme zu sichern. Cybersicherheits- und Datenschutzkontrollen sind unerlässlich, um Unternehmensabläufe (einschließlich Auftrag, Funktionen, Image und Reputation), Unternehmenswerte und Einzelpersonen vor einer Vielzahl von Bedrohungen zu schützen. Zu diesen Bedrohungen gehören feindliche Cyberangriffe, Naturkatastrophen, strukturelle Ausfälle und menschliche Fehler. VMware hat einen externen Prüfungspartner beauftragt, um VMware-Produkte und -Lösungen anhand des in NIST 800-53 aufgeführten Katalogs an Kontrollen zu bewerten. Weitere Informationen finden Sie auf der NIST-Webseite unter https://www.nist.gov/cyberframework.

Informationen zu DISA STIGs

Die Defense Information Systems Agency (DISA) erstellt und veröffentlicht Security Technical Implementation Guides (STIGs). DISA STIGs enthalten technische Anleitungen für das Absichern von Systemen und die Reduzierung von Bedrohungen.

Die Defense Information Systems Agency (DISA) ist die Kampfunterstützungsagentur des US-Verteidigungsministeriums (DoD), die für die Aufrechterhaltung des Sicherheitsstatus des DOD Information Network (DODIN) verantwortlich ist. DISA setzt unter anderem folgende Methode ein, um diese Aufgabe auszuführen: Entwicklung, Verbreitung und Beauftragung der Implementierung von Security Technical Implementation Guides (STIGs). Kurz gesagt: STIGs sind portierbare, standardbasierte Handbücher für Hardening-Systeme. STIGs sind für US-DoD-IT-Systeme obligatorisch und bieten somit eine geprüfte, sichere Grundlage für Nicht-DoD-Einheiten, anhand derer sie ihren Sicherheitsstatus messen können.

Auf der Grundlage von DISA-Protokollen und Feedback übermitteln Anbieter wie VMware Vorschläge für Security Hardening-Anleitungen zur Evaluierung an DISA. Sobald dieser Vorgang abgeschlossen ist, wird das offizielle STIG auf der Website der DISA-Organisation unter https://public.cyber.mil/stigs/ veröffentlicht. VMware enthält sicherheitsbasierte Baselines und Hardening-Anleitungen für vSphere im *vSphere Security Configuration Guide*. Weitere Informationen finden Sie unter https://core.vmware.com/security.

Informationen zu VMware Security Development Lifecycle

Das VMware Security Development Lifecycle (SDL)-Programm identifiziert und mindert Sicherheitsrisiken während der Entwicklungsphase von VMware-Softwareprodukten. VMware betreibt auch das VMware Security Response Center (VSRC), um die Analyse und Behebung von Software-Sicherheitsproblemen in VMware-Produkten durchzuführen.

Unter SDL versteht man die Softwareentwicklungsmethodik, die die Gruppe „VMware Security Engineering, Communication, and Response“ (vSECR) sowie VMware-Produktentwicklungsgruppen einsetzen, um Sicherheitsprobleme zu identifizieren und zu minimieren. Weitere Informationen zum VMware Security Development Lifecycle erhalten Sie auf der Webseite unter https://www.vmware.com/security/sdl.html.

Das VSRC arbeitet mit Kunden und der Sicherheitsforschungs-Community zusammen, um folgende Ziele zu erreichen: Behandlung von Sicherheitsproblemen und rechtzeitige Bereitstellung umsetzbarer Sicherheitsinformationen für Kunden. Weitere Informationen zum VMware Security Response Center erhalten Sie auf der Webseite unter https://www.vmware.com/security/vsrc.html.

Überwachungsprotokollierung

Die Überwachungsprotokollierung von Netzwerkdatenverkehr, Compliance-Warnungen, Firewall-Aktivitäten, Betriebssystemänderungen und Provisioning-Aktivitäten gilt als Best Practice für die Aufrechterhaltung der Sicherheit in jeder IT-Umgebung. Darüber hinaus ist die Protokollierung eine spezifische Anforderung im Rahmen vieler Bestimmungen und Standards.

Einer der ersten Schritte, um sicherzustellen, dass Sie sich der Änderungen an Ihrer Infrastruktur bewusst sind, ist die Überwachung Ihrer Umgebung. Standardmäßig umfasst vSphere Tools, mit denen Sie Änderungen anzeigen und verfolgen können. Beispielsweise können Sie über die Registerkarte „Aufgaben und Ereignisse“ im vSphere Client auf einem beliebigen Objekt in Ihrer vSphere-Hierarchie sehen, welche Änderungen vorgenommen wurden. Sie können PowerCLI auch verwenden, um Ereignisse und Aufgaben abzurufen. Darüber hinaus bietet vRealize Log Insight Überwachungsprotokollierung zur Unterstützung der Erfassung und Aufbewahrung wichtiger Systemereignisse. Darüber hinaus stehen viele Drittanbieter-Tools zur Verfügung, die die Überwachung von vCenter bereitstellen.

Protokolldateien können einen Überwachungspfad bereitstellen, um festzustellen, wer oder was auf einen Host, eine virtuelle Maschine usw. zugreift. Weitere Informationen finden Sie unter Speicherorte der ESXi-Protokolldateien.

Single Sign-On-Audit-Ereignisse

Single Sign-On (SSO)-Überwachungsereignisse sind Aufzeichnungen von Benutzer- oder Systemaktionen für den Zugriff auf die SSO-Dienste.

In vCenter Server 6.7 Update 2 und höher wurde die VMware vCenter Single Sign-On-Überwachung verbessert, indem Ereignisse für die folgenden Vorgänge hinzugefügt wurden:

- Benutzerverwaltung
- Anmelden
- Gruppenerstellung
- Identitätsquelle
- Richtlinienaktualisierungen

Die unterstützten Identitätsquellen sind vsphere.local, integrierte Windows-Authentifizierung (IWA) und Active Directory über LDAP.

Wenn ein Benutzer sich bei vCenter Server über Single Sign-On anmeldet oder Änderungen vornimmt, die SSO betreffen, werden die folgenden Überwachungsereignisse in die SSO-Überwachungsprotokolldatei geschrieben:

- **Anmeldungs- und Abmeldungsversuche:** Ereignisse für alle erfolgreichen und fehlgeschlagenen Anmeldungs- und Abmeldungsvorgänge.
- **Berechtigungsänderung:** Ereignis für eine Änderung an einer Benutzerrolle oder Berechtigungen.
- **Kontoänderung:** Ereignis für die Änderung an den Benutzerkontoinformationen, z. B. Benutzername, Kennwort oder zusätzliche Kontoinformationen.
- **Sicherheitsänderung:** Ereignis für eine Änderung an einer Konfiguration, einem Parameter oder einer Richtlinie im Zusammenhang mit der Sicherheit.
- **Konto aktiviert oder deaktiviert:** Ereignis, wenn ein Konto aktiviert oder deaktiviert wird.
- **Identitätsquelle:** Ereignis für das Hinzufügen, Löschen oder Bearbeiten einer Identitätsquelle.

Im vSphere Client werden Ereignisdaten auf der Registerkarte **Überwachen** angezeigt. Informationen finden Sie in der Dokumentation *vSphere-Überwachung und -Leistung*.

SSO-Überwachungsereignisdaten enthalten die folgenden Details:

- Zeitpunkt, zu dem das Ereignis stattfand.
- Benutzer, der die Aktion durchgeführt hat.
- Beschreibung des Ereignisses.
- Schweregrad des Ereignisses.
- IP-Adresse des Clients, der für die Verbindung zum vCenter Server verwendet wurde, falls verfügbar.

Übersicht über das SSO-Überwachungsereignisprotokoll

Der vSphere Single Sign-On-Vorgang schreibt Überwachungsereignisse in die Datei `audit_events.log` im Verzeichnis `/var/log/audit/sso-events/`,

Vorsicht Bearbeiten Sie die Datei `audit_events.log` nie manuell, da damit die Überwachungsprotokollierung fehlschlagen könnte.

Beachten Sie Folgendes bei der Arbeit mit der Datei `audit_events.log`:

- Die Protokolldatei wird archiviert, sobald sie 50 MB erreicht.
- Es werden maximal 10 Archivdateien aufbewahrt. Wenn die maximale Anzahl erreicht ist, wird die älteste Datei entfernt, wenn ein neues Archiv erstellt wird.

- Die Archivdateien werden mit dem Namen `audit_events-<index>.log.gz` benannt, wobei „index“ eine Zahl zwischen 1 und 10 ist. Das erste erstellte Archiv ist „index 1“, und die Zahl wird mit jedem nachfolgenden Archiv erhöht.
- Die ältesten Ereignisse befinden sich im Archiv „index 1“. Die Datei mit der höchsten Indexnummer ist das neueste Archiv.

Grundlegendes zur Sicherheit und Übereinstimmung – nächste Schritte

Das Durchführen einer Sicherheitsbeurteilung ist der erste Schritt zum Verständnis von Schwachstellen in Ihrer Infrastruktur. Eine Sicherheitsbeurteilung ist Teil einer Sicherheitsüberwachung, bei dem sowohl Systeme als auch Praktiken geprüft werden, einschließlich der Sicherheitsübereinstimmung.

Eine Sicherheitsbeurteilung besteht im Allgemeinen aus einer Überprüfung der physischen Infrastruktur Ihres Unternehmens (Firewalls, Netzwerke, Hardware usw.), um Sicherheitsrisiken und Schwachstellen zu identifizieren. Eine Sicherheitsbeurteilung ist nicht das Gleiche wie eine Sicherheitsüberwachung. Eine Sicherheitsüberwachung umfasst nicht nur eine Überprüfung der physischen Infrastruktur, sondern auch die Prüfung anderer Bereiche wie Richtlinien und Standardverfahren, einschließlich der Sicherheitsübereinstimmung. Nach der Überwachung können Sie über die Schritte entscheiden, mit denen Sie die Probleme innerhalb des Systems beheben.

Stellen Sie sich bei der Vorbereitung einer Sicherheitsüberwachung die folgenden allgemeinen Fragen:

1. Ist für unsere Organisation die Einhaltung bestimmter Übereinstimmungsvorschriften vorgeschrieben? Wenn ja, welche?
2. Wie lang ist unser Überwachungsintervall?
3. Wie lang ist unser internes Selbsteinschätzungsintervall?
4. Haben wir Zugang zu früheren Überwachungsergebnissen, und haben wir diese geprüft?
5. Unterstützt uns eine externe Prüffirma bei der Vorbereitung der Überwachung? Falls ja, inwieweit ist diese Firma mit Virtualisierung vertraut?
6. Führen wir Schwachstellenscans für die Systeme und Anwendungen durch? Wann und wie oft?
7. Worin bestehen unsere internen Cybersicherheitsrichtlinien?
8. Ist Ihre Überwachungsprotokollierung entsprechend Ihren Bedürfnissen konfiguriert? Weitere Informationen hierzu finden Sie unter Überwachungsprotokollierung.

Wenn keine spezifischen Hilfestellungen oder Leitlinien dazu vorliegen, wo Sie anfangen sollten, können Sie Ihre vSphere-Umgebung wie folgt direkt sichern:

- Halten Sie Ihre Umgebung mit den neuesten Software- und Firmware-Patches aktualisiert

- Pflegen Sie eine angemessene Kennwortverwaltung und Hygiene für alle Konten
- Gehen Sie die vom Anbieter genehmigten Sicherheitsempfehlungen durch
- Sehen Sie die VMware Security Configuration Guides ein (siehe Grundlegendes zum vSphere Security Configuration Guide)
- Nutzen Sie die überall bereitgestellten und bewährten Leitlinien von Richtlinienrahmen wie NIST, ISO usw.
- Folgen Sie den Leitlinien aus regulatorischen Übereinstimmungsrahmenwerken wie PCI, DISA und FedRAMP

vCenter Server und FIPS

In vSphere 7.0 Update 2 und höher können Sie FIPS-validierte Kryptografie für die vCenter Server Appliance aktivieren.

FIPS 140-2 ist ein US- und kanadischer Behördenstandard, der Sicherheitsanforderungen für kryptografische Module spezifiziert. vSphere verwendet FIPS-validierte kryptografische Module, die mit denen durch den FIPS 140-2-Standard angegebenen übereinstimmen. Mit einer vSphere FIPS-Unterstützung sollen Konformitäts- und Sicherheitsaktivitäten in verschiedenen regulierten Umgebungen erleichtert werden.

In vSphere 6.7 und höher verwenden ESXi und der vCenter Server FIPS-validierte Kryptografie, um Verwaltungsschnittstellen und die VMware Certificate Authority (VMCA) zu schützen.

Ab vSphere 7.0 Update 2 wird die vCenter Server Appliance durch zusätzliche FIPS-validierte Kryptografie erweitert. Standardmäßig ist diese FIPS-Validierungsoption deaktiviert.

Hinweis vSphere bevorzugt die Kompatibilität gegenüber FIPS, daher müssen einige Komponenten berücksichtigt werden. Weitere Informationen hierzu finden Sie unter Überlegungen bei der Verwendung von FIPS.

FIPS-Module

Ein kryptografisches Modul ist ein Satz von Hardware, Software oder Firmware, die Sicherheitsfunktionen implementiert. ESXi verwendet mehrere FIPS 140-2-validierte kryptografische Module.

Die folgende Tabelle zeigt den Satz von FIPS 140-2-validierten kryptografischen Modulen, die von ESXi verwendet werden.

Tabelle 17-3. FIPS-Module

Kryptografisches Modul	Version der Sicherheitsrichtlinie	Algorithmen (CAVP)	Cryptographic Module Validation Program
Kryptografisches VMkernel-Modul	1.0	AES, SHS, DRBG, HMAC (C 1172)	Zertifikat #3073
VMkernel Cryptographic Module Loader	Nicht anwendbar	HMAC, SHS (C 1171)	Zertifikat #3073
Kryptografisches VMkernel-DRBG-Modul	Nicht anwendbar	AES, DRBG (C 499)	–
VMware OpenSSL FIPS Object Module	2.0.20-vmw	DRBG, AES, SHS, HMAC, DSA, RSA, ECDSA, KAS-FFC, KAS-ECC (C 470)	Zertifikat #3550 und #3857

Aktivieren und Deaktivieren von FIPS auf der vCenter Server Appliance

Sie können validierte FIPS-Kryptographie mithilfe von HTTPS-Anforderungen auf der vCenter Server Appliance aktivieren oder deaktivieren.

Zur Ausführung von HTTP-Anforderungen stehen mehrere Möglichkeiten zur Verfügung. Diese Aufgabe zeigt die Verwendung des Developer Center im vSphere Client zum Aktivieren und Deaktivieren von FIPS auf der vCenter Server Appliance. Im *VMware vCenter Server Management-Programmierhandbuch* finden Sie weitere Informationen zur Verwendung von APIs zum Arbeiten mit der vCenter Server Appliance.

Verfahren

1. Melden Sie sich mit dem vSphere Client beim vCenter Server-System an.
2. Wählen Sie im Menü die Option **Developer Center** aus.
3. Klicken Sie auf **API-Explorer**.
4. Wählen Sie im Dropdown-Menü **API auswählen** die Option **Appliance** aus.
5. Führen Sie einen Bildlauf nach unten durch die Kategorien durch und erweitern Sie **system/security/global_fips**.
6. Erweitern Sie **GET** und klicken Sie auf **Ausführen** unter **Ausprobieren**.

   Sie können die aktuelle Einstellung unter **Antwort** anzeigen.

7 Ändern Sie die Einstellung.

a Zum Aktivieren von FIPS erweitern Sie **PUT**, geben Folgendes in `request_body` ein und klicken auf **Ausführen**.

```
{
"enabled":true
}
```

b Zum Deaktivieren von FIPS erweitern Sie **PUT**, geben Folgendes in `request_body` ein und klicken auf **Ausführen**.

```
{
"enabled":false
}
```

Ergebnisse

Die vCenter Server Appliance wird nach dem Aktivieren oder Deaktivieren von FIPS neu gestartet.

Überlegungen bei der Verwendung von FIPS

Beim Aktivieren von FIPS auf der vCenter Server Appliance weisen bestimmte Komponenten derzeit funktionale Einschränkungen auf.

Nach der Aktivierung von FIPS auf dem vCenter Server sollten keine Unterschiede feststellbar sein. Es gibt jedoch einige Überlegungen, die zu berücksichtigen sind.

Tabelle 17-4. Überlegungen zu FIPS

Produkt oder Komponente	Überlegungen	Problemumgehung:
vSphere Single Sign-On	Wenn Sie FIPS aktivieren, unterstützt vCenter Server nur kryptografische Module für die Verbundauthentifizierung. Folglich funktionieren RSA SecureID und bestimmte CAC-Karten nicht mehr.	Verwenden Sie Verbundauthentifizierung. Details finden Sie in der Dokumentation zur *vSphere-Authentifizierung*.
Nicht-VMware-Plug-Ins und Plug-Ins der vSphere Client-Partner-Benutzeroberfläche	Diese Plug-Ins funktionieren möglicherweise nicht mit aktiviertem FIPS.	Führen Sie ein Upgrade der Plug-Ins durch, um konforme Verschlüsselungsbibliotheken zu verwenden. Weitere Informationen finden Sie unter „Vorbereiten lokaler Plug-Ins für FIPS-Konformität“ unter https://code.vmware.com/docs/13385/preparing-local-plug-ins-for-fips-compliance.
Dateibasierter Sicherungs- und Wiederherstellungsmechanismus von vCenter Server	Die dateibasierte Sicherung und Wiederherstellung mit SMB ist nicht FIPS-konform.	Verwenden Sie ein anderes Protokoll für die Sicherung und Wiederherstellung (FTP, FTPS, HTTP, HTTPS, SFTP oder NFS).