vSphere-Sicherheit

Update 2
Geändert am 27. APR. 2022
VMware vSphere 6.5
VMware ESXi 6.5
vCenter Server 6.5

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.

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.
Verschlüsselung virtueller Maschinen	■ Wie funktioniert VM-Verschlüsselung? ■ KMS-Einrichtung. ■ Verschlüsseln und Entschlüsseln von VMs. ■ Fehlerbehebung und Best Practices.
Verwalten der Konfiguration des TLS-Protokolls	Ändern der Konfiguration des TLS-Protokolls mithilfe eines Befehlszeilen-Dienstprogramms.
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 dem Begleitdokument *Platform Services Controller-Verwaltung* wird erläutert, wie Sie mit den Platform Services Controller-Diensten beispielsweise die Authentifizierung mit vCenter Single Sign-On sowie Zertifikate in Ihrer vSphere-Umgebung verwalten können.

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

Zielgruppe

Diese Informationen sind für erfahrene Systemadministratoren bestimmt, die mit der Windows- oder Linux-VM-Technologie und Datencenteroperationen vertraut sind.

vSphere Web Client und vSphere Client (HTML 5-Client)

Die Anweisungen für Aufgaben in diesem Handbuch basieren auf dem vSphere Web Client. Die meisten Aufgaben in diesem Handbuch lassen sich auch mit dem neuen vSphere Client ausführen. Die neue Terminologie, Topologie und der neue Workflow der vSphere Client-Benutzeroberfläche sind eng an denselben Aspekten und Elementen der vSphere Web Client-Benutzeroberfläche ausgerichtet. Sofern nicht anders angegeben, können Sie die Anweisungen zu vSphere Web Client auf den neuen vSphere Client anwenden.

Hinweis Nicht alle Funktionen im vSphere Web Client wurden für den vSphere Client in der Version vSphere 6.5 implementiert. Eine aktuelle Liste nicht unterstützter Funktionen finden Sie im *Handbuch für Funktions-Updates für den vSphere Client* unter http://www.vmware.com/info?id=1413.

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
27. APR 2022	■ Geringfügiges Update für Storage Views Privileges.
25. MRZ 2022	■ Die Tabelleninformationen wurden aus Ein- und ausgehende Firewall-Ports für ESXi-Hosts, Erforderliche Ports für vCenter Server und Platform Services Controller und Ports, die die Deaktivierung von TLS-Versionen unterstützen entfernt. Weitere Informationen finden Sie im Tool VMware Ports and Protocols™ unter https://ports.vmware.com/. Im Rahmen des Übergangs aller Portinformationen zum Tool Ports und Protocols wurde das Thema „Zusätzliche TCP- und UDP-Ports für vCenter Server“ ebenfalls entfernt. ■ Unter Empfohlene Vorgehensweisen für die Sicherheit von vCenter Server Appliance wurden neue Informationen hinzugefügt.
27. OKT. 2021	■ Geringfügiges Update für Verwenden des vSphere Authentication Proxy zum Hinzufügen eines Hosts zu einer Domäne. ■ Fester Befehl in Sicherstellen einer korrekten SNMP-Konfiguration. ■ Es wurden Befehle zum Anzeigen der aktuellen TLS-Einstellungen in Deaktivieren von TLS-Versionen auf ESXi-Hosts hinzugefügt. ■ Geringfügiges Update für Zurücksetzen von TLS-Konfigurationsänderungen.
14. August 2020	Wir bei VMware legen Wert auf die Verwendung neutraler Sprache. Um dieses Prinzip in unserer Kunden-, Partner- und internen Community zu fördern, ersetzen einen Teil der Terminologie in unseren Inhalten. Wir haben diesen Leitfaden aktualisiert, um Instanzen einer nicht inklusiven Sprache zu entfernen.
26. Juni 2020	■ Geringfügige Updates für Ersetzen von ESXi SSL-Zertifikaten und -Schlüsseln. ■ Ports, die die Deaktivierung von TLS-Versionen unterstützen wurde aktualisiert, um zu verdeutlichen, dass Sie nur eine TLS 1.2-Verbindung zu einer externen Microsoft SQL Server-Datenbank verwenden können. ■ Eine Beschreibung für **Virtuelle Maschine.Konfiguration.Verzweigtes übergeordnetes Element umschalten** wurde in Berechtigungen für das Konfigurieren virtueller Maschinen hinzugefügt. ■ Geringfügiges Update für Verwenden der Benutzerschnittstelle der direkten Konsole (DCUI) für den Zugriff auf die ESXi Shell .
29. August 2019	■ Es wurden Schritte in Synchronisieren der ESXi-Systemuhren mit einem NTP-Server korrigiert. ■ Es wurden kleinere Änderungen an Erforderliche Ports für vCenter Server und Platform Services Controller vorgenommen. ■ Es wurden kleinere Änderungen an Rechte für die Dienstkonfiguration der virtuellen Maschine vorgenommen.

Revision	Beschreibung
16. April 2019	■ Es wurden kleinere Änderungen an Verschlüsseln einer bestehenden virtuellen Maschine oder virtuellen Festplatte vorgenommen. ■ Es wurden Querverweise zu Verschlüsseln von virtuellen Festplatten hinzugefügt. ■ Informationen zum WSManagement-Dienst wurden im Abschnitt Steuern des Zugriffs für CIM-basierte Hardwareüberwachungstools hinzugefügt. ■ Die Schritte im Abschnitt Aktualisieren des vCenter Server-Speichers TRUSTED_ROOTS (Benutzerdefinierte Zertifikate) wurden korrigiert.
26. FEBR. 2019	■ Die Beschreibung „Verwendet für die Kommunikation zwischen Knoten“ für TCP-Port 7444 wurde im Abschnitt Erforderliche Ports für vCenter Server und Platform Services Controller korrigiert.
14. JAN 2019	■ Die maximale Anzahl an Fehlversuchen, bevor das Konto gesperrt wird und wenn das Konto entsperrt wird, wurde im Abschnitt Kennwörter und Kontosperrung für ESXi korrigiert. ■ Informationen zum Aktivieren des CIM-Diensts wurden im Abschnitt Steuern des Zugriffs für CIM-basierte Hardwareüberwachungstools hinzugefügt. ■ Informationen zum Herunterladen des Zertifikats vom vCenter Server wurden im Abschnitt Importieren des vSphere Authentication Proxy-Zertifikats in den ESXi-Host hinzugefügt. ■ Das Konfigurationsdateibeispiel wurde im Abschnitt Einrichten von vSphere Authentication Proxy für die Verwendung von benutzerdefinierten Zertifikaten korrigiert.
09. Nov. 2018	■ Der Speicherort des Skripts `camconfig` für Windows vCenter Server wurde im Abschnitt Aktivieren der Client-Authentifizierung für vSphere Authentication Proxy korrigiert. ■ Informationen über den TRUSTED_ROOTS-Speicher in der Verwenden benutzerdefinierter Zertifikate mit Auto Deploy wurden aktualisiert. ■ Aktivieren von Smartcard-Authentifizierung wurde aktualisiert, um zu verdeutlichen, dass die Zertifikate im PEM-Format vorliegen müssen. ■ Informationen über Verschlüsselungsrechte im Abschnitt Voraussetzungen und erforderliche Berechtigungen für die Verschlüsselung wurden aktualisiert, um zu verdeutlichen, was beim Erstellen einer virtuellen Maschine geschieht. ■ Das Verfahren zur Verwendung von vSphere Web Client wurde im Abschnitt Ändern des Zertifikatmodus aktualisiert. ■ Informationen zum Erstellen eines Benutzers für CIM-Anwendungen wurden im Abschnitt Steuern des Zugriffs für CIM-basierte Hardwareüberwachungstools aktualisiert.
22. Juni 2018	■ Informationen zum Hostverschlüsselungsmodus wurden im Abschnitt Hostverschlüsselungsmodus hinzugefügt. ■ Informationen zum erfolgreichen Sicherungsbeispiel wurden im Abschnitt Führen Sie eine optionale manuelle Sicherung durch aktualisiert. ■ Es wurde Text im Abschnitt Absichern des ESXi-Hypervisors hinzugefügt, der darüber informiert, dass Sie die Authentifizierung mit Benutzername und Kennwort und die Smartcard-Authentifizierung gleichzeitig konfigurieren können. ■ Informationen zum Neukonfigurieren eines eigenständigen ESXi-Hosts wurden im Abschnitt Deaktivieren von TLS-Versionen auf ESXi-Hosts hinzugefügt.
15. Juni 2018	■ Es wurden Schritte im Abschnitt Deaktivieren von TLS-Versionen auf ESXi-Hosts korrigiert. Sie müssen sich beim vCenter Server-System anmelden.

Revision	Beschreibung
05. Juni 2018	■ Die Portinformationen für den vSphere Authentication Proxy wurden im Abschnitt Erforderliche Ports für vCenter Server und Platform Services Controller aktualisiert. ■ Ein Link wurde in den Abschnitten Hinzufügen eines Hosts zu einer Verzeichnisdienst-Domäne, Anzeigen der Verzeichnisdiensteinstellungen und Konfigurieren eines Hosts für die Verwendung von Active Directory hinzugefügt, um weitere Informationen zum Zuweisen von Berechtigungen zu Benutzern und Gruppen aus einer hinzugefügten Active Directory-Domäne zu erhalten. ■ Im Abschnitt Aktivieren oder Deaktivieren von UEFI Secure Boot für eine virtuelle Maschine wurde PowerCLI-Beispielcode und ein aktualisierter Hinweis zum Upgrade einer virtuellen Maschine hinzugefügt, die BIOS auf EFI verwendet. ■ Es wurde ein Link zur VMware vSphere Central-Site im Abschnitt Tabelle 1-2. Sicherheitsressourcen von VMware im Internet hinzugefügt. ■ Informationen zu vMotion sowie zu verschlüsselten und unverschlüsselten virtuellen Maschinen wurden im Abschnitt Verschlüsseltes vSphere vMotion hinzugefügt. ■ Es wurde ein Link für weitere Informationen zum Zuweisen von Berechtigungen zu einem Benutzer für einen ESXi-Host im Abschnitt Rechte für Root-Benutzer hinzugefügt. ■ Im Abschnitt Sichern von vSphere Distributed Switches und verteilten Portgruppen wurde Text hinzugefügt, der darüber informiert, dass für VLANs in einem vSphere Distributed Switch dieselben Regeln wie in einem Standard-Switch gelten. ■ Der Name des *Hardening Guide*, der jetzt als *Security Configuration Guide* bezeichnet wird, wurde im Abschnitt Verwandte Dokumentation aktualisiert. ■ Im Abschnitt Hinzufügen von zulässigen IP-Adressen für einen ESXi-Host wurden Informationen über die Verwendung des vCLI-Befehls hinzugefügt. ■ Ein Link zum VMware-Knowledgebase-Artikel 2008226 wurde im Abschnitt ESXi ESXCLI-Firewall-Befehle hinzugefügt.
18. MAI 2018	■ Im Abschnitt Erforderliche Ports für vCenter Server und Platform Services Controller wurden die Hinweise für die Ports 80 und 443 aktualisiert.
3. Mai 2018	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 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 Web 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 vSphere* finden Sie Informationen zu vSphere Auto Deploy.

Verwenden des Sperrmodus

Im Sperrmodus kann auf ESXi-Hosts standardmäßig nur über vCenter Server zugegriffen werden. Ab vSphere 6.0 können Sie den strengen Sperrmodus oder den normalen Sperrmodus auswählen. Sie können Ausnahmen für Benutzer definieren, um den Direktzugriff auf Dienstkonten, wie beispielsweise Backup-Agents, 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

Ab vSphere 6.0 stellt die VMware Certificate Authority (VMCA) für jeden ESXi-Host ein signiertes Zertifikat bereit, dessen Rootzertifizierungsstelle standardmäßig die VMCA ist. Wenn es von einer Unternehmensrichtlinie verlangt wird, können Sie die vorhandenen Zertifikate durch Zertifikate ersetzen, die von einer Zertifizierungsstelle eines Drittanbieters oder eines Unternehmens signiert wurden.

Siehe Zertifikatsverwaltung für ESXi-Hosts.

Smartcard-Authentifizierung in Betracht ziehen

Ab vSphere 6.0 unterstützt ESXi die Verwendung der Smartcard-Authentifizierung anstelle der Authentifizierung mit dem Benutzernamen und dem 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

Ab vSphere 6.0 wird das Sperren von Konten für den Zugriff über SSH und über das vSphere Web Services SDK 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 dieses Standardverhalten ändern und zusätzliche Maßnahmen zum Schutz Ihrer Umgebung ergreifen.

Denken Sie beim Schutz Ihrer vSphere-Umgebung daran, dass alle mit den vCenter Server-Instanzen verbundenen Dienste geschützt werden müssen. In manchen Umgebungen kann es erforderlich sein, mehrere vCenter Server-Instanzen und eine oder mehrere Platform Services Controller-Instanzen zu schützen.

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, alle Maschinen in der Umgebung und alle Lösungsbenutzer mit einem von VMCA signierten Zertifikat aus. Die Umgebung funktioniert auf diese Weise ab Werk, aber Sie können dieses Standardverhalten an Ihre Unternehmensrichtlinien anpassen. Weitere Informationen finden Sie in der Dokumentation *Platform Services Controller-Verwaltung*.

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 weitere Identitätsquellen (entweder Active Directory oder LDAP) hinzufügen und eine Standardidentitätsquelle bestimmen. Ab diesem Zeitpunkt können Benutzer, die sich bei diesen Identitätsquellen authentifizieren können, auch Objekte anzeigen und Aufgaben ausführen, sofern sie die entsprechende Berechtigung besitzen. Weitere Informationen finden Sie in der Dokumentation *Platform Services Controller-Verwaltung*.

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 6.0 ist mit seinen unterschiedlichen Möglichkeiten der Benutzer- oder Gruppenautorisierung äußerst flexibel. Siehe 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.

Einrichten von NTP

Richten Sie 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 Ihren physischen Computer schützen würden. Deaktivieren Sie eventuell alle ungenutzten Funktionen, minimieren Sie die Nutzung der VM-Konsole 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 Remotekonsole.

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

Verwenden von Vorlagen und Verwaltung durch Skripts

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

Wenn Sie nach der Erstbereitstellung VM-Einstellungen 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 Maschinen in Ordnern gruppieren, um das Scripting zu erleichtern.

Weitere Informationen zu Vorlagen finden Sie unter Verwendung von Vorlagen zum Bereitstellen von virtuellen Maschinen und im Handbuch *Verwaltung virtueller vSphere-Maschinen*. 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 eine VM-Konsole haben Zugriff auf die Energieverwaltung der virtuellen Maschine und auf Konnektivitätssteuerelemente von Wechselmedien. Demzufolge kann eine VM-Konsole einen böswilligen Angriff auf eine virtuelle Maschine ermöglichen.

Verwenden Sie UEFI Secure Boot

Ab vSphere 6.5 können Sie für Ihre virtuelle Maschine 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.

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 8 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 Platform Services Controller- und 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 8 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, Programmdateien 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 vSphere Web 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).

Überlegen Sie auch, ob VMware NSX for vSphere eine gute Lösung zum Schutz der Netzwerkebene in Ihrer Umgebung darstellen könnte.

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-Kennwortbeschränkungen werden durch das Linux-PAM-Modul „pam_passwdqc“ bestimmt. Weitere Informationen zu `pam_passwdqc` finden Sie auf der Linux-manpage und lesen Sie auch 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 vCenter Single Sign On-Administrator lautet standardmäßig administrator@vsphere.local oder administrator@*meinedomäne*, falls Sie während der Installation eine andere Domäne angegeben haben. Dieses Kennwort läuft nicht ab. Ansonsten muss das Kennwort die in der vCenter Single Sign On-Kennwortrichtlinie festgelegten Beschränkungen einhalten. Weitere Informationen dazu finden Sie unter *Platform Services Controller-Verwaltung*.

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 *Platform Services Controller-Verwaltung*. 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 Standardidentitätsquelle. Benutzer können sich bei der entsprechenden Domäne mithilfe des vSphere Web Client und ihrer 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 Appliance

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

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

- Kennwort des Root-Benutzers des Linux-Betriebssystems der Appliance.
- Kennwort für den Administrator der vCenter Single Sign On-Domäne, standardmäßig administrator@vsphere.local.

Über die Konsole der Appliance können Sie das Kennwort des Root-Benutzers ändern und weitere Verwaltungsaufgaben für lokale Benutzer der vCenter Server Appliance ausführen. Siehe *vCenter Server Appliance-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://vspherecentral.vmware.com/t/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.

Tabelle 1-2. Sicherheitsressourcen von VMware im Internet (Fortsetzung)

Thema	Ressource
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	http://www.vmware.com/go/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://www.vmware.com/support/support-resources/hardening-guides.html
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 ein Benutzer überhaupt auf vSphere-Komponenten zugreifen 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. Den Schwerpunkt der Informationen in diesem Abschnitt bilden die Funktionsweise des vCenter Server-Berechtigungsmodells sowie die Vorgehensweise beim Durchführen von Benutzerverwaltungsaufgaben.

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.

Zunächst ist nur der Administrator der vCenter Single Sign-On-Domäne, standardmäßig „administrator@vsphere.local“, autorisiert, sich beim vCenter Server-System anzumelden. Dieser Benutzer kann dann folgende Schritte ausführen:

1. Hinzufügen einer Identitätsquelle, in der Benutzer und Gruppen für vCenter Single Sign On definiert sind. Informationen finden Sie in der Dokumentation *Platform Services Controller-Verwaltung*.
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.

Rollen, Rechte und Berechtigungen (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_8vla7txu/uiConfId/49694343/)

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

Für einen Benutzer oder eine Gruppe autorisieren Sie die Ausführung von Aufgaben für vCenter-Objekte, indem Sie Berechtigungen für das Objekt verwenden.

vSphere 6.0 und höher 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.

vCenter Server-Berechtigungen

Das Berechtigungsmodell für vCenter Server-Systeme basiert auf der Zuweisung von Berechtigungen zu Objekten in der Objekthierarchie. Jede Berechtigung erteilt einem Benutzer oder einer Gruppe eine Reihe von Berechtigungen (d. h. eine Rolle) für das ausgewählte Objekt. Sie können z. B. einen ESXi-Host in der Objekthierarchie auswählen und einer Gruppe von Benutzern eine Rolle zuweisen. Diese Rolle weist diesen Benutzern die entsprechenden Privilegien auf diesem Host zu.

Globale Berechtigungen

Globale Berechtigungen werden auf ein globales Stammobjekt angewendet, das für mehrere Lösungen verwendet wird. Wenn z. B. sowohl vCenter Server als auch vRealize Orchestrator installiert sind, können Sie globale Berechtigungen verwenden. Sie können beispielsweise einer Gruppe von Benutzern Leseberechtigung für alle Objekte in beiden Objekthierarchien zuweisen.

Globale Berechtigungen werden in der gesamten vsphere.local-Domäne repliziert. Sie dienen jedoch nicht zur Autorisierung von Diensten, die in den vsphere.local-Gruppen verwaltet werden. Weitere Informationen hierzu finden Sie unter Globale Berechtigungen.

Gruppenmitgliedschaft in vsphere.local-Gruppen

Der Benutzer der vCenter Single Sign-On-Domäne (standardmäßig administrator@vsphere.local) kann Aufgaben im Zusammenhang mit Diensten ausführen, die im Platform Services Controller enthalten sind. Mitglieder einer Gruppe „vsphere.local“ können bestimmte Aufgaben ausführen. Wenn Sie beispielsweise Mitglied der Gruppe „LicenseService.Administrators“ sind, dürfen Sie Lizenzen verwalten. Informationen finden Sie in der Dokumentation *Platform Services Controller-Verwaltung*.

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.

Grundlegendes zum vCenter Server-Berechtigungsmodell

Das Berechtigungsmodell für vCenter Server-Systeme basiert auf der Zuweisung von Berechtigungen zu Objekten in der vSphere-Objekthierarchie. Jede Berechtigung erteilt einem Benutzer oder einer Gruppe eine Reihe von Rechten (d. h. eine Rolle) für das ausgewählte Objekt.

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.

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. Die 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.

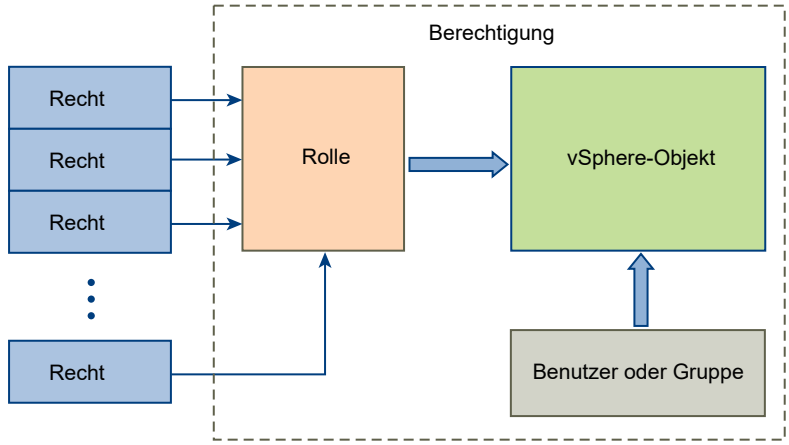
Berechtigungen

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

Rollen

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

Abbildung 2-1. 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-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.

   Berechtigungen werden standardmäßig weitergegeben, d. h., die Gruppe oder der Benutzer verfügt über die ausgewählte Rolle für das ausgewählte Objekt und dessen untergeordnete Objekte.

vCenter Server bietet vordefinierte Rollen 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 Rolle
Alle Berechtigungen und die Objekte, auf die Sie die Berechtigungen anwenden können	Kapitel 11 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.

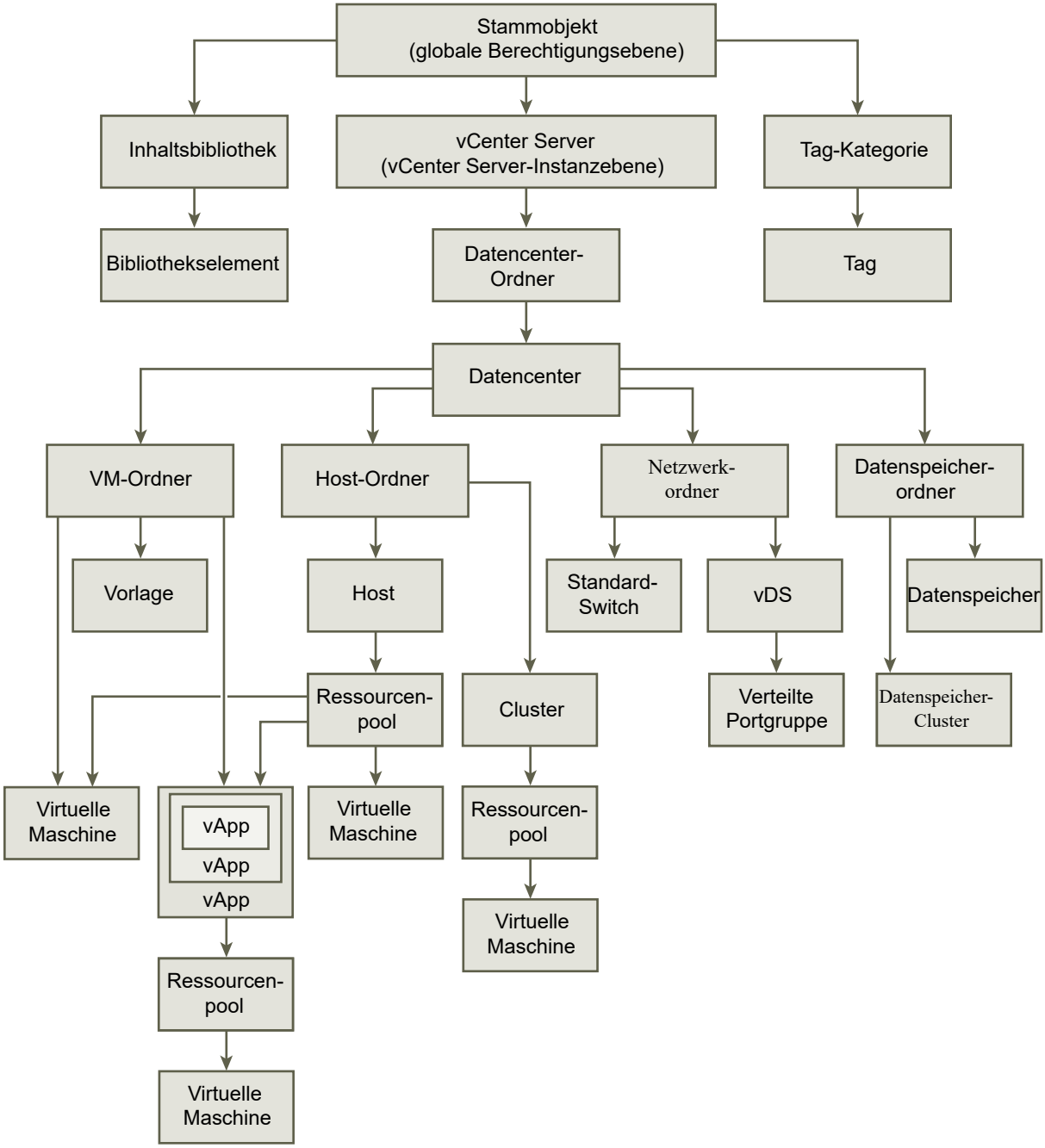
Hierarchische Vererbung von Berechtigungen

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 wird nicht allgemein angewendet. Für ein untergeordnetes Objekt definierte Berechtigungen setzen immer die von übergeordneten Objekten vererbten Berechtigungen außer Kraft.

In dieser 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. Siehe Globale Berechtigungen.

Abbildung 2-2. vSphere-Bestandslistenhierarchie



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

Berechtigte Benutzer können Berechtigungen auf verwalteten Elemente definieren.

- 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. Z. B. möglicherweise über eine Berechtigung fest, dass die Gruppe A auf ein Objekt über Administratorrechte verfügt. Gruppe B VM-Administratorrechte für das gleiche Objekt eventuelle, möglicherweise eine andere Berechtigung erteilen fest.

Wenn ein Objekt Berechtigungen von zwei übergeordneten Objekten erbt, werden die Berechtigungen für ein Objekt zu den Berechtigungen für das andere Objekt hinzugefügt. Beispiel: Eine virtuelle Maschine befindet sich in einem VM-Ordner und gehört auch einem Ressourcenpool an. Diese virtuelle Maschine erbt alle Berechtigungseinstellungen sowohl vom VM-Ordner als auch vom Ressourcenpool.

Einem untergeordneten Objekt zugewiesene Berechtigungen setzen Berechtigungen, die übergeordneten Objekten zugewiesen wurden, immer außer Kraft. Weitere Informationen hierzu finden Sie unter Beispiel 2: Untergeordnete Berechtigungen, die übergeordnete Berechtigungen außer Kraft setzen.

Wenn für dasselbe Objekt mehrere Gruppenberechtigungen 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 besitzt der Benutzer die Rechte, die die Gruppen für dieses Objekt haben.
- Es wurde eine Berechtigung für den Benutzer für das Objekt festgelegt. In diesem Fall hat die Berechtigung des Benutzers Vorrang vor allen Gruppenberechtigungen.

Beispiel 1: Vererbung von mehreren Berechtigungen

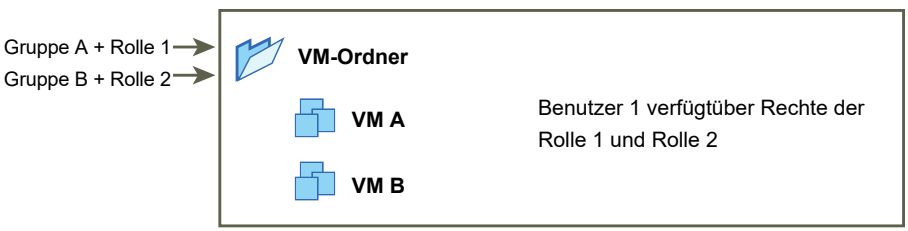
Dieses Beispiel zeigt, wie ein Objekt mehrere Berechtigungen von Gruppen übernehmen kann, die auf einem übergeordneten Objekt Berechtigungen erhalten haben.

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

- Rolle 1 kann virtuelle Maschinen einschalten.
- Rolle 2 kann Snapshots von virtuellen Maschinen erstellen.
- Gruppe A wird Rolle 1 auf VM-Ordner zugeteilt, mit der Berechtigung „An untergeordnete Objekte weitergeben“.
- Gruppe B wird Rolle 2 auf VM-Ordner zugeteilt, mit der Berechtigung „An untergeordnete Objekte weitergeben“.
- Benutzer 1 werden keine speziellen Rechte zugewiesen.

Benutzer 1, der den Gruppen A und B angehört, meldet sich an. Benutzer 1 kann sowohl VM A als auch VM B einschalten und von beiden Snapshots erstellen.

Abbildung 2-3. Beispiel 1: Vererbung von mehreren Berechtigungen



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

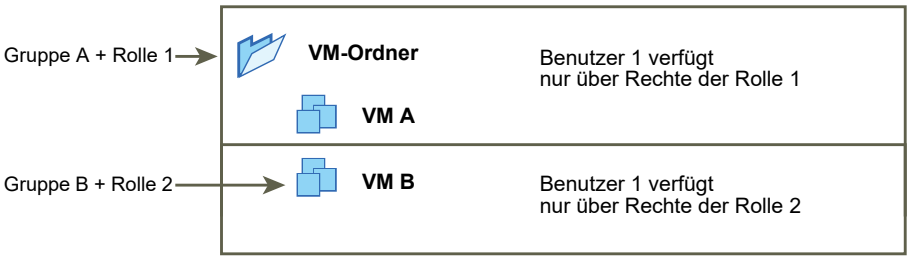
Dieses Beispiel zeigt, wie Berechtigungen, die einem untergeordneten Objekt zugewiesen wurden, die Berechtigungen, die einem übergeordneten Objekt zugewiesen wurden, außer Kraft setzen. Sie können dieses Verhalten dazu verwenden, um den Benutzerzugriff auf bestimmte Bereiche der Bestandsliste einzuschränken.

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

- Rolle 1 kann virtuelle Maschinen einschalten.
- Rolle 2 kann Snapshots von virtuellen Maschinen erstellen.
- Gruppe A wird Rolle 1 auf VM-Ordner zugeteilt, mit der Berechtigung „An untergeordnete Objekte weitergeben“.
- Gruppe B wird die Rolle 2 auf VM B zugeteilt.

Benutzer 1, der den Gruppen A und B angehört, meldet sich an. Weil Rolle 2 auf einer niedrigeren Hierarchieebene zugewiesen wird wie Rolle 1, setzt sie Rolle 1 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 2-4. Beispiel 2: Untergeordnete Berechtigungen, die übergeordnete Berechtigungen außer Kraft setzen



Beispiel 3: Überschreiben der Gruppenrolle durch die Benutzerrolle

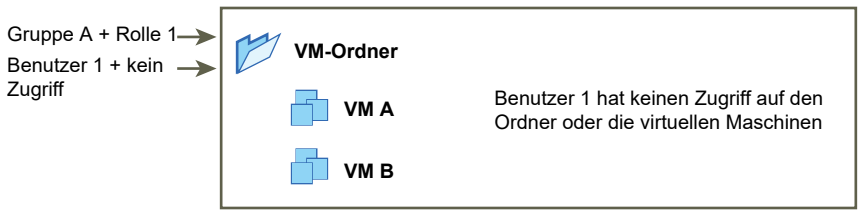
Dieses Beispiel zeigt, wie die einem individuellen Benutzer direkt zugewiesene Rolle die Rechte einer Rolle überschreibt, die einer Gruppe zugeordnet ist.

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.

- Rolle 1 kann virtuelle Maschinen einschalten.
- Gruppe A wird Rolle 1 auf VM-Ordner zugeteilt.
- Benutzer 1 erhält die Rolle „Kein Zugriff“ auf VM-Ordner.

Benutzer 1, der Mitglied der Gruppe A ist, meldet sich an. Die dem Benutzer 1 zugeteilte Rolle „Kein Zugriff“ für den VM-Ordner überschreibt die der Gruppe zugewiesene Rolle. Benutzer 1 kann weder auf VM-Ordner noch auf VM A oder VM B zugreifen.

Abbildung 2-5. 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 hinzufügen 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 diesen Host aus und fügen eine Berechtigung hinzu, mit der der Gruppe eine Rolle erteilt wird, die das Recht **Host.Konfiguration.Arbeitsspeicherkonfiguration** enthält.

Für die Verwaltung von Berechtigungen über den vSphere Web Client müssen Sie mit den folgenden Konzepten vertraut sein:

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.

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. Die 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 Sie dann Benutzern oder Gruppen zuordnen können.

Rollen

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

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 Berechtigungen zuweisen, um die Berechtigungen auf alle Objekte in allen Lösungen anzuwenden. Siehe 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 mehreren Objekten gleichzeitig zuweisen, indem Sie die Objekte in einen Ordner verschieben und die Berechtigungen auf den Ordner anwenden.

Wenn Sie Berechtigungen über den vSphere Web Client zuweisen, müssen Benutzer- und Gruppennamen einschließlich der Groß- und Kleinschreibung genau mit Active Directory übereinstimmen. 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 Web Client zu dem Objekt, für das Sie Berechtigungen zuweisen möchten.
2. Klicken Sie auf die Registerkarte **Berechtigungen**.
3. Klicken Sie auf das Symbol „Hinzufügen“ und klicken Sie dann auf **Hinzufügen**.

4 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 oder wählen Sie einen Namen aus der Liste aus.

      Das System such nach Benutzernamen, Gruppennamen und Beschreibungen.

   c Wählen Sie den Benutzer bzw. die Gruppe aus und klicken Sie auf **Hinzufügen**.

      Der Name wird der Liste **Benutzer** bzw. **Gruppen** hinzugefügt.

   d (Optional) Klicken Sie auf **Namen prüfen**, um zu überprüfen, ob der Benutzer oder die Gruppe in der Identitätsquelle vorhanden ist.

   e Klicken Sie auf **OK**.

5 Wählen Sie eine Rolle aus dem Dropdown-Menü **Zugewiesene Rolle** aus.

   Die Rollen, die dem Objekt zugewiesen sind, erscheinen im Menü. Die Rechte, die dieser Rolle zugewiesen sind, werden im Bereich unterhalb des Rollennamens aufgelistet.

6 (Optional) Um die Weitergabe zu beschränken, deaktivieren Sie das Kontrollkästchen **An untergeordnete Objekte weitergeben**.

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

7 Klicken Sie auf **OK**, um die Berechtigung hinzuzufügen.

Ändern 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 **Weitergeben** ändern. Sie können auch die Berechtigungseinstellung entfernen.

Verfahren

1 Navigieren Sie zum Objekt im Objektnavigator von vSphere Web Client.

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

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

4 Klicken Sie auf das Symbol **Rolle für Berechtigung ändern**.

5 Wählen Sie aus dem Dropdown-Menü **Zugewiesene Rolle** die entsprechende Rolle für den Benutzer oder die Gruppe aus.

6 Schalten Sie das Kontrollkästchen **An untergeordnete Objekte weitergeben** um, um Änderungen an der Berechtigungsvererbung vorzunehmen, und klicken Sie auf **OK**.

Entfernen von Berechtigungen

Berechtigungen für ein Objekt in der Objekthierarchie können Sie für einzelne Benutzer oder für Gruppen entfernen. In diesem Fall verfügt der Benutzer bzw. die Gruppe nicht mehr über die Berechtigungen, die mit der Rolle im Objekt verknüpft sind.

Hinweis Vom System vordefinierte Berechtigungen können nicht entfernt werden.

Verfahren

1. Navigieren Sie zum Objekt im Objektnavigator von vSphere Web Client.
2. Klicken Sie auf die Registerkarte **Berechtigungen**.
3. Klicken Sie auf eine Zeile, um eine Berechtigung auszuwählen.
4. 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 Web Client zum vCenter Server-System.
2. Wählen Sie **Konfigurieren** aus und klicken Sie auf **Allgemein** unter **Einstellungen**.
3. Klicken Sie auf **Bearbeiten** und wählen Sie **Benutzerverzeichnis** aus.
4. Ändern Sie die Werte wie gewünscht.

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 das Kontrollkästchen, um die maximale Anzahl der von vCenter Server angezeigten Benutzer und Gruppen festzulegen.

Option	Beschreibung
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.
Validierung	Deaktivieren Sie das Kontrollkästchen, um die Validierung zu deaktivieren.
Validierungszeitraum	Gibt in Minuten an, wie oft vCenter Server Berechtigungen validiert.

5 Klicken Sie auf **OK**.

Globale Berechtigungen

Globale Berechtigungen werden auf ein globales Stammobjekt angewendet, das für mehrere Lösungen verwendet wird, wie z. B. sowohl für vCenter Server als auch für vRealize Orchestrator. Mithilfe von globalen Berechtigungen können Sie einem Benutzer oder einer Gruppe Rechte für alle Objekte in allen Objekthierarchien erteilen.

Jede Lösung weist ein Stammobjekt in der eigenen Objekthierarchie auf. Das globale Stammobjekt dient als übergeordnetes Objekt für die Stammobjekte aller Lösungen. 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 einen ESXi-Host oder eine virtuelle Maschine. Dabei geben Sie an, dass ein Benutzer oder eine Gruppe über bestimmte Rechte (was als Rolle bezeichnet wird) 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.

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. Klicken Sie auf **Verwaltung** und wählen Sie im Zugriffssteuerungsbereich **Globale Berechtigungen** aus.
2. Klicken Sie auf **Verwalten** und dann auf das Symbol **Berechtigung hinzufügen**.
3. 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 oder wählen Sie einen Namen aus der Liste aus.

      Das System such nach Benutzernamen, Gruppennamen und Beschreibungen.
   c. Wählen Sie den Benutzer bzw. die Gruppe aus und klicken Sie auf **Hinzufügen**.

      Der Name wird der Liste **Benutzer** bzw. **Gruppen** hinzugefügt.
   d. (Optional) Klicken Sie auf **Namen prüfen**, um zu überprüfen, ob der Benutzer oder die Gruppe in der Identitätsquelle vorhanden ist.
   e. Klicken Sie auf **OK**.
4. Wählen Sie eine Rolle aus dem Dropdown-Menü **Zugewiesene Rolle** aus.

   Die Rollen, die dem Objekt zugewiesen sind, erscheinen im Menü. Die Rechte, die dieser Rolle zugewiesen sind, werden im Bereich unterhalb des Rollennamens aufgelistet.
5. Entscheiden Sie, ob das Kontrollkästchen **An untergeordnete Objekte weitergeben** aktiviert bleiben soll.

   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.
6. 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 Root-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 in einem vCenter Server-Bestandslistenobjekt Berechtigungen erteilen, beispielsweise einem ESXi-Host oder einer virtuellen Maschine, kann dieser Benutzer keine Tag-Vorgänge für dieses Objekt ausführen.

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 Root-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** auf dem 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 dasRoot-Objekt 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 Root-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 selbst für das Tag „Production“ über dieses Recht, da Robin über die globale Berechtigung verfügt. 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.

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 Web 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**.

Erstellen von Rollen im vSphere Web Client (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_egsyxkp4/uiConfId/49694343/)

vCenter Server-Systemrollen

Bei einer Rolle handelt es sich um einen vordefinierten Satz an Rechten. Wenn Sie einem Objekt Berechtigungen hinzufügen, kombinieren Sie einen Benutzer oder eine Gruppe mit einer Rolle. In vCenter Server gibt es mehrere Systemrollen, die nicht geändert werden können.

vCenter Server-Systemrollen

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“. Rollen, die Sie erstellen, übernehmen keine Rechte von den 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, über die auch die Rolle „Nur Lesen“ verfügt. Wenn Sie über die Rolle des Administrators 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. Zu den unterstützten identitätsdiensten gehören Windows Active Directory und OpenLDAP 2.4.

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 „Kein Kryptografie-Administrator“

Benutzer mit der Rolle „Kein Kryptografie-Administrator“ für ein Objekt verfügen über dieselben Rechte wie Benutzer mit der Administratorrolle, mit Ausnahme der Rechte **Kryptografievorgänge**. Mit dieser Rolle können Administratoren andere Administratoren bestimmen, die keine virtuellen Maschinen verschlüsseln oder entschlüsseln können oder keinen Zugriff auf verschlüsselte Daten haben, die aber alle anderen administrativen Aufgaben ausführen können.

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.

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.

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.

Erstellen einer benutzerdefinierten Rolle

Sie können benutzerdefinierte Rollen für vCenter Server erstellen, die den in Ihrer Umgebung bestehenden Anforderungen hinsichtlich der Zugriffssteuerung entsprechen. Sie können eine Rolle von Grund auf 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 bei vCenter Server an.
2. Wählen Sie „Home“ aus und klicken Sie auf **Verwaltung > Rollen**.

3 Erstellen Sie die Rolle:

Option	Beschreibung
Erstellen der Rolle von Grund auf	Klicken Sie auf die Schaltfläche **Rolle erstellen**.
Erstellen der Rolle durch Klonen	Wählen Sie eine Rolle aus und klicken Sie auf die Schaltfläche **Rolle 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.

Weitere Informationen hierzu finden Sie unter Kapitel 11 Definierte Rechte.

6 Klicken Sie auf **OK**.

Nächste Schritte

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

Klonen einer Rolle

Sie können eine vorhandene Rolle kopieren, sie umbenennen und bearbeiten. Wenn Sie eine Kopie erstellen, wird die neue Rolle nicht auf Benutzer bzw. Gruppen und Objekte angewendet. Sie müssen Benutzern, Gruppen und Objekten die Rolle zuweisen.

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 mit dem vSphere Web Client bei vCenter Server an.

2 Wählen Sie „Home“, klicken Sie auf **Verwaltung** und klicken Sie dann auf **Rollen**.

3 Wählen Sie eine Rolle aus und klicken Sie auf das Symbol **Rollenaktion klonen**.

4 Geben Sie einen Namen für die geklonte Rolle ein.

5 Aktivieren oder deaktivieren Sie Berechtigungen für die Rolle und klicken Sie auf **OK**.

Bearbeiten einer Rolle

Beim Bearbeiten einer Rolle können Sie die für diese Rolle ausgewählten Berechtigungen ändern. Anschließend werden diese Berechtigungen auf alle Benutzer oder Gruppen angewendet, die der bearbeiteten Rolle zugeordnet sind.

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 mit dem vSphere Web Client bei vCenter Server an.
2. Wählen Sie „Home“, klicken Sie auf **Verwaltung** und klicken Sie dann auf **Rollen**.
3. Wählen Sie eine Rolle aus und klicken Sie auf die Schaltfläche **Rollenaktion bearbeiten**.
4. Aktivieren oder deaktivieren Sie Berechtigungen für die Rolle und klicken Sie auf **OK**.

Best Practices für Rollen und Berechtigungen

Verwenden Sie die empfohlenen Vorgehensweisen für Rollen und Berechtigungen, um die Sicherheit und Verwaltungsfreundlichkeit Ihrer vCenter Server-Umgebung zu maximieren.

VMware empfiehlt die folgenden Vorgehensweisen 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 übernehmen und für Benutzer verfügbar sind.
- 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 wie folgt weitergegeben:
  - An alle vCenter Server-Systeme, die mit demselben Platform Services Controller verknüpft sind.
  - An Platform Services Controller-Instanzen in derselben vCenter Single Sign On-Domäne.
- 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.

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.Raw-Gerät** (wenn eine RDM oder ein SCSI-Passthrough-Gerät verwendet wird)	Administrator
	Auf dem Zielhost, -cluster oder -ressourcenpool: **Ressourcen.Virtuelle Maschine dem 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: **Ressourcen.Virtuelle Maschine dem Ressourcenpool zuweisen**	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: ■ **Ressourcen.Virtuelle Maschine dem Ressourcenpool zuweisen** ■ **Virtuelle Maschine.Bestandsliste.Verschieben**	Administrator
	Auf dem Zielressourcenpool: **Ressourcen.Virtuelle Maschine dem 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): **Ressourcen.Virtuelle Maschine dem 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** ■ **Ressourcen.Virtuelle Maschine dem 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): **Ressourcen.Virtuelle Maschine dem 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**	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. Ab vSphere 6.0 nehmen ESXi-Hosts an der Zertifikatsinfrastruktur 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.

Dieses Kapitel enthält die folgenden Themen:

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 Web 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. 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.

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

Risiken für die Hosts werden standardmäßig wie folgt verringert:

- ESXi Shell und SSH sind standardmäßig deaktiviert.
- 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 Tomcat-Webdienst wird intern 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 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.
- Unsichere Dienste, wie z. B. FTP und Telnet sind nicht installiert, und die Ports für diese Dienste sind standardmäßig geschlossen. Da sicherere Dienste wie SSH und SFTP leicht verfügbar sind, sollten Sie auf einen Einsatz dieser unsicheren Dienste verzichten und sicherere Alternativen verwenden. Verwenden Sie z. B. Telnet mit SSL, um auf virtuelle serielle Ports zuzugreifen, wenn SSH nicht verfügbar ist und Sie Telnet verwenden müssen.

  Wenn Sie unsichere Dienste verwenden müssen und für den Host einen ausreichenden Schutz hergestellt haben, können Sie explizit Ports öffnen, um sie zu unterstützen.
- Verwenden Sie eventuell UEFI Secure Boot für Ihr ESXi-System. Weitere Informationen hierzu finden Sie unter UEFI Secure Boot für ESXi-Hosts.

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 Web 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. Verwenden Sie einen der GUI-Clients oder eine der VMware-CLIs oder -APIs für die Verwaltung Ihrer ESXi-Hosts. 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/.

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 Web Client.

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

vSphere PowerCLI

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

vSphere PowerCLI enthält über 200 Cmdlets, eine Reihe von Beispielskripts und eine Funktionsbibliothek für die Verwaltung und Automatisierung. Weitere Informationen finden Sie in der *vSphere PowerCLI-Dokumentation*.

vSphere Command-Line Interface (vCLI)

vCLI enthält eine Reihe von Befehlen für die Verwaltung von ESXi-Hosts und virtuellen Maschinen. Das Installationsprogramm, mit dem auch das vSphere SDK for Perl installiert wird, kann auf Windows- oder Linux-Systemen ausgeführt werden und installiert ESXCLI-Befehle, `vicfg-` -Befehle und eine Reihe anderer vCLI-Befehle. Weitere Informationen finden Sie in der *Dokumentation zur vSphere Command-Line Interface*.

Ab vSphere 6.0 können Sie auch eine der Skriptschnittstellen des vCloud Suite SDK verwenden, z. B. das vCloud Suite SDK for Python.

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 Web 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

vCLI (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.

ESXi verwendet das Linux-PAM-Modul `pam_passwdqc` für die Verwaltung und Kontrolle der Kennwörter. Ausführliche Informationen finden Sie auf der Manpage zu `pam_passwdqc`.

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 Sie standardmäßig Zeichen aus vier Zeichenklassen verwenden: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen (z. B. Unter- oder Schrägstriche).
- Standardmäßig beträgt die Kennwortlänge mehr als 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.

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 sind Kennwörter mit einer oder zwei Zeichenklassen sowie Kennwortsätze nicht zulässig, da die ersten drei Elemente deaktiviert sind. Kennwörter mit drei oder vier Zeichenklassen erfordern sieben Zeichen. Weitere Informationen finden Sie auf der Manpage zu `pam_passwdqc`.

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. Diesen Standardwert 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
```

Dieses Beispiel erlaubt Kennwortsätze mit mindestens 16 Zeichen und mindestens drei Wörtern, getrennt durch Leerzeichen.

Änderungen an der Datei `/etc/pamd/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 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 der Optionen für `pam_passwdqc` wurden getestet. Führen Sie zusätzliche Tests durch, nachdem Sie Änderungen an den Einstellungen für das Standardkennwort vorgenommen haben.

ESXi-Kontosperrverhalten

Ab vSphere 6.0 wird das Sperren von Konten für den Zugriff über SSH und über das vSphere Web Services SDK 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.

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

SSH-Sicherheit

Sie können SSH verwenden, um sich remote an die ESXi Shell anzumelden und Fehlerbehebungsaufgaben für den Host durchzuführen.

Die SSH-Konfiguration in ESXi wurde zwecks Erweiterung der Sicherheitsstufe verbessert.

Version 1 SSH-Protokoll deaktiviert

VMware bietet keine Unterstützung für das SSH-Protokoll Version 1, sondern verwendet ausschließlich das Version 2-Protokoll. 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 anzugeben.

Sie können den SSH-Schlüssel mithilfe des vSphere-CLI-Befehls `vifs` auf den Host kopieren. In *Erste Schritte mit vSphere-Befehlszeilenschnittstellen* finden Sie weitere Informationen zum Installieren und Verwenden des vSphere-CLI-Befehlssatzes. 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 hierzu finden Sie im VMware-Knowledgebase-Artikel 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.

Hinweis Für ESXi 5.0 und früher kann ein Benutzer mit einem SSH-Schlüssel auf den Host auch dann zugreifen, wenn sich der Host im Sperrmodus befindet. Ab ESXi 5.1 kann ein Benutzer mit einem SSH-Schlüssel nicht mehr auf einen Host im Sperrmodus zugreifen.

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 Benutzername --put Dateiname /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.

Ab vSphere 6.0 ist der MOB 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 Wählen Sie den Host im vSphere Web Client aus und navigieren Sie zu **Erweiterte Systemeinstellungen**.

2 Überprüfen Sie den Wert von **Config.HostAgent.plugins.solo.enableMob** und ändern Sie ihn gegebenenfalls.

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

ESXi-Netzwerksicherheitsempfehlungen

Die Isolierung des Netzwerkverkehrs ist entscheidend für eine sichere ESXi-Umgebung. Verschiedene Netzwerke erfordern verschiedenen Zugriff und verschiedene 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 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. Auf dieses Netzwerk dürfen nur System-, Netzwerk- und Sicherheitsadministratoren Zugriff haben. Verwenden Sie Jump-Box oder Virtual Private Network (VPN), um den Zugriff auf das Managementnetzwerk zu sichern. 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 MD5 verschlüsselt.
  - 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 *Dokumentation zur vSphere-Befehlszeilenschnittstelle*. 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 im *Verwaltungshandbuch für Platform Services Controller*. 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 Dokumentation *VMware vSphere API-Referenz*.

3. Verlängern Sie das Ticket gegebenenfalls alle zwei Minuten.

Zertifikatsverwaltung für ESXi-Hosts

In vSphere 6.0 und höher stattet die VMware Certificate Authority (VMCA) jeden neuen ESXi-Host mit einem signierten Zertifikat aus, bei dem VMCA die standardmäßige Stammzertifizierungsstelle 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 Web 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 5.5 und vSphere 6.x

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

Bis zu vSphere Version 5.5 werden die TLS/SSL-Endpoints lediglich mit einer Kombination aus Benutzername, Kennwort und Fingerabdruck geschützt. Hier können die entsprechenden selbstsignierten Zertifikate durch eigene Zertifikate ersetzt werden. Weitere Informationen erhalten Sie im Dokumentationscenter für vSphere 5.5.

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

Tabelle 3-1. 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 Web 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 Web 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 Web 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

Ab vSphere 6.0 können Sie in vSphere Web 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 Web Client festlegen.

Hostname und IP-Adresse

In vSphere 6.0 und höher kann sich eine Änderung der IP-Adresse oder des Hostnamens 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 3-2. 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

ESXi-Zertifikatverwaltung (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_vkuyp3rf/uiConfId/49694343/)

Host-Upgrades und Zertifikate

Wenn Sie ein Upgrade eines ESXi-Hosts auf ESXi 6.0 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.

Wenn Sie sich dafür entscheiden, kein Upgrade für die Hosts auf ESXi 6.0 oder höher durchzuführen, behalten die Hosts die derzeit verwendeten Zertifikate bei, selbst wenn der Host von einem vCenter Server-System verwaltet wird, das VMCA-Zertifikate verwendet.

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 6.0 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 Web 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 Web 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 6.0 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 Web 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 Web 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. Folgender Workflow wird empfohlen.

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. Folgender Workflow wird empfohlen.

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. Folgender Workflow wird empfohlen.

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. Folgender Workflow wird empfohlen.

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 Web Client ändern. Ändern Sie eventuell das Unternehmen und Ortsangaben. Weitere Informationen hierzu finden Sie unter Ändern der Standardeinstellungen für Zertifikate.

Tabelle 3-3. 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

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

Parameter	Standardwert	Erweiterte Option
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.cn.daysValid
Fester Schwellenwert für Zertifikatsablauf. vCenter Server löst einen roten Alarm aus, wenn dieser Grenzwert erreicht ist.	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 Zertifikatsablauf. vCenter Server löst ein Ereignis aus, wenn dieser Grenzwert erreicht ist.	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.	Standard ist 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 Web 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 Web Client das vCenter Server-System aus, das die Hosts verwaltet.
2. Klicken Sie auf **Konfigurieren** und anschließend auf **Erweiterte Einstellungen**.
3. Geben Sie im Filterfeld **`certmgmt`** ein, um nur Zertifikatverwaltungsparameter anzuzeigen.
4. Ändern Sie den Wert der vorhandenen Parameter entsprechend der Unternehmensrichtlinie und klicken Sie auf **OK**.

   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 Web Client anzeigen. Sie können keine Zertifikatsstatusinformationen für Hosts im Fingerabdruckmodus anzeigen.

Verfahren

1. Navigieren Sie zum Host in der Bestandslistenhierarchie von vSphere Web Client .

   Standardmäßig wird der Zertifikatsstatus in der Anzeige der Hosts nicht eingeblendet.
2. Klicken Sie mit der rechten Maustaste auf das Namensfeld und wählen Sie **Spalten anzeigen/ ausblenden** aus.
3. Wählen Sie **Zertifikat gültig bis** aus, klicken Sie auf **OK** und führen Sie bei Bedarf einen Bildlauf nach rechts durch.

   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.

4 (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. Siehe 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 Web Client anzeigen. Die Informationen über das Zertifikat können bei der Fehlerbehebung nützlich sein.

Verfahren

1 Navigieren Sie zum Host im Navigator von vSphere Web Client.

2 Wählen Sie **Konfigurieren** aus.

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 8 Monate oder weniger bis zum Ablauf (Standard). **Ablauf steht bevor** Es fehlen nur noch 2 Monate oder weniger bis zum Ablauf (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 Web 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 das Zertifikat schon abgelaufen ist, müssen Sie die Verbindung mit dem Host trennen und dann wieder herstellen.

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

Verfahren

1. Navigieren Sie zum Host im Navigator von vSphere Web Client.
2. Wählen Sie **Konfigurieren** aus.
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 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 Web Client den vCenter Server aus, den die Hosts verwalten.
2. Klicken Sie auf **Konfigurieren** und unter „Einstellungen“ auf **Erweiterte Einstellungen**.

3 Klicken Sie auf **Bearbeiten**.

4 Geben Sie im Feld „Filter“ den Ausdruck **`certmgmt`** ein, um nur die Zertifikatverwaltungsschlüssel anzuzeigen.

5 Ändern Sie den Wert von `vpxd.certmgmt.mode` in **custom**, wenn Sie Ihre eigenen Zertifikate verwenden möchten, oder in **thumbprint**, wenn Sie vorübergehend in den Fingerabdruckmodus wechseln möchten. Klicken Sie anschließend auf **OK**.

6 Starten Sie den vCenter Server-Dienst neu.

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 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 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: mindestens 2.048 Bit (PEM-kodiert)
- PEM-Format. VMware unterstützt PKCS8 und PKCS1 (RSA-Schlüssel). Wenn Schlüssel zu VECS hinzugefügt werden, werden sie in PKCS8 konvertiert.
- x509 Version 3
- Für Stammzertifikate muss die Zertifizierungsstellenerweiterung auf „true“ festgelegt sein, und „cert sign“ muss in der Liste der Anforderungen vorhanden sein.

- „SubjectAltName“ muss DNS-Name=<Maschinen-FQDN> enthalten
- CRT-Format
- Enthält die folgenden Schlüsselverwendungen: Digitale Signatur, 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.

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 Web 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.

Ersetzen eines Standardzertifikats und -schlüssels mit dem vifs-Befehl

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

Sie führen `vifs` als vCLI-Befehl aus. Weitere Informationen finden Sie unter *Erste Schritte mit vSphere-Befehlszeilenschnittstellen*.

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 Web 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.

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 Web 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.

Nächste Schritte

Aktualisieren Sie den TRUSTED_ROOTS-Speicher von vCenter Server. Siehe 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 dem vCenter Server-System an, das die ESXi-Hosts verwaltet.

   Melden Sie sich bei dem Windows-System, auf dem Sie die Software installiert haben, oder bei der vCenter Server Appliance-Shell an.

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 <path_to_RootCA>
```

Option	Beschreibung
Linux	`//usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish <path_to_RootCA>`
Windows	`C:\Program Files\VMware\vCenter Server\vmafdd\dir-cli trustedcert publish <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 <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: mindestens 2.048 Bit (PEM-kodiert)
  - PEM-Format. VMware unterstützt PKCS8 und PKCS1 (RSA-Schlüssel). Wenn Schlüssel zu VECS hinzugefügt werden, werden sie in PKCS8 konvertiert.
  - x509 Version 3
  - Für Stammzertifikate muss die Zertifizierungsstellenerweiterung auf „true“ festgelegt sein, und „cert sign“ muss in der Liste der Anforderungen vorhanden sein.
  - „SubjectAltName“ muss DNS-Name=<Maschinen-FQDN> enthalten

- CRT-Format
- Enthält die folgenden Schlüsselverwendungen: Digitale Signatur, 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 `rbd-ca.crt` und die Schlüsseldatei `rbd-ca.key`.

Verfahren

1 Sichern Sie die standardmäßigen ESXi-Zertifikate.

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

2 Beenden Sie im vSphere Web Client den Auto Deploy-Dienst.

   a Wählen Sie **Verwaltung** und klicken Sie unter **Bereitstellung** auf **Systemkonfiguration**.

   b Klicken Sie auf **Dienste**.

   c Klicken Sie mit der rechten Maustaste auf den Dienst, der beendet werden soll, und wählen Sie **Beenden**.

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.

Option	Beschreibung

Windows	`cd C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli.exe`
	`vecs-cli entry delete --store TRUSTED_ROOTS --alias rbd_cert`
	`vecs-cli entry create --store TRUSTED_ROOTS --alias rbd_cert`
	`--cert /etc/vmware-rbd/ssl/rbd-ca.crt`

Linux	`cd /usr/lib/vmware-vmafd/bin/vecs-cli`
	`vecs-cli entry delete --store TRUSTED_ROOTS --alias rbd_cert`
	`vecs-cli entry create --store TRUSTED_ROOTS --alias rbd_cert`
	`--cert /etc/vmware-rbd/ssl/rbd-ca.crt`

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 Auto Deploy-Server verwendet das Root-Zertifikat, das Sie zum TRUSTED_ROOTS-Speicher hinzugefügt haben.

Hinweis Falls nach dem Ersetzen des Zertifikats Probleme mit Auto Deploy auftreten, siehe VMware-Knowledgebase-Artikel 2000988.

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` der 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 den Host neu oder senden Sie `ssl_reset`-Ereignisse zu allen Diensten, die die Schlüssel verwenden.

```
for s in /etc/init.d/*; do $s | grep ssl_reset > /dev/null; if [ $? == 0 ]; then $s ssl_reset; fi; done
```

Anpassen von Hosts mit dem Sicherheitsprofil

Viele wichtige Sicherheitseinstellungen für Ihren Host können Sie über das Fenster „Sicherheitsprofil“ im vSphere Web 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. Reduzieren 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 das Sicherheitsprofil für jeden Host im vSphere Web Client. Siehe 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.

Mit dem vibauthor-Tool von VMware Labs können Sie benutzerdefinierte VIBs erstellen. Um das benutzerdefinierte VIB zu installieren, müssen Sie die Akzeptanzebene des ESXi-Hosts in „CommunitySupported“ ändern. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel 2007381.

Hinweis Wenn Sie sich an den technischen Support von VMware wenden, um ein Problem auf einem ESXi-Host zu prüfen, auf dem ein CommunitySupported VIB installiert ist, kann der VMware Support verlangen, dass dieses CommunitySupported VIB als einer der Schritte zur Fehlerbehebung deinstalliert wird, um festzustellen, ob das VIB mit dem geprüften Problem in Zusammenhang steht.

ESXi-Firewall-Konzepte (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_8qp59yqe/uiConfId/49694343/)

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 Web Client oder an der Befehlszeile konfigurieren.

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. Navigieren Sie zum Host im Navigator von vSphere Web Client.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter „System“ auf **Sicherheitsprofil**.

   Der vSphere Web Client zeigt eine Liste der aktiven eingehenden und ausgehenden Verbindungen mit den entsprechenden Firewallports an.
4. Klicken Sie im Abschnitt „Firewall“ auf **Bearbeiten**.

   Die Anzeige enthält Firewallregelsätze, die den Namen der Regel und die zugeordneten Informationen einschließen.

5 Wählen Sie die zu aktivierenden Regelsätze oder heben Sie die Auswahl der zu deaktivierenden Regelsätze auf.

Spalte	Beschreibung
Ein- und ausgehende Ports	Die Ports, die von vSphere Web Client für den Dienst geöffnet werden.
Protokoll	Protokoll, das vom Dienst verwendet wird.
Daemon	Status der dem Dienst zugeordneten Daemons.

6 Für einige Dienste können Dienstdetails verwaltet werden.

- Verwenden Sie die Schaltflächen **Starten**, **Anhalten** oder **Neu starten**, um den Status eines Dienstes vorübergehend zu ändern.
- Ändern Sie die Startrichtlinie, damit der Dienst mit dem Host oder mit Port-Verwendung startet.

7 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.

8 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.

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

Hinzufügen zulässiger IP-Adressen zur ESXi-Firewall (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_0ugsspa2/uiConfId/49694343/)

Verfahren

1 Navigieren Sie zum Host im Navigator von vSphere Web Client.

2 Klicken Sie auf **Konfigurieren**.

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

4 Klicken Sie im Abschnitt „Firewall“ auf **Bearbeiten** und wählen Sie einen Dienst aus der Liste aus.

5 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

6 Klicken Sie auf **OK**.

Ein- und ausgehende Firewall-Ports für ESXi-Hosts

Im vSphere Web 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 Web 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, wird empfohlen, die Firewall-Konfiguration anhand von ESXCLI-Befehlen oder mit dem vSphere Web Services SDK zu automatisieren.

Firewall-Befehlsreferenz

Sie können die ESXi Shell- oder vSphere CLI-Befehle verwenden, um ESXi an der Befehlszeile zu konfigurieren und die Firewall-Konfiguration zu automatisieren. Unter *Erste Schritte mit vSphere-Befehlszeilenschnittstellen* finden Sie eine Einführung. *vSphere Command-Line Interface Concepts and Examples* enthält Beispiele für die Verwendung von ESXCLI für den Umgang mit Firewalls und Firewall-Regeln. Informationen zum Erstellen benutzerdefinierter Firewall-Regeln finden Sie im VMware-Knowledgebase-Artikel 2008226.

Tabelle 3-4. 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 die Firewallmodul- und Regelsatz-Konfigurationsdateien.
`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.
`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.

Beispiele für Firewall-Befehle

Die folgenden Beispiele stammen aus einem Blog-Beitrag auf virtuallyGhetto.

1 Bestätigen Sie einen neuen Regelsatz mit der Bezeichnung virtuallyGhetto.

```
esxcli network firewall ruleset rule list | grep virtuallyGhetto
```

2 Geben Sie bestimmte IP-Adressen oder IP-Bereiche an, um auf einen bestimmten Dienst zuzugreifen. Mit folgendem Beispiel wird die Option `allow all` deaktiviert und ein spezieller Bereich für den virtuallyGhetto-Dienst eingerichtet.

```
esxcli network firewall ruleset set --allowed-all false --ruleset-id=virtuallyGhetto
esxcli network firewall ruleset allowedip add --ip-address=172.30.0.0/24 --ruleset-id=virtuallyGhetto
```

Anpassen von ESXi-Diensten über das Sicherheitsprofil

Ein ESXi-Host umfasst mehrere Dienste, die standardmäßig ausgeführt werden. Sie können Dienste über das Sicherheitsprofil deaktivieren bzw. aktivieren, wenn die Unternehmensrichtlinie dies zulässt.

Verwenden des vSphere Web Client zum Aktivieren des Zugriffs auf die ESXi Shell 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 Web Client ändern.

Tabelle 3-5. 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.
SSH	Gestoppt	Der SSH-Clientdienst, der Remoteverbindungen über Secure Shell ermöglicht
Auslastungsbasierter Gruppierungs-Daemon	Wird ausgeführt	Auslastungsbasierte Gruppierung
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

Tabelle 3-5. ESXi-Dienste im Sicherheitsprofil (Fortsetzung)

Dienst	Standard	Beschreibung
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 Web Client aktiviert werden. Siehe *Installation und Einrichtung von vSphere*.
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 Diensts im Sicherheitsprofil

Sie können einen Dienst, der im Sicherheitsprofil aufgelistet ist, über den vSphere Web Client aktivieren oder deaktivieren.

Nach der Installation werden bestimmte Dienste standardmäßig ausgeführt, andere sind angehalten. In manchem Fällen sind zusätzliche Einrichtungsschritte erforderlich, damit ein Dienst in der vSphere Web Client-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 Web Client her.

Verfahren

1. Navigieren Sie zu einem Host in der vSphere Web Client-Bestandsliste und wählen Sie einen Host aus.
2. Klicken Sie auf **Konfigurieren**.
3. Wählen Sie unter „System“ die Option **Sicherheitsprofil** aus und klicken Sie auf **Bearbeiten**.
4. Führen Sie einen Bildlauf zu dem Dienst aus, den Sie ändern möchten.
5. Wählen Sie im Bereich „Dienstdetails“ **Starten**, **Beenden** oder **Neu starten** aus, um den Hoststatus einmalig zu ändern, bzw. wählen Sie eine Option aus dem Menü **Startrichtlinie** aus, um den Hoststatus auch über Neustarts hinweg zu ändern.
   - **Automatisch starten, wenn ein Port geöffnet ist, und beenden, wenn alle Ports geschlossen werden**: 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.

- **Mit dem Host starten und beenden**: Der Dienst wird unmittelbar nach dem Host gestartet und unmittelbar vor dem Herunterfahren des Hosts beendet. Ebenso wie **Automatisch starten, wenn ein Port geöffnet ist, und beenden, wenn alle Ports geschlossen werden** bedeutet diese Option, dass der Dienst regelmäßig versucht, seine Aufgaben zu erledigen, z. B. das Kontaktieren des angegebenen NTP-Servers. 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 als Teil des Herunterfahrens beendet. Sobald der Host jedoch eingeschaltet wird, wird auch der Dienst erneut gestartet, sodass der vom Benutzer festgelegte Status beibehalten bleibt.

Hinweis Diese Einstellungen gelten nur für Diensteinstellungen, die über den vSphere Web Client 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.

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.

Ab vSphere 6.0 haben Sie die Wahl zwischen dem normalen und dem strengen Sperrmodus mit jeweils unterschiedlicher Sperrstärke. In vSphere 6.0 steht Ihnen außerdem eine Liste ausgenommener Benutzer bereit. 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.

Sperrmodus in vSphere 6 (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_zg4ylgu0/uiConfId/49694343/)

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 Web 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. Ab vSphere 6.0 werden ESXi- oder SSH-Sitzungen für Benutzer ohne Administratorrechte beendet.

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

Tabelle 3-6. 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

Tabelle 3-6. Verhalten im Sperrmodus (Fortsetzung)

Dienst	Normaler Modus	Normaler Sperrmodus	Strenger Sperrmodus
ESXi Shell (soweit 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
SSH (soweit 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. Ab vSphere 6.0 wird die Sitzung für alle anderen Benutzer beendet. Dies betrifft sowohl den normalen als auch den strengen Sperrmodus.

Aktivieren des Sperrmodus über vSphere Web Client

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 von vSphere Web 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 beendet.

6 Klicken Sie auf **OK**.

Deaktivieren des Sperrmodus mit dem vSphere Web Client

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

In vSphere 6.0 können Sie den Sperrmodus wie folgt deaktivieren:

Über den vSphere Web Client

Benutzer können sowohl den normalen Sperrmodus als auch den strengen Sperrmodus über den vSphere Web 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 zum Host im Navigator von vSphere Web 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.

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 Web 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.

Für ESXi 6.0 und höher bleiben die Benutzerberechtigen beim Aktivieren des Sperrmodus erhalten. 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 Web 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 beim 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 Ausfälle von 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 Web 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

Wenn es sich um einen schwerwiegenden Fehler handelt, können Sie über die erweiterte Option DCUI.Access den Sperrmodus 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 Web 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 Objektnavigator von vSphere Web 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

In vSphere 6.0 und höher können Sie Benutzer über den vSphere Web Client zur Liste „Ausnahme für 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 von vSphere Web 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 Pluszeichen, um ausgenommene Benutzer hinzuzufügen.

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. Sie können die Akzeptanzebene des Hosts ändern, wenn Sie VIBs einer niedrigeren Ebene zulassen möchten. 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 Web 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. VMware leitet Support-Anrufe für VIBs dieser Akzeptanzebene an die Support-Organisation des Partners weiter.

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. VMware leitet Support-Anrufe für VIBs dieser Akzeptanzebene an die Support-Organisation des Partners weiter.

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 acceptance_level`
vSphere Client (HTML5-basierter Client) oder vSphere Web Client	a Wählen Sie einen Host in der Bestandsliste aus. b Wählen Sie die Registerkarte **Konfigurieren** aus. c Erweitern Sie **System**, und wählen Sie **Sicherheitsprofil** aus. d Klicken Sie auf die Schaltfläche **Bearbeiten** für die Akzeptanzebene des Host-Image-Profils und wählen Sie die Akzeptanzebene.

Zuweisen von Rechten für ESXi-Hosts

In den meisten Fällen erteilen Sie Berechtigungen, indem Sie den Benutzern Rechte auf ESXi-Hostobjekte erteilen, 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 Web 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

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

- Root-Benutzer. Weitere Informationen hierzu finden Sie unter Rechte für Root-Benutzer.
- vpxuser. Weitere Informationen hierzu finden Sie unter vpxuser-Rechte.
- dcui-Benutzer. Weitere Informationen hierzu finden Sie unter DCUI-Benutzerrechte.

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.

Rechte für 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.

Dieses gemeinsame Root-Konto kann den Angriff auf einen ESXi-Host vereinfachen, 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-Rechte

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

vCenter Server hat Administratorberechtigungen auf dem Host, der die Anwendung verwaltet. So kann vCenter Server zum Beispiel virtuelle Maschinen auf Hosts verschieben und die Konfiguration virtueller Maschinen ändern.

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 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-Benutzerrechte

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 darf.

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 mithilfe von NTP 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 Objektnavigator von vSphere Web 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

Verwenden Sie vSphere Web Client, um einer Verzeichnisdienst-Domäne beizutreten. 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 zum Host im Navigator von vSphere Web 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 von vSphere Web 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 und Platform Services Controller.

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 den vSphere Web Client oder über 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 im vSphere Web Client 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 Stellen Sie mit dem vSphere Web Client eine Verbindung zu einem vCenter Server-System her.

2 Klicken Sie auf **Verwaltung** und anschließend auf **Systemkonfiguration** unter **Bereitstellung**.

3 Klicken Sie auf **Dienste** und anschließend auf den **VMware vSphere Authentication Proxy**-Dienst.

4 Klicken Sie in der Menüleiste oben im Fenster auf das grüne Symbol **Dienst starten**.

5 (Optional) Nachdem der Dienst gestartet wurde, klicken Sie auf **Aktionen > Starttyp bearbeiten** und klicken Sie auf **Automatisch**, um den Start automatisch durchführen zu lassen.

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 Web Client

Sie können vSphere Authentication Proxy eine Domäne über den vSphere Web 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 Web Client eine Verbindung zu einem vCenter Server-System her.

2 Klicken Sie auf **Verwaltung** und anschließend auf **Systemkonfiguration** unter **Bereitstellung**.

3 Klicken Sie auf **Dienste**, auf den Dienst **VMware vSphere Authentication Proxy** und dann auf **Bearbeiten**.

4 Geben Sie den Namen der Domäne ein, der vSphere Authentication Proxy Hosts hinzufügen soll, sowie den Namen eines Benutzers mit Active Directory-Berechtigungen zum Hinzufügen von Hosts zur Domäne.

   Die anderen Felder in diesem Dialogfeld dienen nur zu Informationszwecken.

5 Klicken Sie auf das Auslassungszeichen, um das Kennwort für den Benutzer hinzuzufügen und zu bestätigen, und klicken Sie auf **OK**.

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

Sie können vSphere Authentication Proxy eine Domäne über den vSphere Web 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 Melden Sie sich bei der vCenter Server-Appliance oder der vCenter Server-Windows-Maschine als Benutzer mit Administratorberechtigungen an.

2 Führen Sie den Befehl aus, um den Zugriff auf die Bash-Shell zu aktivieren.

```
shell
```

3 Navigieren Sie zu dem Verzeichnis, in dem sich das **camconfig**-Skript befindet.

Betriebssystem	Speicherort
vCenter Server-Appliance	`/usr/lib/vmware-vmcam/bin/`
vCenter Server Windows	`C:\Program Files\VMware\vCenter Server\vmcamd\`

4 Führen Sie folgenden Befehl aus, um die Domäne und die Active Directory-Anmeldeinformationen des Benutzers der Konfiguration von Authentication Proxy hinzuzufügen.

```
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 von *user* angegebenen Benutzernamen, um die Konten für ESXi-Hosts in Active Directory zu erstellen. Daher muss der Benutzer über die Berechtigung verfügen, Konten in der Active Directory-Domäne, der Sie die Hosts hinzufügen, zu erstellen. 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 ESXi ein von einer Stammzertifizierungsstelle signiertes Zertifikat verwendet, stellen Sie sicher, dass das von einer Stammzertifizierungsstelle signierte Zertifikat zum vCenter Server-System hinzugefügt wurde. Weitere Informationen hierzu finden Sie unter Zertifikatsverwaltung für ESXi-Hosts.

Verfahren

1. Stellen Sie mit dem vSphere Web Client eine Verbindung zu einem vCenter Server-System her.
2. Navigieren Sie im vSphere Web Client zum Host und klicken Sie auf **Konfigurieren**.
3. Wählen Sie unter **Einstellungen** die Option **Authentifizierungsdienste** aus.
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 bei der vCenter Server-Appliance oder der vCenter Server-Windows-Maschine als Benutzer mit Administratorberechtigungen an.
2. Führen Sie den Befehl aus, um den Zugriff auf die Bash-Shell zu aktivieren.

   ```
   shell
   ```

3. Navigieren Sie zu dem Verzeichnis, in dem sich das **camconfig**-Skript befindet.

Betriebssystem	Speicherort
vCenter Server-Appliance	`/usr/lib/vmware-vmcam/bin/`
vCenter Server Windows	`C:\Program Files\VMware\vCenter Server\vmcamd\`

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.

  vCenter Server Appliance

  `/var/lib/vmware/vmcam/ssl/rui.crt`

  vCenter Server – Windows

  `C:\ProgramData\VMware\vCenterServer\data\vmcamd\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

Wenn Sie ein neues, von VMCA bereitgestelltes Zertifikat oder ein neues Zertifikat, das VMCA als untergeordnetes Zertifikat enthält, erzeugen möchten, befolgen Sie die Schritte in diesem Thema.

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 Platform Services Controllers 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 Platform Services Controllers 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.

Betriebssystem	Speicherort
vCenter Server Appliance	`/var/lib/vmware/vmcam/ssl/rui.crt`
vCenter Server – Windows	`C:\ProgramData\VMware\vCenterServer\data\vmcamd\ssl\rui.crt`

3 Heben Sie die Registrierung von vSphere Authentication Proxy auf.

a Navigieren Sie zu dem Verzeichnis, in dem sich das `camregister`-Skript befindet.

Betriebssystem	Befehle
vCenter Server Appliance	`/usr/lib/vmware-vmcam/bin`
vCenter Server – Windows	`C:\ProgramData\VMware\vCenterServer\data\vmcamd\ssl\rui.crt`

b Führen Sie den folgenden Befehl aus.

```
camregister --unregister -a VC_address -u user
```

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
vSphere Web Client	a Klicken Sie auf **Verwaltung** und anschließend auf **Systemkonfiguration** unter **Bereitstellung**. b Klicken Sie auf **Dienste** und anschließend auf den Dienst **VMware vSphere Authentication Proxy** und halten Sie den Dienst an.
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 full_path_to_rui.crt -k
full_path_to_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**.

Smartcard-Authentifizierung deaktivieren

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 vSphere Web 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 über den vSphere Web Client Benutzer 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.

- Verwenden des vSphere Web Client zum Aktivieren des Zugriffs auf die ESXi Shell

  Sie können den vSphere Web Client verwenden, um lokalen Zugriff und Remotezugriff (SSH) auf die ESXi Shell zu aktivieren und die Zeitüberschreitungswerte für die Verfügbarkeits- und Leerlaufzeiten festzulegen.

- Verwenden der Benutzerschnittstelle der direkten Konsole (DCUI) 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 die ESXi-Konfigurationsaufgaben mit dem vSphere Web Client, vSphere CLI oder vSphere PowerCLI durch. Melden Sie sich bei der ESXi Shell (vormals Support-Modus oder TSM) nur zwecks Fehlerbehebung an.

Verwenden des vSphere Web Client zum Aktivieren des Zugriffs auf die ESXi Shell

Sie können den vSphere Web Client verwenden, um lokalen Zugriff und Remotezugriff (SSH) auf die ESXi Shell zu aktivieren und die Zeitüberschreitungswerte für die Verfügbarkeits- und Leerlaufzeiten festzulegen.

Hinweis Greifen Sie auf den Host zu, indem Sie den vSphere Web Client, Remote-Befehlszeilentools (vCLI 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 im Navigator von vSphere Web Client.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter „System“ auf **Sicherheitsprofil**.
4. Klicken Sie im Bereich „Dienste“ auf **Bearbeiten**.
5. Wählen Sie einen Dienst aus der Liste aus.
   - ESXi Shell
   - SSH
   - Benutzerschnittstelle der direkten Konsole

6 Klicken Sie auf **Dienstdetails** und wählen Sie die Startrichtlinie **Manuell starten und stoppen** aus.

   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**.

7 Wählen Sie **Starten**, um den Dienst zu aktivieren.

8 Klicken Sie auf **OK**.

Nächste Schritte

Legen Sie die Zeitüberschreitungswerte für die Verfügbarkeits- und Leerlaufzeiten der ESXi Shell fest. Informationen hierzu unter Erstellen einer Zeitüberschreitung für die ESXi Shell-Verfügbarkeit im vSphere Web Client und Erstellen einer Zeitüberschreitung für ESXi Shell-Sitzungen im Leerlauf im vSphere Web Client

Erstellen einer Zeitüberschreitung für die ESXi Shell-Verfügbarkeit im vSphere Web Client

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 von vSphere Web Client.

2 Klicken Sie auf **Konfigurieren**.

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

4 Wählen Sie `UserVars.ESXiShellTimeOut` aus und klicken Sie auf **Bearbeiten**.

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 im vSphere Web Client

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. Dies können Sie verhindern, 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 Web Client aus steuern.

Verfahren

1. Navigieren Sie zum Host im Navigator von vSphere Web Client.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter „System“ auf **Erweiterte Systemeinstellungen**.
4. Wählen Sie UserVars.ESXiShellInteractiveTimeOut, klicken Sie auf das Symbol **Bearbeiten** und geben Sie die Einstellung für die Zeitüberschreitung an.
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 (DCUI) 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 verwenden, um den lokalen und den Remotezugriff auf die ESXi Shell zu ermöglichen. Sie greifen über die mit dem Host verbundene physische Konsole auf die Benutzerschnittstelle der direkten Konsole zu.

Hinweis Änderungen am Host, die mit der Benutzerschnittstelle der direkten Konsole, dem vSphere Web Client, ESXCLI oder anderen Verwaltungs-Tools vorgenommen wurden, werden stündlich oder beim ordnungsgemäßen Herunterfahren des Systems dauerhaft gespeichert. Änderungen können verlorengehen, falls der Host ausfällt, bevor sie festgeschrieben wurden.

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 Erstellen einer Zeitüberschreitung für die ESXi Shell-Verfügbarkeit in der Benutzerschnittstelle der direkten Konsole und Erstellen einer Zeitüberschreitung für ESXi Shell-Sitzungen im Leerlauf.

Erstellen einer Zeitüberschreitung für die ESXi Shell-Verfügbarkeit in der Benutzerschnittstelle der direkten Konsole

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 Wählen Sie im Menü „Optionen für den Fehlerbehebungsmodus“ die Option **ESXi Shell- und SSH-Zeitüberschreitungen ändern** aus und drücken Sie die Eingabetaste.
2 Geben Sie den Zeitüberschreitungswert für die Verfügbarkeit ein.

   Sie müssen den SSH-Dienst und den ESXi Shell-Dienst neu starten, damit die Einstellungen wirksam werden.
3 Drücken Sie wiederholt die Eingabetaste und die Esc-Taste, bis Sie zurück zum Hauptmenü der Benutzerschnittstelle der direkten Konsole gelangt sind.
4 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 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. Dies können Sie verhindern, indem Sie eine Zeitüberschreitung für Sitzungen im Leerlauf festlegen.

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.

Sie können die Zeitüberschreitung über die Benutzerschnittstelle der direkten Konsole (DCUI) in Sekunden oder über den vSphere Web Client in Minuten festlegen.

Verfahren

1. Wählen Sie im Menü „Optionen für den Fehlerbehebungsmodus“ die Option **ESXi Shell- und SSH-Zeitüberschreitungen ändern** aus und drücken Sie die Eingabetaste.
2. Geben Sie die Leerlauf-Zeitüberschreitung in Sekunden ein.

   Sie müssen den SSH-Dienst und den ESXi Shell-Dienst neu starten, damit die Einstellungen wirksam werden.
3. Drücken Sie wiederholt die Eingabetaste und die Esc-Taste, bis Sie zurück zum Hauptmenü der Benutzerschnittstelle der direkten Konsole gelangt sind.

Ergebnisse

Wenn die Sitzung sich im Leerlauf befindet, werden die Benutzer nach Ablauf der Zeitüberschreitungszeitspanne abgemeldet.

Anmelden bei der ESXi Shell zur Fehlerbehebung

Führen Sie die ESXi-Konfigurationsaufgaben mit dem vSphere Web Client, vSphere CLI oder vSphere PowerCLI durch. 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

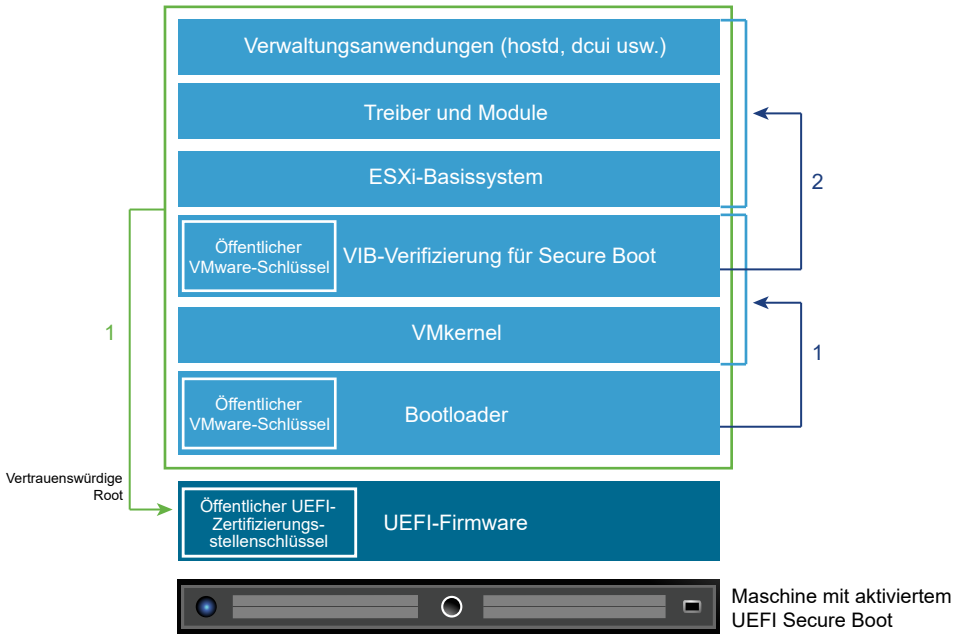
kryptografisch signiert ist. Ab vSphere 6.5 unterstützt ESXi den sicheren Start, falls die entsprechende Option in der Hardware aktiviert ist.

UEFI Secure Boot – Übersicht

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 Host, für den ein Upgrade auf ESXi 6.5 durchgeführt wurde, überprüfen Sie die Kompatibilität anhand der Anweisungen unter Ausführen des Validierungsskripts für den sicheren Start auf einem aktualisierten ESXi-Host. Wenn Sie für einen ESXi-Host ein Upgrade mithilfe von `esxcli`-Befehlen durchführen, wird der Bootloader nicht aktualisiert. In diesem Fall können Sie keinen Secure Boot für dieses System durchführen.

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.

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 Upgrade 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`.

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 einer Befehlszeilenschnittstelle (CLI) wie z. B. vCLI 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 den vSphere Web Client oder den vCLI-Befehl `esxcli system syslog` zum Konfigurieren des syslog-Dienstes verwenden.

Informationen zur Verwendung des `esxcli system syslog`-Befehls und anderen vCLI-Befehlen finden Sie unter *Erste Schritte mit vSphere-Befehlszeilenschnittstellen*.

Verfahren

1. Wählen Sie den Host im Bestandslistenbereich des vSphere Web Client aus.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie unter „System“ auf **Erweiterte Systemeinstellungen**.
4. Filter für **`syslog`**.
5. Um das Protokollieren global einzurichten, wählen Sie die zu ändernde Einstellung aus und klicken Sie auf das Symbol **Bearbeiten**.

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 finden Sie in der Dokumentation zum auf dem Remotehost installierten syslog-Dienst.

6 (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 Klicken Sie auf das Symbol **Bearbeiten** und geben Sie die Anzahl der Rotationen und die gewünschte Protokollgröße an.

7 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.

Komponente	Speicherort	Zweck
VMkernel	`/var/log/vmkernel.log`	Zeichnet Aktivitäten in Verbindung mit virtuellen Maschinen und ESXi auf.
VMkernel-Warnungen	`/var/log/vmkwarning.log`	Zeichnet Aktivitäten in Verbindung mit virtuellen Maschinen auf.
VMkernel-Übersicht	`/var/log/vmksummary.log`	Wird verwendet, um die Betriebszeit und die Verfügbarkeitsstatistiken für ESXi (kommagetrennt) zu bestimmen.
ESXi-Hostagenten-Protokoll	`/var/log/hostd.log`	Enthält Informationen zum Agenten, mit dem der ESXi-Host und seine virtuellen Maschinen verwaltet und konfiguriert werden.
vCenter-Agent-Protokoll	`/var/log/vpxa.log`	Enthält Informationen zum Agenten, der mit vCenter Server kommuniziert (wenn der Host von vCenter Server verwaltet wird).

Komponente	Speicherort	Zweck
Shell-Protokoll	`/var/log/shell.log`	Enthält einen Datensatz mit allen Befehlen, die in die ESXi Shell eingegeben wurden, und die Shell-Ereignisse (z. B. bei Aktivierung der Shell).
Authentifizierung	`/var/log/auth.log`	Enthält alle Ereignisse, die sich auf die Authentifizierung für das lokale System beziehen.
Systemmeldungen	`/var/log/syslog.log`	Enthält alle allgemeinen Protokollmeldungen und kann zur Fehlerbehebung verwendet werden. Diese Informationen befanden sich vorher in der Protokolldatei „messages“.
Virtuelle Maschinen	Dies ist dasselbe Verzeichnis wie für die Konfigurationsdateien der jeweiligen virtuellen Maschine mit dem Namen „vmware.log“ und „vmware*.log“. Beispiel: `/vmfs/volumes/`*`Datenspeicher`*`/`*`virtuelle Maschine`*`/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.

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.

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

- Wenn das lokale Windows-Administratorkonto aktuell die Administratorrolle vCenter Server aufweist, entfernen Sie diese Rolle und weisen Sie die Rolle einem oder mehreren benannten vCenter Server-Administratorkonten zu. 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.

  Hinweis Ab vSphere 6.0 hat der lokale Administrator standardmäßig keine vollständigen Administratorrechte mehr für vCenter Server.

- Installieren Sie vCenter Server mit einem Dienstkonto und nicht mit einem Windows-Konto. Das Dienstkonto muss ein Konto mit Administratorrechten für die lokale Maschine sein.
- 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 Web 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 Web Client-Zertifikate

Weisen Sie Benutzer von vSphere Web Client oder anderen Clientanwendungen an, Zertifikatverifizierungswarnungen auf keinen Fall zu ignorieren. 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 Web Client ändern.

Verfahren

1. Wählen Sie den vCenter Server in der Objekthierarchie von vSphere Web Client aus.
2. Klicken Sie auf **Konfigurieren**.
3. Klicken Sie auf **Erweiterte Einstellungen** und geben Sie **`VimPasswordExpirationInDays`** im Filterfeld ein.
4. 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.

Schützen des vCenter Server Windows-Hosts

Schützen Sie den Windows-Host, auf dem vCenter Server ausgeführt wird, gegen Sicherheitsrisiken und Angriffe, indem Sie sicherstellen, dass die Hostumgebung so sicher wie möglich ist.

- Achten Sie darauf, dass das Betriebssystem, die Datenbank und die Hardware für das vCenter Server-System auf dem aktuellen Stand sind. Wenn vCenter Server nicht unter einem Betriebssystem ausgeführt wird, das auf dem aktuellen Stand ist, kann es zu Störungen kommen und vCenter Server wird dadurch gegebenenfalls Angriffen ausgesetzt.
- Achten Sie darauf, dass das vCenter Server-System mit den aktuellsten Patches versehen ist. Wenn Sie immer die letzten Betriebssystem-Patches einlesen, besteht für den Server ein geringeres Angriffsrisiko.
- Sorgen Sie für den Schutz des Betriebssystems auf dem vCenter Server-Host. Der Schutz umfasst Antivirus- und Antimalware-Software.

- Vergewissern Sie sich, dass auf jedem Windows-Computer in der Infrastruktur die Einstellungen für die Remote Desktop Protocol-Hostkonfiguration (RDP) festgelegt sind, um den höchsten Grad der Verschlüsselung gemäß branchenüblichen oder internen Richtlinien sicherzustellen.

Hinweise zur Kompatibilität von Betriebssystem und Datenbank finden Sie unter *vSphere-Kompatibilitätstabellen*.

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 die Begrenzung 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 Web Client, ein Windows-System, in dem Sie PowerCLI verwenden, oder ein anderer SDK-basierter Client.
- Systemen, auf denen Add-On-Komponenten wie VMware vSphere Update Manager laufen.
- Infrastrukturdiensten wie DNS, Active Directory und NTP.
- Anderen Systemen, auf denen Komponenten laufen, die für die Funktionen des vCenter Server-Systems wesentlich sind.

Verwenden Sie eine lokale Firewall auf dem Windows-System, auf dem das vCenter Server-System läuft, oder eine Netzwerk-Firewall. Beziehen Sie IP-basierte Zugriffsbeschränkungen ein, damit nur notwendige Komponenten mit dem vCenter Server-System kommunizieren können.

Auswerten 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 Man-in-the-Middle-Angriffe. Die folgenden Komponenten sind anfällig, wenn sie auf einem Linux-Betriebssystem laufen.

- vCLI-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 Jump-Box-Systeme, um sicherzustellen, dass Linux-Clients sich hinter dem Jump befinden.

Überprüfen von vSphere Web Client-Plug-Ins

vSphere Web 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 Erhöhung der Sicherheit eine vSphere Web Client-Installation, die ausschließlich autorisierte Erweiterungen vertrauenswürdiger Quellen enthält.

Im Lieferumfang einer vCenter-Installation ist das erweiterbare vSphere Web Client-Framework enthalten. Sie können dieses Framework verwenden, um den vSphere Web 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 Web Client installiert, kann das Plug-In auf der Berechtigungsstufe dieses Administrators beliebige Befehle ausführen.

Zum Schutz vor einer möglichen Manipulation des vSphere Web 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 Web 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 Appliance

Verwenden Sie alle empfohlenen Vorgehensweisen zum Absichern eines vCenter Server-Systems zum Absichern Ihrer vCenter Server Appliance. Mit zusätzlichen Schritten können Sie Ihre Appliance sicherer machen.

Konfigurieren von NTP

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. NTP vereinfacht 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 Appliance mit einem NTP-Server.

Beschränken des vCenter Server Appliance-Netzwerkzugriffs

Beschränken Sie den Zugriff auf Komponenten, die für die Kommunikation mit der vCenter Server Appliance 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. Ab vSphere 6.0 sind Nicht-ASCII-Zeichen zulässig. Administratoren können die Standard-Kennwortrichtlinien ändern. Informationen finden Sie in der Dokumentation *Platform Services Controller-Verwaltung*.

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 mithilfe der Sperrrichtlinien von vCenter Single Sign-On diese Standardeinstellungen ändern. Informationen finden Sie in der Dokumentation *Platform Services Controller-Verwaltung*.

Ab vSphere 6.0 ist der vCenter Single Sign On-Domänenadministrator, standardmäßig „administrator@vsphere.local“, 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 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 Web Client überprüft.

Hinweis Standardmäßig bleiben die Zertifikate bei Upgrades erhalten.

Verfahren

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

Überprüfen der Aktivierung der SSL-Zertifikatsvalidierung über eine Netzwerkdatei-Kopie

Network File Copy (NFC) umfasst einen FTP-Dienst für vSphere-Komponenten, bei dem der Dateityp beachtet wird. Ab vSphere 5.5 verwendet ESXi NFC standardmäßig für Vorgänge wie das Kopieren und Verschieben von Daten zwischen Datenspeichern, aber möglicherweise müssen Sie es aktivieren, wenn es deaktiviert ist.

Wenn „SSL über NFC“ aktiviert wird, sind Verbindungen zwischen vSphere-Komponenten über NFC sicher. Mit dieser Verbindung können Man-in-the-Middle-Angriffe innerhalb eines Datencenters verhindert werden.

Da das Verwenden von NFC über SSL zu einem gewissen Leistungsabfall führt, ist es möglicherweise ratsam, diese erweiterten Einstellungen in einigen Entwicklungsumgebungen zu deaktivieren.

Hinweis Legen Sie diesen Wert explizit auf „true“ fest, wenn Sie Skripts zur Überprüfung des Werts verwenden.

Verfahren

1 Stellen Sie über den vSphere Web Client eine Verbindung mit dem vCenter Server her.

2 Klicken Sie auf **Konfigurieren**.

3 Klicken Sie auf **Erweiterte Einstellungen** und geben Sie den folgenden Schlüssel und Wert im unteren Bereich des Dialogfelds ein.

Feld	Wert
Schlüssel	config.nfc.useSSL
Wert	Wahr

4 Klicken Sie auf **OK**.

Erforderliche Ports für vCenter Server und Platform Services Controller

Das vCenter Server-System muss sowohl unter Windows als auch in der Appliance Daten an jeden verwalteten Host senden und Daten aus den vSphere Web Client- und Platform Services Controller-Diensten empfangen können. Die Quell- und Zielhosts müssen Daten untereinander 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 vCenter Server 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.

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 Web 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.

Dieses Kapitel enthält die folgenden Themen:

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 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. Klicken Sie in der Bestandsliste mit der rechten Maustaste auf eine virtuelle Maschine und wählen Sie **Einstellungen bearbeiten** aus.
2. Klicken Sie auf die Registerkarte **VM-Optionen** und erweitern Sie **Startoptionen**.
3. Stellen Sie sicher, dass unter **Startoptionen** die Firmware auf **EFI** festgelegt ist.
4. Wählen Sie Ihre Aufgabe. Aktivieren Sie das Kontrollkästchen **Sicherer Start**, um den sicheren Start zu aktivieren. Klicken Sie dann auf **OK**.
   - Aktivieren Sie das Kontrollkästchen **Sicherer Start**, um den sicheren Start zu aktivieren.
   - Deaktivieren Sie das Kontrollkästchen **Sicherer Start**, um den sicheren Start zu deaktivieren.

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, aber Sie können diesen Wert bei Bedarf ändern. 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. Melden Sie sich bei einem vCenter Server-System unter Verwendung von vSphere Web Client an und suchen Sie die virtuelle Maschine.
   a. Wählen Sie im Navigator **VMs und Vorlagen** aus.
   b. Suchen Sie die virtuelle Maschine in der Hierarchie.
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.

Verhindern des Verkleinerns von virtuellen Festplatten

Benutzer ohne Administratorberechtigung im Gastbetriebssystem können virtuelle Festplatten verkleinern. Durch das Verkleinern einer virtuellen Festplatte wird nicht verwendeter Speicherplatz wieder verfügbar gemacht. Wenn Sie eine virtuelle Festplatte allerdings wiederholt verkleinern, wird die Festplatte möglicherweise nicht mehr verfügbar und kann eine Dienstverweigerung (Denial of Service) verursachen. Um dies zu verhindern, sperren Sie die Möglichkeit, Festplatten zu verkleinern.

Voraussetzungen

- Schalten Sie die virtuelle Maschine aus.
- Stellen Sie sicher, dass Sie Root- oder Administratorrechte auf der virtuellen Maschine besitzen.

Verfahren

1. Melden Sie sich bei einem vCenter Server-System unter Verwendung von vSphere Web Client an und suchen Sie die virtuelle Maschine.
   a. Wählen Sie im Navigator **VMs und Vorlagen** aus.
   b. Suchen Sie die virtuelle Maschine in der Hierarchie.
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 die folgenden Parameter hinzu bzw. bearbeiten Sie sie.

Name	Wert
`isolation.tools.diskWiper.disable`	Wahr
`isolation.tools.diskShrink.disable`	Wahr

6. Klicken Sie auf **OK**.

Ergebnisse

Wenn Sie diese Funktion deaktivieren, können Sie Festplatten einer virtuellen Maschine nicht verkleinern, wenn ein Datenspeicher keinen Speicherplatz mehr hat.

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. Durch Einsatz einer Vorlage zum Erfassen eines abgesicherten Basisbetriebssystem-Images ohne installierte Anwendungen können Sie sicherstellen, dass alle virtuellen Maschinen mit einem bekannten grundlagenenden 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 Schnittstellen

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. Durch Einsatz einer Vorlage zum Erfassen eines abgesicherten Basisbetriebssystem-Images ohne installierte Anwendungen können Sie sicherstellen, dass alle virtuellen Maschinen mit einem bekannten grundlagenenden 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 *Verwaltung virtueller vSphere-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 mit der 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.

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.

Verwenden Sie Grenzwerte nur, wenn Sie die Auswirkung vollkommen verstehen.

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 *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.

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 Melden Sie sich bei einem vCenter Server-System mit dem vSphere Web Client an.

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:

- Diskettenlaufwerke
- Serielle Ports
- Parallele Schnittstellen
- USB-Controller
- CD-ROM-Laufwerke

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.

Verfahren

1 Melden Sie sich bei einem vCenter Server-System unter Verwendung von vSphere Web Client an und suchen Sie die virtuelle Maschine.

a Wählen Sie im Navigator **VMs und Vorlagen** aus.

b Suchen Sie die virtuelle Maschine in der Hierarchie.

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. Nur der Textkonsolenmodus ist noch 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. Melden Sie sich bei einem vCenter Server-System unter Verwendung von vSphere Web Client an und suchen Sie die virtuelle Maschine.
   a. Wählen Sie im Navigator **VMs und Vorlagen** aus.
   b. Suchen Sie die virtuelle Maschine in der Hierarchie.
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.unity.push.update.disable`
   - `isolation.tools.ghi.launchmenu.change`
   - `isolation.tools.memSchedFakeSampleStats.disable`
   - `isolation.tools.getCreds.disable`
   - `isolation.tools.ghi.autologon.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 Melden Sie sich bei einem vCenter Server-System unter Verwendung von vSphere Web Client an und suchen Sie die virtuelle Maschine.

   a Wählen Sie im Navigator **VMs und Vorlagen** aus.

   b Suchen Sie die virtuelle Maschine in der Hierarchie.

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 Web Client aktivieren.

Für diese Optionen wird standardmäßig der empfohlene Wert eingestellt. 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 Melden Sie sich bei einem vCenter Server-System mit dem vSphere Web Client an.

2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie auf **Einstellungen bearbeiten**.

3 Klicken Sie auf **VM-Optionen** und anschließend auf **Konfiguration bearbeiten**.

4 Stellen Sie sicher, dass in den Spalten „Name“ und „Wert“ die folgenden Werte enthalten sind, oder klicken Sie auf **Zeile hinzufügen**, um Werte hinzuzufügen.

Name	Empfohlener 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.

5 Klicken Sie auf **OK**.

6 (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 Web Client als Benutzer an, der über **Administrator**-Rechte in dem vCenter Server-System verfügt, in dem Sie die Rolle erstellen möchten.
2. Klicken Sie auf **Verwaltung** und wählen Sie **Rollen** aus.
3. Klicken Sie auf das Symbol **Rollenaktion erstellen** und geben Sie einen Namen für die Rolle ein.

   Geben Sie beispielsweise **`Administrator ohne Gastzugriff`** ein.
4. Wählen Sie **Alle Rechte** aus.
5. Deaktivieren Sie **Alle Rechte.Virtuelle Maschine.Gastvorgänge**, um die Gastvorgangsrechte zu entfernen.
6. Klicken Sie auf **OK**.

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 in virtuellen Maschinen können Geräte verbinden oder trennen, beispielsweise Netzwerkadapter und CD-ROM-Laufwerke. Sie können auch Geräteeinstellungen ändern. Entfernen Sie diese Geräte, um die Sicherheit der virtuellen Maschinen zu verstärken. Wenn Sie ein Gerät nicht entfernen möchten, können Sie die Einstellungen des Gastbetriebssystems ändern, um zu verhindern, dass Benutzer oder Prozesse auf einer virtuellen Maschine den Gerätestatus ändern.

Voraussetzungen

Schalten Sie die virtuelle Maschine aus.

Verfahren

1. Melden Sie sich bei einem vCenter Server-System unter Verwendung von vSphere Web Client an und suchen Sie die virtuelle Maschine.
   a. Wählen Sie im Navigator **VMs und Vorlagen** aus.
   b. Suchen Sie die virtuelle Maschine in der Hierarchie.
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. Überprüfen Sie, dass die folgenden Werte in den Spalten „Name“ und „Wert“ vorhanden sind, oder klicken Sie auf **Zeile hinzufügen**, um sie hinzuzufügen.

Name	Wert
isolation.device.connectable.disable	Wahr
isolation.device.edit.disable	Wahr

   Diese Optionen heben die Einstellungen in der Systemsteuerung von VMware Tools auf dem Gastbetriebssystem auf.
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. Melden Sie sich bei einem vCenter Server-System unter Verwendung von vSphere Web Client an und suchen Sie die virtuelle Maschine.
   a. Wählen Sie im Navigator **VMs und Vorlagen** aus.
   b. Suchen Sie die virtuelle Maschine in der Hierarchie.

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 **Zeile 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.

Verschlüsselung virtueller Maschinen

6

Ab vSphere 6.5 können Sie die Vorteile der Verschlüsselung von virtuellen Maschinen nutzen. Bei der Verschlüsselung wird nicht nur Ihre virtuelle Maschine geschützt, sondern auch die Festplatten und andere Dateien der virtuellen Maschine. Sie können eine vertrauenswürdige Verbindung zwischen vCenter Server und dem KMS (Key Management Server) herstellen. vCenter Server kann Schlüssel vom KMS nach Bedarf abrufen.

Sie verwalten verschiedene Aspekte der VM-Verschlüsselung in unterschiedlicher Weise.

- Verwalten Sie die Einrichtung der vertrauenswürdigen Verbindung mit dem KMS und führen Sie die meisten Verschlüsselungs-Workflows über den vSphere Web Client durch.
- Verwalten Sie die Automatisierung von einigen erweiterten Funktionen über das vSphere Web Services SDK. Siehe *Programmierhandbuch zum vSphere Web Services SDK* und *VMware vSphere API-Referenz*.
- Verwenden Sie das `crypto-util`-Befehlszeilen-Tool direkt auf dem ESXi-Host für einige Sonderfälle, zum Beispiel für das Entschlüsseln der Core-Dumps in einem `vm-support`-Paket.

Verschlüsselung von virtuellen vSphere-Maschinen – Überblick (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_4f7i39o8/uiConfId/49694343/)

Dieses Kapitel enthält die folgenden Themen:

Wie vSphere Virtual Machine Encryption Ihre Umgebung schützt

Mit vSphere Virtual Machine Encryption können Sie 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.

Verwendete Schlüssel

Für die Verschlüsselung werden zwei Arten von Schlüsseln verwendet.

- Der ESXi-Host generiert und verwendet interne Schlüssel zum Verschlüsseln von virtuellen Maschinen und Festplatten. Diese Schlüssel werden als DEKs (Data Encryption Keys, Datenverschlüsselungsschlüssel) verwendet und sind XTS-AES-256-Schlüssel.
- vCenter Server fordert Schlüssel aus dem KMS an. Diese Schlüssel werden als „Schlüsselverschlüsselungsschlüssel“ (Key Encryption Key – KEK) verwendet und sind AES-256-Schlüssel. vCenter Server speichert nur die ID jedes KEK, nicht jedoch den Schlüssel selbst.
- 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 KMS an und macht ihn für ESXi verfügbar. ESXi kann dann die internen Schlüssel nach Bedarf 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, den vCenter Server aus dem KMS abruft, entsperrt ein verschlüsseltes Paket in der VMX-Datei, die interne Schlüssel und andere Geheimschlüssel enthält.

Wenn Sie vSphere Web Client zum Erstellen einer verschlüsselten virtuellen Maschine verwenden, werden standardmäßig alle virtuellen Festplatten 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.

Hinweis Core-Dumps auf dem vCenter Server-System werden nicht verschlüsselt. Stellen Sie sicher, dass der Zugriff auf das vCenter Server-System geschützt ist.

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. Weitere Informationen hierzu finden Sie unter Rechte für Verschlüsselungsvorgänge. Die standardmäßige Systemrolle „Administrator“ umfasst alle Berechtigungen für **Kryptografische Vorgänge**. Eine neue Rolle, „Kein Kryptografie-Administrator“ unterstützt alle Administratorberechtigungen außer den Berechtigungen für **Kryptografische Vorgänge**.

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 Web Client unterstützt viele der kryptografischen Vorgänge. Für andere Aufgaben können Sie die vSphere API verwenden.

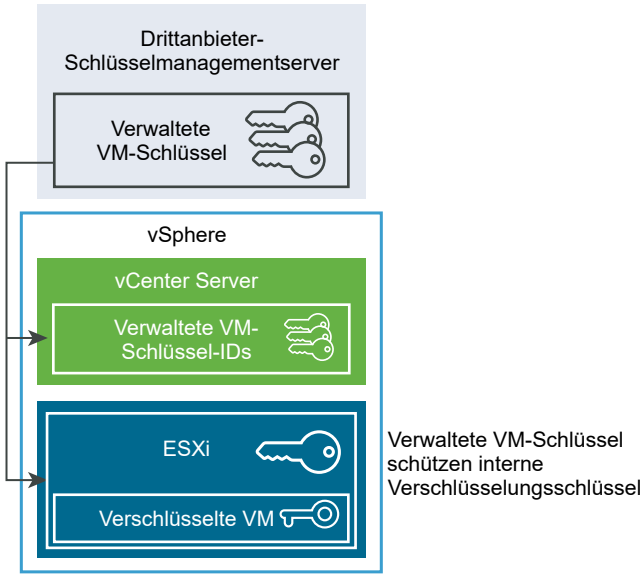
Tabelle 6-1. Schnittstellen für das Durchführen von kryptografischen Vorgängen

Schnittstelle	Vorgänge	Informationen
vSphere Web Client	Erstellen einer verschlüsselten virtuellen Maschine Verschlüsseln und Entschlüsseln virtueller Maschinen	Dieses Handbuch.
vSphere Web Services SDK	Erstellen einer verschlüsselten virtuellen Maschine Verschlüsseln und Entschlüsseln virtueller Maschinen Durchführen einer tiefen Neuverschlüsselung einer virtuellen Maschine (verwenden eines anderen DEK) Durchführen einer flachen Neuverschlüsselung einer virtuellen Maschine (verwenden eines anderen KEK)	*Programmierhandbuch zum vSphere Web Services SDK* *VMware vSphere API-Referenz*
`crypto-util`	Entschlüsseln verschlüsselter Core-Dumps, Prüfen, ob Dateien verschlüsselt sind, und Durchführen anderer Verwaltungsaufgaben direkt auf dem ESXi-Host	Befehlszeilen-Hilfe. vSphere VM-Verschlüsselung und Core-Dumps

vSphere Virtual Machine Encryption-Komponenten

Ein externer KMS, das vCenter Server-System und Ihre ESXi-Host tragen zur vSphere Virtual Machine Encryption-Lösung bei.

Abbildung 6-1. Architektur von vSphere Virtual Encryption



KMS (Key Management Server, Schlüsselmanagementserver)

vCenter Server fordert Schlüssel von einem externen KMS an. Der KMS generiert und speichert die Schlüssel und leitet sie an vCenter Server zur Verteilung weiter.

Sie können den vSphere Web Client oder die vSphere API verwenden, um einen Cluster mit KMS-Instanzen zum vCenter Server-System hinzuzufügen. Wenn Sie mehrere KMS-Instanzen in einem Cluster verwenden, müssen alle Instanzen vom selben Anbieter stammen und Schlüssel replizieren.

Wenn Ihre Umgebung verschiedene KMS-Anbieter in unterschiedlichen Umgebungen verwendet, können Sie ein KMS-Cluster für jeden KMS hinzufügen und einen KMS-Standardcluster angeben. Der erste hinzugefügte Cluster wird zum Standardcluster. 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 KMS Ihrer Wahl zu gewährleisten.

vCenter Server

Nur vCenter Server verfügt über die Anmeldedaten für die Anmeldung beim KMS. Ihre ESXi-Hosts verfügen nicht über diese Anmeldedaten. vCenter Server ruft Schlüssel vom KMS ab und leitet diese an die ESXi-Hosts weiter. Der vCenter Server speichert keine KMS-Schlüssel, sondern nur eine Liste mit Schlüssel-IDs.

vCenter Server überprüft die Berechtigungen der Benutzer, die Kryptografie-Vorgänge durchführen. Sie können den vSphere Web 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 Web Client-Ereigniskonsole anzeigen und exportieren können. Jedes Ereignis enthält den Benutzer, die Uhrzeit, die Schlüssel-ID und den Kryptografie-Vorgang.

Die Schlüssel aus dem KMS werden als Schlüssel für Verschlüsselungsschlüssel verwendet.

ESXi-Hosts

ESXi-Hosts sind verantwortlich für einige Aspekte des Verschlüsselungs-Workflows.

- 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. Siehe 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.

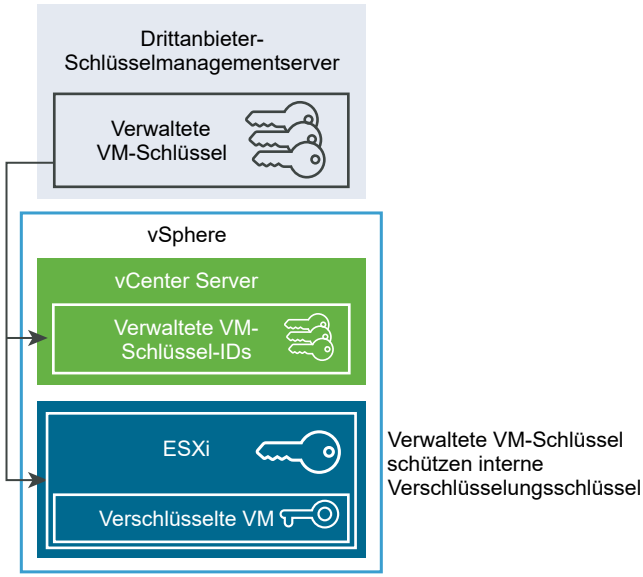
Die vom ESXi-Host generierten Schlüssel werden in diesem Dokument als interne Schlüssel bezeichnet. Diese Schlüssel fungieren normalerweise als Schlüssel zur Datenverschlüsselung.

Prozessablauf bei der Verschlüsselung

Nachdem der vCenter Server mit dem KMS verbunden wurde, können Benutzer mit entsprechenden Rechten verschlüsselte virtuelle Maschinen und Festplatten erstellen. Diese Benutzer können auch andere Verschlüsselungsvorgänge wie die Verschlüsselung bestehender virtueller Maschinen und die Entschlüsselung von verschlüsselten virtuellen Maschinen ausführen.

Der Prozessablauf enthält den KMS, den vCenter Server und den ESXi-Host.

Abbildung 6-2. Architektur von vSphere Virtual Encryption



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 Standard-KMS 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 KMS 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.

Wenn Sie später eine virtuelle Maschine entschlüsseln möchten, können Sie deren Speicherrichtlinie ändern. 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.

Verschlüsseln von virtuellen Maschinen und Festplatten (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_rndb367u/uiConfId/49694343/)

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. Wenn Sie auf dem vSphere Web Client eine verschlüsselte virtuelle Maschine erstellen, werden alle virtuellen Festplatten verschlüsselt. 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 6-2. 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 ändern, wenn eine oder mehrere Festplatten nicht verschlüsselt werden sollen. 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. Im vSphere Web Client werden die Größe und weitere Attribute, darunter der Verschlüsselungsstatus, angezeigt. Möglicherweise wird jedoch nicht die richtige Speicherrichtlinie angezeigt. Passen Sie der Einheitlichkeit halber die Speicherrichtlinien an.
Hinzufügen einer vorhandenen verschlüsselten Festplatte zu einer unverschlüsselten virtuellen Maschine.	Dieser Anwendungsfall wird nicht unterstützt.

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.

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 Zweck der Verschlüsselung virtueller Maschinen und virtueller Festplatten zu akzeptieren. Bevor Kryptografievorgänge auf einem Host stattfinden können, muss der Hostverschlüsselungsmodus aktiviert werden. Der Hostverschlüsselungsmodus wird oft automatisch aktiviert, kann aber auch explizit aktiviert werden. 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 dem Abrufen von Schlüsseln aus dem Schlüsselmanagementserver-Cluster 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.

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.

Anforderungen an den Festplattenspeicher

Zur Verschlüsselung einer virtuellen Maschine ist im Vergleich zum bisherigen Speicherbedarf mindestens der doppelte Speicherplatz nötig.

Verschlüsseltes vSphere vMotion

Ab vSphere 6.5 verwendet vSphere vMotion immer Verschlüsselung beim Migrieren von verschlüsselten virtuellen Maschinen. 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 für nicht verschlüsselte virtuelle Maschinen in den vCenter Server-Instanzen.
- vSphere unterstützt nicht vMotion für verschlüsselte virtuelle Maschinen in den vCenter Server-Instanzen. Da eine vCenter-Instanz nicht verifizieren kann, ob eine andere vCenter-Instanz mit demselben Schlüsselmanagementsystem-Cluster verbunden ist, stehen die korrekten Verschlüsselungsschlüssel für einen erfolgreichen VM-Verschlüsselungsvorgang nicht zur Verfügung. Als Folge hiervon wird vMotion in dieser Situation derzeit nicht unterstützt.
- Für nicht verschlüsselte virtuelle Maschinen werden alle Varianten von verschlüsseltem vSphere vMotion unterstützt. Für die Migration zwischen vCenter Server-Instanzen ist gemeinsam genutzter Speicher erforderlich.

Was wird verschlüsselt?

Bei verschlüsselten Festplatten werden die übertragenen Daten nicht verschlüsselt. Für nicht verschlüsselte Festplatten wird die Storage vMotion-Verschlüsselung nicht unterstützt.

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*.

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.

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

Befolgen Sie diese allgemeinen empfohlenen Vorgehensweisen, um Probleme zu vermeiden.

- Verschlüsseln Sie keine virtuellen vCenter Server Appliance-Maschinen.
- Wenn Ihr ESXi-Host abstürzt, rufen Sie so schnell wie möglich 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 KMS-Clusternamen sehr sorgfältig. Wenn sich der KMS-Clustername eines bereits verwendeten KMS ändert, wechseln VMs, die mit Schlüsseln von diesem KMS verschlüsselt wurden, beim Einschalten oder bei der Registrierung in einen gesperrten Zustand. Entfernen Sie in diesem Fall den KMS vom vCenter Server und fügen Sie ihn mit dem Clusternamen 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 Verschlüsselungsprozess verschlüsselt Daten auf dem Host, bevor sie in den Speicher geschrieben werden. Backend-Speicherfunktionen wie beispielsweise Deduplizierung und Kompression sind für verschlüsselte virtuelle Maschinen möglicherweise nicht effektiv. Ziehen Sie bei der Verbindung der vSphere VM-Verschlüsselung Speicherausgleiche in Betracht.
- 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 Web 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 Kennwort-Dump-Option 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 KMS-Verfügbarkeit garantieren und Schlüssel auf dem KMS überwachen.

- Sie müssen die entsprechenden Richtlinien erstellen und anwenden, die eine KMS-Verfügbarkeit sicherstellen.

  Wenn der KMS nicht verfügbar ist, sind VM-Vorgänge nicht möglich, bei denen vCenter Server den Schlüssel vom KMS 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 KMS-Lösungen beinhalten HA (High Availability)-Funktionen. Sie können den vSphere Web Client oder die API verwenden, um einen KMS-Cluster und die verbundenen KMS-Server anzugeben.

- 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
  - Entfernt
  - Entfernt 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“, „Entfernt“ oder „Entfernt 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 KMS 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 KMS abrufen. Wenn es sich bei dem Schlüsselzustand um „Deaktiviert“, „Manipuliert“, „Entfernt“ oder „Entfernt 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 KMS 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*.

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 Abschluss 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.

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.

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 eine Interoperabilität in vSphere 6.5 möglich ist.

Sie können bestimmte Aufgaben nicht für eine verschlüsselte virtuelle Maschine vornehmen.

- Für die meisten VM-Verschlüsselungsvorgänge muss die virtuelle Maschine eingeschaltet sein. Sie können eine verschlüsselte virtuelle Maschine klonen und beim Einschalten der virtuellen Maschine eine oberflächliche erneute Verschlüsselung vornehmen.
- Sie können eine verschlüsselte virtuelle Maschine nicht anhalten oder fortsetzen.
- Snapshot-Vorgänge weisen einige Beschränkungen auf.
  - Wenn Sie einen Snapshot einer verschlüsselten virtuellen Maschine erstellen, können Sie das Kontrollkästchen **Speicher der virtuellen Maschine erfassen** nicht aktivieren.
  - Sie können eine virtuelle Maschine mit vorhandenen Snapshots nicht verschlüsseln. Konsolidieren Sie alle vorhandenen Snapshots, bevor Sie die Verschlüsselung durchführen.

Sie können vSphere Virtual Machine Encryption im reinen IPv6- oder gemischten Modus verwenden. Sie können den KMS mit IPv6-Adressen konfigurieren. vCenter Server und der KMS können nur mit IPv6-Adressen konfiguriert werden.

Bestimmte Funktionen können mit vSphere Virtual Machine Encryption nicht ausgeführt werden.

- vSphere Fault Tolerance
- Das Klonen wird bedingt unterstützt.
  - Vollständige Klone werden unterstützt. Der Klon erbt den übergeordneten Verschlüsselungszustand und alle Schlüssel. Zur Verwendung neuer Schlüssel können Sie einen vollständigen Klon erneut verschlüsseln oder den vollständigen Klon entschlüsseln.

    Verknüpfte Klone werden unterstützt und der Klon erbt den übergeordneten Verschlüsselungszustand und alle Schlüssel. Sie können den verknüpften Klon nicht entschlüsseln oder einen verknüpften Klon nicht mit unterschiedlichen Schlüsseln erneut verschlüsseln.
- vSphere ESXi Dump Collector
- Migration mit vMotion einer verschlüsselten virtuellen Maschine auf eine andere vCenter Server-Instanz. Die verschlüsselte Migration mit vMotion einer nicht verschlüsselten virtuellen Maschine wird unterstützt.
- vSphere Replication
- Inhaltsbibliothek

- Nicht alle Sicherungslösungen, die VMware vSphere Storage API - Data Protection (VADP) für die Sicherung von virtuellen Festplatten verwenden, werden unterstützt.
  - VADP SAN-Sicherungslösungen werden nicht unterstützt.
  - Im laufenden Betrieb hinzugefügte VADP-Lösungen werden unterstützt, wenn der Anbieter die Verschlüsselung der Proxy-VM unterstützt, die als Teil eines Sicherungs-Workflows erstellt wird. Der Anbieter muss über die Rechte für **Verschlüsselungsvorgänge.Virtuelle Maschine verschlüsseln** verfügen.
  - VADP NBD-SSL-Sicherungslösungen werden unterstützt. Die Anwendung des Anbieters muss über die Rechte für **Verschlüsselungsvorgänge.Direkter Zugriff** verfügen.
- Sie können vSphere Virtual Machine Encryption mit IPv6 im gemischten Modus verwenden, aber nicht in einer reinen IPv6-Umgebung. Das Herstellen einer Verbindung zu einem KMS mit lediglich einer IPv6-Adresse wird nicht unterstützt.
- Sie können vSphere Virtual Machine Encryption nicht für die Verschlüsselung auf anderen VMware-Produkten verwenden, wie zum Beispiel VMware Workstation.
- 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.
- Sie können auf einer verschlüsselten virtuellen Maschine keine Anhalten- oder Arbeitsspeicher-Snapshot-Vorgänge durchführen.

Bestimmte Konfigurationstypen von VM-Festplatten werden mit vSphere Virtual Machine Encryption nicht unterstützt.

- VMware vSphere Flash Read Cache
- Erstklassige Festplatten
- RDM (Raw Device Mapping)
- Multiwriter- oder freigegebene Festplatten (MSCS, WSFC oder Oracle RAC). Wenn eine virtuelle Festplatte verschlüsselt wird und wenn Sie versuchen, auf der Seite **Einstellungen bearbeiten** der virtuellen Maschine einen Multiwriter auszuwählen, wird die Schaltfläche **OK** deaktiviert.

Verwenden von Verschlüsselung in Ihrer vSphere-Umgebung 7

Die Verwendung von Verschlüsselung in Ihrer vSphere-Umgebung erfordert ein gewisses Maß an Vorbereitung. Wenn Sie Ihre Umgebung eingerichtet haben, können Sie 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 unter *Programmierhandbuch zum vSphere Web Services SDK*. Informationen zu diesem Tool finden Sie der `crypto-util`-Befehlszeilenhilfe.

Einrichten des Schlüsselmanagementserver-Clusters

Bevor Sie mit den Verschlüsselungsaufgaben für virtuelle Maschinen beginnen können, müssen Sie den Schlüsselmanagementserver-Cluster einrichten. Die Aufgabe umfasst das Hinzufügen des Schlüsselmanagementservers (KMS) und das Herstellen des Vertrauens mit dem KMS. Wenn Sie einen Cluster hinzufügen, werden Sie aufgefordert, ihn als Standard-Cluster festzulegen. Sie können den Standard-Cluster explizit ändern. vCenter Server stellt Schlüssel vom Standard-Cluster bereit.

Der KMS muss den Key Management Interoperability Protocol (KMIP) 1.1-Standard 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.

Einrichten der Schlüsselmanagementserver für die Verschlüsselung virtueller Maschinen (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_e2z40gys/uiConfId/49694343/)

Hinzufügen eines KMS zu vCenter Server

Sie können Ihrem vCenter Server-System vom vSphere Web Client oder über die öffentliche API einen KMS hinzufügen.

vCenter Server erstellt einen KMS-Cluster, wenn Sie die erste KMS-Instanz hinzufügen.

- Wenn Sie den KMS hinzufügen, werden Sie aufgefordert, diesen Cluster als Standard festzulegen. Sie können später den Standard-Cluster explizit ändern.
- Nachdem vCenter Server den ersten Cluster erstellt hat, können Sie KMS-Instanzen des gleichen Anbieters dem Cluster hinzufügen.
- Sie können den Cluster mit nur einer KMS-Instanz einrichten.
- Wenn Ihre Umgebung KMS-Lösungen anderer Anbieter unterstützt, können Sie mehrere KMS-Cluster hinzufügen.
- Wenn Ihre Umgebung mehrere KMS-Cluster enthält und Sie den Standard-Cluster löschen, müssen Sie explizit einen anderen Standard festlegen. Weitere Informationen hierzu finden Sie unter Festlegen des Standard-KMS-Clusters.

Voraussetzungen

- Stellen Sie sicher, dass der Schlüsselserver 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**
- Sie können den KMS mit IPv6-Adressen konfigurieren.
  - vCenter Server und der KMS können nur mit IPv6-Adressen konfiguriert werden.

Verfahren

1. Melden Sie sich mit dem vSphere Web 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 dann auf **Schlüsselmanagementserver**.
4. Klicken Sie auf **KMS hinzufügen**, geben Sie im Assistenten die KMS-Informationen an und klicken Sie auf **OK**.

Option	Wert
KMS-Cluster	Wählen Sie für einen neuen Cluster **Neuen Cluster erstellen** aus. Wenn ein Cluster vorhanden ist, können Sie diesen Cluster auswählen.
Clustername	Name des KMS-Clusters. Wenn Ihre vCenter Server-Instanz nicht mehr verfügbar ist, benötigen Sie möglicherweise diesen Namen, um eine Verbindung zum KMS herzustellen.
Serveralias	Alias für den KMS. Sie benötigen dieses Alias möglicherweise für die Verbindung zum KMS, wenn Ihre -vCenter Server-Instanz ausfällt.
Serveradresse	IP-Adresse oder FQDN des KMS.
Serverport	Port, an dem vCenter Server eine Verbindung zum KMS herstellt.
Proxy-Adresse	Optionale Proxy-Adresse für die Verbindung zum KMS.

Option	Wert
Proxyport	Optionaler Proxyport für die Verbindung zum KMS.
Benutzername	Einige KMS-Anbieter 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 KMS diese Funktion unterstützt und Sie beabsichtigen, ihn zu verwenden.
Kennwort	Einige KMS-Anbieter 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 KMS diese Funktion unterstützt und Sie beabsichtigen, es zu verwenden.

Herstellen einer vertrauenswürdigen Verbindung durch den Austausch von Zertifikaten

Nach dem Hinzufügen des KMS zum vCenter Server-System können Sie eine vertrauenswürdige Verbindung herstellen. Der spezifische Prozess hängt von den Zertifikaten ab, die der KMS akzeptiert, und von der Unternehmensrichtlinie.

Voraussetzungen

Fügen Sie den KMS-Cluster hinzu.

Verfahren

1. Melden Sie sich beim vSphere Web Client an und wählen Sie ein vCenter Server-System aus.
2. Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselmanagementserver** aus.
3. Wählen Sie die KMS-Instanz aus, mit der Sie eine vertrauenswürdige Verbindung herstellen möchten.
4. Klicken Sie auf **vertrauenswürdige Verbindung mit KMS einrichten**.
5. Wählen Sie die entsprechenden Option für den Server aus und durchlaufen Sie die Schritte.

Option	Informationen hierzu unter
CA-Root-Zertifikat	Verwenden der Root-CA-Zertifikatsoption zum Herstellen einer vertrauenswürdigen Verbindung.
Zertifikat	Verwenden der Zertifikatsoption zum Herstellen einer vertrauenswürdigen Verbindung.
Neue Zertifikatssignieranforderung	Verwenden der Option „Neue Zertifikatsignierungsanforderung“ zum Herstellen einer vertrauenswürdigen Verbindung.
Zertifikat und privaten Schlüssel hochladen	Verwenden der Option zum Hochladen des Zertifikats und des privaten Schlüssels, um eine vertrauenswürdige Verbindung herzustellen.

Verwenden der Root-CA-Zertifikatsoption zum Herstellen einer vertrauenswürdigen Verbindung

Einige KMS-Anbieter verlangen, dass Sie Ihr 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. Melden Sie sich beim vSphere Web Client an und wählen Sie ein vCenter Server-System aus.
2. Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselmanagementserver** aus.
3. Wählen Sie die KMS-Instanz aus, mit der Sie eine vertrauenswürdige Verbindung herstellen möchten.
4. Wählen Sie **Root-CA-Zertifikat** aus und klicken Sie auf **OK**.

   Im Dialogfeld „Root-CA-Zertifikat herunterladen“ steht bereits das Root-Zertifikat, das vCenter Server zur Verschlüsselung verwendet. Dieses Zertifikat wird in VECS gespeichert.
5. Kopieren Sie das Zertifikat in die Zwischenablage oder laden Sie das Zertifikat als Datei herunter.
6. 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 der vertrauenswürdigen Verbindung.

Verwenden der Zertifikatsoption zum Herstellen einer vertrauenswürdigen Verbindung

Einige KMS-Anbieter 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 Melden Sie sich beim vSphere Web Client an und wählen Sie ein vCenter Server-System aus.

2 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselmanagementserver** aus.

3 Wählen Sie die KMS-Instanz aus, mit der Sie eine vertrauenswürdige Verbindung herstellen möchten.

4 Wählen Sie **Zertifikat** und klicken Sie auf **OK**.

   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.

5 Kopieren Sie das Zertifikat in die Zwischenablage oder laden Sie es als Datei herunter.

6 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 der vertrauenswürdigen Verbindung.

Verwenden der Option „Neue Zertifikatsignierungsanforderung“ zum Herstellen einer vertrauenswürdigen Verbindung

Einige KMS-Anbieter verlangen, dass vCenter Server eine Zertifikatsignieranforderung (CSR) generiert und sie 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 Melden Sie sich beim vSphere Web Client an und wählen Sie ein vCenter Server-System aus.

2 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselmanagementserver** aus.

3 Wählen Sie die KMS-Instanz aus, mit der Sie eine vertrauenswürdige Verbindung herstellen möchten.

4 Wählen Sie **Neue Zertifikatsignierungsanforderung** und klicken Sie auf **OK**.

5 Im Dialogfeld kopieren Sie das vollständige Zertifikat aus dem Textfeld in die Zwischenablage oder laden Sie es als Datei herunter. Klicken Sie anschließend auf **OK**.

   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.

6 Folgen Sie den Anweisungen Ihres KMS-Anbieters zum Einreichen der Zertifikatsignierungsanforderung.

7 Wenn Sie vom KMS-Anbieter das signierte Zertifikat erhalten, klicken Sie erneut auf **Schlüsselmanagementserver** und wählen Sie erneut **Neue Zertifikatsignierungsanforderung**.

8 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 **OK**.

Nächste Schritte

Schließen Sie die Vertrauensbeziehung ab. Weitere Informationen hierzu finden Sie unter Einrichten der vertrauenswürdigen Verbindung.

Verwenden der Option zum Hochladen des Zertifikats und des privaten Schlüssels, um eine vertrauenswürdige Verbindung herzustellen

Einige KMS-Anbieter verlangen, dass Sie das KMS-Serverzertifikat und den privaten Schlüssel auf 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 Melden Sie sich beim vSphere Web Client an und wählen Sie ein vCenter Server-System aus.

2 Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselmanagementserver** aus.

3 Wählen Sie die KMS-Instanz aus, mit der Sie eine vertrauenswürdige Verbindung herstellen möchten.

4 Wählen Sie **Zertifikat und privater Schlüssel hochladen** und klicken Sie auf **OK**.

5 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.

6 Fügen Sie die Schlüsseldatei in das untere Textfeld ein oder klicken Sie auf **Datei hochladen**, um die Schlüsseldatei hochzuladen.

7 Klicken Sie auf **OK**.

Nächste Schritte

Schließen Sie die Vertrauensbeziehung ab. Weitere Informationen hierzu finden Sie unter Einrichten der vertrauenswürdigen Verbindung.

Festlegen des Standard-KMS-Clusters

Sie müssen den Standard-KMS-Cluster festlegen, wenn Sie den ersten Cluster nicht als Standard-Cluster festlegen oder wenn es mehrere Cluster in Ihrer Umgebung gibt und Sie den Standard-Cluster entfernen.

Voraussetzungen

Als Best Practice stellen Sie sicher, dass auf der Registerkarte **Schlüsselmanagementserver** der Verbindungsstatus als „Normal“ mit einem grünen Häkchen angezeigt wird.

Verfahren

1 Melden Sie sich beim vSphere Web Client an und wählen Sie ein vCenter Server-System aus.

2 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Mehr** unter **Schlüsselmanagementserver**.

3 Wählen Sie den Cluster aus und klicken Sie auf **KMS-Cluster als Standard festlegen**.

   Wählen Sie den Server nicht aus. Das Menü zum Festlegen des Standard-Clusters steht nur für den Cluster zur Verfügung.

4 Klicken Sie auf **Ja**.

   Das Wort `default` erscheint neben dem Clusternamen.

Einrichten der vertrauenswürdigen Verbindung

Sofern Sie im Dialogfeld **Server hinzufügen** nicht aufgefordert wurden, eine vertrauenswürdige Verbindung mit dem KMS-Server einzurichten, müssen Sie die vertrauenswürdige Verbindung nach erfolgtem Zertifikataustausch 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 über die Option **KMS-Zertifikat aktualisieren** das Zertifikat explizit als vertrauenswürdig fest.

- Laden Sie ein untergeordnetes KMS-Zertifikat oder das KMS-CA-Zertifikat mithilfe der Option **KMS-Zertifikat hochladen** in vCenter Server hoch.

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. Melden Sie sich beim vSphere Web Client an und wählen Sie ein vCenter Server-System aus.
2. Klicken Sie auf **Konfigurieren** und wählen Sie **Schlüsselmanagementserver** aus.
3. Wählen Sie die KMS-Instanz aus, mit der Sie eine vertrauenswürdige Verbindung herstellen möchten.
4. Zum Einrichten der Vertrauensbeziehung aktualisieren Sie das KMS-Zertifikat oder laden Sie es hoch.

Option	Aktion
KMS-Zertifikat aktualisieren	a Klicken Sie auf **Alle Aktionen** und wählen Sie **KMS-Zertifikat aktualisieren** aus. b Klicken Sie im daraufhin angezeigten Dialogfeld auf **Vertrauenswürdigkeit**.
KMS-Zertifikat hochladen	a Klicken Sie auf **Alle Aktionen** und wählen Sie **KMS-Zertifikat hochladen** aus. b Klicken Sie im daraufhin angezeigten Dialogfeld auf **Datei hochladen**, laden Sie eine Zertifikatdatei hoch und klicken Sie auf **OK**.

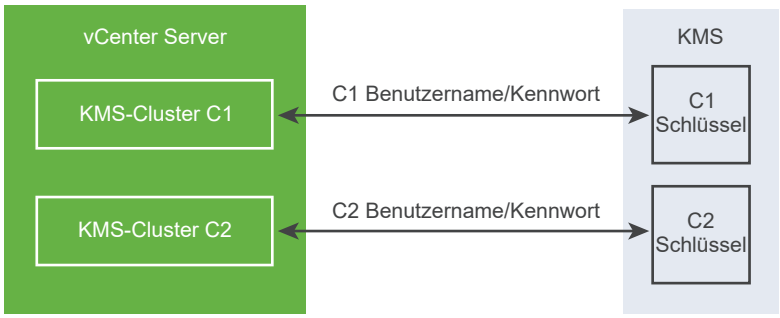
Einrichten getrennter KMS-Cluster für unterschiedliche Benutzer

Sie können für Ihre Umgebung verschiedene KMS-Verbindungen für unterschiedliche Benutzer der gleichen KMS-Instanz einrichten. Mehrere KMS-Verbindungen sind hilfreich,wenn Sie beispielsweise verschiedenen Abteilungen in Ihrem Unternehmen Zugriff auf unterschiedliche Sätze von KMS-Schlüsseln erteilen möchten.

Wenn Sie mehrere KMS-Cluster verwenden, können Sie den gleichen KMS zum Trennen von Schlüsseln verwenden. Das Vorhandensein getrennter Schlüsselsätze ist im Fall verschiedener Geschäftsbereiche oder Kunden entscheidend.

Hinweis Nicht alle KMS-Anbieter unterstützen mehrere Benutzer.

Abbildung 7-1. Verbinden von vCenter Server mit dem KMS für zwei unterschiedliche Benutzer



Voraussetzungen

Richten Sie die Verbindung mit dem KMS ein. Weitere Informationen hierzu finden Sie unter Einrichten des Schlüsselmanagementserver-Clusters.

Verfahren

1. Erstellen Sie die beiden Benutzer mit entsprechenden Benutzernamen und Kennwörtern, z. B. C1 und C2, im KMS.
2. Melden Sie sich bei vCenter Server an und erstellen Sie den ersten KMS-Cluster.
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 KMS-Cluster und fügen Sie den gleichen KMS hinzu, aber verwenden Sie den zweiten Benutzernamen und das zweite Kennwort (C2).

Ergebnisse

Die beiden Cluster haben unabhängige Verbindungen zum KMS und verwenden unterschiedliche Schlüsselsätze.

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 die Verschlüsselung der virtuellen Maschine mit anderen E/A-Filtern durchführen möchten, finden Sie im Handbuch zu *vSphere-Speicher* nähere Informationen.

Voraussetzungen

- Richten Sie die Verbindung mit dem KMS-Server ein.

  Obwohl eine Speicherrichtlinie für die VM-Verschlüsselung auch ohne KMS-Verbindung erstellt werden kann, können Sie Verschlüsselungsaufgaben erst durchführen, nachdem die vertrauenswürdige Verbindung mit dem KMS-Server eingerichtet wurde.

- Erforderliche Rechte: **Verschlüsselungsvorgänge.Verschlüsselungsrichtlinien verwalten**.

Verfahren

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

2 Wählen Sie **Home** aus, klicken Sie auf **Richtlinien und Profile** und klicken Sie dann auf **VM-Speicherrichtlinien**.

3 Klicken Sie auf **VM-Speicherrichtlinie erstellen**.

4 Geben Sie die Werte für die Speicherrichtlinie an.

   a Geben Sie den Namen der Speicherrichtlinie sowie eine optionale Beschreibung ein und klicken Sie auf **Weiter**.

   b Wenn dieser Assistent neu für Sie ist, lesen Sie die Informationen zur **Richtlinienstruktur** und klicken Sie auf **Weiter**.

   c Aktivieren Sie das Kontrollkästchen **Gemeinsame Regeln in der VM-Speicherrichtlinie verwenden**.

   d Klicken Sie auf **Komponente hinzufügen** und wählen Sie **Verschlüsselung > Standardeigenschaften der Verschlüsselung** aus und klicken Sie auf **Weiter**.

   Die Standardeigenschaften sind in den meisten Fällen geeignet. Eine benutzerdefinierte Richtlinie ist nur dann erforderlich, wenn Sie die Verschlüsselung mit anderen Funktionen wie Caching oder Replikation kombinieren möchten.

   e Deaktivieren Sie das Kontrollkästchen **Regelsätze in der Speicherrichtlinie verwenden** und klicken Sie auf **Weiter**.

   f Lassen Sie auf der Seite **Speicherkompatibilität** die Option „Kompatibel“ aktiviert und klicken Sie auf **Weiter**.

   g Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

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 manchen Fällen ist das explizite Aktivieren des Verschlüsselungsmodus erforderlich. Weitere Informationen hierzu finden Sie unter Voraussetzungen und erforderliche Berechtigungen für die Verschlüsselung.

Voraussetzungen

Erforderliche Berechtigung: **Kryptografische Vorgänge.Host registrieren**

Verfahren

1 Führen Sie zum Aktivieren des Hostverschlüsselungsmodus die folgenden Schritte durch:
2 Stellen Sie mit dem vSphere Web Client eine Verbindung zu vCenter Server her.
3 Wählen Sie den ESXi-Host aus und klicken Sie auf **Konfigurieren**.
4 Klicken Sie unter „System“ auf **Sicherheitsprofil**.
5 Scrollen Sie nach unten zu „Hostverschlüsselungsmodus“ und klicken Sie auf **Bearbeiten**.
6 Wählen Sie **Aktiviert** aus und klicken Sie auf **OK**.

Deaktivieren des Hostverschlüsselungsmodus

Der Hostverschlüsselungsmodus wird automatisch aktiviert, wenn Sie eine Verschlüsselungsaufgabe durchführen. 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.

Verfahren

1 Heben Sie die Registrierung für alle verschlüsselten virtuellen Maschinen auf dem Host auf.
2 Heben Sie die Registrierung des Hosts bei vCenter Server auf.
3 Starten Sie den Host neu.
4 Registrieren Sie den Host wieder bei vCenter Server.

Ergebnisse

Wenn Sie dem Host keine verschlüsselten virtuellen Maschinen hinzufügen, ist der Hostverschlüsselungsmodus deaktiviert.

Erstellen einer verschlüsselten virtuellen Maschine

Nachdem Sie den KMS eingerichtet haben, können Sie beginnen, verschlüsselte virtuelle Maschinen zu erstellen. Eine neue virtuelle Maschine wird verschlüsselt, wenn Sie sie mit einer Speicherrichtlinie für die Verschlüsselung erstellen.

Hinweis Das Erstellen einer verschlüsselten virtuellen Maschine geht schneller und beansprucht weniger Speicherressourcen als das Verschlüsseln einer vorhandenen virtuellen Maschine. Verschlüsseln Sie, wenn möglich, die virtuelle Maschine im Rahmen des Erstellungsprozesses.

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 Web 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 > Neue virtuelle Maschine** und befolgen Sie die Eingabeaufforderungen zum Erstellen einer verschlüsselten 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 Berechtigungen zum Erstellen von verschlüsselten virtuellen Maschinen verfügen. Weitere Informationen hierzu finden Sie unter Voraussetzungen und erforderliche Berechtigungen für die Verschlüsselung.
Speicher auswählen	Wählen Sie eine VM-Speicherrichtlinie mit Verschlüsselung aus (das mitgelieferte Beispiel lautet „VM-Verschlüsselungsrichtlinie“). Wählen Sie 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. 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 die Schlüssel für einen Klon zu ändern, schalten Sie den Klon aus und führen

Sie über die API eine flache Neuverschlüsselung aus. Weitere Informationen finden Sie unter *Programmierhandbuch zum vSphere Web Services SDK*.

Die virtuelle Maschine muss nicht ausgeschaltet werden, um sie zu klonen.

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**
  - Wenn der Hostverschlüsselungsmodus nicht auf „Aktiviert“ festgelegt ist, benötigen Sie außerdem **Verschlüsselungsvorgänge.Host registrieren**-Berechtigungen.

Verfahren

1. Stellen Sie mit dem vSphere Web 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 die virtuelle Maschine und befolgen Sie die Eingabeaufforderungen, um den Klon einer verschlüsselten virtuellen Maschine zu erstellen.

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 nicht im Rahmen des Klonvorgangs ändern.
Klonoptionen auswählen	Wählen Sie Klonoptionen wie in der Dokumentation zu *Verwaltung virtueller vSphere-Maschinen* beschrieben aus.
Bereit zum Abschließen	Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

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.

Sie können eine virtuelle Maschine nicht über das Menü **Einstellungen bearbeiten** verschlüsseln. Sie können virtuelle Festplatten einer verschlüsselten virtuellen Maschine über das Menü **Einstellungen bearbeiten** verschlüsseln.

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 Web 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, die Sie verwenden möchten, in der Dropdown-Liste aus.
   - Um die virtuelle Maschine und deren Festplatte zu verschlüsseln, wählen Sie eine Speicherrichtlinie für die Verschlüsselung aus und klicken Sie auf **Auf alle anwenden**.
   - Um die virtuelle Maschine, jedoch nicht deren virtuelle Festplatten zu verschlüsseln, wählen Sie die Speicherrichtlinie für die Verschlüsselung für VM-Home und andere Speicherrichtlinien für die virtuellen Festplatten aus und klicken Sie auf **Übernehmen**.

   Die virtuelle Festplatte einer nicht verschlüsselten virtuellen Maschine kann nicht verschlüsselt werden.
4. Alternativ können Sie virtuelle Festplatte auch über das Menü **Einstellungen bearbeiten** verschlüsseln.
   a. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
   b. Lassen Sie die Option **Virtuelle Hardware** ausgewählt.
   c. Öffnen Sie die virtuelle Festplatte, deren Speicherrichtlinie Sie ändern möchten, und wählen Sie eine Option aus dem Dropdown-Menü **VM-Speicherrichtlinie** aus.
   d. Klicken Sie auf **OK**.

Entschlüsseln einer verschlüsselten virtuellen Maschine oder virtuellen Festplatte

Sie können eine virtuelle Maschine entschlüsseln, indem Sie ihre Speicherrichtlinie ändern.

Für alle verschlüsselten virtuellen Maschinen ist verschlüsseltes vMotion erforderlich. Während der Entschlüsselung der virtuellen Maschine werden die Einstellungen für verschlüsseltes vMotion beibehalten. Um diese Einstellung zu ändern, damit kein verschlüsseltes vMotion mehr verwendet wird, ändern Sie die Einstellung explizit.

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 Web Client eine Verbindung zu vCenter Server her.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, die Sie ändern möchten, und wählen Sie **VM-Richtlinien > VM-Speicherrichtlinie bearbeiten** aus.

   Sie können die Speicherrichtlinie für die Dateien der virtuellen Maschine, dargestellt von VM-Home, und die Speicherrichtlinie für virtuelle Festplatten festlegen.
3. Wählen Sie aus dem Dropdown-Menü eine Speicherrichtlinie aus.
   - Um die virtuelle Maschine und deren Festplatten zu entschlüsseln, klicken Sie auf **Auf alle anwenden**.
   - Um eine virtuelle Festplatte, aber nicht die virtuelle Maschine zu entschlüsseln, wählen Sie eine Speicherrichtlinie für die virtuelle Festplatte aus dem Dropdown-Menü in der Tabelle aus. Ändern Sie die Richtlinie für VM-Home nicht.

   Es ist nicht möglich, die virtuelle Maschine zu entschlüsseln und die Festplatte verschlüsselt zu lassen.
4. Klicken Sie auf **OK**.
5. (Optional) Sie können jetzt 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

Wenn Sie eine verschlüsselte virtuelle Maschine über den vSphere Web Client erstellen, werden alle virtuellen Festplatten, die Sie während der Erstellung der virtuellen Maschine hinzufügen, verschlüsselt. 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 erläutert, 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**.

Verfahren

1. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine im vSphere Web Client und wählen Sie **VM-Richtlinien > VM-Speicherrichtlinie bearbeiten** aus.
2. Wählen Sie die Festplatte aus, für die Sie die Speicherrichtlinie ändern möchten, und wählen Sie die gewünschte Richtlinie (z. B. „Datastore Default“) aus.

Beheben von Problemen in Bezug auf fehlende Schlüssel

Unter bestimmten Umständen kann der ESXi-Host den Schlüssel (KEK) für eine verschlüsselte virtuelle Maschine oder eine verschlüsselte virtuelle Festplatte nicht aus 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 oder Löschen der virtuellen Maschine. Sie werden in einem vCenter Server-Alarm informiert, wenn sich eine verschlüsselte virtuelle Maschine im gesperrten Modus befindet.

Falls der VM-Schlüssel nicht verfügbar ist, wird der Zustand der virtuellen Maschine im vSphere Web Client 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.
```

Verfahren

1 Falls das Problem die Verbindung zwischen dem vCenter Server-System und dem KMS ist, stellen Sie die Verbindung wieder her.

   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.

   Nach jedem Neustart muss ein ESXi-Host 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.

2 Wenn die Verbindung wiederhergestellt wurde, registrieren Sie die virtuelle Maschine. Wenn beim Registrieren der virtuellen Maschine ein Fehler auftritt, stellen Sie sicher, dass Sie über das Recht **Kryptografievorgänge.VM registrieren** 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 nicht mehr auf dem KMS verfügbar ist, wird ein VM-Alarm erzeugt und folgende Meldung im Ereignisprotokoll angezeigt:

   `Die virtuelle Maschine ist gesperrt, weil Schlüssel auf dem KMS-Cluster fehlen.`

   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.

   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 KMS-Clusternamen 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.

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 KMS-Cluster 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 KMS-Cluster besteht, wird ein Alarm erzeugt und folgende Meldung im Ereignisprotokoll angezeigt:

   ```
   Auf dem Host muss der Verschlüsselungsmodus aktiviert sein, und der KMS-Cluster ist nicht verfügbar.
   ```

   Sie müssen die Schlüssel manuell im KMS-Cluster überprüfen und die Verbindung zum KMS-Cluster wiederherstellen.

2 Wenn Schlüssel fehlen, wird ein Alarm erzeugt und folgende Meldung im Ereignisprotokoll angezeigt:

   ```
   Auf dem Host muss der Verschlüsselungsmodus aktiviert sein, und der Schlüssel ist auf dem KMS-Cluster nicht verfügbar.
   ```

   Sie müssen die fehlenden Schlüssel manuell auf dem KMS-Cluster wiederherstellen.

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 KMS-Cluster tauschen zwei Arten von Zertifikaten aus: Server- und Clientzertifikate. Der VMware Endpoint Certificate Store (VECS) auf dem vCenter Server-System speichert die Serverzertifikate und ein Clientzertifikat pro KMS-Cluster. 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 beim vSphere Web Client an und wählen Sie ein vCenter Server-System aus.
2. Klicken Sie auf die Registerkarte **Konfigurieren**.
3. Klicken Sie unter **Einstellungen** auf **Erweiterte Systemeinstellungen** und dann auf **Bearbeiten**.
4. Filtern Sie nach oder scrollen Sie zu dem Konfigurationsparameter `vpxd.kmscert.threshold`.
5. Geben Sie Ihren Wert in Tagen ein und klicken Sie auf **OK**.

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 abstürzt, 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.

In der folgenden Tabelle werden die für jeden Core-Dump-Typ verwendeten Verschlüsselungsschlüssel angezeigt.

Tabelle 7-1. Core-Dump-Verschlüsselungsschlüssel

Core-Dump-Typ	Verschlüsselungsschlüssel (ESXi 6.5)
ESXi-Kernel	Hostschlüssel
Benutzer-World (hostd)	Hostschlüssel
Verschlüsselte virtuelle Maschine (VM)	Hostschlüssel

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 das Windows-System, auf dem vCenter Server ausgeführt wird, bzw. der vCenter Server Appliance 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 Web 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 Web 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 angefordert wird, und klicken Sie dann auf **Beenden**.
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.

Ergebnisse

Exportieren von Host-Support-Paketen mit Kennwörtern (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_xum9fnl1/uiConfId/49694343/)

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 Hostschlüssel 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-Dump verwendete ESXi-Hostschlüssel 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 zdumpEncryptedzdumpUnencrypted`

Sichern der vSphere-Netzwerke

8

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.

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.

Ein Diagramm mit den Firewallports finden Sie im VMware-Knowledgebase-Artikel 2131180.

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 Web Client, über andere UI-Clients oder Clients, die die vSphere API verwenden, Daten erhalten. Während des normalen Betriebs überwacht vCenter Server die Daten von den verwalteten Hosts und Clients an bestimmten Ports. vCenter Server geht auch davon aus, dass die verwalteten Hosts die Daten von vCenter Server an bestimmten Ports überwachen. Wenn sich zwischen diesen Elementen eine Firewall befindet, muss sichergestellt werden, dass Firewall-Ports für den Datenverkehr geöffnet wurden.

Firewalls können Sie auch an anderen Access Points im Netzwerk hinzufügen, in Abhängigkeit von der Netzwerknutzung und der für Clients erforderlichen Sicherheitsstufe. Bestimmen Sie die Installationspunkte für Ihre Firewalls anhand der Sicherheitsrisiken für Ihre Netzwerkkonfiguration. Die folgenden Firewall-Installationspunkte werden häufig verwendet.

- Zwischen dem vSphere Web 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 Web Client auf virtuelle Maschinen zugreifen, zwischen dem vSphere Web Client und dem ESXi-Host. Diese Verbindung ist ein Zusatz zu der Verbindung zwischen dem vSphere Web 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. Die Vorgehensweise zum Öffnen von Ports richtet sich danach, ob Sie eine vCenter Server Appliance- oder eine vCenter Server Windows-Installation verwenden.

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 Web Client-Zugriff und Firewall-Befehlen. Eine Liste der Ports finden Sie unter Ein- und ausgehende Firewall-Ports für ESXi-Hosts.

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
- Eine der vSphere-Befehlszeilenschnittstellen
- 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. Siehe *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 Web Client oder direkt mit dem ESXi-Host vom VMware Host Client aus herstellen.

Herstellen der Verbindung zu einer browserbasierten VM-Konsole über den vSphere Web Client

Beim Herstellen einer Verbindung mit dem vSphere Web 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 Web Client verwenden und eine Verbindung zu einer browserbasierten VM-Konsole herstellen, muss der folgende Zugriff möglich sein:

- Die Firewall muss vSphere Web Client den Zugriff auf vCenter Server auf Port 9443 erlauben.
- Die Firewall muss vCenter Server den Zugriff auf den ESXi-Host auf Port 902 erlauben.

Herstellen der Verbindung zu einer eigenständigen VM-Konsole über den vSphere Web Client

Falls Sie den vSphere Web Client verwenden und eine Verbindung zu einer eigenständigen VM-Konsole herstellen, muss der folgende Zugriff möglich sein:

- Die Firewall muss vSphere Web Client den Zugriff auf vCenter Server auf Port 9443 erlauben.
- Die Firewall muss der eigenständigen VM-Konsole den Zugriff auf vCenter Server auf Port 9443 sowie den Zugriff auf den ESXi-Host auf Port 902 erlauben.

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 den Zugriff auf den ESXi-Host auf Port 443 und 902 erlauben.

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 Web Client anzeigen und ändern. Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

MAC-Adressänderungen

Die Sicherheitsrichtlinie eines virtuellen Switches beinhaltet die Option **MAC-Adressänderungen**. Diese Option betrifft Datenverkehr, der von einer virtuellen Maschine empfangen wird.

Wenn die Option **MAC-Adressänderungen** auf **Akzeptieren** festgelegt ist, akzeptiert ESXi Anforderungen, die geltende MAC-Adresse 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 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-NetzwerkLastausgleich im Unicast-Modus verwenden. Bei Verwendung des Microsoft-NetzwerkLastausgleichs im Standard-Multicast-Modus haben die Adapter nicht die gleiche MAC-Adresse.

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.

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.

Informationen zum Konfigurieren des VM-Adapters für den Promiscuous-Modus finden Sie 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*.

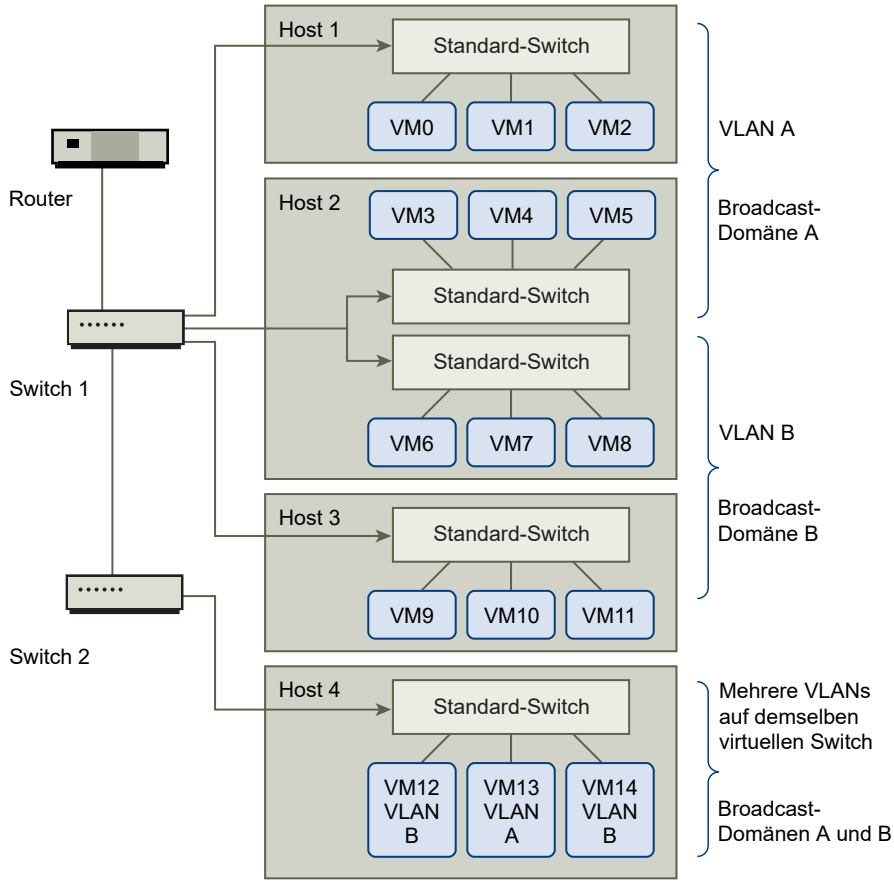
Absichern virtueller Maschinen durch VLANs

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 8-1. 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 4095 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.

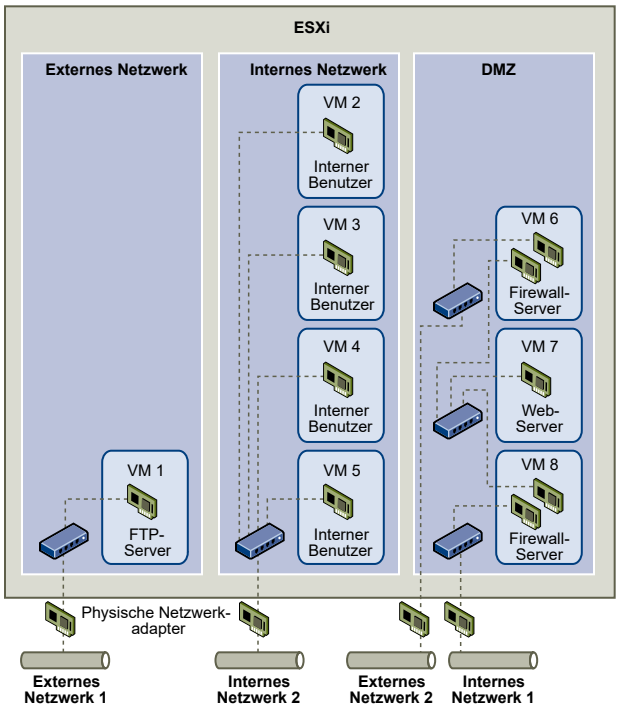
   Auf einem Standard-Switch können Sie den VLAN-Netzwerkmodus auf Switch- oder Portgruppenebene konfigurieren, und auf einem Distributed Switch auf der Ebene der verteilten Portgruppe oder des Ports.

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 8-2. Konfigurierte externe Netzwerke, interne Netzwerke und DMZ auf einem ESXi-Host



In der Abbildung wurde ein Host vom Systemadministrator in drei eigenständige virtuelle Maschinenzonen eingeteilt: 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 Gruppe virtueller Maschinen 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 Nutzer verwendet werden. Das interne Netzwerk1 ist der Verbindungskanal, den die Marketingabteilung zur Veröffentlichung des Inhalts von 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 vollständig 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 dann dazu verwendet werden kann, Datenpakete zu übertragen.

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 Web 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 vSphere-CLI-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 vSphere-CLI-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.

Option	Beschreibung
--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`.
--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 vSphere-CLI-Befehls ESXCLI 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 *Name_der_Sicherheitsrichtlinie*** ein.

Auflisten der verfügbaren IPsec-Sicherheitsrichtlinien

Die verfügbaren Sicherheitsrichtlinien können Sie mit dem vSphere-CLI-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 vSphere-CLI-Befehls ESXCLI 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` ■ `alle`
`--flow-direction=` ***Richtung***	Wählen Sie als Richtung, in der Sie den Datenverkehr überwachen möchten, entweder `in` oder `out` aus.

Option	Beschreibung
--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. ■ `Keine`: Keine Aktion ausführen ■ `Verwerfen`: 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 vSphere-CLI-Befehls ESXCLI 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 den Befehl **esxcli network ip ipsec sp remove --sa-name*Name der Sicherheitsrichtlinie*** in die Eingabeaufforderung 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.

SNMP muss auf jedem ESXi-Host konfiguriert werden. Für die Konfiguration können Sie vCLI, PowerCLI oder das vSphere Web Services SDK verwenden.

Detaillierte Setup-Informationen für SNMP 3 finden Sie in der Publikation *Überwachung und Leistung*.

Verfahren

1. Führen Sie folgenden Befehl aus, um festzustellen, ob SNMP aktuell 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.

- Wenn Spanning Tree aktiviert ist, stellen Sie sicher, dass physische Switch-Ports mit Portfast konfiguriert sind. Da virtuelle Switches von VMware STP nicht unterstützen, muss Portfast für Ports physischer Switches, die mit einem ESXi-Host verbunden sind, konfiguriert sein, um Schleifen im Netzwerk des physischen Switches zu vermeiden. Wenn Portfast nicht konfiguriert wird, können Leistungs- und Verbindungsprobleme auftreten.
- 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. Durch diese Informationen kann sich das Risiko für einen erfolgreichen Man-in-the-Middle-Angriffe erhöhen. 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 verwenden VLAN 1 als natives VLAN. Frames in einem nativen VLAN werden nicht mit „1“ gekennzeichnet. ESXi weist kein natives VLAN auf. 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 die Portspiegelung erforderlich ist, sollten Sie sicherstellen, dass alle Ziel-VLAN-, Port- und Uplink-IDs der Portspiegelung stimmen.

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

Netzwerkisolierungspraktiken können Sie die Netzwerksicherheit in der vSphere-Umgebung erheblich 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 besonders vertrauliche Umgebungen ein kontrolliertes Gateway oder eine andere kontrollierte Methode für den Zugriff auf das Verwaltungsnetzwerk. 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 Jump-Boxes, die Verwaltungs-Clients 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.

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. Melden Sie sich beim vSphere Web Client an.
2. Wählen Sie den Host aus und 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

9

Einige empfohlene Vorgehensweisen für die Sicherheit, wie das Einrichten von 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 Web 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 Maschinen in Ihrem vSphere-Netzwerk nicht synchronisiert sind, werden SSL-Zertifikate, die zeitabhängig sind, bei der Kommunikation zwischen Netzwerkmaschinen möglicherweise nicht als gültig erkannt.

Nicht synchronisierte Systemuhren können Authentifizierungsprobleme verursachen, was zu einem Fehlschlag beim Installieren der vCenter Server Appliance führen bzw. verhindern kann, dass der vpxd-Dienst der vCenter Server Appliance gestartet wird.

Stellen Sie sicher, dass alle Windows-Hostmaschinen, auf denen vCenter Server ausgeführt wird, mit dem NTP (Network Time Server)-Server synchronisiert sind. Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel http://kb.vmware.com/kb/1318.

Um ESXi-Systemuhren mit einem NTP-Server zu synchronisieren, können Sie den VMware Host Client verwenden. Informationen zum Bearbeiten der Uhrzeitkonfiguration auf einem ESXi-Host finden Sie in der Dokumentation *Verwaltung eines einzelnen Hosts von vSphere*.

- Synchronisieren der ESXi-Systemuhren mit einem NTP-Server

  Bevor Sie vCenter Server installieren oder die vCenter Server Appliance bereitstellen, sollten Sie sicherstellen, dass die Systemuhren aller Maschinen im vSphere-Netzwerk synchronisiert sind.

- Konfigurieren der Uhrzeitsynchronisierungseinstellungen in vCenter Server Appliance

  Sie können die Uhrzeitsynchronisierungseinstellungen in vCenter Server Appliance nach der Bereitstellung ändern.

Synchronisieren der ESXi-Systemuhren mit einem NTP-Server

Bevor Sie vCenter Server installieren oder die vCenter Server Appliance bereitstellen, sollten Sie sicherstellen, dass die Systemuhren aller Maschinen im vSphere-Netzwerk synchronisiert sind.

Diese Aufgabe erläutert, wie Sie NTP über den VMware Host Client einrichten. Sie können stattdessen den vCLI-Befehl `vicfg-ntp` verwenden. Weitere Informationen finden Sie in der *vSphere Command-Line Interface-Referenz*.

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. (Optional) Legen Sie die Startrichtlinie und den Dienststatus fest.
7. Klicken Sie auf **Speichern**.

   Der Host wird mit dem NTP-Server synchronisiert.

Konfigurieren der Uhrzeitsynchronisierungseinstellungen in vCenter Server Appliance

Sie können die Uhrzeitsynchronisierungseinstellungen in vCenter Server Appliance nach der Bereitstellung ändern.

Wenn Sie vCenter Server Appliance bereitstellen, können Sie als Uhrzeitsynchronisierungsmethode entweder die Verwendung eines NTP-Servers oder der VMware Tools wählen. Wenn sich die Uhrzeiteinstellungen in Ihrem vSphere-Netzwerk ändern, können Sie vCenter Server Appliance 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 noch 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 Appliance verwenden. Wenn Sie sich für die native Uhrzeitsynchronisierungssoftware entscheiden, wird die regelmäßigen Uhrzeitsynchronisierung durch VMware Tools für vCenter Server Appliance deaktiviert und umgekehrt.

Verwenden der Uhrzeitsynchronisierung von VMware Tools

Sie können die vCenter Server Appliance 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 Appliance-Konfiguration

Wenn Sie die vCenter Server Appliance für die Verwendung der NTP-basierten Uhrzeitsynchronisierung einrichten möchten, müssen Sie zuerst die NTP-Server zur vCenter Server Appliance-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 NTP-Server zur vCenter Server Appliance-Konfiguration hinzu, indem Sie den `ntp.server.add`-Befehl ausführen.

   Führen Sie beispielsweise folgenden Befehl aus:

   ```
   ntp.server.add --servers IP-addresses-or-host-names
   ```

   Hier ist *IP-addresses-or-host-names* eine kommagetrennte Liste der IP-Adressen oder Hostnamen der NTP-Server.

   Dieser Befehl fügt der Konfiguration NTP-Server hinzu. Wenn die Uhrzeitsynchronisierung auf einem NTP-Server basiert, wird der NTP-Daemon neu gestartet, um die neuen NTP-Server zu laden. Andernfalls werden mit diesem Befehl die neuen NTP-Server nur zur vorhandenen NTP-Konfiguration hinzugefügt.

3 (Optional) Um alte NTP-Server zu löschen und neue zur vCenter Server Appliance-Konfiguration hinzuzufügen, führen Sie den `ntp.server.set`-Befehl aus.

   Führen Sie beispielsweise folgenden Befehl aus:

   ```
   ntp.server.set --servers IP-addresses-or-host-names
   ```

   Hier ist *IP-addresses-or-host-names* eine kommagetrennte Liste der IP-Adressen oder Hostnamen der NTP-Server.

   Dieser Befehl löscht alte NTP-Server aus der Konfiguration und richtet die Eingabe-NTP-Server in der Konfiguration ein. Wenn die Uhrzeitsynchronisierung auf einem NTP-Server basiert, wird der NTP-Daemon neu gestartet, um die neue NTP-Konfiguration zu laden. Andernfalls ersetzt dieser Befehl nur die Server in der NTP-Konfiguration durch die als Eingabe bereitgestellten Server.

4 (Optional) Führen Sie den 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. Falls die NTP-Synchronisierung aktiviert ist, 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.

Nächste Schritte

Falls die NTP-Synchronisierung deaktiviert ist, können Sie die Zeitsynchronisierungseinstellungen in der vCenter Server Appliance konfigurieren, die auf einem NTP-Server basieren soll. Siehe Synchronisieren der Uhrzeit in vCenter Server Appliance mit einem NTP-Server.

Synchronisieren der Uhrzeit in vCenter Server Appliance mit einem NTP-Server

Sie können die Uhrzeitsynchronisierungseinstellungen in vCenter Server Appliance so konfigurieren, dass sie auf einem NTP-Server basieren.

Voraussetzungen

Richten Sie in der vCenter Server Appliance-Konfiguration mindestens einen NTP-Server (Network Time Protocol) ein. Siehe Hinzufügen oder Ersetzen von NTP-Servern in der vCenter Server Appliance-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 Virtual SAN*.

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 9-1. Kerberos-Sicherheitstypen

		ESXi 6.0	ESXi 6.5
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. Sie können eine der vSphere-Befehlszeilenschnittstellen (vCLI, PowerCLI usw.) verwenden, 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 Web Client

Um zu verhindern, dass Angreifer eine Sitzung im Leerlauf verwenden können, müssen Sie unbedingt Zeitüberschreitungen für ESXi Shell und vSphere Web Client festlegen.

Zeitüberschreitung für ESXi Shell

Für ESXi Shell können Sie die folgenden Zeitüberschreitungen über den vSphere Web 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 Web Client

vSphere Web Client-Sitzungen werden standardmäßig nach 120 Minuten beendet. Sie können diesen Standardwert in der Datei `webclient.properties` ändern, wie in der Dokumentation *vCenter Server und Hostverwaltung* erläutert.

Verwalten der Konfiguration des TLS-Protokolls mit dem TLS-Konfiguratorprogramm

10

Standardmäßig sind in vSphere die TLS-Protokollversionen 1.0, 1.1 und 1.2 aktiviert. Mit dem TLS-Konfiguratorprogramm können Sie TLS-Protokollversionen aktivieren oder deaktivieren. Sie können TLS 1.0 oder sowohl TLS 1.0 als auch TLS 1.1 deaktivieren.

Bevor Sie neu konfigurieren, beachten Sie Ihre Umgebung.

- Stellen Sie sicher, dass bei vCenter Server, Platform Services Controller, vSphere Update Manager und ESXi-Hosts innerhalb der Umgebung Softwareversionen ausgeführt werden, die das Deaktivieren von TLS-Versionen unterstützen. Finden Sie in VMware-Knowledgebase-Artikel 2145796 für eine Liste der VMware-Produkte, die Deaktivierung von TLS 1.0 unterstützen.
- Stellen Sie sicher, dass andere Produkte von VMware sowie Drittanbieter-Produkte ein aktiviertes TLS-Protokoll unterstützen. Je nach Ihrer Konfiguration, die TLS 1.2 oder TLS 1.1 und TLS 1.2 werden können.

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, Platform Services Controller und ESXi-Hosts verwenden. Sie können TLS 1.0 oder sowohl TLS 1.0 als auch TLS 1.1 deaktivieren.

vCenter Server und ESXi verwenden Ports, die für TLS-Protokolle aktiviert oder deaktiviert werden können.

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.

In der vCenter Server Appliance befindet sich vSphere Update Manager im selben System wie vCenter Server. In vCenter Server unter Windows konfigurieren Sie TLS durch Bearbeiten von Konfigurationsdateien. Weitere Informationen hierzu finden Sie unter Deaktivieren von TLS-Versionen in vSphere Update Manager.

Hinweise und Vorsichtsmaßnahmen

- Stellen Sie sicher, dass die Legacy-ESXi-Hosts, die von vCenter Server verwaltet werden, eine aktivierte TLS-Version unterstützen, und zwar entweder TLS 1.1 und TLS 1.2 oder nur TLS 1.2. Durch Deaktivieren einer TLS-Version in vCenter Server 6.5 kann vCenter Server Legacy-ESXi-Hosts der Version 5.x und 6.0 nicht mehr verwalten. Führen Sie ein Upgrade dieser Hosts auf Versionen durch, die TLS 1.1 oder TLS 1.2 unterstützen.
- Eine reine TLS 1.2-Verbindung kann mit einem externen Microsoft SQL Server oder einer externen Oracle-Datenbank verwendet werden.
- Deaktivieren Sie TLS 1.0 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*.
- In folgenden Situationen müssen Sie Hostdienste neu starten, nachdem TLS-Konfigurationsänderungen vorgenommen wurden.
  - Wenn Sie die Änderungen direkt auf den ESXi-Host anwenden.
  - Wenn Sie die Änderungen über die Clusterkonfiguration mithilfe von Hostprofilen anwenden.

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.

1 Wenn in Ihrer Umgebung vSphere Update Manager unter Windows vorhanden ist und vSphere Update Manager sich auf einem separaten System befindet, deaktivieren Sie Protokolle explizit durch Bearbeiten von Konfigurationsdateien. Weitere Informationen hierzu finden Sie unter Deaktivieren von TLS-Versionen in vSphere Update Manager.

   vSphere Update Manager in der vCenter Server Appliance ist immer im vCenter Server-System enthalten, und das Skript aktualisiert den entsprechenden Port.

2 Installieren Sie das TLS-Konfigurationsprogramm auf dem vCenter Server und dem Platform Services Controller. Wenn in Ihrer Umgebung ein eingebetteter Platform Services Controller verwendet wird, installieren Sie das Dienstprogramm nur auf dem vCenter Server.

3 Führen Sie das Dienstprogramm auf vCenter Server aus.

4 Führen Sie das Dienstprogramm 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.

5 Wenn Ihre Umgebung eine oder mehrere Platform Services Controller-Instanzen verwendet, führen Sie das Dienstprogramm für jede Instanz aus.

Voraussetzungen

Sie führen diese Konfiguration auf Systemen mit vSphere 6.0 U3 und auf Systemen mit vSphere 6.5 aus. Sie haben dabei zwei Möglichkeiten.

- Deaktivieren Sie TLS 1.0 und aktivieren Sie TLS 1.1 und TLS 1.2.
- Deaktivieren Sie TLS 1.0 und TLS 1.1 und aktivieren Sie TLS 1.2.

Installieren des TLS-Konfigurationsprogramms

Das TLS-Konfigurationsprogramm können Sie von MyVMware.com herunterladen und auf Ihrem lokalen Computer installieren. Nach der Installation sind zwei Skripts verfügbar. Ein Skript dient der Konfiguration von vCenter Server und Platform Services Controller, das andere Skript der ESXi-Konfiguration.

In der vCenter Server Appliance werden vSphere Update Manager-Ports durch das Skript aktualisiert. In vCenter Server bearbeiten Sie vSphere Update Manager-Konfigurationsdateien. Weitere Informationen hierzu finden Sie unter Deaktivieren von TLS-Versionen in vSphere Update Manager.

Voraussetzungen

Sie benötigen ein MyVMware-Konto, um das Skript herunterzuladen.

Verfahren

1. Melden Sie sich bei Ihrem MyVMware-Konto an und wechseln Sie zu vSphere.
2. Suchen Sie das Produkt und die Produktversion, für die Sie eine Lizenz besitzen, wählen Sie VMware vCenter Server aus und klicken Sie auf **Go to Downloads** (Zu Downloads wechseln).
3. Wählen Sie das VMware vSphere-TLS-Konfigurationsprogramm aus und laden Sie die folgende Datei herunter.

Betriebssystem	Datei
Windows	`VMware-vSphereTlsReconfigurator-`*`version-build_number`*`.x86_64.msi`
Linux	`VMware-vSphereTlsReconfigurator-`*`version-build_number`*`.x86_64.rpm`

4. Laden Sie Datei auf vCenter Server hoch und installieren Sie die Skripts.

   In Umgebungen mit einem externen Platform Services Controller laden Sie die Datei auch in den Platform Services Controller hoch.

Betriebssystem	Prozedur
Windows	a Melden Sie sich als Benutzer mit Administratorrechten an. b Kopieren Sie die Datei `VMware-vSphereTlsReconfigurator-`*`version-build_number`*`.x86_64.msi`, die Sie soeben heruntergeladen haben. c Installieren Sie die MSI-Datei.

Linux	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 Kopieren Sie die Datei `VMware-vSphereTlsReconfigurator-`*`version-build_number`*`.x86_64.rpm` mithilfe eines SCP-Clients in die Appliance.
	c Wenn die Bash-Shell derzeit nicht aktiviert ist, führen Sie die folgenden Befehle aus.
	`shell.set --enabled true`
	`shell`
	d Wechseln Sie in das Verzeichnis, in dem sich die hochgeladene RPM-Datei befindet, und führen Sie den folgenden Befehl aus.
	`rpm -Uvh VMware-vSphereTlsReconfigurator-`*`version-build_number`*`.x86_64.rpm`

Ergebnisse

Nach Abschluss der Installation finden Sie die Skripts an folgenden Speicherorten.

Betriebssystem	Speicherort
Windows	■ `C:\Program Files\VMware\CIS\vSphereTLSReconfigurator\VcTlsReconfigurator` ■ `C:\Program Files\VMware\CIS\vSphereTLSReconfigurator\EsxTlsReconfigurator`
Linux	■ `/usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator` ■ `/usr/lib/vmware-vSphereTlsReconfigurator/EsxTlsReconfigurator`

Führen Sie eine optionale manuelle Sicherung durch

Das TLS-Konfigurationsprogramm führt jedes Mal eine Sicherung durch, wenn das Skript vCenter Server, Platform Services Controller oder vSphere Update Manager auf dem vCenter Server Appliance ändert. 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 und Platform Services Controller ist das Standardverzeichnis für Windows und die Appliance unterschiedlich.

Betriebssystem	Sicherungsverzeichnis
Windows	`c:\users\`*`current_user`*`\appdata\local\temp\`*`yearmonthday`*`T`*`time`*
Linux	`/tmp/`*`yearmonthday`*`T`*`time`*

Verfahren

1 Wechseln Sie zum Verzeichnis `vSphereTlsReconfigurator` und anschließend zum Unterverzeichnis `VcTlsReconfigurator`.

Betriebssystem	Befehl
Windows	`C:\Program Files\VMware\CIS\vSphereTlsReconfigurator\` `cd VcTlsReconfigurator`
Linux	`cd /usr/lib/vmware-vSphereTlsReconfigurator/` `cd VcTlsReconfigurator`

2 Führen Sie den folgenden Befehl aus, um eine Sicherungskopie in einem bestimmten Verzeichnis zu erstellen.

Betriebssystem	Befehl
Windows	*`directory_path`*`\VcTlsReconfigurator> reconfigureVc backup -d `*`backup_directory_path`*
Linux	*`directory_path`*`/VcTlsReconfigurator> ./reconfigureVc backup -d `*`backup_directory_path`*

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=6.5.0, build=4635484
For more information refer to the following article: https://kb.vmware.com/kb/2147469
Log file: "C:\ProgramData\VMware\vCenterServer\logs\vSphere-
TlsReconfigurator\VcTlsReconfigurator.log".
================= Backing up vCenter Server TLS configuration ==================
Using backup directory: c:\users\<username>\appdata\local\temp\20161108T161539
Backing up: vspherewebclientsvc
Backing up: vmware-autodeploy-waiter
Backing up: rhttpproxy
Backing up: VMwareSTS
Backing up: vsphere-ui
Backing up: VMWareDirectoryService
Backing up: VMWareCAMService
```

4 (Optional) Wenn Sie später eine Wiederherstellung durchgeführt haben, können Sie den folgenden Befehl ausführen.

```
reconfigure restore -d tmp directory or custom backup directory path
```

Deaktivieren von TLS-Versionen auf vCenter Server-Systemen

Mit dem TLS-Konfigurationsprogramm können Sie TLS-Versionen auf vCenter Server-Systemen deaktivieren. Im Rahmen dieses Vorgangs können Sie sowohl TLS 1.1 als auch TLS 1.2 oder aber 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 als Benutzer an, der Skripts ausführen kann, und navigieren Sie zu dem Verzeichnis, in dem sich das Skript befindet.

Betriebssystem	Befehl
Windows	`cd C:\Programme\VMware\CIS\vSphereTlsReconfigurator\VcTlsReconfigurator`
Linux	`cd /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator`

2 Führen Sie den Befehl in Abhängigkeit von Ihrem Betriebssystem und der gewünschten 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.

Betriebssystem	Befehl
Windows	`directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.1 TLSv1.2`
Linux	`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.

Betriebssystem	Befehl
Windows	`directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.2`
Linux	`directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2`

3 Wenn in Ihrer Umgebung andere vCenter Server-Systeme vorhanden sind, wiederholen Sie den Vorgang auf jedem vCenter Server-System.

4 Wiederholen Sie die Konfiguration auf jedem ESXi-Host und jedem Platform Services Controller.

Deaktivieren von TLS-Versionen auf ESXi-Hosts

Mit dem TLS-Konfigurationsprogramm können Sie TLS-Versionen auf einem ESXi-Host deaktivieren. Im Rahmen dieses Vorgangs können Sie sowohl TLS 1.1 als auch TLS 1.2 oder aber nur TLS 1.2 aktivieren.

Für ESXi-Hosts verwenden Sie ein anderes Skript als für die anderen Komponenten Ihrer vSphere-Umgebung.

Hinweis Das Skript deaktiviert sowohl TLS 1.0 als auch TLS 1.1, außer Sie geben die Option `-p` an.

Um die aktuellen TLS-Versionen anzuzeigen, können Sie eine Verbindung zu einem ESXi-Host herstellen und `openssl`-Befehle ähnlich den folgenden ausführen:

```
openssl s_client -tls1 -connect localhost:443 | head -5
openssl s_client -tls1_1 -connect localhost:443 | head -5
openssl s_client -tls1_2 -connect localhost:443 | head -5
```

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.

In diesem Verfahren wird erläutert, wie Sie die Aufgabe auf einem einzelnen Host durchführen. Sie können ein Skript zum Konfigurieren von mehreren Hosts schreiben.

Verfahren

1 Melden Sie sich beim vCenter Server-System mit dem Benutzernamen und dem Kennwort des vCenter Single Sign-On-Benutzers an, der Skripts ausführen darf.

2 Navigieren Sie zu dem Verzeichnis, in dem sich das Skript befindet.

Betriebssystem	Befehl
Windows	`cd ..\EsxTlsReconfigurator`
Linux	`cd ../EsxTlsReconfigurator`

3 Führen Sie auf einem 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.

Betriebssystem	Befehl
Windows	`reconfigureEsx vCenterCluster -c` *`Cluster_Name`* `-u` *`Administrative_User`* `-p TLSv1.1 TLSv1.2`
Linux	`./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.

Betriebssystem	Befehl
Windows	`reconfigureEsx vCenterCluster -c` *`Cluster_Name`* `-u` *`Administrative_User`* `-p TLSv1.2`
Linux	`./reconfigureEsx vCenterCluster -c` *`Cluster_Name`* `-u` *`Administrative_User`* `-p TLSv1.2`

4 Führen Sie auf einem einzelnen Host einen der folgenden Befehle aus.

- Um TLS 1.0 zu deaktivieren und sowohl TLS 1.1 also auch TLS 1.2 auf einem einzelnen Host zu aktivieren, führen Sie den folgenden Befehl aus.

Betriebssystem	Befehl
Windows	`reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u Administrative_User -p TLSv1.1 TLSv1.2`
Linux	`./reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u Administrative_User -p TLSv1.1 TLSv1.2`

Hinweis Zur Neukonfiguration eines eigenständigen ESXi-Hosts (der nicht Teil eines vCenter Server-Systems ist) verwenden Sie die Optionen `ESXiHost -h` *HOST* `-u` *ESXi_ USER*. 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. So aktivieren Sie beispielsweise TLS 1.1 und TLS 1.2 auf zwei ESXi-Hosts:

```
reconfigureEsx ESXiHost -h 198.51.100.2 198.51.100.3 -u root -p TLSv1.1 TLSv1.2
```

- Um TLS 1.0 und TLS 1.1 zu deaktivieren und nur TLS 1.2 auf einem einzelnen Host zu aktivieren, führen Sie den folgenden Befehl aus.

Betriebssystem	Befehl
Windows	`reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u Administrative_User -p TLSv1.2`
Linux	`./reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u Administrative_User -p TLSv1.2`

5 Starten Sie den ESXi-Host neu, um die TLS-Protokolländerungen abzuschließen.

Deaktivieren von TLS-Versionen auf Platform Services Controller-Systemen

Wenn in Ihrer Umgebung ein oder mehrere Platform Services Controller-Systeme vorhanden sind, können Sie mit dem TLS-Konfigurationsprogramm die unterstützten TLS-Versionen ändern.

Wenn in Ihrer Umgebung nur ein eingebetteter Platform Services Controller verwendet wird, müssen Sie diese Aufgabe nicht ausführen.

Hinweis Fahren Sie mit dieser Aufgabe erst fort, nachdem Sie bestätigt haben, dass auf jedem vCenter Server-System eine kompatible TLS-Version ausgeführt wird. Wenn Instanzen von vCenter Server 6.0.x oder 5.5.x mit vCenter Server verbunden sind, kommunizieren diese Instanzen nicht mehr mit dem Platform Services Controller, wenn Sie TLS-Versionen deaktivieren.

Sie können TLS 1.0 und TLS 1.1 deaktivieren und TLS 1.2 aktiviert lassen, oder Sie können nur TLS 1.0 deaktivieren und TLS 1.1 und TLS 1.2 aktiviert lassen.

Voraussetzungen

Stellen Sie sicher, dass die Hosts und Dienste, mit denen der Platform Services Controller eine Verbindung herstellt, über ein unterstütztes Protokoll kommunizieren können. Die Authentifizierung und Zertifikatsverwaltung wird vom Platform Services Controller ausgeführt, weshalb Sie sorgfältig darauf achten sollten, welche Dienste möglicherweise betroffen sind. Für Dienste, die nur über nicht unterstützte Protokolle kommunizieren, wird die Verbindung getrennt.

Verfahren

1 Melden Sie sich beim Platform Services Controller als Benutzer an, der Skripts ausführen kann, und navigieren Sie zu dem Verzeichnis, in dem sich das Skript befindet.

Betriebssystem	Befehl
Windows	`cd C:\Programme\VMware\CIS\vSphereTlsReconfigurator\VcTlsReconfigurator`
Linux	`cd /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator`

2 Sie können die Aufgabe im Platform Services Controller unter Windows oder in der Platform Services Controller-Appliance durchführen.

- Um TLS 1.0 zu deaktivieren und sowohl TLS 1.1 also auch TLS 1.2 zu aktivieren, führen Sie den folgenden Befehl aus.

Betriebssystem	Befehl
Windows	*directory_path*\VcTlsReconfigurator> reconfigureVc update -p TLSv1.1 TLSv1.2
Linux	*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.

Betriebssystem	Befehl
Windows	*directory_path*\VcTlsReconfigurator> reconfigureVc update -p TLSv1.2
Linux	*directory_path*\VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2

3 Wenn in Ihrer Umgebung andere Platform Services Controller-Systeme vorhanden sind, wiederholen Sie den Vorgang.

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.

Sie können eine Wiederherstellung nur durchführen, wenn Sie zuvor die Konfiguration gesichert haben.

Führen Sie die Wiederherstellung in dieser Reihenfolge durch.

1 vSphere Update Manager.

  Wenn in Ihrer Umgebung eine separate vSphere Update Manager-Instanz auf einem Windows-System ausgeführt wird, müssen Sie zuerst vSphere Update Manager aktualisieren.

2 vCenter Server

3 Platform Services Controller

Verfahren

1 Stellen Sie eine Verbindung mit dem Windows-Computer oder der Appliance her.

2 Melden Sie sich bei dem System an, auf dem Sie Änderungen zurücksetzen machen möchten.

Betriebssystem	Prozedur
Windows	1 Melden Sie sich als Benutzer mit Administratorrechten an. 2 Wechseln Sie zum Verzeichnis `VcTlsReconfigurator`. `cd C:\Program Files\VMware\CIS\vSphereTlsReconfigurator\VcTlsReconfigurator`

Linux	1 Stellen Sie mithilfe von SSH eine Verbindung mit der Appliance her und melden Sie sich als Benutzer mit Berechtigungen zum Ausführen von Skripts an.
	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-vSphereTlsReconfigurator/VcTlsReconfigurator`

3 Prüfen Sie die vorherige Sicherung.

Betriebssystem	Prozedur

Windows	`C:\ProgramData\VMware\vCenterServer\logs\vSphere-TlsReconfigurator\VcTlsReconfigurator.log`
	Die Ausgabe ähnelt derjenigen im folgenden Beispiel.
	`c:\users\username\appdata\local\temp\20161108T161539`
	`c:\users\username\appdata\local\temp\20161108T171539`

Linux	`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`

4 Führen Sie einen der folgenden Befehle aus, um eine Wiederherstellung vorzunehmen.

Betriebssystem	Prozedur

Windows	`reconfigureVc restore -d Directory_path_from_previous_step`
	Beispiel:
	`reconfigureVc restore -d c:\users\username\appdata\local\temp\20161108T171539`

Linux	`reconfigureVc restore -d Directory_path_from_previous_step`
	Beispiel:
	`reconfigureVc restore -d /tmp/20161117T172920`

5 Wiederholen Sie diesen Vorgang für alle anderen vCenter Server-Instanzen.

6 Wiederholen Sie diesen Vorgang für alle anderen Platform Services Controller-Instanzen.

Deaktivieren von TLS-Versionen in vSphere Update Manager

In vSphere Update Manager 6.0 Update 3 und höher sind die TLS-Protokollversionen 1.0, 1.1 und 1.2 standardmäßig aktiviert. Sie können TLS Version 1.0 und TLS Version 1.1 deaktivieren, aber für TLS Version 1.2 ist dies nicht möglich.

Sie können die Konfiguration des TLS-Protokolls für andere Dienste mithilfe des TLS-Konfigurationsprogramms verwalten. Für vSphere Update Manager müssen Sie das TLS-Protokoll jedoch manuell neu konfigurieren.

Die Änderung der Konfiguration des TLS-Protokolls beinhaltet möglicherweise die folgenden Aufgaben.

- Deaktivieren von TLS Version 1.0, während TLS Version 1.1 und TLS Version 1.2 aktiviert bleiben.
- Deaktivieren von TLS Version 1.0 und TLS Version 1.1, während TLS Version 1.2 aktiviert bleibt.
- Erneutes Aktivieren einer deaktivierten TLS-Protokollversion.

Deaktivieren früherer TLS-Versionen für Update Manager-Port 9087

Frühere TLS-Versionen können Sie für Port 9087 deaktivieren, indem Sie die Konfigurationsdatei `jetty-vum-ssl.xml` ändern. Die Vorgehensweise für Port 8084 ist anders.

Hinweis Bevor Sie eine TLS-Version deaktivieren, stellen Sie sicher, dass keiner der Dienste, die mit vSphere Update Manager kommunizieren, diese Version verwendet.

Voraussetzungen

Beenden Sie den vSphere Update Manager-Dienst. Informationen finden Sie in der Dokumentation *Installieren und Verwalten von VMware vSphere Update Manager*.

Verfahren

1 Beenden Sie den vSphere Update Manager-Dienst.

2 Navigieren Sie zum Installationsverzeichnis von Update Manager, das für vSphere 6.0 und vSphere 6.5 unterschiedlich ist.

Version	Speicherort
vSphere 6.0	`C:\Programme (x86)\VMware\Infrastructure\Update Manager`
vSphere 6.5	`C:\Programme\VMware\Infrastructure\Update Manager`

3 Erstellen Sie eine Sicherungskopie der Datei `jetty-vum-ssl.xml` und öffnen Sie die Datei.

4 Deaktivieren Sie frühere TLS-Versionen durch Ändern der Datei.

Option	Beschreibung

Deaktivieren Sie TLS 1.0 und lassen Sie TLS 1.1 und TLS 1.2 aktiviert.	`<Set name="ExcludeProtocols">`
	`  <Array type="java.lang.String">`
	`  <Item>TLSv1</Item>`
	`  </Array>`
	`</Set>`

Deaktivieren Sie TLS 1.0 und TLS 1.1 und lassen Sie TLS 1.2 aktiviert.	`<Set name="ExcludeProtocols">`
	`  <Array type="java.lang.String">`
	`  <Item>TLSv1</Item>`
	`  <Item>TLSv1.1</Item>`
	`  </Array>`
	`</Set>`

5 Speichern Sie die Datei.

6 Starten Sie den vSphere Update Manager-Dienst neu.

Deaktivieren früherer TLS-Versionen für Update Manager-Port 8084

Frühere TLS-Versionen können Sie für Port 8084 deaktivieren, indem Sie die Konfigurationsdatei `vci-integrity.xml` ändern. Die Vorgehensweise für Port 9087 ist anders.

Hinweis Bevor Sie eine TLS-Version deaktivieren, stellen Sie sicher, dass keiner der Dienste, die mit vSphere Update Manager kommunizieren, diese Version verwendet.

Voraussetzungen

Beenden Sie den vSphere Update Manager-Dienst. Informationen finden Sie in der Dokumentation *Installieren und Verwalten von VMware vSphere Update Manager*.

Verfahren

1 Beenden Sie den vSphere Update Manager-Dienst.

2 Navigieren Sie zum Installationsverzeichnis von Update Manager, das für Version 6.0 und 6.5 unterschiedlich ist.

Version	Speicherort
vSphere 6.0	`C:\Programme (x86)\VMware\Infrastructure\Update Manager`
vSphere 6.5	`C:\Programme\VMware\Infrastructure\Update Manager`

3 Erstellen Sie eine Sicherungskopie der Datei `vci-integrity.xml` und öffnen Sie die Datei.

4 Fügen Sie ein `<sslOptions>`-Tag in der Datei `vci-integrity.xml` hinzu.

```
<ssl>
      <handshakeTimeoutMs>120000</handshakeTimeoutMS>
      <sslOptions>sslOptions_value</sslOptions>
</ssl>

<ssl>
      <privateKey>ssl/rui.key</privateKey>
      <certificate>ssl/rui.crt</certificate>
      <sslOptions>sslOptions_value</sslOptions>
</ssl>
```

5 In Abhängigkeit von der TLS-Version, die Sie deaktivieren möchten, verwenden Sie einen der folgenden Dezimalwerte im `<sslOptions>`-Tag.

- Um nur TLS Version 1.0 zu deaktivieren, verwenden Sie den Dezimalwert 117587968.
- Um TLS Version 1.0 und TLS Version 1.1 zu deaktivieren, verwenden Sie den Dezimalwert 386023424.

6 Speichern Sie die Datei.

7 Starten Sie den vSphere Update Manager-Dienst neu.

Erneutes Aktivieren deaktivierter TLS-Versionen für Update Manager-Port 9087

Wenn Sie eine TLS-Version für Update Manager-Port 9087 deaktivieren und Probleme auftreten, können Sie die Version erneut aktivieren. Die Vorgehensweise für die erneute Aktivierung von Port 8084 ist anders.

Das erneute Aktivieren einer früheren TLS-Version hat Auswirkungen auf die Sicherheit.

Verfahren

1 Beenden Sie den vSphere Update Manager-Dienst.

2 Navigieren Sie zum Installationsverzeichnis von Update Manager, das für Version 6.0 und 6.5 unterschiedlich ist.

Version	Speicherort
vSphere 6.0	`C:\Programme (x86)\VMware\Infrastructure\Update Manager`
vSphere 6.5	`C:\Programme\VMware\Infrastructure\Update Manager`

3 Erstellen Sie eine Sicherungskopie der Datei `jetty-vum-ssl.xml` und öffnen Sie die Datei.

4 Entfernen Sie das TLS-Tag, das der TLS-Protokollversion entspricht, die Sie aktivieren möchten.

Entfernen Sie beispielsweise `<Item>TLSv1.1</Item>` in der Datei `jetty-vum-ssl.xml`, um TLS Version 1.1 zu aktivieren.

5 Speichern Sie die Datei.

6 Starten Sie den vSphere Update Manager-Dienst neu.

Erneutes Aktivieren deaktivierter TLS-Versionen für Update Manager-Port 8084

Wenn Sie eine TLS-Version für Update Manager-Port 8084 deaktivieren und Probleme auftreten, können Sie die Version erneut aktivieren. Die Vorgehensweise für Port 9087 ist anders.

Das erneute Aktivieren einer früheren TLS-Version hat Auswirkungen auf die Sicherheit.

Verfahren

1 Beenden Sie den vSphere Update Manager-Dienst.

2 Navigieren Sie zum Installationsverzeichnis von Update Manager, das für Version 6.0 und 6.5 unterschiedlich ist.

Version	Speicherort
vSphere 6.0	`C:\Programme (x86)\VMware\Infrastructure\Update Manager`
vSphere 6.5	`C:\Programme\VMware\Infrastructure\Update Manager`

3 Erstellen Sie eine Sicherungskopie der Datei `vci-integrity.xml` und öffnen Sie die Datei.

4 Ändern Sie den im `<sslOptions>`-Tag verwendeten Dezimalwert oder löschen Sie das Tag, um alle TLS-Versionen zuzulassen.

- Verwenden Sie den Dezimalwert 117587968, um TLS 1.1 zu aktivieren, aber TLS 1.0 deaktiviert zu lassen.
- Entfernen Sie das Tag, um sowohl TLS 1.1 als auch TLS 1.0 erneut zu aktivieren.

5 Speichern Sie die Datei.

6 Starten Sie den vSphere Update Manager-Dienst neu.

Definierte Rechte

11

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 Bereitstellungsfunktion für Aktualisierungen des Systemzustands
- Host-CIM-Rechte
- Rechte für die Hostkonfiguration
- Hostbestandsliste
- Rechte für lokale Hostoperationen
- vSphere Replication-Rechte von Hosts
- Hostprofil-Berechtigungen
- Netzwerkberechtigungen
- Leistungsrechte
- Rechte für Berechtigungen
- Profilgesteuerte Speicherrechte
- Rechte für Ressourcen
- Rechte für geplante Aufgaben
- Sitzungsrechte
- Storage Views Privileges
- Rechte für Aufgaben
- Transfer Service-Rechte
- 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
- dvPort-Gruppenrechte
- vApp-Rechte
- vServices-Rechte
- vSphere-Tag-Berechtigungen

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 11-1. 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
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.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 die Änderung 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 vSphere*.

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 11-2. 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
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 *Platform Services Controller-Verwaltung* 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 11-3. Rechte für Hostzertifikate

Rechtename	Beschreibung	Erforderlich bei
Zertifikate.Zertifikate verwalten	Ermöglicht die Zertifikatsverwaltung für ESXi-Hosts.	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.

Tabelle 11-4. Rechte für Inhaltsbibliotheken

Rechtename	Beschreibung	Erforderlich bei
Inhaltsbibliothek.Bibliothekselement hinzufügen	Ermöglicht das Hinzufügen von Elementen in einer Bibliothek.	Bibliothek
Inhaltsbibliothek.Lokale Bibliothek erstellen	Ermöglicht die Erstellung lokaler Bibliotheken auf dem festgelegten vCenter Server-System.	vCenter Server
Inhaltsbibliothek.Abonnierte Bibliothek erstellen	Ermöglicht die Erstellung abonnierter Bibliotheken.	vCenter Server
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.Abonnierte Bibliothek löschen	Ermöglicht das Löschen einer abonnierten 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

Tabelle 11-4. Rechte für Inhaltsbibliotheken (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
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 Import von Inhalten impliziert, aktivieren Sie dieses Recht nur, wenn es notwendig ist und keine Sicherheitsbedenken für den Benutzer, der den Import ausführt, existieren.	Bibliothek
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.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 Web 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 11-4. Rechte für Inhaltsbibliotheken (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Inhaltsbibliothek.Abonnierte Bibliothek aktualisieren	Ermöglicht die Aktualisierung der Eigenschaften einer abonnierten Bibliothek.	Bibliothek
Inhaltsbibliothek.Konfigurationseinstellungen anzeigen	Ermöglicht das Anzeigen der Konfigurationseinstellungen. Diesem Recht sind keine Benutzerschnittstellenelemente auf dem vSphere Web 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 11-5. Rechte für Verschlüsselungsvorgänge

Rechtename	Beschreibung	Erforderlich bei
Kryptografievorgänge.Direktzugriff	Erlaubt Benutzern den Zugriff auf verschlüsselte Ressourcen. Beispielsweise können Benutzer virtuelle Maschinen exportieren, mit NFC auf virtuelle Maschinen zugreifen usw.	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
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

Tabelle 11-5. Rechte für Verschlüsselungsvorgänge (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
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.Schlüsselserver 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 Web 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 nicht 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 11-5. 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

Rechte für Datencenter

Rechte für Datencenter steuern die Fähigkeit, Datencenter in der Bestandsliste des vSphere Web 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 11-6. 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

Tabelle 11-6. Rechte für Datencenter (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Datencenter.Datencenter entfernen	Ermöglicht das Entfernen eines Datencenters. Um diesen Vorgang durchführen zu können, müssen Sie sowohl für das Objekt als auch für das übergeordnete Objekt über diese Berechtigung verfügen.	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 11-7. 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

Tabelle 11-7. Berechtigungen für Datenspeicher (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
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 11-8. 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

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 11-9. 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

Tabelle 11-9. Rechte für vSphere Distributed Switch (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
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
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

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 11-10. 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 11-11. 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 11-12. 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

Tabelle 11-12. Rechte für Ordner (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
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 11-13. 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

Tabelle 11-13. Globale Rechte (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
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 in Zusammenhang mit einem Alarm.	Beliebiges Objekt
Global.Dienst-Manager	Ermöglicht die Verwendung des `resxtop`-Befehls in der vSphere-CLI.	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 11-14. 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 11-15. 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

Tabelle 11-15. Rechte für die Hostkonfiguration (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
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
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 11-16. 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

Tabelle 11-16. Rechte für die Hostbestandsliste (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
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
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 11-17. 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 11-18. 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 11-19. 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

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 11-20. 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
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 11-21. 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 11-22. 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 Web 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 11-23. 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 11-24. 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
Ressourcen.Virtuelle Maschine dem 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 11-25. 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 11-26. Sitzungsrechte

Rechtename	Beschreibung	Erforderlich bei
Sitzungen.Benutzeridentität annehmen	Ermöglicht das Annehmen der Identität eines anderen Benutzers. Diese Funktion wird von Erweiterungen verwendet.	Root-vCenter Server
Sitzungen.Meldung	Ermöglicht das Festlegen der globalen Meldung beim Anmelden.	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

Storage Views Privileges

Storage Views privileges control privileges for Storage Monitoring Service 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 11-27. Storage Views Privileges

Privilege Name	Description	Required On
Speicheransichten.Dienst konfigurieren	Allows privileged users to use all Storage Monitoring Service APIs. Use **Speicheransichten.Anzeigen** for privileges to read-only Storage Monitoring Service APIs.	Root-vCenter Server
Speicheransichten.Anzeigen	Allows privileged users to use read-only Storage Monitoring Service 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 11-28. 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 Web Client zugeordnet.	Root-vCenter Server
Aufgaben.Aufgabe aktualisieren	Erlaubt einer Erweiterung die Aktualisierung einer benutzerdefinierten Aufgabe. Diesem Recht sind keine Benutzerschnittstellenelemente auf dem vSphere Web Client zugeordnet.	Root-vCenter Server

Transfer Service-Rechte

Transfer Service-Rechte werden intern von VMware verwendet. Diese Rechte sollten Sie nicht verwenden.

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 11-29. Berechtigungen für das Konfigurieren virtueller Maschinen

Rechtename	Beschreibung	Erforderlich bei
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.Erweitert	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.Ressourcen ändern	Ermöglicht das Ändern der Ressourcenkonfiguration für eine Gruppe von VM-Knoten in einem vorgegebenen Ressourcenpool.	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.Festplattenänderungsverfolgung	Ermöglicht das Aktivieren bzw. Deaktivieren der Änderungsverfolgung für Festplatten der virtuellen Maschine.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Festplatten-Lease	Ermöglicht Festplatten-Lease-Vorgänge für eine virtuelle Maschine.	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

Tabelle 11-29. Berechtigungen für das Konfigurieren virtueller Maschinen (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
Virtuelle Maschine.Konfiguration.Host-USB-Gerät	Ermöglicht das Verbinden eines hostbasierten USB-Geräts mit einer virtuellen Maschine.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Arbeitsspeicher	Ermöglicht das Ändern der Größe des Arbeitsspeichers, der der virtuellen Maschine zugeteilt ist.	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
Virtuelle Maschine.Konfiguration.Raw-Gerät	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.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

Tabelle 11-29. Berechtigungen für das Konfigurieren virtueller Maschinen (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
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.Einstellungen	Ermöglicht das Ändern der allgemeinen Einstellungen der virtuellen Maschine.	virtuelle Maschinen
Virtuelle Maschine.Konfiguration.Platzierung der Auslagerungsdatei	Ermöglicht das Ändern der Richtlinie zur Platzierung der Auslagerungsdatei für eine virtuelle 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

Die Rechte für Gastvorgänge auf virtuellen Maschinen steuern die Fähigkeit, mit Daten und Programmen innerhalb des Gastbetriebssystems einer virtuellen Maschine mit der API zu interagieren.

Weitere Informationen zu diesen Vorgängen finden Sie in der Dokumentation *VMware vSphere API Reference*.

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 11-30. 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 virtuelle 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 Web Client zugeordnet.	virtuelle Maschinen
Virtuelle Maschine.Gastbetriebssysteme.Programmausführung im Gastbetriebssystem	Ermöglicht Gastvorgänge auf virtuelle Maschinen, die das Ausführen eines Programms in der virtuellen Maschine einschließen. Diesem Recht sind keine Benutzerschnittstelleneleme nte auf dem vSphere Web Client zugeordnet.	virtuelle Maschinen
Virtuelle Maschine.Gastbetriebssysteme.Abfragen des Gastbetriebssystems	Ermöglicht Gastvorgänge auf virtuelle Maschinen, die Abfragen des Gastbetriebssystems einschließen, wie z. B. das Auflisten von Dateien im Gastbetriebssystem. Diesem Recht sind keine Benutzerschnittstelleneleme nte auf dem vSphere Web 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 11-31. 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 11-31. 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.Sicherungsvorgang auf der virtuellen Maschine	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 11-31. 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 11-32. 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. Aufheben der Registrierung	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 11-33. 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.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 11-33. 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 11-34. 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. Dienstkonfigurationen verwalten	Ermöglicht das Erstellen, Ändern und Löschen von VM-Diensten.
Virtuelle Maschine. Dienstkonfiguration. Dienstkonfiguration ändern	Ermöglicht das Ändern der bestehenden Dienstkonfiguration der virtuellen Maschine.

Tabelle 11-34. Rechte für die Dienstkonfiguration der virtuellen Maschine (Fortsetzung)

Rechtename	Beschreibung
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 11-35. 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 11-36. 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

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 11-37. 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 11-37. 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

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 11-38. 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
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

Tabelle 11-38. vApp-Rechte (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
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 Web 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

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 11-39. 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 11-40. 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.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-Bereich erstellen	Ermöglicht das Erstellen eines Tag-Bereichs.	Beliebiges Objekt
vSphere Tagging.vSphere Tag löschen	Ermöglicht das Löschen einer Tag-Kategorie.	Beliebiges Objekt
vSphere Tagging.vSphere Tag-Kategorie löschen	Ermöglicht das Löschen einer Tag-Kategorie.	Beliebiges Objekt
vSphere Tagging.vSphere Tag-Bereich löschen	Ermöglicht das Löschen eines Tag-Bereichs.	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

Tabelle 11-40. vSphere-Tag-Berechtigungen (Fortsetzung)

Rechtename	Beschreibung	Erforderlich bei
vSphere Tagging.vSphere Tag-Bereich bearbeiten	Ermöglicht das Bearbeiten eines Tag-Bereichs.	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